

CrowdStrike Provides Target and Advanced DoW Zero Trust Activities

Table of Contents

1. Introduction	3
2. DoD Zero Trust Reference Architecture Description and CrowdStrike Capability Summary	5
2.1 Bottom Line Up Front (BLUF)	5
2.2 DoD Zero Trust Reference Architecture Capabilities	5
2.3 Summary of CrowdStrike's Implementation and Integration Support for DoD Zero Trust Activities	6
3. DoD Zero Trust Pillars and Capabilities with CrowdStrike Implementation of Activities	7
3.1 User Pillar	7
3.2 Device Pillar	14
3.3 Application and Workload Pillar	23
3.4 Data Pillar	30
3.5 Network and Environment Pillar	39
3.6 Automation and Orchestration Pillar	46
3.7 Visibility and Analytics Pillar	59
4. Capability Recommendations and Activity Outcomes	69
1 User Pillar Capabilities	69
2 Device Pillar Capabilities	71
3 Application and Workload Pillar Capabilities	73
4 Data Pillar Capabilities	75
5 Network and Environment Pillar Capabilities	77
6 Automation and Orchestration Pillar Capabilities	78
7 Visibility and Analytics Pillar Capabilities	80

1. Introduction

In a time of increasing threats to U.S. businesses and the U.S. economy as a whole, the public sector is closing ranks in a revolutionizing way. For too long, network architectures have been designed from the legacy “castle-and-moat” perspective of securing connectivity. Many networks are composed of complex virtual local area configurations and complex firewall appliances along with the myriad rules that apply to them. And some networks are cordoned off from the outside world by firewalls alone. Defenders have walked around their castles of legacy systems wondering how long an archaic operating system server will be used for critical business functions. They have seen computers unlocked, cubicles that have a password on a sticky note near the keyboard. They have looked out and marveled at the view of their walls and moats, deterrent signs and cameras, thinking, “Someone would have to get through all of this to access a suspicious cubicle, to find the server everyone knows the password to, or to piggyback into the server room.” An adversary would have to do a long laundry list of nearly impossible things to access their data. But a stranger they don’t recognize has been following them around the whole time.

Advanced persistent threats and eCrime adversaries can exploit compromised credentials and other security vulnerabilities to penetrate networks (in as fast as **fifty-one seconds**), elevate privileges and rapidly move laterally to disrupt mission-critical systems and steal confidential data. In fact, according to the **CrowdStrike 2025 Global Threat Report**, 79% of observed attacks in 2024 did not use malware, making it difficult for traditional security solutions to distinguish legitimate activity from an adversary attack. CrowdStrike noted that 52% of the vulnerabilities we observed were related to initial access, further showing that adversaries are logging in instead of breaking in.

The U.S. has tried to put laws and frameworks in place to better protect data, assets, applications and services over the years, but fulfilling the many compliance requirements has been a significant challenge. And even if an organization is fully compliant, the way credentials and identities are being stolen and abused circumvents these controls and allows adversaries to exploit data. The laws, regulations and frameworks below are great steps in the right direction:

Laws and Regulations	FISMA
	Executive Order 14028
	Office of Management and Budget (OMB) Memo M-22-09 on Zero Trust
	OMB Memo M-21-31 on Logging
	Executive Order 14116 for the U.S. Coast Guard (USCG)
	National Cybersecurity Strategy
Frameworks	DoD Zero Trust Reference Architecture (ZT RA)
	NIST SP 800-207
	NIST SP 800-137
	NIST SP 800-53
	DoD Cloud Strategy

However, it is clear we need to act to provide better cyber mission assurance to warfighters and all other cyber defenders. The above regulations and frameworks are a snapshot of the U.S.'s commitment to the “never trust, always verify” mindset that defenders must adopt to secure devices, applications, assets and services. The adage that Zero Trust is a journey, not a technology, is true, and the DoD is doing significant initial work in this journey. The DoD will continue to monitor, revisit and validate how it defines and implements standards. Though Zero Trust is not a technology alone, it leverages technology for its implementation. With an array of best-of-breed and analyst-verified solutions to multiple information security domain problems, CrowdStrike is well positioned to aid the DoD, U.S. Coast Guard and all others trying to implement the DoD ZT RA.

Current Landscape

The very first line in the DoD Zero Trust Strategy highlights the threat that defenders face. In the [DoD Zero Trust Strategy](#), the DoD CIO penned, “Our adversaries are in our networks, exfiltrating our data, and exploiting the Department’s users.” The strategy goes on to acknowledge that despite the power, redundancy and sophistication defenders have added to their perimeter defenses, these defenses are not enough. The adversaries are in our nation’s networks. In early 2024, the directors of the NSA, CISA, FBI and NCD all testified to the threat posed by the People’s Republic of China. They outlined exactly how the adversary was in our networks and staging to do us harm if the need arose. Conference after conference has discussed the burgeoning potential threats to our internet-connected lives. Adversaries are continually increasing in number, getting faster and getting help by collaborating, organizing and sharing the profits. And the cyber workforce and skills gaps present additional challenges, as the number of defenders in the six services — along with those hired to help warfighters defend the cyber terrain — is not enough to address every threat. Defenders can no longer live by the adage of “trust but verify” — instead, this must evolve to “Zero Trust and verify.”

The DoD has put together a comprehensive plan to protect every door, file cabinet, binder, conversation and movement in an environment where adversaries are following defenders around and pilfering their data. The DoD ZT RA offers a promising way to identify threats, protect the attack surface and significantly improve the defenses of our data, applications, assets and services (DAAS) by driving up the costs of adversaries' efforts and increasing the chance of discovering threats and effectively responding to them.

The threat landscape is changing even more with the popularization and deployment of AI and machine learning (ML). AI/ML can be leveraged as a force multiplier to aid cyber defenders in the triage of countless alerts, allowing them to elevate their focus to the adversary’s mission, whether it is espionage, prepositioning or other harm. Adversaries are also leveraging AI to increase the speed of their attacks and aid in highly sophisticated social engineering attacks.

At CrowdStrike, the use of AI/ML in cyber defense is not new — it has been baked into the company’s platform approach since the inception of its cyber threat intelligence (CTI) and next-generation antivirus (NGAV) 12 years ago.

This white paper outlines how the CrowdStrike Falcon® platform implements the Activities prescribed to provide the Capabilities indicated in the DoD ZT RA. It also demonstrates how CrowdStrike is partnering with members of the DoD and integrating with existing vendors in their security stack to help them achieve maturity across the pillars.

Additionally, this white paper explores the DoD ZT RA and highlights how the DoD and USCG can advance in their Zero Trust journey by leveraging the 400+ integrations CrowdStrike has with the other assets and products in their cybersecurity programs.

2. DoD Zero Trust Reference Architecture Description and CrowdStrike Capability Summary

The Zero Trust initiative represents a transformative step forward in the DoD's commitment to advancing cybersecurity and implementing guidance from NSM-8. The DoD Zero Trust Reference Architecture embeds advanced security controls seamlessly into DoD networks.

2.1 Bottom Line Up Front (BLUF)

CrowdStrike's self assessment of the DoD Zero Trust Reference Architecture indicates that 83 of the 152 Zero Trust Activities are natively met by the Falcon Platform. This platform approach helps to optimize achievement of Zero Trust strategic objectives in a way that is flexible and provides over 400 integrations with the existing security stacks of the six services.

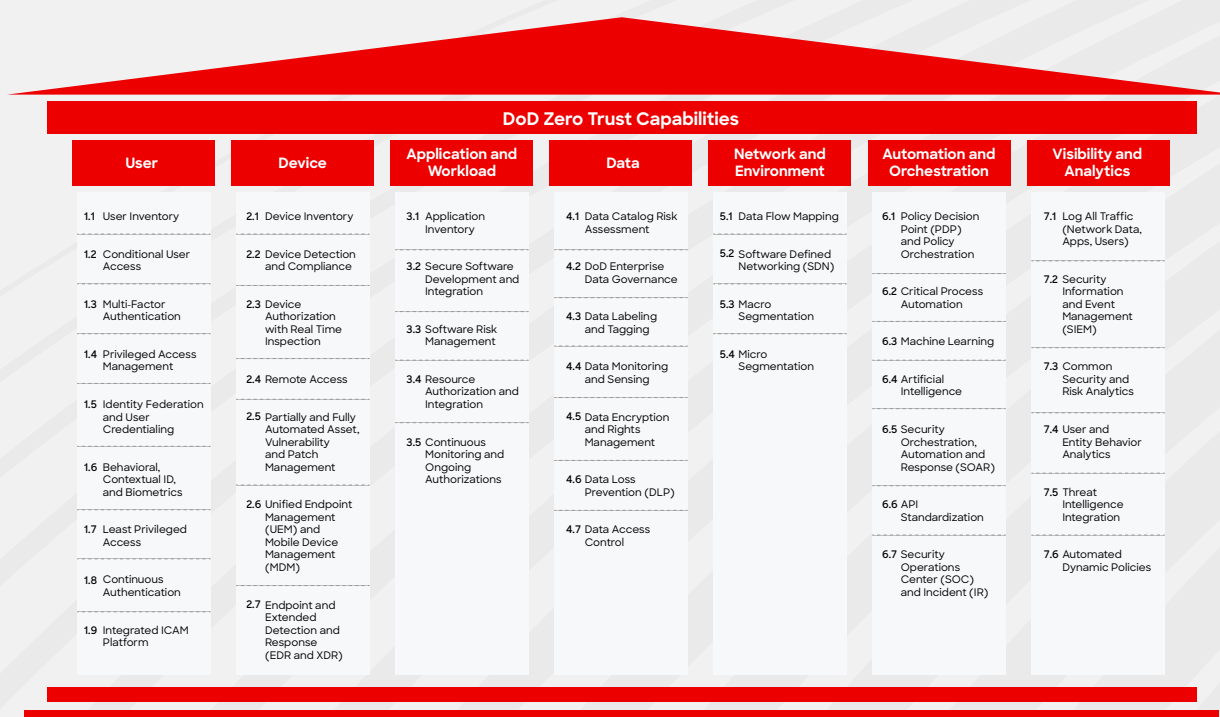
Overarching Breakdown of the 152 Activities That CrowdStrike Implements or Supports Through Integration

The CrowdStrike Falcon platform is built from the ground up to secure the modern enterprise by stopping breaches in real time on endpoints, workloads or identities, independent of location or network.

Activities	Implemented	Supports or Integrated	Roadmapped	N/A or DoD Role
Target Level	48	13	0	30
Advanced Level	35	14	2	10
Totals	83	27	2	40

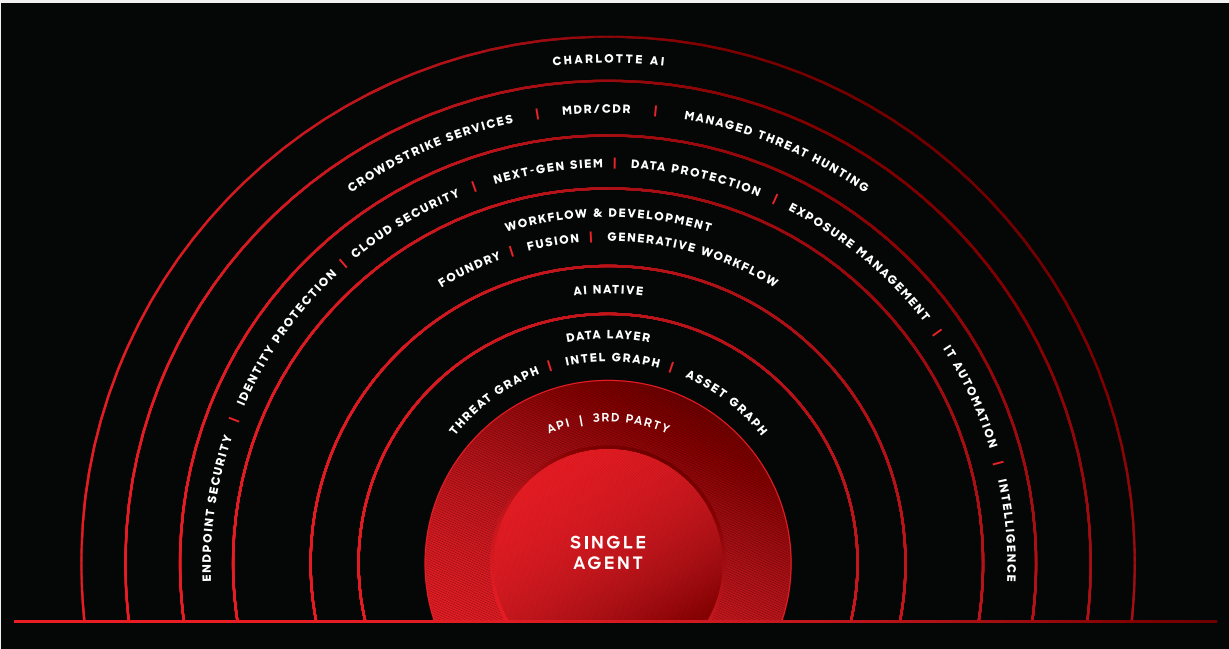
2.2 DoD Zero Trust Reference Architecture Capabilities

These 45 Capabilities are subdivided into 152 Activities or requirements.

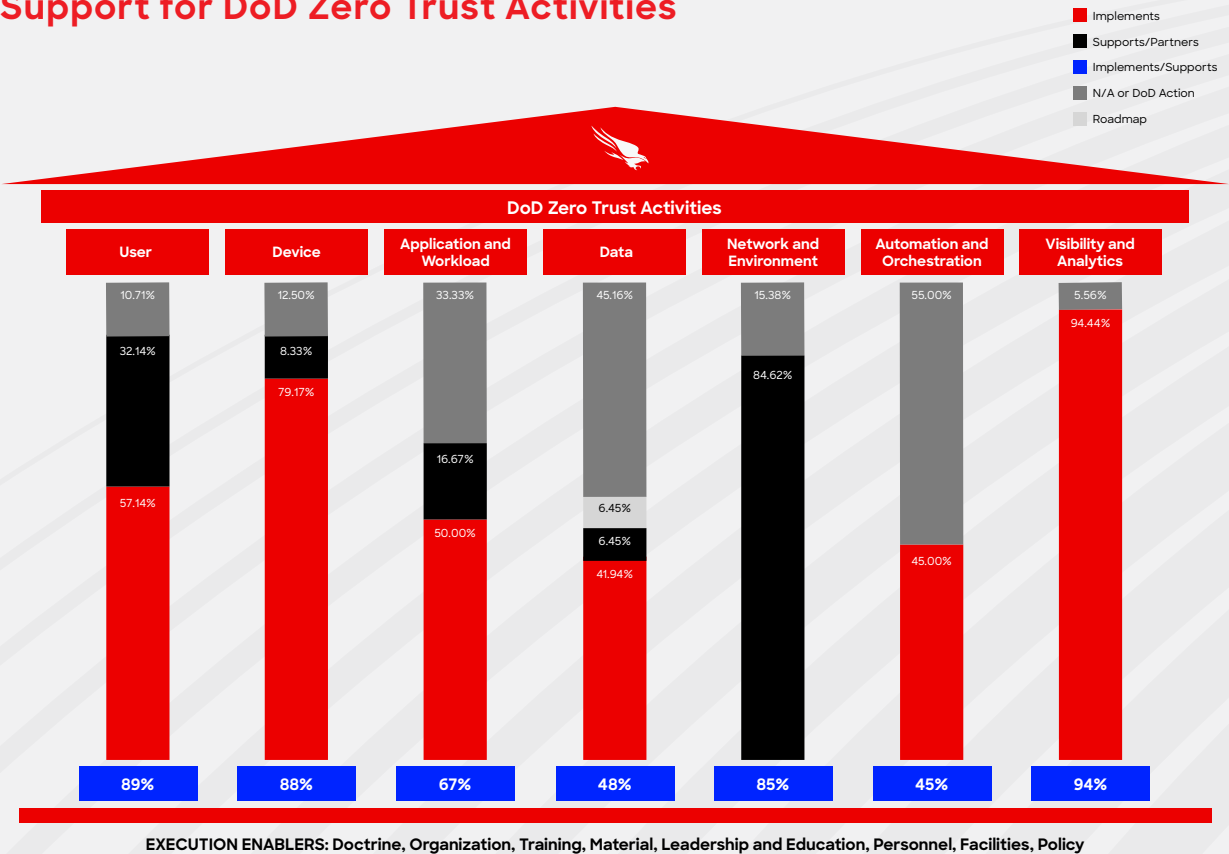


CrowdStrike Falcon Platform

CrowdStrike provides a platform approach to implementing Zero Trust.



2.3 Summary of CrowdStrike's Implementation and Integration Support for DoD Zero Trust Activities



3. DoD Zero Trust Pillars and Capabilities with CrowdStrike Implementation of Activities

3.1 User Pillar

Pillar Summary

The **DoD Zero Trust Architecture (ZTA) User Pillar** centers on ensuring that user identities are continuously authenticated and authorized before granting access to resources. It emphasizes strong identity and access management (IAM) practices, such as enforcing least-privilege access, using adaptive authentication methods and applying risk-based conditional access. The goal is to prevent unauthorized access, lateral movement and misuse of credentials by continuously verifying users based on their roles, behavior and access needs.

CrowdStrike supports the DoD's Zero Trust journey with its cloud-native, scalable architecture, providing comprehensive identity protection and access control across complex enterprise environments. The Falcon platform offers enhanced visibility by continuously monitoring user behavior and identity security in real time, validating that access is based on risk posture and dynamic assessments. With robust support for Zero Trust frameworks, CrowdStrike integrates seamlessly with existing security ecosystems to enable adaptive, least-privilege access policies. This helps organizations proactively secure identities, prevent lateral movement and mitigate threats from credential misuse and unauthorized access.

Challenges

- 1. Inventory User:** Regular and privileged users, along with applications and services, must be consistently identified and integrated into an inventory that requires ongoing updates and modifications.
 - **Unified Identity:** All users (privileged, standard, human and programmatic), applications and services must be consistently identified and maintained in an updated inventory. This inventory integrates with lifecycle management processes such as Joiner, Mover, Leaver and Returner activities.
 - **DoD Authoritative Sources:** Identity sources (e.g., AMID, NIS, AFID) are established or augmented with local authoritative systems as necessary. Manual processes are leveraged initially, with plans to transition to automated identity management (IDM).
- 2. Conditional User Access:** Transitioning from traditional role-based access control to dynamic, attribute-driven access rules requires maturity and integration across various systems, including a federated identity, credential and access management (ICAM) solution and enterprise roles.
 - **Dynamic Access Rules:** Transitioning from traditional role-based access control to dynamic, attribute-based access relies on federated ICAM solutions and risk-aware automation.
 - **Rule Development:** Periodic authentication activities evolve into dynamic access controls using AI and ML for real-time decision-making and privilege management.

- 3. Multifactor Authentication (MFA):** Establishing a centralized MFA solution and an identity provider (IdP) is challenging, especially when retiring local or built-in accounts and integrating external users.
 - **IdP and MFA Integration:** Establish a centralized, cloud-capable IdP integrated with DoD-approved MFA solutions.
 - Support compliance with cybersecurity standards (e.g., FIPS 140-2, FIPS 197) and integration with enterprise public key infrastructure (PKI) for trusted certificate management.
 - Enable biometric capabilities and alternative authentication methods for mission-critical applications.
 - **Cloud Migration:** Move IdP and ICAM solutions to resilient cloud environments while maintaining enclave/denied, degraded, intermittent or limited (DDIL) local capabilities for disconnected operations.
 - 4. Privileged Account Management (PAM):** Removing permanent elevated privileges involves ongoing monitoring, automating privilege escalation approvals and integrating analytics for anomaly detection.
 - **Dynamic Privilege Models:**
 - Implement just-in-time (JIT) and Just Enough Administration (JEA) methods for managing privileged access.
 - Integrate PAM solutions with applications and services for automated approvals, privilege escalation and anomaly detection.
 - **Risk-Based Exceptions:** Applications/services that cannot integrate with PAM are managed using a risk-based methodology, with plans for decommissioning unsupported solutions.
 - 5. Identity Lifecycle Management (ILM):** Standardizing ILM processes and integrating them with organizational IdP/IDM solutions is complex, especially when transitioning to an enterprise-wide solution or identity federation.
 - **Standardized Processes:**
 - Standardize ILM processes across the enterprise, integrating with centralized IdP and ICAM solutions.
 - Automate the identification and management of user attributes, groups, credentials and permissions.
 - **Exception Handling:** Evaluate risk-based exceptions regularly, ensuring alignment with enterprise policies and transitioning exceptions into compliance where possible.
 - 6. User and Entity Behavior Analytics (UEBA):** Expanding basic UEBA functionality to include organization-specific attributes and integrating it with user management systems for enhanced threat detection presents implementation challenges.
 - **Integrated Analytics:**
 - Extend UEBA functionality to incorporate organization-specific attributes for advanced threat detection.
 - Integrate UEBA and user activity monitoring (UAM) with PAM and ICAM to enable behavior-based decision-making for dynamic access.
 - **Cross-Pillar Analytics:** Leverage AI/ML analytics from UEBA for continuous improvement in authentication and privilege management.
 - 7. Continuous Authentication:** Moving from legacy single authentication to continuous, attribute-based authentication (based on user activity and privileges) requires significant coordination and system integration across the enterprise.
-

CrowdStrike Implementation Modules

- CrowdStrike Falcon® Identity Protection
- CrowdStrike Falcon® Insight XDR

CrowdStrike Module Descriptions

CrowdStrike Falcon Identity Protection provides real-time security for identity-based threats by unifying identity and endpoint protection. It delivers visibility across cloud, on-premises and hybrid environments, utilizing AI to detect anomalies and stop adversaries before they move laterally. The solution also enables dynamic, risk-based conditional access and continuous monitoring, extending protection to legacy systems. With seamless integration and support for Zero Trust frameworks, Falcon Identity Protection empowers organizations to block cross-domain attacks, automate password resets (and compromised password detection) and enhance security across all identity layers.

CrowdStrike Falcon Insight XDR provides AI-powered endpoint detection and response (EDR) with world-class threat intelligence, enabling organizations to detect and respond to adversaries in real time. It enhances visibility across endpoints and other data sources, offering rapid responses through Falcon Real Time Response (RTR) and CrowdStrike Falcon® Fusion SOAR. By leveraging AI-led investigations and MITRE ATT&CK® mappings, Falcon Insight XDR reduces false positives and empowers teams to respond efficiently to threats, offering unified, extended control across various environments.

Capability Recommendations and Activity Outcomes

1.1 User Inventory

- **CrowdStrike Falcon Identity Protection** provides real-time visibility and continuous updates of users, maintaining an up-to-date inventory. It distinguishes between regular and privileged users, ensuring dynamic tracking and monitoring to meet ongoing user management needs.
- **CrowdStrike Falcon Insight XDR** provides complete endpoint visibility across the organization by continuously monitoring and analyzing endpoint activity in real time. It ensures a current and accurate inventory of all assets while enabling security teams to effectively track and manage both standard and privileged users throughout the enterprise.
- **Mapped Outcomes:**
 - **1.1.1 Authoritative Source of Identity**
 - **Identified Managed Regular Users:** Continuous reviews ensure regular users are identified and tracked with enterprise-approved governance.
 - **Identified Managed Privileged Users:** Inventory and telemetry monitor privileged accounts dynamically, reducing the risk of misuse.

1.2 Conditional User Access

- **CrowdStrike Falcon Identity Protection** supports dynamic, attribute-driven access control by continuously monitoring user behavior, risk factors and context to adapt access permissions in real time. It integrates with IAM systems, enabling seamless enforcement of enterprise roles and federated ICAM policies. This allows organizations to transition from traditional role-based access control to more flexible, risk-based access rules across diverse environments.
- **CrowdStrike Falcon Insight XDR** enables organizations to enhance access control processes by correlating cross-domain telemetry. This integration allows security teams to gain real-time insights and visibility, supporting a shift from traditional role-based access to more dynamic, attribute-driven access control systems.
- **Mapped Outcomes:**
 - **1.2.1 Implement App-Based Permissions per User, 1.2.2-1.2.3 Rule-Based Dynamic Access, 1.2.4-1.2.5 Enterprise Government Roles and Permissions**
 - **Enterprise Roles/Attributes Vetted and Approved via ICAM Governance Processes:** Integrated attributes are federated and aligned with governance-approved roles.
 - **Components Identify Attributes Associated with PAM Activities:** Continuous telemetry correlation supports attribute identification and policy alignment.
 - **Access Limited to Users with Appropriate Enterprise Authentication and Authorization:** Risk-based access controls ensure only authorized users access sensitive functions and data.
 - **JIT/JEA Permissions Implemented for Administrative Users:** Dynamic permissions for privileged users are applied through automated processes.
 - **Build policies based on AI/ML:** Components enabled to build policies based on AI/ML-informed behavioral analysis and risk posture of all identities within the organization.

1.3 Multifactor Authentication

- **CrowdStrike Falcon Identity Protection** enforces MFA and continuously monitors for identity-based threats in real time. It provides protection by detecting and stopping attacks that leverage compromised credentials and integrates with existing identity systems to enhance overall security. Falcon Identity Protection ensures secure access by evaluating user behavior and risk, allowing organizations to manage identity threats effectively.
 - **Mapped Outcomes:**
 - **1.3.1 Organizational MFA, 1.3.2-1.3.3 Alternative Flexible MFA**
 - **Enforcement of MFA for Critical Applications/Services:** MFA is enforced across critical services to ensure secure user access.
 - **Continuous Monitoring for Identity-Based Threats:** Identity-based threats, such as credential abuse, are detected and mitigated through continuous monitoring and risk-based assessments.
 - **Integration with Identity Systems:** Seamless integration with identity systems ensures consistent enforcement of MFA policies across environments.
-

1.4 Privileged Account Management

- **CrowdStrike Falcon Identity Protection** provides real-time monitoring of identity-based threats, including those involving privileged accounts. It detects and stops attacks leveraging compromised credentials and ensures secure access by continuously evaluating user behavior and risk. The platform integrates with existing identity systems to protect against identity-driven attacks like password spraying and privilege abuse.
- **CrowdStrike Falcon Insight XDR** supports PAM by monitoring device activity and correlating telemetry to detect suspicious behavior, which can help identify abnormal privilege escalations. The solution provides enhanced visibility and rapid response capabilities, reducing the risks associated with privileged accounts.
- **Mapped Outcomes:**
 - **1.4.1-1.4.2 Implement System and Migrate Privileged Users, 1.4.3-1.4.4 Real-Time Approvals and JIT/JEA Analytics**
 - **Applications and Devices that Support/Do Not Support PAM Identified:** Monitors privileged account usage across devices and applications.
 - **Privileged Activities Migrated to PAM and Fully Managed:** Enables JIT/JEA permissions to reduce risk.
 - **High-Risk Accounts Managed with JIT/JEA Access:** Supports privilege escalation management and approval workflows.

1.5 Identity Federation and User Credentialing

- **CrowdStrike Falcon Identity Protection** integrates with existing IdPs and IDM systems to ensure real-time threat detection and secure access. It supports transitions to enterprise-wide identity federation by continuously assessing user risk. Falcon Identity Protection provides dynamic, risk-based access decisions to safeguard identities against evolving threats.
 - **Mapped Outcomes:**
 - **1.5.2-1.5.4 Identity Lifecycle Management**
 - **Automated Identity Processes Implemented:** CrowdStrike Falcon Identity Protection integrates with existing IdPs and IDM systems to automate identity activities, ensuring real-time user risk assessment and secure access.
 - **Integrated with Enterprise ICAM Processes and Tools:** Supports enterprise ICAM processes by dynamically correlating user behavior with critical identity attributes and enabling risk-based decisions.
 - **Primary Identity Management Functions Transitioned to Cloud:** Facilitates enterprise-wide identity federation and cloud-based solutions, aligning with advanced DoD Zero Trust requirements for scalability and automation.
-

1.6 Behavioral, Contextual ID and Biometrics

- **CrowdStrike Falcon Identity Protection** enhances UEBA by leveraging advanced behavior analytics to detect identity-based threats in real time. It integrates with user management systems, providing continuous assessment of user risk and detecting anomalies based on organization-specific attributes. This enables more accurate threat detection, addressing the challenges of expanding UEBA functionality to include custom attributes for enhanced security.
- **Mapped Outcomes:**
 - **1.6.1 Implement UEBA and UAM Tooling, 1.6.2-1.6.3 User Activity Monitoring**
 - **UEBA Correlated with Master User Record and Enterprise IdP:** Enables advanced threat detection and anomaly identification.
 - **Integrated with JIT/JEA for Critical and General Services:** Supports automated privilege approvals with behavioral insights.
 - **Entity Monitoring Enhanced Across Services:** Expands analytics scope for comprehensive threat management.

1.7 Least-Privilege Access

- **CrowdStrike Falcon Identity Protection** provides continuous identity threat detection and monitoring to assess least-privilege access and secure identities across hybrid environments. It detects and prevents identity-based attacks by monitoring for credential misuse and anomalous activity while integrating seamlessly with enterprise identity systems.
- **Mapped Outcomes:**
 - **1.7.1 Deny User by Default Policy**
 - **Authentication Implemented Across Applications per Session:** Enforces session-based access controls based on user and endpoint risk.
 - **Transaction Authentication Implemented Based on Security Attributes:** Dynamically assesses user risk for each transaction, enforcing adaptive policies.

1.8 Continuous Authentication

- **CrowdStrike Falcon Identity Protection** strengthens continuous authentication by integrating with IdPs to authenticate, authorize and validate requestors for real-time monitoring and risk-based access decisions. These IdP integrations enable secure, continuous authentication by evaluating user activity and enforcing security policies. This approach provides a scalable and resilient framework for enterprise-wide identity security.
 - **Mapped Outcomes:**
 - **1.8.1 Single Authentication, 1.8.2 Periodic Authentication, 1.8.3-1.8.4 Continuous Authentication**
 - **Authentication Implemented Across Applications per Session:** Enforces session-based access controls tailored to specific user, source, and destination contexts. Policies can be defined to authenticate users every time, once per session, or based on customizable time intervals (e.g., 24 hours, 7 days, or 30 days), ensuring secure and compliant access across enterprise applications.
-

- **Periodic Authentication Implemented During Sessions:** Enables re-authentication within an active session based on security attributes or predefined intervals, such as every 24 hours or weekly. This approach strengthens session integrity while dynamically adjusting to changing security contexts, ensuring ongoing compliance and mitigating risks.
- **Transaction Authentication Implemented Based on Security Attributes:** Dynamically enforces adaptive authentication policies for high-risk or privilege-sensitive actions. Actions such as token revocation, session termination, or policy updates can be orchestrated through integrated IDaaS providers like Entra ID and Okta, leveraging response actions triggered by detected identity-based threats.

1.9 Integrated ICAM Platform

- **CrowdStrike Falcon Identity Protection** enhances identity management by integrating with enterprise Identity Providers (IdPs) to authenticate, authorize, and validate user activity. These integrations allow for real-time monitoring and assessment of risk-based access policies, enabling scalable and resilient identity security.
- **Mapped Outcomes:**
 - **1.9.2-1.9.3 Enterprise PKI/Identity Protection**
 - **Strengthened Enterprise Identity Security:** Enables secure and continuous authentication by integrating with IdPs to evaluate user activity and enforce access policies across all environments.
 - **Authentication Across Applications:** Applies session-based access controls based on user and endpoint context, ensuring consistent and compliant access decisions.
 - **Dynamic Risk-Based Access Decisions:** Assesses user activity in real time to enforce adaptive security policies for high-risk or critical transactions.

3.2 Device Pillar

Pillar Summary

The **DoD ZTA Device Pillar** focuses on securing and managing all devices that interact with the network to mitigate security risks. This pillar requires continuous verification of device health, compliance and security posture. Each device, whether managed or unmanaged, must be authenticated, must be monitored and must have its risk posture assessed before it can access any resources. Devices must maintain compliance with security policies such as encryption, patching and endpoint protection in line with the broader Zero Trust strategy that eliminates implicit trust.

CrowdStrike supports the DoD's Zero Trust journey through the Falcon platform, which is built on a scalable, cloud-native architecture. The platform enables comprehensive endpoint, identity and workload protection, helping the DoD secure devices across hybrid and multi-cloud environments. The Falcon platform enhances visibility and control over both managed and unmanaged devices by using a single lightweight agent that provides continuous real-time security posture assessments. This platform integrates with other security tools to enforce conditional access policies based on the device's security state and user behavior.

This layered defense approach enables the DoD to meet its Zero Trust goals, protecting data and applications while reducing complexity across its ecosystem.

Challenges

1. **Device Inventory:** DoD organizations maintain an approved inventory of all devices accessing the network, including detailed attributes like machine certificates, patch status and vulnerabilities.

DoD Components migrate manual device inventories to automated enterprise device managementsolutions. Attributes such as compliance and integration status are tracked, and devices critical to services are mandated for enterprise device management to ensure consistent management and automation.

2. **Device Detection and Compliance:** Asset management systems must detect devices connecting to the network and confirm their compliance, ensuring adherence to IT and cybersecurity standards.

DoD Components implement solutions — e.g., STIGs, Comply-to-Connect (C2C) and unified endpoint management (UEM) — to confirm device compliance. Enterprise standards ensure device baseline checks are integrated, enabling compliance-driven access policies.

3. **Device Authorization and Inspection:** Real-time device authorization integrates advanced tooling — e.g., NGAV and file integrity monitoring (FIM) — and organizational PKI systems to assess device risk posture and monitor activity for anomalies.

DoD Components implement solutions like FIM, NGAV and UEBA for risk posture assessments and anomaly detection. PKI solutions are deployed for device authentication, integrating certificates into device authorization.

4. **Remote Access:** Least-privilege access for devices is audited and expanded to include bring your own device (BYOD) and internet of things (IoT) devices using the enterprise IdP, with phased support for broader device types.

DoD Components use enterprise device management and unified endpoint and device management (UEDM) to support managed BYOD and IoT devices. Dynamic access policies enforce least-privilege access, ensuring compliance with Zero Trust principles.

5. **Asset, Vulnerability and Patch Management:** DoD organizations establish processes for testing and deploying vendor patches for connected devices, combining human oversight and management across the organization.

DoD Components procure and implement tools for asset, vulnerability and patch management. These tools integrate minimum compliance standards (e.g., STIGs, C2C, UEM) and APIs for automation and integration, ensuring Zero Trust target functionality is met.

CrowdStrike Implementation Modules

- CrowdStrike Falcon Insight XDR
- CrowdStrike Falcon Identity Protection
- CrowdStrike Falcon® for IT
- CrowdStrike® Falcon Prevent®
- CrowdStrike Falcon Next-Gen SIEM
- CrowdStrike Falcon® for Mobile
- CrowdStrike Falcon® for XIoT
- CrowdStrike Falcon® Cloud Security
- CrowdStrike Falcon® Exposure Management
 - CrowdStrike Falcon® Discover
 - CrowdStrike Falcon® Spotlight
- CrowdStrike Falcon® FileVantage

CrowdStrike Module Descriptions

CrowdStrike Falcon Insight XDR provides AI-powered EDR with world-class threat intelligence, enabling organizations to detect and respond to adversaries in real time. It enhances visibility across endpoints and other data sources, offering rapid responses through Falcon RTR and Falcon Fusion SOAR. By leveraging AI-led investigations and MITRE ATT&CK mappings, Falcon Insight XDR reduces false positives and empowers teams to respond efficiently to threats, offering unified, extended control across various environments.

CrowdStrike Falcon Identity Protection provides real-time security for identity-based threats by unifying identity and endpoint protection. It delivers visibility across cloud, on-premises and hybrid environments, utilizing AI to detect anomalies and stop adversaries before they move laterally. The solution also enables dynamic, risk-based conditional access and continuous monitoring, extending protection to legacy systems. With seamless integration and support for Zero Trust frameworks, Falcon Identity Protection empowers organizations to block cross-domain attacks and reduce password resets while enhancing security across all identity layers.

CrowdStrike Falcon for IT delivers real-time visibility, response and automation, ensuring enterprise resilience through a unified view of all endpoints. By tracking key attributes such as endpoint uptime, performance metrics, certificates, patch status and vulnerabilities, Falcon for IT enables proactive endpoint management and risk mitigation. Falcon for IT correlates this data with CrowdStrike Falcon® Next-Gen SIEM, improving the detection of potential threats and streamlining forensic investigations. Additionally, Falcon for IT facilitates emergency patching, ensuring rapid response to critical vulnerabilities and optimizing both security and operational efficiency across the entire infrastructure.

CrowdStrike Falcon Prevent (NGAV) provides powerful malware prevention by using AI and ML to block known and unknown threats, including fileless attacks and ransomware. This cloud-native solution replaces legacy antivirus (AV) with signatureless protection that is effective both online and offline, reducing false positives and improving security efficiency.

CrowdStrike Falcon Next-Gen SIEM centralizes security data to provide advanced analytics and real-time threat detection, enabling organizations to monitor, detect, and respond to threats with greater efficiency. Integrated with extended detection and response (XDR) capabilities, it delivers a unified platform for streamlined investigations and enhanced incident response. Built on a scalable, cloud-native architecture, Falcon Next-Gen SIEM provides comprehensive visibility into security environments, helping organizations identify risks, ensure compliance, and maintain robust security posture across hybrid and multi-cloud environments.

CrowdStrike Falcon for Mobile extends endpoint protection to mobile devices, ensuring that Android and iOS endpoints are secured from sophisticated malware and phishing attacks. This solution helps organizations monitor mobile endpoint activities, enabling threat detection and incident response in real time for mobile environments.

CrowdStrike Falcon for XIoT provides protection for IoT devices, safeguarding them from emerging threats. It offers visibility and security across IoT ecosystems, addressing risks from both internal and external sources by identifying and mitigating vulnerabilities within connected devices.

CrowdStrike Falcon Cloud Security protects workloads in public, private and hybrid cloud environments by providing continuous monitoring and protection. It detects misconfigurations, vulnerabilities and advanced threats in cloud infrastructures, enabling proactive cloud security management.

CrowdStrike Falcon Discover and Falcon Exposure Management provides asset discovery and visibility, enabling organizations to identify unmanaged devices, shadow IT and security gaps across their networks. By providing real-time visibility into an organization's IT environment, Falcon Discover helps mitigate risks posed by unknown or unmanaged assets.

CrowdStrike Falcon Spotlight offers continuous, real-time vulnerability management for endpoints, helping organizations identify and prioritize vulnerabilities across their infrastructure. By automating the vulnerability scanning and remediation process, it helps reduce the attack surface and improve overall security posture.

CrowdStrike Falcon FileVantage provides real-time File Integrity Monitoring (FIM) to track critical changes to files, folders, and registries, ensuring continuous visibility into harmful or unauthorized modifications. It monitors for anomalies that could compromise security and integrates with detailed dashboards to help security teams quickly identify risks. With robust threat intelligence and actionable insights, Falcon FileVantage enhances compliance with regulatory standards and strengthens the security posture of devices across environments.

Capability Recommendations and Activity Outcomes

2.1 Device Inventory

- **CrowdStrike Falcon Spotlight and Falcon Discover/Falcon Exposure Management** help DoD organizations maintain a comprehensive inventory of all devices accessing their network by offering real-time asset discovery and visibility across endpoints and cloud environments. They continuously track device vulnerabilities, providing detailed insights into exposures through AI-powered assessments and external attack surface management. These solutions enable efficient risk assessment and prioritization, ensuring an up-to-date inventory with full visibility into all devices and significantly enhancing the organization's security posture.
- **CrowdStrike Falcon for IT** delivers real-time visibility and response capabilities that empower organizations to efficiently manage their entire IT infrastructure. With continuous monitoring, it offers instant insights into device performance, certificate management, real-time vulnerability identification and response, and system misconfigurations, helping teams address potential issues before they escalate. Falcon for IT integrates with IT workflows to automate remediation processes, allowing for swift response to detected risks. This real-time approach ensures that organizations maintain up-to-date, secure device inventories while reducing response times to emerging threats.
- **Mapped Outcomes:**
 - **2.1.1 Device Health Tool Gap Analysis, 2.1.2 Non-Person Entity (NPE)/PKI Device Under Management, 2.1.3-2.1.4 Enterprise IdP**
 - **Comprehensive Device Inventory:** Real-time visibility into devices accessing the network, including endpoints and cloud environments, ensures continuous updates and accurate tracking.
 - **Risk Prioritization:** AI-powered assessments and external monitoring provide insights into vulnerabilities, enabling effective prioritization of risks.
 - **Automation Support:** Integration with existing workflows automates remediation processes, enhancing efficiency in maintaining a secure inventory.

2.2 Device Detection and Compliance

- **CrowdStrike Falcon Discover and Falcon Exposure Management** enable DoD organizations to detect and confirm the compliance of all devices connecting to their network. By offering asset discovery across endpoints and cloud environments, these solutions help ensure adherence to IT and cybersecurity standards. These solutions track vulnerabilities through AI-powered assessments and external attack surface management, enabling organizations to efficiently prioritize risks and maintain an up-to-date inventory for security and regulatory compliance.
-

- **Mapped Outcomes:**

- **2.2.1-2.2.2 Implement C2C and Compliance-Based Network Authorization**

- **Compliance Verification:** Checks for regulatory compliance and continuous monitoring across endpoints and cloud systems helps ensure adherence to IT and security standards.
 - **Risk Tracking:** Regular assessments help maintain compliance by identifying vulnerabilities and noncompliant devices for prioritization and mitigation.
 - **Dynamic Inventory:** Real-time updates provide a comprehensive view of all assets, helping organizations remain compliant with evolving regulatory needs.

2.3 Device Authorization and Inspection

- **CrowdStrike Falcon Prevent** integrates NGAV technology to enable real-time device authorization, continuously monitoring device behavior to assess risk posture. It leverages machine learning and behavioral analysis to detect known and unknown threats, providing advanced threat detection without relying on signatures. This allows Falcon Prevent to inspect devices for anomalies and ensure secure, compliant access across the network.
 - **CrowdStrike Falcon® FileVantage** offers real-time FIM to ensure secure device authorization and inspection by tracking critical changes in files, folders and registries. It continuously monitors for anomalies and unauthorized modifications, providing visibility into harmful changes that could compromise the device's security posture. With detailed dashboards and threat intelligence integration, Falcon FileVantage helps security teams quickly identify risks and maintain compliance with regulatory standards.
 - **CrowdStrike Falcon Insight XDR** integrates real-time monitoring and advanced tooling by correlating telemetry across endpoints and other security domains. It uses AI-powered detection and response to continuously assess device risk posture, identifying anomalies and unauthorized activities. With integrated support for NGAV and visibility across systems, Falcon Insight XDR enables organizations to efficiently inspect and authorize devices while quickly responding to potential threats.
 - **Mapped Outcomes:**
 - **2.3.1 Entity Activity Monitoring, 2.3.3 Implement Application Containment and FIM Tools, 2.3.4 Integrate NGAV Tools with C2C, 2.3.5 Fully Integrate Device Security Stack with CDC as Appropriate, 2.3.7 Enterprise PKI Pt. 2**
 - **Real-Time Authorization:** Devices are authorized based on behavioral analysis and risk posture assessments, identifying and mitigating anomalies.
 - **File Integrity Tracking:** Critical changes to files, folders and registries are continuously monitored to detect unauthorized modifications and prevent compromises.
 - **Comprehensive Inspection:** Telemetry from multiple systems is correlated to continuously monitor and detect unauthorized activities, ensuring secure device access.
-

2.4 Remote Access

- **CrowdStrike Falcon Identity Protection** enables least-privilege access for remote devices, including BYOD and IoT devices, by integrating with enterprise IdPs and providing real-time identity threat detection and response. It enables risk-based access controls and uses advanced behavioral analytics to assess user behavior and device security posture, ensuring that only compliant devices are granted access. This solution expands to support multiple device types through phased integration with IdPs like Microsoft Entra ID, allowing secure, dynamic access management across a wide range of environments.
- **CrowdStrike Falcon Discover and Falcon Exposure Management** help meet the Remote Access requirement by offering complete visibility and risk management for devices, including BYOD and IoT devices, through asset discovery and real-time exposure assessment. It continuously monitors device risk posture and vulnerabilities to ensure secure access across various environments. With support for diverse device types, Falcon Discover/Falcon Exposure Management enables phased implementation of secure access and helps maintain compliance with organizational security standards.
- **Mapped Outcomes:**
 - **2.4.1 Deny Device by Default Policy, 2.4.2 Managed and Limited BYOD and IoT Support, 2.4.3-2.4.4 Managed and Full BYOD and IoT Support**
 - **Least-Privilege Access Enforcement:** Enforces risk-based access controls for remote devices, ensuring only compliant devices and users are granted access.
 - **Phased Integration:** Expands secure access management to various device types, including BYOD and IoT devices, through staged support.
 - **Behavioral Analysis:** Advanced analytics evaluate user and device security posture dynamically to enable secure, risk-based access.

2.5 Partially and Fully Automated Asset, Vulnerability and Patch Management

- **CrowdStrike Falcon Spotlight, Falcon Discover and Falcon Exposure Management** provide continuous asset discovery and vulnerability assessment across all environments, including on-premises, cloud and IoT systems. These solutions allow DoD organizations to identify exposures, prioritize vulnerabilities using AI-driven insights and streamline remediation with both native and third-party tools, ensuring that patches are deployed efficiently across connected devices. By integrating advanced vulnerability intelligence, Falcon Spotlight and Falcon Discover/Exposure Management help security teams maintain a secure and compliant environment.
 - **CrowdStrike Falcon for IT** delivers real-time visibility, response and automation across hardware, software and user assets. Falcon for IT provides automation workflows for various enterprise use cases such as machine state updates, policy execution and vulnerability response, ensuring scalable and effective UEM.
-

- **Mapped Outcomes:**

- **2.5.1 Partially and Fully Automated Asset, Vulnerability and Patch Management**

- **Continuous Discovery:** Vulnerabilities across environments — including on-premises, cloud and IoT systems — are identified and assessed.
 - **Prioritized Remediation:** Risks are prioritized based on severity, enabling effective patch deployment and remediation workflows.
 - **Automated Management:** Workflow automation streamlines updates, policy execution and remediation tasks for scalable endpoint management.

2.6 Unified Endpoint Management

- **CrowdStrike Falcon for IT** streamlines operations and enhances security with real-time visibility across endpoints, servers and cloud workloads. Empowering IT and security teams with actionable insights, it enables swift response and complete control. Key features include asset discovery, software inventory and deployment, vulnerability visibility and remediation, and device management, and all these features are designed to eliminate blind spots and accelerate remediation. Seamlessly integrated with the broader Falcon platform, it drives efficiency while supporting faster, more informed decision-making.
 - **CrowdStrike Falcon Spotlight, Falcon Discover and Falcon Exposure Management** provide continuous, real-time visibility into an organization's attack surface, helping to identify and prioritize vulnerabilities before they can be exploited. By mapping exposures across endpoints, identities and cloud assets, they enable organizations to proactively reduce risk and strengthen their overall security posture. With automated discovery and assessment capabilities, these solutions help security teams focus on the most critical vulnerabilities, ensuring that remediation efforts are targeted and efficient. This approach empowers organizations to maintain secure configurations, streamline regulatory compliance and enhance operational resilience across their IT environment.
 - **CrowdStrike Falcon Identity Protection** integrates endpoint and identity security to stop identity-based attacks in real time. It provides continuous visibility into identity threats, enforces risk-based access policies and delivers frictionless authentication to enhance user security without disrupting workflows. By monitoring for credential misuse, lateral movement and other identity risks, it ensures secure configurations and strengthens access control. With its proactive approach to securing identities, organizations can streamline compliance enforcement, reduce attack surfaces and maintain centralized oversight of user and device assets across the enterprise.
 - **CrowdStrike Falcon for Mobile** provides advanced protection for Android and iOS devices, addressing mobile-specific threats with real-time detection and prevention. It delivers complete visibility into all mobile devices, allowing organizations to proactively identify and stop malicious activity. With its lightweight, nonintrusive architecture, Falcon for Mobile ensures security without disrupting user experience or device performance. Seamlessly integrating into the Falcon platform, it enhances the overall security posture by extending endpoint protection to mobile environments, enabling centralized management and a unified approach to securing all endpoints.
-

- **Mapped Outcomes:**

- **2.6.1 Implement UEM or Equivalent Tools, 2.6.2-2.6.3 Enterprise Device Management**

- **Automated Inventory and Vulnerability Management:** Manual inventory processes are replaced with automated solutions, enabling real-time tracking and reporting for all devices, including critical services. These systems provide insights into endpoint vulnerabilities, ensuring that asset data remains consistent and accessible for operational, security and compliance needs.
- **Compliance Monitoring and Enforcement:** Devices are continuously monitored to ensure adherence to minimum compliance standards, with actionable insights for remediation of noncompliant devices. Compliance data is integrated into asset management systems, enabling centralized reporting and visibility to maintain secure configurations across all managed devices.
- **Centralized Asset Management and Oversight:** Comprehensive asset management systems enable tracking and secure management of user devices — such as desktops, laptops and mobile devices — regardless of location. This unified framework supports seamless operations across distributed environments and ensures IT compliance through centralized reporting.
- **Unified Device and Location-Agnostic Management:** Devices, including critical and noncritical assets, are securely managed irrespective of their physical location, supporting both on-premises and remote environments. This automation reduces manual intervention, ensuring uniform enforcement of security policies while maintaining operational readiness.
- **Timely Patch and Configuration Management:** Timely patch application and secure configurations are ensured to prevent vulnerabilities. Critical services and mobile devices are integrated into broader management frameworks to maintain compliance, security and operational efficiency across all endpoints.

2.7 EDR and XDR

- **CrowdStrike Falcon Insight XDR** extends detection and response beyond endpoints by integrating telemetry from various security domains. This integration enhances visibility and detection capabilities, ensuring comprehensive coverage across the organization's security landscape. By correlating data from multiple sources, Falcon Insight XDR identifies and manages exceptions through a risk-based approach, facilitating continuous operation and adherence to security policies.
 - **CrowdStrike Falcon Next-Gen SIEM** centralizes security data, enabling advanced analytics and real-time threat detection. Its integration with XDR capabilities allows for the incorporation of Zero Trust advanced functionalities. This integration provides a unified platform for monitoring, detection and response, enhancing the organization's security posture.
-

- **CrowdStrike Falcon Prevent** delivers NGAV protection by utilizing ML and behavioral analysis to detect and prevent known and unknown threats. Falcon Prevent's integration with Falcon Insight XDR and Falcon Next-Gen SIEM ensures that endpoint protection data contributes to the broader security ecosystem, enhancing overall threat detection and response capabilities.
- **CrowdStrike Falcon Identity Protection** focuses on securing identities by providing real-time visibility and continuous monitoring of user activities. Falcon Identity Protection integrates with other Falcon platform modules and allows third-party integrations to enforce Zero Trust principles, ensuring that access decisions are based on continuous risk assessments. This integration supports an organization's strategy to manage exceptions methodically and maintain secure operations.
- **Mapped Outcomes:**
 - **2.7.1-2.7.3 EDR and XDR**
 - **Comprehensive Detection and Response:** Integrates telemetry from multiple domains to deliver unified endpoint detection and response, advanced analytics and real-time incident management. Ensures critical data is transferred to centralized systems for validation and operational checks.
 - **Prioritized Integration and Coverage:** Methodically identifies and prioritizes integration points, operationalizing them to provide expanded security coverage, enhanced data correlation and a streamlined response framework.
 - **Extended Alerting and Automated Response:** Enables advanced alerting and automated incident response through integration with analytics tools, enhancing threat detection, mitigation and Zero Trust access management.

3.3 Application and Workload Pillar

Pillar Summary

The **DoD ZTA Application and Workload Pillar** is focused on securing applications and the workloads they handle. This involves continuous verification of the security posture of applications as well as ensuring workloads are protected from compromise. In modern environments, workloads can include cloud services, containers and traditional on-premises applications. As these workloads increasingly span hybrid and multi-cloud infrastructures, they must be continuously monitored for vulnerabilities, unauthorized access and compliance with security policies.

CrowdStrike supports the Application and Workload Pillar of the DoD's Zero Trust journey by leveraging cloud-native architecture to secure applications and workloads with threat detection and continuous visibility. The CrowdStrike Falcon platform enables real-time monitoring, allowing organizations to quickly identify and remediate security incidents. The Falcon platform helps reduce the attack surface by enforcing least-privilege access policies and identifying lateral movement of attackers within compromised workloads. Additionally, the Falcon platform integrates with DevSecOps pipelines, ensuring that applications are continuously secured as they are developed and deployed.

Challenges

- 1. Application Inventory:** DoD organizations enforce continuous validation for application access using dynamic risk-based policies tied to user identity, device posture and application specifics. DoD Components support this by maintaining an inventory of approved applications, tracking attributes like supportability, hosting, version, responsible teams, licensing and dependencies.
 - 2. Secure Software Development and Integration:** Security is integrated into the software development lifecycle with automation, continuous validation in continuous integration/continuous delivery (CI/CD) pipelines and vulnerability management, ensuring compliance with DoD standards. Runtime security functions, automated approvals and streamlined processes enhance secure updates, testing and deployments.
 - 3. Software Risk Management:** Workloads across on-premises, cloud and hybrid environments are safeguarded through segmentation, least-privilege access and ongoing risk assessments. DoD Components enhance these protections by implementing runtime security functions, automating vulnerability resolution and strengthening supply chain security through supplier sourcing, approved repositories and risk management practices.
 - 4. Resource Authorization and Integration:** DoD organizations prioritize secure API and microservices management by focusing on design, authentication and continuous monitoring. To further strengthen access controls, DoD Components use approved API gateways and integrate resource authorization policies with attributes like data loss prevention (DLP), data rights management (DRM) and microsegmentation, enabling risk-based access decisions and fine-grained control over users, devices and services.
 - 5. Continuous Monitoring and Ongoing Authorizations:** DoD organizations leverage automation to standardize control monitoring, integrate testing into DevSecOps and resolve deviations through cross-pillar infrastructure. Dashboards and analytics provide real-time insights to support authorizations and ensure compliance across environments.
-

CrowdStrike Implementation Modules

- CrowdStrike Falcon Cloud Security
- CrowdStrike Falcon for IT
- CrowdStrike Falcon Discover/Falcon Exposure Management
- CrowdStrike Falcon Next-Gen SIEM
- CrowdStrike Falcon Insight XDR
- CrowdStrike Identity Protection

CrowdStrike Module Descriptions

CrowdStrike Falcon Cloud Security delivers advanced monitoring and comprehensive protection for applications and workloads across cloud and hybrid environments. By continuously analyzing critical attributes such as host integrity, container compliance, Kubernetes configurations and cloud resources, it helps to ensure workloads remain secure and aligned with stringent security principles. Seamless integration with diverse infrastructures enhances operational efficiency and ensures consistent threat response.

CrowdStrike Falcon for IT provides unified monitoring and control over endpoints and workloads, enabling organizations to maintain security and operational efficiency. Through real-time queries and actionable insights, Falcon for IT ensures continuous assessment of application health, workload compliance and security posture. By analyzing critical attributes such as resource utilization, access permissions and workload vulnerabilities, it supports risk-based decision-making and enforces strong security policies.

CrowdStrike Falcon Discover and Falcon Exposure Management provide comprehensive visibility into assets, applications and potential risks across cloud, on-premises and hybrid environments. By identifying, cataloging and monitoring connected systems and applications, it ensures that only authorized applications and components are utilized, aligning with established security protocols. With seamless integration across infrastructures, Falcon Discover/Falcon Exposure Management enables system owners to inventory and manage their environments effectively while prioritizing remediation efforts. This unified approach ensures secure operations, consistent policy enforcement and enhanced protection of critical resources.

CrowdStrike Falcon Next-Gen SIEM centralizes security data, providing advanced analytics and real-time monitoring to ensure comprehensive visibility into user activity, application access, and device events. Built on a scalable, cloud-native architecture, the solution integrates seamlessly with existing access gateways and policy enforcement systems, enabling organizations to maintain consistent application of security policies across hybrid and multi-cloud infrastructures. By consolidating security data and streamlining compliance reporting, Falcon Next-Gen SIEM helps identify risks and enhances the overall security posture of applications and workloads.

CrowdStrike Falcon Insight XDR extends detection and response capabilities across endpoints, workloads, and applications, providing real-time visibility and advanced threat detection. Built on a cloud-native architecture, it enables continuous monitoring to identify vulnerabilities, unauthorized access, and compliance gaps across hybrid and multi-cloud environments. Falcon Insight XDR integrates seamlessly with existing security infrastructure, allowing organizations to reduce the attack surface by detecting lateral movement and enforcing least-privilege access policies. With its unified view of security events, the solution empowers organizations to quickly remediate incidents and maintain a robust security posture for modern workloads.

CrowdStrike Falcon Identity Protection safeguards identities by continuously monitoring and assessing user activities across hybrid and multi-cloud environments to detect and prevent identity-based attacks. Leveraging real-time visibility, it enforces conditional access policies to ensure secure access based on user context and risk posture. Built on a cloud-native architecture, Falcon Identity Protection integrates with existing identity providers to provide advanced protection against compromised credentials and lateral movement threats. By delivering actionable insights and enforcing least-privilege access, the solution enhances security for modern applications and workloads while ensuring compliance with organizational policies.

Recommendations and Activity Outcomes

3.1 Application Inventory

- **CrowdStrike Falcon for IT** provides real-time enterprise visibility and response, offering advanced capabilities to manage and secure applications across the enterprise. By enabling deep app queries and insights into application performance, resource utilization and security posture, Falcon for IT ensures accurate and up-to-date tracking of all enterprise applications. Its continuous monitoring detects misconfigurations and performance issues, empowering IT teams to proactively address potential risks before they escalate. Integrated with existing workflows, Falcon for IT simplifies application management and enhances operational efficiency while ensuring compliance with security policies. This comprehensive approach supports resilient IT infrastructure by combining real-time insights with automated remediation for optimal application performance and security.
- **CrowdStrike Falcon Discover and Falcon Exposure Management** enhance application inventory by providing continuous asset discovery and deep visibility across the enterprise. It identifies all applications — including their versions, hosting environments, licensing and dependencies — while mapping external exposure risks and highlighting potential vulnerabilities or misconfigurations. This functionality ensures a complete understanding of the application landscape, enabling organizations to assess risks effectively, prioritize critical issues and maintain compliance. By offering a comprehensive view of application environments, Falcon Discover/Falcon Exposure Management supports proactive security management and strengthens the overall resilience of the enterprise.

- **CrowdStrike Falcon Cloud Security** provides advanced detection for cloud and application workloads through its cloud security posture management (CSPM), cloud workload protection (CWP) and application security posture management (ASPM) capabilities. CSPM ensures secure cloud configurations by identifying misconfigurations, vulnerabilities and compliance risks while providing automated remediation across multi-cloud environments. CWP focuses on runtime protection for cloud workloads — including containers and virtual machines — ensuring intricate defense against active threats and maintaining workload integrity. ASPM enhances application security by monitoring and managing application configurations, dependencies and compliance, ensuring secure and efficient application deployment. Together, these modules deliver comprehensive visibility and security for cloud and hybrid infrastructures.
- **Mapped Outcomes:**
 - **3.1.1 Application/Code Identification**
 - **Comprehensive Application Inventory:** Real-time discovery and monitoring ensure continuous updates and accurate validation of application attributes.
 - **Risk-Based Insights:** Automated detection and prioritization of misconfigurations and vulnerabilities enhance security management.
 - **Operational Efficiency:** Real-time visibility, response and automation streamline inventory management and compliance.

3.2 Secure Software Development and Integration

- **CrowdStrike Falcon Cloud Security** integrates advanced threat intelligence, runtime protection and compliance capabilities directly into development workflows. Its APIs enable seamless integration with CI/CD pipelines, automating vulnerability scanning and prioritization in real time to reduce security bottlenecks. Developers gain visibility into misconfigurations and exposed credentials through continuous runtime monitoring, ensuring cloud-native applications remain secure throughout their lifecycle. With compliance-focused features, Falcon Cloud Security enhances code quality, mitigates risks early and accelerates secure software delivery with lightweight, scalable and cloud-native architecture.
- **Mapped Outcomes:**
 - **3.2.1-3.2.2 Build DevSecOps Software Factory, 3.2.3-3.2.4 Automate Application Security and Code Remediation**
 - **Integration of Security Controls:** Zero Trust security controls and runtime protection are embedded into software development and deployment processes.
 - **Automated Detection and Remediation:** Supports the identification of vulnerabilities, misconfigurations and compliance risks, facilitating secure API gateways and automated remediation.
 - **Enhanced Application Security Testing:** Enables the integration of static and dynamic application security testing into DevSecOps workflows.
 - **Comprehensive Visibility and Inventory:** Provides detailed monitoring of cloud and application attributes for continuous validation and compliance.

3.3 Software Risk Management

- **CrowdStrike Falcon Cloud Security** enables organizations to meet software risk management requirements by integrating robust tools and processes across the development, deployment and runtime stages. By leveraging capabilities such as secure configurations, application dependency management and runtime protection, organizations can evaluate supplier risks, streamline repository oversight, track vulnerabilities and ensure continuous validation of application security. These features enhance compliance, operational security and efficiency throughout the software lifecycle.
- **Mapped Outcomes:**
 - **3.3.1 Secure Software Development Framework and Software Bills of Material (SBOMs), 3.3.2-3.3.3 Vulnerability Management Program, 3.3.4 Continual Validation**
 - **Standardized Supplier Risk Management:** Visibility into the origin and maintenance history of software libraries aids in assessing supplier sourcing risks. This transparency helps maintain the integrity of the software supply chain by identifying and managing risks associated with third-party components.
 - **Repository and Bill of Materials Oversight:** SBOM capabilities allow organizations to track application origins, supportability and risk posture. This supports supply chain transparency and informed risk management by providing detailed insights into software components and their dependencies.
 - **Integrated Vulnerability Tracking and Management:** Cloud vulnerability management enables organizations to identify and manage vulnerabilities across cloud environments and workloads. Continuous detection and real-time threat intelligence facilitate effective vulnerability management in compliance with organizational policies.
 - **Continuous Validation for Application Development:** Security is integrated into the CI/CD pipeline, enforcing predefined image and infrastructure as code (IaC) policies. This ensures that security principles are applied throughout the development lifecycle, maintaining consistent security standards for applications developed within and outside CI/CD workflows.
 - **Secure Application Deployment and Runtime Monitoring:** Runtime protection for cloud workloads ensures that applications maintain secure operational integrity post-deployment. Continuous monitoring of application configurations and dependencies helps validate secure deployments and compliance.

3.4 Resource Authorization and Integration

- **CrowdStrike Falcon Next-Gen SIEM** centralizes log management and monitoring to enable detailed visibility into user activities and device access while supporting compliance reporting and data-driven policy updates. By seamlessly integrating with access gateways and policy enforcement systems, this module ensures consistent policy application across resources. The enhanced visibility and centralized oversight provided by Falcon Next-Gen SIEM allow organizations to efficiently identify noncompliant or at-risk applications for decommissioning or exceptions while maintaining comprehensive system-wide activity tracking.
- **CrowdStrike Falcon Insight XDR** unifies monitoring and correlation of activities across endpoints, networks and cloud environments, enabling a comprehensive approach to security. Automated response workflows mitigate risks efficiently while supporting attribute-based decisions by integrating enriched data from various security domains. By delivering faster threat responses and consistent policy enforcement, XDR enables comprehensive resource authorization and efficient handling of noncompliant or at-risk applications for exception or decommissioning.
- **CrowdStrike Falcon Identity Protection** enforces strong access controls through MFA and integrates user behavior insights to refine policy enforcement decisions. By aligning identity and device authentication with access gateways, this module enhances the security of external-facing applications and services. These capabilities reduce the risk of unauthorized access, strengthen compliance with authentication policies and ensure that authorization processes are enriched with identity context information for precise, risk-based decisions.
- **Mapped Outcomes:**
 - **3.4.1-3.4.2 Access Control Decision, 3.4.3-3.4.4 Software-Defined Compute (SDC) Resource Authorization, 3.4.5-3.4.6 Enrich Attributes for Resource Authorization**
 - **Standardized Resource Authorization:** Centralizes visibility into resource activities and enables secure access control by integrating identity verification through Falcon Identity Protection and Falcon Next-Gen SIEM.
 - **Policy Enforcement Integration:** Falcon Insight XDR enables consistent enforcement of policies across all environments while Falcon Identity Protection aligns user authentication with access gateway requirements.
 - **Attribute-Based Access Control:** Provides enriched logs for data-driven attribute analysis with Falcon Next-Gen SIEM and integrates user and device attributes for precise authorization using Falcon Identity Protection and Falcon Insight XDR.
 - **Efficient Exception Management:** Streamlines the identification of applications for decommissioning or exception through Falcon Next-Gen SIEM and Falcon Insight XDR, ensuring consistent handling of noncompliant resources in accordance with organizational policy.

3.5 Continuous Monitoring and Ongoing Authorizations

- **CrowdStrike Falcon Cloud Security** addresses the need for control derivation, testing and monitoring by integrating CSPM, CWP and ASPM. CSPM ensures secure configurations and compliance by identifying and remediating misconfigurations and vulnerabilities, and CWP provides runtime protection for cloud workloads, safeguarding containers and virtual machines. ASPM manages application configurations, dependencies and compliance, enhancing the efficiency of deployment processes. Together, these capabilities enable comprehensive monitoring, streamlined authorization processes and alignment with organizational objectives to standardize security controls.
- **Mapped Outcomes:**
 - **3.5.1-3.5.2 Continuous Authorization to Operate (cATO)**
 - **Standardized Monitoring and Control:** Enables consistent monitoring by identifying and addressing deviations in cloud configurations through CSPM, protecting workloads with CWP, and managing configurations and dependencies with ASPM.
 - **Integration of Control Testing:** Supports security testing during development and deployment with ASPM. CSPM and CWP ensure controls are aligned with compliance and runtime protection as part of operational processes.
 - **Control Derivation and Resolution:** Streamlines the derivation and applicability of controls using CSPM and ASPM to maintain secure configurations and compliance requirements while CWP resolves deviations in runtime environments.
 - **Authorization Tracking and Insights:** Tracks compliance, control deviations and authorization statuses through dashboards, with analytics delivering actionable insights to inform decisions and ensure adherence to policies.

3.4 Data Pillar

Pillar Summary

The **DoD ZTA Data Pillar** focuses on securing data by implementing stringent access controls, governance mechanisms and comprehensive monitoring processes. Central to this effort is the alignment of DAAS policies with Zero Trust outcomes, ensuring that data access is managed based on the properties of users, devices and data itself. Software-defined storage (SDS) plays a critical role in scaling data access control, enabling the efficient management of permissions while maintaining operational agility. These systems are implemented in a phased, risk-based approach to ensure successful integration while reducing disruptions. Additionally, identity attributes are incorporated into access control policies, ensuring interoperability across DLP, DRM and SDS solutions while adhering to governance standards.

The Data Pillar also emphasizes protecting data integrity and confidentiality by continuously governing and monitoring its use. Governance mechanisms are established to define how data is accessed and shared, and monitoring tools are deployed to oversee data activity across critical and regulated repositories. Integration with the enterprise IdP ensures that identity attributes align with Zero Trust principles, facilitating secure and efficient data access. By combining governance, access control and monitoring, the Data Pillar ensures that data is consistently protected against unauthorized access, breaches and misuse. These capabilities are critical to the DoD's mission, providing a secure foundation for operations and enabling informed decision-making at all levels.

Challenges

- 1. Data Catalog Risk Alignment:** As stewards of mission-critical information, DoD data owners must identify, inventory and maintain an accurate record of all data within their purview, ensuring any changes to the data landscape are automatically detected and reflected in the catalog. Regular reviews are essential to uncover risks such as data loss, unauthorized access or malicious attacks that could compromise national security. By maintaining an up-to-date data catalog, DoD data owners enable proactive risk management, support Zero Trust objectives and uphold the integrity and availability of critical data assets.
- 2. DoD Enterprise Data Governance:** The DoD faces the challenge of implementing enterprise-wide data tagging and classification standards that support Zero Trust objectives while ensuring scalability through manual and automated processes. Establishing thorough governance practices is critical to securely controlling, accessing and sharing data across diverse organizations with varying missions and infrastructure. Achieving interoperability is complex, requiring effective integration of DRM overlays, protection mechanisms and SDS policies aligned with best practices. Overcoming these challenges demands a coordinated effort to enhance data security, maintain operational consistency and meet stringent cybersecurity and Zero Trust goals.

- 3. Data Labeling and Tagging:** DoD personnel must implement data labeling and tagging processes that comply with enterprise governance policies while ensuring scalability through automation. Granular data attributes are essential for attribute-driven access controls, enabling machine-enforceable policies, situational awareness and risk assessment. Establishing consistent tagging processes and automating labeling practices supports real-time decision-making and dynamic, risk-aware operations. Collaboration across organizations ensures that Zero Trust metadata and advanced functionality attributes are standardized and incorporated into tagging efforts. Unsupported data repositories require risk-based evaluations for decommissioning, and applying standardized tags to supported repositories ensures consistency, accuracy and alignment with DoD ZTA objectives.
 - 4. Data Monitoring and Sensing:** DoD personnel must capture active metadata to track data access, sharing and usage while adhering to enterprise cybersecurity standards. DLP and DRM enforcement points are monitored to detect and respond to threats, with critical and regulatory-protected data tracked using file and database monitoring tools integrated into security information and event management (SIEM) systems. Data outside the scope of DLP and DRM solutions, such as file shares and databases, is monitored for anomalous activity using alternative tools. Expanded monitoring and integration of additional data attributes enhance decision-making and support Zero Trust functionalities.
 - 5. Data Loss Prevention:** DoD personnel face the challenge of managing DLP enforcement points to align with enterprise cybersecurity standards while ensuring effective data protection. DLP solutions begin in a “monitor-only” mode to minimize business disruption and are later transitioned to a “prevent” mode using analytics and extended data tagging attributes. Collaboration with cyber functions ensures that observed data loss activity is addressed through attribution techniques that track data movement and invoke protection measures such as encryption and obfuscation. File and database monitoring tools are deployed to oversee critical and regulated data types, with analytics integrated into SIEM systems to enhance situational awareness. These efforts, combined with risk-based expansion and Zero Trust tagging, strengthen DLP effectiveness and support DoD ZTA compliance.
 - 6. Data Access Control:** DoD personnel face the challenge of ensuring appropriate data access based on user, device and data properties while maintaining compliance with Zero Trust principles. Governance mechanisms ensure that DAAS policies align with Zero Trust outcomes, and these mechanisms are supported by SDS solutions to scale and manage permissions effectively. SDS technologies are implemented in a phased, risk-based manner, integrating with DLP and DRM tools to enhance interoperability and data protections. Identity attributes required for Zero Trust target functionalities are incorporated through integration with the enterprise IdP. These efforts ensure a unified approach to data access control, improving security and operational efficiency across DoD organizations.
-

CrowdStrike Implementation Modules

- CrowdStrike Falcon® Data Protection
- CrowdStrike Falcon Next-Gen SIEM
- CrowdStrike Falcon Cloud Security

CrowdStrike Module Descriptions

CrowdStrike Falcon Data Protection provides comprehensive visibility and control over data movement across endpoints, portable electronics (USB) and cloud applications, ensuring compliance with granular access policies. By integrating data classification and policy enforcement, it prevents unauthorized access and data exfiltration. Continuous monitoring supports secure handling of sensitive information throughout its lifecycle. The solution further prevents data leakage in web-based applications, safeguarding information across diverse environments.

CrowdStrike Falcon Next-Gen SIEM delivers enhanced visibility and streamlined threat detection across diverse environments, integrating data from endpoints, cloud workloads, identities and other sources. Its scalable architecture and efficient data management enable organizations to centralize security operations without the overhead of traditional systems. By providing comprehensive log analysis and actionable insights, Falcon Next-Gen SIEM enables incident response and continuous monitoring. The solution's automated workflows and seamless integration with existing infrastructures enhance operational efficiency and ensure consistent enforcement of security policies. Falcon Next-Gen SIEM equips organizations to respond to threats with speed and precision while maintaining alignment with modern security principles.

CrowdStrike Falcon Cloud Security enables continuous protection and monitoring of cloud and hybrid environments by delivering advanced discovery and classification capabilities. Falcon Cloud Security identifies sensitive data and ensures it is tagged, cataloged and monitored to provide visibility and secure dynamic cloud workloads. The solution enables granular access controls and aligns data policies with established security standards to support compliance. With seamless integration into diverse infrastructures, Falcon Cloud Security allows organizations to detect anomalies, prevent unauthorized access and enable data encryption in transit and at rest. This unified approach helps secure critical cloud resources while enhancing operational efficiency.

Recommendations and Activity Outcomes

4.1 Data Catalog Risk Assessment

- **CrowdStrike Falcon Cloud Security** addresses key requirements for data identification, classification, governance and risk assessment. Leveraging its capabilities for monitoring, securing and managing data environments, Falcon Cloud Security enables comprehensive visibility and governance over data types, usage and associated risks. This provides alignment with enterprise oversight policies, promotes secure and compliant operations, and strengthens the organization's ability to identify, mitigate and manage risks to data availability, integrity and confidentiality.
-

- **CrowdStrike Falcon Data Protection** offers comprehensive capabilities for identifying, classifying and safeguarding organizational data. It ensures that an enterprise data catalog is built and maintained, enabling centralized visibility into data types, metadata and governance policies. This solution promotes proactive risk identification, governance oversight and secure configurations, ensuring compliance with enterprise policies and mitigating risks associated with data exposure, integrity loss or unauthorized access. These capabilities strengthen organizational resilience and ensure seamless alignment with data governance objectives.
- **Mapped Outcomes:**
 - **4.1.1 Data Catalog Risk Alignment**
 - **Data Identification and Inventory Management:** Enables the creation of a comprehensive enterprise-wide data catalog that inventories all data types across applications and services, categorizing them based on classification levels. This facilitates governance, oversight and alignment with enterprise policies by linking metadata, governance policies and data usage for reference.
 - **Risk Assessment and Categorization:** Empowers data owners to assess risks related to data exposure, loss of integrity or availability while maintaining detailed metadata about data types and their associated risks. This promotes a comprehensive strategy for identifying and mitigating vulnerabilities to ensure robust risk management.
 - **Governance Enablement and Oversight:** Provides centralized visibility into the data catalog, allowing enterprise governing bodies to effectively oversee risks, compliance and governance policies. This ensures alignment with organizational objectives and promotes accurate decision-making regarding data use and security.
 - **Standardization of Security and Compliance:** Implements consistent controls and configurations across all applications and services, ensuring alignment with classification levels and enterprise policies. This supports a unified approach to data security and compliance requirements, strengthening organizational security postures.
 - **Proactive Risk Mitigation and Insights:** Leverages dashboards and analytics to deliver actionable insights into data-related risks, enabling real-time visibility and informed decision-making. These tools empower data owners and governing bodies to take swift action to mitigate vulnerabilities and enhance organizational resilience.
 - **Enhanced Governance Policies and Catalog Updates:** Ensures regular updates to the data catalog, aligning data types for all applications and services with enterprise governance requirements. This promotes accuracy, compliance and an actionable view of the data environment.

4.2 DoD Enterprise Data Governance

- **CrowdStrike Falcon Data Protection** equips organizations with the tools and capabilities necessary to meet enterprise data governance requirements by identifying, classifying and safeguarding data across environments. It supports compliance with enterprise-wide policies through centralized visibility, consistent protection mechanisms and proactive governance oversight. By mitigating risks related to data exposure, integrity loss and unauthorized access, Falcon Data Protection enhances organizational resilience. Its ability to streamline compliance with standardized controls and enforce governance policies strengthens data integrity and confidentiality, ensuring alignment with enterprise data protection objectives.
- **Mapped Outcomes:**
 - **4.2.1 Define Data Tagging Standards, 4.2.2 Interoperability Standards, 4.2.3 Develop Software-Defined Storage Policy**
 - **Data Tagging and Classification Standards:** Supports the establishment of data tagging standards by facilitating the identification and classification of data objects based on enterprise and industry best practices. Automated tagging mechanisms ensure future scalability and government alignment.
 - **Data Governance Policy Enforcement:** Enables the definition and enforcement of, access control and data sharing. These policies are based on cybersecurity inputs, ensuring effective control at the data object level while maintaining consistency across the enterprise.
 - **Interoperability and Secure Data Sharing:** Facilitates interoperability standards through the integration of data rights management overlays and protection mechanisms, ensuring secure and standardized data sharing across components.
 - **Software-Defined Storage Policy Enablement:** Assists in the development and refinement of policies for SDS, including minimum attribution requirements that align with enterprise standards. This supports the evaluation and adoption of advanced storage strategies based on industry best practices.
 - **Monitoring and Compliance:** Provides visibility into compliance with data governance policies through dashboards and analytics. These tools help track data governance implementation and ensure that components align with enterprise-defined patterns and standards.

4.3 Data Labeling and Tagging

- **CrowdStrike Falcon Data Protection** offers a unified platform that combines data protection and endpoint security, facilitating compliance with enterprise data governance policies. This approach supports the creation of comprehensive data catalogs, aiding in the identification and mitigation of potential risks related to data loss or unauthorized access.
-

- **Mapped Outcomes:**
 - **4.3.1 Implement Data Tagging and Classification Tools, 4.3.4-4.3.5 Automated Data Tagging and Support**
 - **Data Labeling and Tagging Compliance:** Provides tools for data owners to define custom data classifications and maintain alignment with enterprise governance policies.
 - **Automation for Scalability and Accuracy:** Streamlines data protection processes using unified tools, enabling automation to improve scalability and accuracy.
 - **Comprehensive Data Cataloging:** Supports the creation and maintenance of an enterprise data catalog by providing deep, real-time visibility into data movement, governance policies and usage metadata.
 - **Risk Assessment and Mitigation:** Enhances monitoring capabilities to identify risks related to data loss or unauthorized access, supporting proactive mitigation strategies.

4.4 Data Monitoring and Sensing

- **CrowdStrike Falcon Data Protection** enables organizations to achieve comprehensive visibility and control over sensitive data assets through advanced monitoring, logging and enforcement. By integrating file and database monitoring with standardized logging schemas, Falcon Data Protection supports effective data governance and compliance. The solution enhances detection and response capabilities by delivering analytics to centralized systems, fostering collaboration between data management and cybersecurity operations. This approach ensures that sensitive data, such as regulatory-protected data and data designated as critical, is consistently monitored, managed and safeguarded across repositories, endpoints and services.
- **CrowdStrike Falcon Next-Gen SIEM** delivers centralized, scalable monitoring and analytics to provide comprehensive visibility into sensitive data activity, enforce logging standards and unify data oversight across environments. The solution ensures that business rules for data usage are applied consistently, logs from critical data repositories are integrated and regulated data is actively monitored for anomalies. By aggregating and correlating insights into a single pane of glass, this solution supports seamless collaboration between data management and security teams, enabling precise detection, incident response and compliance reporting.
- **CrowdStrike Falcon Cloud Security** provides data monitoring and protection by integrating capabilities that enforce consistent logging, monitor critical and regulated data, and enhance visibility across data repositories. By unifying file, database and application activity monitoring, the solution supports compliance with business rules for data access, sharing and transformation while delivering insights into anomalous and unauthorized activities. The solution consolidates data monitoring across environments, enabling centralized visibility and seamless integration with enterprise systems for incident response and governance.

- **Mapped Outcomes:**
 - **4.4.1 DLP Enforcement Point Logging and Analysis, 4.4.2 DRM Enforcement Point Logging and Analysis, 4.4.3-4.4.4 File Activity Monitoring, 4.4.5 Database Activity Monitoring, 4.4.6 Comprehensive Data Activity Monitoring**
 - **Standardized Logging Enforcement:** Ensures a consistent and unified logging schema at component levels to monitor and manage DLP and DRM enforcement points. Enhances visibility into data activity, supports access control and helps ensure compliance.
 - **Critical and Regulated Data Monitoring:** Actively identifies and monitors sensitive data and files — e.g., Controlled Unclassified Information (CUI), personally identifiable information (PII) and protected health information (PHI) — across repositories, applications and services. Integrates logs and insights into centralized systems, such as SIEM solutions, for comprehensive oversight and real-time analysis.
 - **Database Activity Monitoring and Integration:** Monitors regulated databases containing sensitive data types, integrating analytics into enterprise security tools like SIEM solutions, a policy decision point (PDP) and dynamic access controls. Supports real-time decision-making, strengthens data governance and enhances response mechanisms.
 - **Unified Data Monitoring:** Provides a consistent and holistic view of sensitive data activity across diverse repositories, applications and services. Employs integrated monitoring mechanisms and centralized systems to support data governance.
 - **Anomaly Detection and Incident Response:** Monitors data beyond the scope of traditional DLP and DRM solutions, such as unmanaged databases and file shares. Identifies unauthorized or malicious activity and facilitates rapid incident containment and response.
 - **Cross-System Analytics Integration:** Aggregates and correlates data monitoring insights into centralized analytics systems like SIEM solutions or a PDP. Aligns operational insights with compliance and security objectives, enabling informed decision-making and seamless coordination.

4.6 Data Loss Prevention

- **CrowdStrike Falcon Data Protection** ensures comprehensive DLP by integrating automated tagging, enforcement mechanisms and analytics to monitor, protect and enforce data security measures effectively. The solution strengthens data privacy and protection by incorporating attributes such as data origin, movement across boundaries and applied protection measures like encryption or obfuscation. By aligning DLP capabilities with cybersecurity operations and transitioning from monitoring to prevention mode, organizations can proactively mitigate data loss while minimizing business disruptions.
-

- **Mapped Outcomes:**
 - **4.6.1 Implement Enforcement Points, 4.6.2-4.6.4 DLP Enforcement with Data Tags and Analytics**
 - **Formal Collaboration with Cybersecurity:** Establishes processes to share data loss activity observations with cybersecurity teams, enabling cooperative enforcement and enhanced response capabilities.
 - **Transition from Monitor to Prevention Mode:** Supports the phased approach of deploying DLP solutions, which are initially in “monitor-only” mode to reduce operational impacts, and then transitioning them to “prevention” mode using advanced analytics.
 - **Indicator Identification and Enforcement:** Identifies and integrates key indicators to support enforcement at control points, enhancing visibility and enforcement capabilities across data flows.
 - **Automated Data Tagging Integration:** Implements automated tagging techniques to identify and fill gaps in enforcement points, ensuring comprehensive DLP coverage and attribute integration.
 - **Extended Data Tag Attributes:** Incorporates extended data tag attributes at enforcement points to strengthen prevention measures, supporting dynamic protection of sensitive data.
 - **Deployment of Approved DLP Tools:** Deploys and integrates DLP solutions with tagged data attributes at identified enforcement points, ensuring seamless operation and alignment with organizational data security policies.

4.7 Data Access Control

- **CrowdStrike Falcon Cloud Security** provides a robust framework for implementing data access control by integrating governance policies, attribute-based access mechanisms and infrastructure-level protections. By aligning data access control with enterprise and component-level policies, the solution ensures unauthorized entities are prevented from accessing sensitive data. It facilitates phased, automated implementation of attribute-based policies, integrates seamlessly with enterprise IdPs and supports interoperability with DLP, DRM and SDS infrastructures. The solution enables organizations to protect data across all applications, helping to ensure policy compliance and enhanced access control capabilities.
 - **CrowdStrike Falcon Data Protection** strengthens data access control by implementing governance policies, automated attribute-based access mechanisms and seamless integration with IdPs and underlying security solutions. The solution enables organizations to ensure that unauthorized entities and devices are prevented from accessing sensitive data by leveraging fine-grained access controls. Its capability to integrate with DLP, DRM and SDS infrastructures ensures comprehensive protection and interoperability across security tools. Organizations can adopt a phased implementation approach to ensure effective policy deployment and measurable results.
-

– **Mapped Outcomes:**

- **4.7.1-4.7.3 Integrate DAAS Access with SDS Policy, 4.7.4-4.7.5 Integrate Solution(s) and Policy with Enterprise IdP, 4.7.7 Implement SDS Tool and/or integrate with DRM Tool**
 - **Enterprise and Component Policy Integration:** Develops, supports and enforces DAAS access policies aligned with enterprise and component governance mechanisms, ensuring consistent and effective access control measures.
 - **Automated Attribute-Based Policies:** Implements fine-grained, attribute-based DAAS policies using automated mechanisms, enabling efficient, scalable and consistent control over data access across applications and services.
 - **Phased Risk-Based Implementation:** Adopts a phased approach to integrating SDS technology and functionalities with DAAS policies, ensuring outcomes are measurable and adjustments can be made to optimize effectiveness based on risk and performance.
 - **Identity Provider Integration:** Ensures seamless integration of SDS functionalities with enterprise IdPs (e.g., through APIs, LDAP, SAML) to support fine-grained, attribute-based access control for all users, devices and NPEs.
 - **Interoperability Across Security Tools:** Configures and integrates SDS infrastructure with existing DLP, DRM and data protection solutions, facilitating cohesive protection, monitoring and response across systems.
 - **Unauthorized Access Prevention:** Establishes strong access control mechanisms based on data, user, device and NPE properties, ensuring that unauthorized entities and devices cannot access sensitive data.

3.5 Network and Environment Pillar

Pillar Summary

The **DoD ZTA Network and Environment Pillar** focuses on securing network infrastructure through segmentation, automation and centralized management. Network flows are segmented into control, management and data planes using software-defined networking (SDN) infrastructure and technologies like logical zones, microsegmentation and macrosegmentation. These measures restrict lateral movement, enforce attribute and role-based access, and protect data in transit. Policies are enforced through programmable APIs, decision points and segmentation gateways, allowing real-time access decisions and enabling consistent policy implementation across the enterprise.

DoD organizations continuously map and monitor network traffic to reconcile data flows, validate access attempts and safeguard resources. Automated SDN solutions enable centralized control, separation of network planes and integration with cross-pillar analytics for informed access decisions. Host-level process microsegmentation is applied where possible, and virtual environments implement automation to manage policy changes efficiently. These efforts ensure that network assets are protected against unauthorized access, vulnerabilities and lateral movement, aligning with the core principles of Zero Trust.

Challenges

- 1. Data Flow Mapping:** DoD organizations face the challenge of reconciling data flows to ensure authorized access and protection of network and DAAS resources by gathering, mapping and visualizing traffic patterns. This effort includes tagging programmatic access, such as APIs, to maintain oversight and control. To address this, granular network access rules and policies are developed collaboratively with DoD Components, ensuring alignment with future supportability requirements. These policies are implemented in existing network technologies, like next-generation firewalls and intrusion prevention systems, leveraging data tagging and classification standards to develop API filters and formalize decision points within the SDN architecture.
- 2. Software-Defined Networking:** DoD organizations must define API decision points and implement programmable SDN infrastructure to separate the control and data planes for centralized management and improved security. Necessary APIs and programmatic interfaces are developed to automate decision-making at authentication decision points, application delivery proxies and segmentation gateways. SDN infrastructure is deployed with capabilities like segmentation and centralized logging into SIEM solutions for monitoring, while basic segmentation methods like IPv6/virtual local area networks (VLANs) are used to organize traffic across planes. Advanced analytics and cross-pillar data sources, such as user and entity activity monitoring, enable real-time, machine learning-assisted access decisions and consistent policy enforcement across the enterprise.

3. **Macrosegmentation:** Establishing network boundaries and securing networked assets against unauthorized access is a key challenge for DoD organizations. Macrosegmentation strategies focus on validating users, devices or NPEs before granting access to remote resources. Service-based architectures are deployed to restrict lateral movement between public and private components, with proxy and enforcement checks integrated based on device attributes and behavior. Logical network zones are established to support mission- and organization-specific macrosegmentation efforts, further reducing lateral movement and enhancing control within the SDN environment.
4. **Microsegmentation:** Defining and documenting network segmentation based on identity and application access is critical for virtualized and cloud environments in DoD networks. Microsegmentation is implemented within SDN infrastructure to segment service components like the web, application and database layers, and automation is used to enforce policy changes through programmatic APIs. Host-level process segmentation further enhances security by limiting access based on real-time decisions and predefined policies. To protect data in transit, policies are informed by detailed data flow mapping and monitoring, addressing use cases such as coalition information sharing and protection across architectural components.

CrowdStrike Implementation Modules

- CrowdStrike Falcon Identity Protection
- CrowdStrike Falcon Insight XDR
- CrowdStrike Falcon Discover/Falcon Exposure Management
- CrowdStrike Falcon Next-Gen SIEM
- CrowdStrike Falcon Firewall Management

CrowdStrike Module Descriptions

CrowdStrike Falcon Identity Protection enhances organizational security by enabling real-time access enforcement, risk-based authentication and visibility into identity-related vulnerabilities across environments. This solution supports granular access controls and segmentation strategies by integrating seamlessly with existing infrastructures to validate user and device attributes, ensuring secure access to critical resources. It empowers organizations to secure network resources through identity-based policies, dynamic controls and continuous monitoring to mitigate risk and enhance operational security.

CrowdStrike Falcon Insight XDR provides unified visibility and response capabilities across endpoints, networks and applications, enabling organizations to enforce granular access controls and optimize data flow management. By integrating telemetry from multiple sources, it supports the implementation of policies for access validation, segmentation of traffic flows and centralized monitoring of the control and data planes. The solution seamlessly integrates with existing infrastructures to deliver real-time insights and enforce standardized policies, such as API-driven segmentation and secure data flow mapping. Falcon Insight XDR empowers organizations to enhance security through continuous monitoring, dynamic policy updates and comprehensive network resource protection.

CrowdStrike Falcon Discover/Falcon Exposure Management provide comprehensive visibility into assets and potential vulnerabilities across an organization's infrastructure. By identifying and mapping data flows, these tools enable organizations to reconcile network traffic patterns and enforce appropriate access controls. The solution supports the creation of segmentation strategies, ensuring resources are secured through defined boundaries and dynamic policy updates. Seamless integration with existing infrastructures ensures operational efficiency while enabling real-time access decisions and protections. Falcon Discover/Falcon Exposure Management empowers organizations to manage risk effectively and maintain consistent enforcement of security principles across their environments.

CrowdStrike Falcon Next-Gen SIEM provides enhanced visibility and streamlined threat detection by centralizing data collection across diverse sources, including endpoints, cloud workloads and networks. Its scalable architecture enables efficient management of logs and events, facilitating real-time analysis and detection of anomalous activities. The solution supports granular policy enforcement and segmentation strategies by integrating data flows and access control mechanisms with existing infrastructures. Automated workflows and advanced log correlation improve incident response times and operational efficiency. Falcon Next-Gen SIEM ensures continuous monitoring and consistent enforcement of security policies, empowering organizations to secure their environments effectively.

CrowdStrike Falcon Firewall Management provides centralized control and visibility for host-based firewall policies, enabling organizations to enforce consistent security configurations across their environments. Built on a scalable, cloud-native architecture, the solution simplifies firewall rule management, automates policy updates, and ensures alignment with security standards. Falcon Firewall Management helps restrict unauthorized access, prevent lateral movement, and safeguard sensitive data by monitoring and managing network traffic at the endpoint level. By integrating with existing security infrastructure, the solution supports comprehensive threat prevention and strengthens an organization's overall security posture.

Recommendations and Activity Outcomes

5.2 Software-Defined Networking

- **CrowdStrike Falcon Identity Protection** delivers robust solutions aligned with SDN requirements by enabling automation, segmentation and integration across network environments. It supports API-driven automation for authentication and segmentation, ensures visibility and control through centralized monitoring and integrates seamlessly with network analytics tools. These capabilities facilitate efficient access control, enhance network performance and maintain consistent policy enforcement. Furthermore, by leveraging dynamic decision-making mechanisms and real-time monitoring, organizations can ensure their SDN infrastructure aligns with standardized policies and operational objectives.
- **CrowdStrike Falcon Insight XDR** delivers a comprehensive approach to addressing SDN requirements by providing enhanced visibility, real-time monitoring and actionable insights. It enables seamless integration of segmentation and authentication capabilities with centralized logging and analytics to ensure network security and performance. By automating key processes and leveraging standardized APIs, organizations can maintain consistent policy enforcement and streamline access decisions. These features optimize SDN infrastructure, enhance situational awareness and align with operational and security objectives.

- **CrowdStrike Falcon Next-Gen SIEM** enhances SDN capabilities by delivering comprehensive visibility, centralized logging and actionable analytics to streamline monitoring and automation tasks. By integrating standardized APIs, it supports seamless implementation of key SDN components, such as authentication decision points, application delivery control proxies and segmentation gateways. Through automated reporting, policy enforcement and real-time insights, organizations can optimize network performance, ensure segmentation and maintain alignment with operational and security standards.
- **Mapped Outcomes:**
 - **5.2.1 Define SDN APIs, 5.2.2 Implement SDN Infrastructure, 5.2.3 Segment Flows into Control, Management and Data Planes, 5.2.4 Network Asset Discovery and Optimization, 5.2.5 Real-Time Access Decisions**
 - **Standardized API Implementation and Integration:** Supports the integration and automation of authentication decision points, application delivery control proxies and segmentation gateways through machine-readable APIs and standardized schemas, ensuring consistent execution of tasks and centralized logging in unified repositories, such as SIEM and security orchestration, automation and response (SOAR) solutions.
 - **Segmentation and Network Flow Management:** Implements IPv6 and VLAN-based logical and physical segmentation to organize traffic across the control, management and data planes, automating NetOps reporting for centralized monitoring, operational decision-making and secure transport flow segmentation.
 - **Access Control and Risk-Based Decision-Making:** Enables real-time, risk-based access decisions using cross-functional data sources like user and entity activity monitoring, ensuring unified policy enforcement, consistent security configurations and integrated monitoring with real-time analytics.
 - **Integrated Monitoring, Analytics and Reporting:** Centralizes log collection, analysis and reporting for actionable insights, integrating with SIEM/SOAR platforms to enhance threat detection, ensure policy compliance and provide real-time policy access decisions.
 - **Optimization and Performance Controls:** Improves network performance through SDN analytics, supports technical refresh cycles with up-to-date security measures and enforces consistent security policies across the enterprise for optimal operations.
 - **Secure Data Transmission and Connectivity:** Protects data in transit through end-to-end transport network segmentation and ensures secure coalition information sharing with high connectivity standards.

5.3 Macrosegmentation

- **CrowdStrike Falcon Identity Protection** enables the implementation of macrosegmentation by enforcing logical network zones and restricting lateral movement based on device attributes, location and behavior. It supports centralized monitoring, proxy enforcement checks and compliance tracking to ensure secure configurations and alignment with organizational objectives. These capabilities streamline access policies, enhance visibility and mitigate risks associated with lateral movement while helping organizations maintain compliance with mission-critical requirements.
- **CrowdStrike Falcon Insight XDR and CrowdStrike Falcon® Firewall Management** facilitate the implementation of macrosegmentation by enabling continuous monitoring, enforcing logical network zones and restricting lateral movement through device attributes, location and behavior-based access control. They integrate proxy enforcement checks and dynamic security policies while delivering real-time visibility into network activities and compliance status. These capabilities ensure secure configurations, improve firewall and access policy management, and align with operational objectives to reduce risks and streamline network segmentation.
- **Mapped Outcomes:**
 - **5.3.1 Macrosegmentation, 5.3.2 Mission-Based Macrosegmentation**
 - **Implementation and Enforcement of Logical Macrosegmentation Zones:** Establishes logical network zones to restrict lateral movement between public and private architecture components, integrating proxy and enforcement checks for device attributes, location and traffic patterns to ensure compliance with lifecycle, policy and operational standards.
 - **Attribute-Based Access and Policy Enforcement:** Enforces access control through dynamic evaluation of device behavior, traffic patterns and contextual attributes and configures application-specific security stacks to refine firewall rules and restrict unauthorized movement.
 - **Comprehensive Monitoring and Compliance Validation:** Tracks compliance deviations and monitors network flows for alignment with access policies and organizational standards, centralizing monitoring and reporting to validate device behavior and provide actionable insights through dashboards and analytics.
 - **Integration of Proxy and Security Principles:** Integrates proxy checks with SDN solutions to dynamically analyze activities and enforce security configurations while continuously monitoring and adjusting controls to align with compliance requirements and operational goals.

5.4 Microsegmentation

- **CrowdStrike Falcon Identity Protection** supports microsegmentation by enabling granular access control, host-level isolation and policy-driven network segmentation to protect sensitive processes and data flows. It integrates dynamic decision-making capabilities with real-time monitoring to ensure compliance with access policies and security standards. By segmenting services and processes at the host and network levels and incorporating API-based policy controls, organizations can enhance their security posture, streamline operations and protect data in transit across architectural components.
- **CrowdStrike Falcon Insight XDR and CrowdStrike Falcon Firewall Management** support microsegmentation by enforcing granular controls at the workload and device levels, restricting lateral movement through dynamic policies based on attributes such as device behavior, location and data sensitivity. By providing comprehensive monitoring, proxy enforcement checks and streamlined configuration management, they ensure secure workload isolation and compliance with access and operational policies. These features enhance visibility, simplify policy enforcement and reduce security risks across segmented environments.
- **CrowdStrike Falcon Next-Gen SIEM** facilitates the implementation of microsegmentation by offering detailed visibility, centralized monitoring and real-time policy enforcement across segmented environments. Its capabilities enable granular access control, host- and process-level isolation, and API-driven automation for policy adjustments, ensuring compliance with operational and security standards. By integrating with SDN infrastructures, it provides actionable insights for protecting data in transit, maintaining segmentation integrity and supporting dynamic policy deployments.
- **Mapped Outcomes:**
 - **5.4.1 Implement Microsegmentation, 5.4.2 Application and Device Microsegmentation, 5.4.3 Process Microsegmentation, 5.4.4 Protect Data in Transit**
 - **Granular Workload and Process Segmentation:** Implements fine-grained microsegmentation at the host, container and process levels to isolate workloads and critical services such as web, application and database components. Dynamically enforces segmentation policies to restrict lateral movement based on security requirements, device attributes, data sensitivity and contextual parameters such as client or tenant traffic patterns.
 - **Integration of Proxy and Enforcement Checks:** Establishes proxy and enforcement checks for device attributes, behavior and access flows to uphold compliance, lifecycle and policy principles. Activities are continuously evaluated to refine security policies, enforce access restrictions and ensure alignment with organizational standards.

- **Dynamic Policy Management and Automation:** Leverages application-specific security stacks to configure firewalls, automate policy changes and enforce microsegmentation rules across diverse workloads. API-driven decision points and distributed next-generation firewalls or endpoint agents in virtual hosting environments ensure consistent policy enforcement and operational compliance.
- **Comprehensive Monitoring and Policy Compliance:** Centralizes monitoring and reporting to track compliance deviations and validate segmentation policies through actionable dashboards and analytics. Logs and monitoring outputs are integrated into analytics systems for real-time access decisions, continuous improvement and alignment with organizational security standards.
- **Role- and Attribute-Based Access Control:** Assigns role-, attribute- and condition-based access controls to users and devices, restricting privileged access on a per-identity basis. Logical network zones and policy-based controls ensure secure resource utilization while aligning with access requirements.
- **Data Protection Across Architectural Components:** Mandates protection of data in transit during coalition information sharing and across system boundaries, ensuring security across segmented environments. Policies safeguard sensitive data flows and integrate protection mechanisms throughout architectural components to maintain segmentation integrity.

3.6 Automation and Orchestration Pillar

Pillar Summary

The **DoD ZTA Automation and Orchestration Pillar** focuses on streamlining security operations through automation, orchestration and enhanced policy enforcement. DoD organizations collect and document rule-based policies to orchestrate actions across the security stack, enabling effective automation of DAAS access and security workflows. SOAR tools are deployed to integrate workflows, enrich threat intelligence and trigger automated playbooks for incident response. Repetitive tasks, such as data enrichment and security controls, are addressed using robotic process automation (RPA) and predefined workflows, improving efficiency and consistency across security operations.

This pillar emphasizes the establishment of programmatic standards, such as APIs, to enable consistent automation and orchestration across the enterprise. Policies and rulesets are enforced using PDPs and policy enforcement points (PEPs) to monitor, enable and terminate connections between users, devices and DAAS resources. Incident response is enhanced with enrichment from internal and external threat intelligence sources, ensuring workflows adapt to evolving threats. SOCs are tasked with deploying, operating and maintaining automated monitoring and response capabilities, providing visibility and tactical implementation across the enterprise. This integrated approach ensures that automation and orchestration align with Zero Trust principles to strengthen the DoD's security posture.

Challenges

1. **PDP and Policy Orchestration:** DoD organizations maintain a consistent and comprehensive device inventory while aligning device compliance with enterprise security profiles across pillars. Devices accessing mission-critical services adhere to established security policies, with iterative updates and dynamic integration of access profiles. This ensures secure, risk-based access decisions while minimizing disruption to mission-critical operations.
 2. **Critical Process Automation:** DoD organizations automate asset, vulnerability and patch management processes to improve efficiency and compliance. Transitioning manual tasks to automated workflows enables real-time visibility into device posture, streamlines patch deployment and accelerates vulnerability resolution, supporting both target and advanced DoD ZTA requirements.
 3. **Machine Learning:** DoD organizations use machine learning models to analyze device behavior and enhance compliance verification. Tagged and classified data help establish baselines, enabling dynamic detection of noncompliance and vulnerabilities. This supports more accurate risk assessments and strengthens anomaly detection capabilities.
 4. **Artificial Intelligence:** DoD organizations deploy AI to automate risk-based decisions and proactively mitigate threats. AI enhances device posture assessment by analyzing historical patterns, anticipating risks and addressing vulnerabilities before they escalate, freeing up human resources for other critical tasks.
 5. **SOAR:** DoD organizations integrate SOAR solutions to automate device detection, response and anomaly management. By embedding playbooks into workflows, organizations ensure efficient device authorization, inspection and rapid response to security events, strengthening compliance with Zero Trust principles.
-

6. **API Standardization:** DoD organizations standardize APIs to ensure interoperability among automation and orchestration tools. Consistent protocols enable seamless integration, supporting data exchange and real-time coordination across systems for device compliance and authorization processes.
7. **SOC and Incident Response:** DoD organizations automate incident response workflows to improve speed and effectiveness in addressing device security incidents. Integrating threat intelligence and automating manual processes reduces response times and enhances the organization's ability to manage unauthorized access or anomalies, aligning with Zero Trust standards.

CrowdStrike Implementation Modules

- CrowdStrike Falcon Cloud Security
- CrowdStrike Falcon Next-Gen SIEM
- CrowdStrike Falcon Insight XDR
- CrowdStrike Falcon Identity Protection
- CrowdStrike Falcon Exposure Management
- CrowdStrike Falcon Exposure Management/Falcon Discover/Falcon Spotlight
- CrowdStrike Falcon® for XIoT
- CrowdStrike Falcon for IT
- CrowdStrike Falcon for Mobile
- CrowdStrike Falcon Prevent (NGAV)
- CrowdStrike Falcon Firewall Management
- CrowdStrike Falcon® Device Control
- CrowdStrike Falcon FileVantage
- CrowdStrike Falcon Fusion SOAR

CrowdStrike Module Descriptions

CrowdStrike Falcon Cloud Security delivers comprehensive protection for cloud workloads and containers, providing continuous visibility and real-time threat detection across multi-cloud environments. Built on a scalable, cloud-native platform, it automates security operations by integrating seamlessly with DevOps workflows to enforce consistent policies and streamline vulnerability management. Falcon Cloud Security enables security teams to identify misconfigurations, secure workloads, and respond to threats efficiently, ensuring that cloud infrastructures remain resilient against evolving risks while maintaining compliance with security standards.

CrowdStrike Falcon Next-Gen SIEM unifies security data from across an organization to streamline threat detection, investigation and response. With native SOAR functionalities, it automates critical workflows, embeds playbooks and accelerates incident response. The solution ensures seamless interoperability through API standardization and supports automated categorization of tasks, enabling organizations to transition manual processes to automated workflows. Falcon Next-Gen SIEM enriches threat intelligence with actionable insights, improving operational efficiency and response times. Its ability to integrate with existing infrastructures supports DoD objectives to enhance asset management, patch deployment and security incident workflows, ensuring consistent enforcement of documented policies while maintaining operational efficiency.

CrowdStrike Falcon Insight XDR provides advanced capabilities to detect, investigate and respond to threats across an organization's environment, ensuring comprehensive visibility and efficient security operations. By integrating with existing infrastructures, Falcon Insight XDR supports streamlined workflows and real-time coordination through standardized APIs and programmatic interfaces. The platform incorporates SOAR functionalities, enabling the automation of repetitive tasks, the integration of enriched threat intelligence and the use of automated playbooks for incident response. These capabilities align with the Automation and Orchestration Pillar's emphasis on automating security processes, improving response workflows and maintaining operational consistency. Falcon Insight XDR empowers organizations to enforce policies effectively, optimize incident management and enhance their overall security posture.

CrowdStrike Falcon Identity Protection enhances security by providing continuous monitoring and real-time detection of identity-based threats across an organization's infrastructure. The solution supports automation and orchestration of workflows, integrating seamlessly with existing systems through standardized APIs to ensure consistent data exchange and coordination. Falcon Identity Protection addresses critical security challenges by automating repetitive tasks, enriching threat intelligence and embedding playbooks for rapid response to identity threats. Its ability to streamline workflows and enforce access policies aligns with the Automation and Orchestration Pillar's objectives of enhancing policy enforcement, automating processes and improving incident response. By centralizing identity protection efforts and ensuring real-time threat detection, Falcon Identity Protection empowers organizations to maintain a robust and efficient security posture.

CrowdStrike Falcon Exposure Management/Falcon Discover/Falcon Spotlight provides comprehensive visibility into an organization's security posture, enabling teams to identify, prioritize and remediate vulnerabilities across their IT environment. Built on a cloud-native platform, the solution continuously monitors for risks, misconfigurations and potential attack paths while automating critical workflows such as asset identification, vulnerability prioritization and remediation efforts. It integrates seamlessly with existing workflows and infrastructures through standardized APIs, enabling data exchange, policy enforcement and orchestration across tools. By embedding playbooks, leveraging automation capabilities and enriching threat intelligence, the solution accelerates incident resolution, ensures real-time alignment with security policies and streamlines remediation efforts. Delivering actionable insights and automated risk prioritization, it empowers organizations to strengthen defenses, reduce exposure to evolving threats and enhance efficiency, consistency and compliance in managing security gaps.

CrowdStrike Falcon for XIoT provides real-time visibility and protection for extended internet of things (XIoT) devices, enabling organizations to secure unmanaged and mission-critical connected assets. Built on a cloud-native platform, the solution continuously monitors device activity to detect vulnerabilities, misconfigurations and potential attack vectors. By integrating seamlessly with existing workflows, Falcon for XIoT enforces security policies, automates risk mitigation and helps ensure compliance across diverse IoT environments. This comprehensive approach helps organizations safeguard sensitive systems and reduce exposure to evolving threats within the XIoT ecosystem.

CrowdStrike Falcon for IT offers comprehensive asset visibility and management across endpoints, servers and cloud workloads, enabling organizations to query their entire IT estate and receive prompt, accurate responses. This capability facilitates streamlined fleet management, compliance, forensic investigations and performance monitoring through a single, lightweight agent. By automating complex use cases across security and IT, Falcon for IT enhances operational efficiency and supports the enforcement of security policies. Falcon for IT's integration capabilities support the establishment of PDPs and PEPs to manage resource access and enforce security policies. Overall, Falcon for IT provides a unified solution that enhances automation, orchestration and policy enforcement in IT and security operations.

CrowdStrike Falcon for Mobile delivers advanced protection for iOS and Android devices, offering real-time visibility and detection of threats targeting mobile endpoints. Built on a cloud-native platform, it continuously monitors for vulnerabilities, unauthorized access, and malicious activity, ensuring mobile devices remain secure and compliant with organizational policies. Falcon for Mobile integrates seamlessly with security workflows, enabling automated responses and consistent enforcement of policies across the mobile environment. By providing actionable insights and robust protection, the solution helps organizations safeguard sensitive data and maintain a strong security posture for mobile endpoints.

CrowdStrike Falcon Prevent (NGAV) delivers comprehensive next-generation antivirus protection, combining real-time detection and prevention of malware and fileless attacks with continuous monitoring of endpoint activity. Built on a cloud-native platform, it leverages behavioral analysis to block sophisticated threats while enforcing security policies across devices. Falcon Prevent integrates seamlessly with existing security workflows, enabling automated responses and consistent policy application. By providing detailed visibility into endpoint threats and streamlining threat mitigation, the solution strengthens an organization's security posture and safeguards against evolving attack vectors.

CrowdStrike Falcon Firewall Management simplifies the management of host-based firewall policies by providing centralized control and visibility across environments. Built on a cloud-native platform, it enables security teams to automate policy enforcement, streamline rule management, and ensure compliance with organizational security standards. The solution monitors network traffic at the endpoint level, helping to identify and block unauthorized access while mitigating risks associated with lateral movement. By integrating seamlessly with security workflows, Falcon Firewall Management enhances efficiency, reduces complexity, and strengthens an organization's overall security posture.

CrowdStrike Falcon Device Control enables organizations to manage and secure USB devices with centralized visibility and granular policy enforcement. Built on a cloud-native platform, it allows security teams to monitor and control device usage, ensuring compliance with organizational security standards. Falcon Device Control helps prevent unauthorized data transfers and mitigates risks associated with removable media by enforcing detailed access policies. By integrating seamlessly with existing workflows, the solution enhances visibility, streamlines policy management, and strengthens endpoint security across the enterprise.

CrowdStrike Falcon FileVantage provides real-time file integrity monitoring (FIM) to track and secure critical changes to files, folders, and registries across the enterprise. Built on a cloud-native platform, the solution delivers continuous visibility into unauthorized modifications and anomalies, enabling organizations to quickly identify potential risks and maintain compliance with regulatory standards. Falcon FileVantage simplifies security operations by integrating seamlessly with existing workflows, ensuring consistent policy enforcement and strengthening the overall security posture of critical assets.

CrowdStrike Falcon Fusion SOAR streamlines security operations by automating workflows, integrating threat intelligence, and triggering real-time responses to security incidents. Built on a cloud-native platform, Falcon Fusion enables organizations to create and enforce rule-based policies, automate repetitive tasks, and enhance incident response with predefined playbooks. By integrating seamlessly with existing security tools, the solution delivers actionable insights, ensures consistent policy enforcement, and improves operational efficiency, helping organizations adapt quickly to evolving threats and maintain a strong security posture.

Recommendations and Business Outcomes

6.1 Policy Decision Point and Policy Orchestration

- **CrowdStrike Falcon for IT** provides capabilities that enhance policy enforcement oversight through improved visibility, automation and risk-based evaluation. By leveraging insights from the User, Data, Network and Device Pillars, organizations can monitor and enforce compliance with access policies that align with operational needs. This solution streamlines policy enforcement oversight by integrating mission-critical profiles, addressing exceptions systematically and iteratively refining enforcement strategies. These capabilities ensure alignment with security requirements while supporting operational flexibility.
- **CrowdStrike Falcon Next-Gen SIEM** enhances policy enforcement oversight by delivering unified insights into security events across user, data, network and device domains. By leveraging real-time visibility and centralized event management, organizations can oversee and refine enterprise security profiles. Falcon Next-Gen SIEM supports iterative tuning of enforcement strategies and risk-based management of exceptions, ensuring streamlined and effective access policy enforcement. These capabilities simplify operational oversight and enable proactive responses to deviations while maintaining alignment with organizational requirements.

- **CrowdStrike Falcon Insight XDR** enhances policy enforcement oversight by delivering XDR capabilities across user, data, network and device domains. Its ability to aggregate and contextualize information across these domains supports the enforcement of enterprise security profiles and iterative tuning of enforcement strategies. The solution also enables proactive management of risk-based exceptions, ensuring that access controls remain aligned with operational priorities. By providing centralized visibility and streamlined oversight, Falcon Insight XDR simplifies policy enforcement and enhances security outcomes.
 - **CrowdStrike Falcon Identity Protection** enhances policy enforcement oversight by providing visibility and control over identity-related activities across user, data, network and device domains. This solution supports the creation and management of enterprise security profiles by monitoring access activities and enforcing policies in alignment with organizational goals. By integrating mission-critical identity policies and employing risk-based exception management, it ensures streamlined oversight and iterative refinement of enforcement strategies. These capabilities enable effective policy oversight while maintaining alignment with access control requirements and operational flexibility.
 - **CrowdStrike Falcon Exposure Management/Falcon Discover** enhances policy enforcement oversight by identifying and mitigating risks across user, data, network and device domains. It provides visibility into vulnerabilities and misconfigurations, enabling organizations to align enforcement policies with operational objectives. By integrating risk-based prioritization and iterative tuning of enforcement strategies, Falcon Exposure Management/Falcon Discover/Falcon for XIoT supports streamlined oversight and effective management of access policies, ensuring security while maintaining operational flexibility.
 - **CrowdStrike Falcon for XIoT** enables comprehensive visibility and security for XIoT devices, addressing key requirements for policy enforcement and orchestration. The solution continuously monitors connected assets, identifies vulnerabilities and enforces rule-based access policies to ensure compliance with predefined security requirements. By supporting centralized visibility and automated workflows, Falcon for XIoT assists in defining, updating and enforcing DAAS access procedures while providing real-time insights into device activity. These capabilities align with the need for PDPs and PEPs by enabling consistent monitoring, access determinations and enforcement of security policies across XIoT environments.
 - **Mapped Outcomes:**
 - **6.1.1 Policy Inventory and Development, 6.1.2 Component Access Profile Rules, 6.1.3-6.1.4 Enterprise Security Profile**
 - **Enterprise Security Profile Oversight:** Provides centralized visibility into security profiles, ensuring that access policies for user, data, network and device domains are enforced consistently and effectively.
 - **Comprehensive Visibility and Exposure Management:** Provides detailed insights into vulnerabilities, misconfigurations and identity-related activities, ensuring enforcement of security policies across user, data, network and device contexts.
-

- **Simplified Profile Oversight and Policy Enforcement:** Supports streamlined oversight of security profiles by reducing complexity, enabling broader access configurations tailored for both operational and mission-critical requirements.
- **Streamlined Access Monitoring and Enforcement Oversight:** Facilitates the alignment of enforcement strategies with operational priorities, reducing complexity while helping to ensure compliance across domains.
- **Iterative Enforcement Refinement:** Enables continuous evaluation and adjustment of enforcement strategies to optimize access control configurations, aligning them with organizational objectives and security requirements.
- **Risk-Based Exception Oversight:** Implements structured and methodical management of exceptions, prioritizing risk assessment and mitigation while maintaining robust security enforcement across all domains.

6.2 Critical Process Automation

- **CrowdStrike Falcon Fusion SOAR** enhances critical process automation by facilitating the integration and interoperability of security instruments, enabling actionable workflows and advanced orchestration. By categorizing task activities into manual and automated processes, organizations can streamline operations, retire redundant manual activities and focus on automating critical workflows. Falcon Fusion SOAR establishes a robust baseline of instrument interoperability, ensuring seamless integration into workflows to meet functional requirements and enhance service provisioning.
- **CrowdStrike Falcon Next-Gen SIEM** streamlines critical process automation by enabling comprehensive integration of manual and automated task activities into centralized workflows. By establishing baseline interoperability for security orchestration tools, organizations can align task activities with operational objectives, optimize service provisioning and achieve seamless automation. Falcon Next-Gen SIEM supports the categorization and prioritization of interoperability points, ensuring efficient service integration and workflow automation that meets advanced functionality requirements.
- **CrowdStrike Falcon for IT** supports critical process automation by enabling the organization and integration of manual and automated workflows, ensuring task activities are aligned with operational goals. By establishing baseline interoperability for security tools, Falcon for IT facilitates seamless integration of actionable information and service provisioning. This solution allows organizations to streamline operational workflows, retire unnecessary manual processes and optimize advanced functionality through automated workflows.
- **CrowdStrike Falcon Insight XDR** enables effective critical process automation by streamlining task categorization, interoperability and workflow integration. It facilitates the identification and organization of manual and automated activities, supporting the retirement of redundant processes. By establishing baseline interoperability for security tools and integrating service provisioning into automated workflows, organizations can optimize operational efficiency and meet advanced functional requirements.

- **Mapped Outcomes:**
 - **6.2.1 Task Automation Analysis, 6.2.2-6.2.3 Enterprise Integration and Workflow Provisioning**
 - **Task Activity Categorization and Optimization:** Facilitates the identification, enumeration and categorization of task activities into manual and automated processes, enabling organizations to analyze manual tasks for retirement, streamline operations and focus on automation where possible.
 - **Baseline Instrument Interoperability:** Establishes foundational interoperability for security orchestration tools, ensuring actionable and relevant information is seamlessly integrated into workflows and aligned with operational requirements.
 - **Workflow Automation and Service Integration:** Enables the integration and automation of service provisioning into workflows, ensuring alignment with advanced functionality and operational goals while optimizing task execution.
 - **Interoperability Prioritization and Service Optimization:** Supports the identification and prioritization of instrument interoperability points, facilitating workflow optimization and ensuring efficient service provisioning to meet both baseline and advanced operational requirements.

6.4 Artificial Intelligence

- **CrowdStrike Falcon Insight XDR** supports the enforcement of security standards by delivering comprehensive visibility into threats and integrating data from multiple sources. This capability allows workflows to address policy gaps, streamline rule enforcement and establish automated processes for critical tasks. By integrating contextual information and automating responses, organizations can ensure operational consistency while aligning with compliance and risk management goals.
 - **CrowdStrike Falcon Identity Protection** strengthens the enforcement of identity-based policies and workflows by safeguarding access across enterprise systems. Through visibility into identity-based risks and integration with existing security policies, organizations can apply access controls, refine security profiles and automate workflows to align with compliance and operational objectives. Automated identity protection processes reduce manual intervention while enhancing the consistency and security of access management.
 - **CrowdStrike Falcon Prevent** empowers organizations to streamline automation and decision-making processes by identifying areas for improvement and integrating advanced tools into workflows. It enables proactive adjustments to automated workflows based on operational patterns, enhancing efficiency and reducing manual oversight. This solution supports the establishment of requirements for tool implementation, ensuring workflows are optimized for risk mitigation and operational consistency.
-

- **Mapped Outcomes:**
 - **6.4.1 Implement AI Automation Tools, 6.4.2 AI Driven by Analytics Decides Automation and Orchestration Modifications**
 - **Identification of Improvement Areas:** Supports the evaluation of existing methodologies to identify and address areas where enhancements can improve operational workflows, streamline processes and drive efficiency while aligning with organizational goals.
 - **Tool Requirement Development and Implementation:** Facilitates the establishment of requirements for advanced tools, enabling their efficient procurement, seamless integration and alignment with identified improvement areas.
 - **Workflow Automation and Proactive Adjustments:** Enables the integration of operational patterns and trends into workflows, allowing anticipatory adjustments to reduce risks, enhance efficiency and maintain operational consistency.
 - **Reduction of Manual Oversight:** Transitions decision-making processes to automated workflows, minimizing manual intervention and freeing up personnel to focus on strategic and higher-value initiatives.

6.5 Security Orchestration, Automation and Response

- **CrowdStrike Falcon Fusion SOAR** facilitates the seamless integration of tools and workflows. It allows for the identification of areas of improvement, enabling streamlined operations and reducing manual intervention. By optimizing workflows and automating response actions, organizations can align with operational goals, enhance decision-making processes and maintain a proactive security posture.
- **Mapped Outcomes:**
 - **6.5.1 Response Automation Analysis, 6.5.2 Plan SOAR Tools Implementation, 6.5.3 Implement Playbooks**
 - **Identification of Improvement Areas:** Supports the evaluation of existing methodologies to identify and address areas for operational enhancement, ensuring workflows and automation processes are optimized.
 - **Tool Integration and Workflow Optimization:** Facilitates the seamless integration of tools into workflows, enabling efficient operations and aligning workflows with organizational requirements.
 - **Automation of Response Activities:** Enables automated execution of response activities within workflows, ensuring swift and consistent handling of security incidents and reducing reliance on manual intervention.
 - **Enhanced Operational Efficiency:** Reduces manual workload by automating decision-making processes, freeing personnel to focus on strategic initiatives while ensuring continuous workflow operation.

6.7 SOC Incident Response

- **CrowdStrike Falcon Identity Protection** strengthens the enforcement of identity-based policies and workflows by safeguarding access across enterprise systems. Through visibility into identity-based risks and integration with existing security policies, organizations can apply access controls, refine security profiles and automate workflows to align with compliance and operational objectives. Automated identity protection processes reduce manual intervention while enhancing the consistency and security of access management.
 - **CrowdStrike Falcon Cloud Security** enhances operational workflows by monitoring cloud configurations, addressing misconfigurations and automating compliance processes. By integrating CWP and compliance management into organizational frameworks, organizations can standardize controls, automate routine tasks and align operational priorities with regulatory requirements. These measures improve the visibility and security of cloud environments while ensuring efficient deployment and maintenance practices.
 - **CrowdStrike Falcon Exposure Management/Falcon Discover/Falcon Spotlight** supports the enforcement of security policies by identifying asset configurations, risk exposures and operational gaps. By leveraging insights from internal data and external enrichment sources, organizations can prioritize and streamline workflows to apply policies that meet operational objectives. Automated processes reduce manual efforts in managing access rules, policy tuning and task categorization, aligning outcomes with compliance and operational standards.
 - **CrowdStrike Falcon Insight XDR** facilitates critical needs in SOC and incident response functions by offering comprehensive detection, visibility and response capabilities. It enhances workflows by enabling threat identification, enrichment with contextual and external data sources, and the automation of incident response processes. Organizations can leverage advanced orchestration and automation to replace manual processes, streamline decision-making and enhance operational efficiency while ensuring adherence to industry best practices.
 - **CrowdStrike Falcon Next-Gen SIEM** streamlines security operations by centralizing data collection, identifying compliance gaps and automating workflows. By integrating data from various components and aligning with organizational policies, it allows for the development of consistent access rules, automated task execution and effective incident response. These capabilities enhance visibility, operational efficiency and compliance adherence.
 - **CrowdStrike Falcon for IT** optimizes workflows by integrating asset management, vulnerability assessment and configuration tracking into operational processes. This ensures alignment with organizational policies, streamlines task execution and improves visibility into infrastructure health. Automating manual tasks and aligning workflows with compliance requirements reduces complexity, mitigates risks and enhances operational efficiency.
-

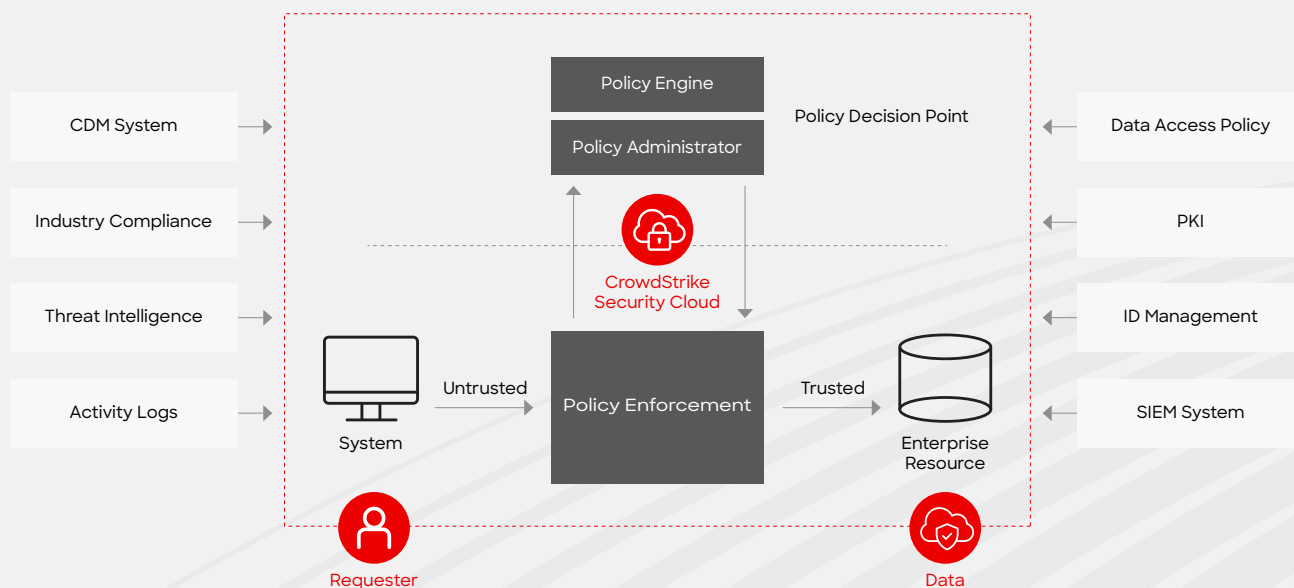
- **CrowdStrike Falcon Prevent** addresses cybersecurity requirements by safeguarding endpoints through proactive protection measures and streamlined workflows. This ensures alignment with enterprise policies while enabling organizations to manage risks, refine access rules and optimize task automation. By integrating endpoint protection capabilities into operational frameworks, organizations can strengthen their security posture while supporting compliance objectives.
 - **CrowdStrike Falcon Firewall Management** strengthens the enforcement of security policies and streamlines firewall rule management to meet operational requirements. By integrating policy controls with workflows, organizations can refine access rules, automate repetitive processes and align operations with compliance standards. These capabilities reduce manual efforts and improve consistency across network security implementations.
 - **CrowdStrike Falcon Device Control** supports the enforcement of security policies by managing device access and usage, ensuring alignment with enterprise standards. By incorporating device control into workflows, organizations can create refined access rules, automate processes and maintain compliance with operational requirements. This approach minimizes manual intervention, reduces risk and enhances the consistency of security implementations across devices.
 - **CrowdStrike Falcon FileVantage** supports the enforcement of security policies by monitoring file integrity and identifying unauthorized changes to critical files. Through integration with workflows, organizations can establish processes to track changes, automate responses and align file monitoring activities with compliance and operational standards. These capabilities reduce the likelihood of undetected changes, enhance transparency and streamline file management.
 - **CrowdStrike Falcon Exposure Management/Falcon Discover** supports the enforcement of security policies by identifying asset configurations, risk exposures and operational gaps. By leveraging insights from internal data and external enrichment sources, organizations can prioritize and streamline workflows to apply policies that meet operational objectives. Automated processes reduce manual efforts in managing access rules, policy tuning and task categorization, aligning outcomes with compliance and operational standards.
 - **CrowdStrike Falcon for Mobile** helps organizations manage mobile device security by identifying vulnerabilities, ensuring compliance with security policies and automating response workflows. By integrating mobile security into broader operational processes, organizations can establish consistent access rules, streamline task execution and align device management with compliance requirements. This approach reduces manual effort, enhances operational efficiency and mitigates risks associated with mobile endpoints.
 - **CrowdStrike Falcon Fusion SOAR** streamlines orchestration and automation workflows by integrating security tools, enabling task automation and facilitating consistent incident response processes. By centralizing operational data and aligning workflows with policy requirements, organizations can optimize task execution, ensure compliance and improve operational visibility. These measures reduce manual effort, enhance process consistency and support policy-driven automation.
-

– **Mapped Outcomes:**

- **6.7.1-6.7.3 Workflow Environment, 6.7.4 Automated Workflow**
 - **Asset and Policy Alignment:** Establishes visibility into assets and their alignment with existing policies, identifying gaps and ensuring workflows incorporate relevant business and mission context for comprehensive coverage.
 - **Workflow Structuring for Security Profiles:** Creates structured workflows that integrate access profile rules and enterprise security profiles, ensuring consistent application across varied mission-critical and non-mission-critical activities.
 - **Policy and Rule Validation:** Ensures security policies align with operational needs by identifying gaps and inconsistencies. Workflow adjustments enforce rules effectively across enterprise and component levels.
 - **Development of Access and Security Profiles:** Facilitates the creation and refinement of access profiles and security rules, which are tailored for operational needs, and distinguishes between mission-critical and non-mission-critical tasks.
 - **Policy Enforcement and Risk Mitigation:** Aligns identity and endpoint management with enterprise security policies, enforcing rules that limit unauthorized access while addressing risks.
 - **Automation of Tasks and Processes:** Reduces manual effort by categorizing tasks into automated and manual workflows, focusing on security tasks, policy management and compliance activities.
 - **Automation of Compliance and IT Tasks:** Streamlines compliance management and IT operations by automating routine tasks, asset tracking and vulnerability management. Structured, risk-based processes handle exceptions.
 - **Integration of Enrichment Sources and Security Data:** Consolidates data from internal and external sources into workflows, improving prioritization, policy development and decision-making for security and compliance.
 - **Integration of Endpoint and Cloud Data:** Incorporates insights from devices, cloud workloads and endpoints into workflows, supporting better-informed security decisions and operational actions.
 - **Integration with Security Tools and Frameworks:** Consolidates operational tools and security frameworks into centralized workflows, facilitating improved coordination and alignment with enterprise objectives.
 - **Policy Compliance and Workflow Integration:** Aligns automation processes and orchestration tasks with organizational policies, incorporating operational requirements into standardized workflows.

- **Development of Automated Playbooks:** Creates and automates playbooks to ensure consistent execution of workflows tailored to critical and non-critical processes.
- **Standardization and Compliance Assurance:** Establishes standardized processes across operational and regulatory domains, improving transparency, reducing complexity and aligning with compliance goals.
- **Optimization of Security and IT Processes:** Streamlines task execution and policy management by iterating workflows, ensuring alignment with organizational goals and improving efficiency.
- **Visibility and Monitoring:** Enhances tracking and reporting of compliance and security across workloads and deployments, using dashboards and analytics to maintain oversight.

The CrowdStrike Falcon Platform Delivers NIST SP 800-207 PDP/PEP Functionality in the Cloud



3.7 Visibility and Analytics Pillar

Pillar Summary

The **DoD ZTA Visibility and Analytics Pillar** focuses on collecting, analyzing and correlating data across all pillars to enhance threat detection and response. DoD organizations prioritize log and flow sources — including network, device, user and application logs — which are collected in standardized formats and processed through SIEM systems. These systems develop rules and alerts for common threats, integrate CTI feeds and mature over time to include advanced analytics such as UEBA and anomaly detection. User and device baselines are established to profile typical behavior and detect deviations, contributing to the creation of threat profiles and risk assessments.

As analytics capabilities expand, DoD organizations integrate outputs with cross-pillar solutions, improving detection and response for advanced threats. Centralized CTI teams aggregate intelligence from all Zero Trust pillars and apply actionable insights to security operations. SOCs and computer network defense service providers (CNDSPs) utilize the collected data to monitor, detect and respond to threats dynamically, correlating behaviors and events. This ensures continuous visibility across the enterprise, supporting the rapid identification of risks and enabling effective enforcement of Zero Trust principles.

Challenges

- 1. Log All Traffic (Network, Data, Apps, Users):** DoD Components must prioritize logging all traffic — including network, data, applications and user activities — to align with Zero Trust objectives. A key challenge is identifying and collecting high-priority logs from sources like firewalls, endpoints and Active Directory before addressing lower-priority logs. An open, industry-standard log format has been mandated to ensure interoperability across the DoD Enterprise, with a continuous migration of legacy systems to this standard. These efforts enable consistent data aggregation and normalization as well as improved visibility, addressing Zero Trust requirements comprehensively.
 - 2. Security Information and Event Management:** Scaling the capabilities of existing SIEM systems is crucial for effective threat detection and response. DoD Components must use SIEM solutions to create basic threat event rules, such as rules for malware or phishing, and expand their use to include CTI feeds and anomaly detection rules. Advanced data sources like XDR and UEBA are integrated to detect sophisticated patterns of malicious activity. Additionally, all assets must be correlated within SIEM systems to provide actionable data for vulnerability assessments and enhanced incident response speeds.
 - 3. Common Security and Risk Analytics:** DoD Components face the challenge of implementing analytics tools that span all Zero Trust pillars to provide actionable insights and intelligence. These tools analyze user behavior patterns and deviations using techniques such as machine learning and UEBA to identify risks. Analytics capabilities must adapt to evolving threats, incorporating new baselines, profiles and risk assessments for enhanced detection and response. This integration ensures continuous improvement in risk analytics across the enterprise.
-

4. **User and Entity Behavior Analytics:** Developing baselines for user and role behaviors is a critical step in improving detection capabilities. DoD Components must establish activity benchmarks, enabling identification of abnormal patterns and risks. This baseline approach expands to include unmanaged and nonstandard devices, such as IoT and operational technology (OT) devices, with profiles created for these device types. Advanced analytics using AI and ML continuously refine these baselines, enabling the detection of subtle anomalies and better integration across Zero Trust pillars.
5. **Threat Intelligence Integration:** Expanding CTI programs is essential to aggregate and analyze threat data across Zero Trust pillars. DoD Components must establish CTI teams, leveraging shared intelligence from centralized feeds to enhance situational awareness. Threat intelligence is continuously analyzed to enforce appropriate actions and controls, adapting to emerging risks as solutions mature. This approach ensures proactive threat management and strengthens cross-pillar security capabilities.
6. **Automated Dynamic Policies:** DoD organizations are increasingly leveraging AI and ML to enable dynamic, risk-based access decisions. Existing rule-based dynamic access data is used to train AI/ML algorithms, improving decision-making and enabling broader access control across resources. These advanced algorithms adapt over time, integrating analytics outputs to refine their functionality and strengthen Zero Trust enforcement. Automated, AI-enabled network access supports scalability and responsiveness to evolving risks.

CrowdStrike Implementation Modules

- CrowdStrike Falcon Exposure Management
- CrowdStrike Falcon for XIoT
- CrowdStrike Falcon Identity Protection
- CrowdStrike Falcon for IT
- CrowdStrike Falcon Insight XDR
- CrowdStrike Falcon Next-Gen SIEM
- CrowdStrike Falcon Prevent
- CrowdStrike Counter Adversary Operations
- CrowdStrike Falcon Adversary Intelligence
- CrowdStrike Falcon Fusion SOAR

CrowdStrike Module Descriptions

CrowdStrike Falcon Exposure Management provides organizations with comprehensive visibility into connected assets — including unmanaged and IoT devices — while identifying and prioritizing risks across their environment. By integrating seamlessly with existing infrastructures, it allows for the monitoring of activity trends and supports dynamic policy updates to secure critical resources. Falcon Exposure Management/Falcon for XIoT empowers organizations to proactively manage exposure, reconcile network activity and enforce consistent security measures in alignment with operational priorities.

CrowdStrike Falcon for XIoT provides comprehensive security across all XIoT environments — including IoT, OT and internet of medical things (IoMT) environments — by delivering advanced visibility and proactive risk management. With zero infrastructure or network configuration changes, organizations can instantly identify and monitor all XIoT assets, achieving full visibility. The solution prioritizes vulnerabilities using real-time adversary intelligence to ensure critical issues are addressed promptly. By visualizing and understanding the relationships between assets across XIoT and IT environments, Falcon for XIoT enhances security posture and incident response, offering a unified approach to managing security policies, configurations and responses across the entire attack surface.

CrowdStrike Falcon Identity Protection enhances security by providing continuous visibility and monitoring of user activity, enabling the detection of anomalous behaviors and unauthorized access attempts. The solution integrates seamlessly with existing infrastructures to enforce identity-based policies, correlating user behavior patterns with threat alerts to prioritize high-risk actions. By supporting the creation of identity baselines, it ensures organizations can differentiate normal activity from potential threats while maintaining accurate and actionable insights for rapid response. Falcon Identity Protection empowers organizations to manage and secure identities effectively, aligning with the need for continuous visibility and analytics across user activities and associated risks.

CrowdStrike Falcon for IT enhances operational efficiency by providing real-time visibility into IT assets, users and activities, supporting streamlined monitoring and policy enforcement. It simplifies log and flow source prioritization, enabling organizations to focus on collecting and analyzing high-priority data from critical systems such as endpoints and Active Directory. The solution integrates with existing SIEM solutions, supporting the creation of actionable rules, alerts and correlations that improve detection and response capabilities. By leveraging a standardized approach to asset management and analytics, Falcon for IT ensures continuous oversight, helping organizations align their monitoring and compliance efforts with essential visibility and security requirements.

CrowdStrike Falcon Insight XDR delivers extended visibility and detection capabilities by integrating data across endpoints, networks and workloads, enabling organizations to monitor critical activities and respond effectively to threats. It supports the identification and prioritization of log and flow sources, ensuring the collection and correlation of high-value data for actionable insights. The solution integrates seamlessly with existing SIEM solutions, enhancing alerting and detection capabilities with comprehensive threat correlation and streamlined response workflows. By unifying visibility, threat intelligence and response mechanisms, Falcon Insight XDR empowers organizations to meet critical monitoring, detection and response requirements while maintaining operational efficiency.

CrowdStrike Falcon Next-Gen SIEM offers advanced capabilities for comprehensive monitoring, threat detection and response by centralizing and analyzing logs from diverse data sources. It supports the prioritization of high-value logs from systems such as firewalls and endpoints, ensuring streamlined data collection and correlation across the enterprise. By enhancing threat intelligence integration and enabling the development of actionable alerts, the solution improves situational awareness and speeds up incident response. Falcon Next-Gen SIEM ensures organizations can maintain effective oversight, reconcile network activity and enforce security policies while seamlessly integrating with existing infrastructure for efficient operations.

CrowdStrike Falcon Prevent provides comprehensive endpoint protection by detecting and preventing known and unknown threats in real time while ensuring efficient incident response. The solution enables organizations to collect and prioritize data from critical systems, ensuring integration with existing infrastructures and maintaining visibility across endpoints. By leveraging centralized monitoring and correlating threat data with user activity baselines, it ensures rapid detection and actionable insights to address risks effectively. Falcon Prevent equips organizations with the tools to streamline security operations and enforce consistent policies across their environments while helping them align with critical monitoring and response requirements.

CrowdStrike Counter Adversary Operations/CrowdStrike Falcon® Adversary Intelligence strengthens organizational defenses by leveraging proactive threat intelligence to identify and neutralize adversary actions before they cause harm. Organizations can develop actionable threat intelligence policies, establish baselines for normal activity and correlate data with security events for comprehensive visibility. By aligning operational strategies with real-time insights and coordinated response capabilities, they can effectively protect critical assets and enforce robust security measures.

CrowdStrike Falcon Fusion SOAR delivers comprehensive automation and orchestration capabilities, enabling the seamless collection, correlation and analysis of log and flow sources across the enterprise. By integrating with existing SIEM infrastructures, it enhances threat detection through customizable rules, automated alerts and enrichment with CTI feeds. Falcon Fusion SOAR supports the establishment of user and device behavior baselines, identifying anomalies to aid in risk assessments and threat profiling. These capabilities empower organizations to dynamically monitor and respond to threats while maintaining consistent visibility and alignment with operational security priorities.

Recommendations and Business Outcomes

7.1 Log All Traffic (Network, Data, Apps, Users)

- **CrowdStrike Falcon Exposure Management** provides organizations with comprehensive visibility and risk prioritization across all connected assets, including IoT and unmanaged devices. By enabling the collection and analysis of network, data, application and user traffic, the solution aligns visibility and monitoring processes with risk-based priorities to improve security outcomes. Organizations can leverage this solution to profile devices, prioritize log and flow sources, and ensure consistent policy enforcement by using standardized formats and prioritization frameworks. These capabilities streamline the operationalization of monitoring strategies, enhance risk alignment and provide actionable insights to meet visibility and traffic logging requirements.
 - **CrowdStrike Falcon for XIoT** provides real-time visibility and protection for XIoT devices, identifying and mitigating vulnerabilities across connected assets. It continuously monitors device activity and configurations, offering deep insights into risks while enabling security teams to detect and respond to threats effectively. By enforcing granular policies, Falcon for XIoT helps secure critical assets, streamline compliance, protect sensitive data and enhance operational resilience.
-

- **CrowdStrike Falcon Identity Protection** enables comprehensive visibility into user activity, offering real-time monitoring and detection of suspicious behaviors to secure access to critical systems and applications. By supporting the collection and analysis of user activity data, it helps organizations prioritize logs and flows, ensuring risk-aligned monitoring and enforcement of access policies. This solution facilitates the creation of baselines for user activity, enabling the detection of deviations and ensuring actions are aligned with mission-critical priorities. These capabilities enhance the ability to scale monitoring strategies, streamline operational processes and ensure consistent enforcement of policies across user activity and access points.
 - **CrowdStrike Falcon Next-Gen SIEM** delivers comprehensive monitoring and analysis capabilities by centralizing log and flow data from multiple sources, enabling organizations to manage security risks effectively. The solution supports prioritizing critical data sources such as firewalls, endpoints and applications while ensuring the use of standardized log formats for consistent data aggregation and interoperability. By correlating user and device activities, it provides actionable insights for identifying high-risk behaviors and streamlining monitoring strategies. These capabilities enhance operational processes, align monitoring frameworks with mission priorities, and support scalable and risk-aligned visibility across the enterprise.
 - **CrowdStrike Falcon for IT** enables organizations to streamline monitoring and visibility across IT operations by providing real-time insights into devices, users and applications. It supports the collection and prioritization of logs and flows from critical infrastructure components such as endpoints and Active Directory, ensuring consistent data aggregation using standardized formats. This solution enables organizations to assess user and device activities based on risk, enhancing visibility into network and application traffic while optimizing operational workflows. These capabilities ensure scalable monitoring strategies, risk-aligned visibility and actionable insights for improving compliance and security enforcement.
 - **Mapped Outcomes:**
 - **7.1.1 Scale Considerations, 7.1.2 Log Parsing, 7.1.3 Log Analysis**
 - **Comprehensive Monitoring:** Supports the identification, collection and prioritization of logs and flow sources, including firewalls, endpoints, network devices and Active Directory. This ensures critical data is captured and monitored effectively, aligning monitoring efforts with mission-critical priorities.
 - **Standardized Logging Practices:** Implements open, industry-standard log formats to enable consistent and interoperable data collection, integration and analysis across all environments. These practices ensure seamless data aggregation and support comprehensive visibility into network, application and user activity.
 - **Risk-Based Activity Prioritization:** Assists in creating baselines for user and device activities, identifying high-risk behaviors and prioritizing monitoring strategies based on operational and security goals. This ensures that monitoring efforts focus on the most critical behaviors and traffic patterns across networks, applications and users.
-

- **Scalable Monitoring Framework:** Provides tools and strategies to analyze and scale monitoring needs effectively, aligning them with operational considerations and mission requirements. This facilitates effective resource allocation and supports continuous improvement in visibility and oversight.
- **Operational Integration:** Facilitates the creation or optimization of governance structures to integrate monitoring processes seamlessly into existing workflows. This ensures consistent enforcement of policies, effective alignment with organizational objectives and streamlined monitoring strategies.

7.2 Security Information and Event Management

- **CrowdStrike Falcon Next-Gen SIEM** enables organizations to enhance their security posture by unifying data collection, detection, response and workflow automation within a single platform. This integration facilitates the development of comprehensive rules and alerts for common and advanced threat events, incorporating CTI feeds to detect anomalies effectively. By leveraging XDR capabilities alongside UEBA, security teams gain improved visibility into assets and user activities, allowing for rapid incident response and informed decision-making.
 - **CrowdStrike Falcon Identity Protection** enhances security operations by continuously monitoring and analyzing identity-based activity to detect anomalous user behavior and prevent identity-driven attacks. By integrating with SIEM tools, Falcon Identity Protection enables CNDSPs and SOCs to process and exploit identity data effectively, providing actionable insights for advanced alerting and incident response. The solution establishes user and device baselines, leveraging these baselines to refine security controls, automate responses to common threat events and streamline security analysis. These capabilities ensure alignment with security requirements, enabling organizations to detect and mitigate identity-related threats efficiently.
 - **Mapped Outcomes:**
 - **7.2.1-7.2.3 Threat Alerting, 7.2.4 Asset ID and Alert Correlation, 7.2.5 User/Role Baselines**
 - **Development of Threat Correlation Rules:** Facilitates the creation of rules for both common and advanced threat events, enhancing detection and alerting mechanisms. These rules help security teams identify and address potential threats effectively, ensuring robust incident response.
 - **Integration of Cyber Threat Intelligence:** Incorporates threat intelligence data feeds to enrich alerting systems, enabling the identification of deviations and anomalies indicative of sophisticated threats. This integration enhances visibility into potential risks and provides actionable insights for proactive mitigation.
 - **Inclusion of Advanced Data Sources:** Utilizes data from XDR systems, UEBA and user activity monitoring to refine detection of anomalous patterns and activities. By leveraging these data sources, organizations gain a more comprehensive understanding of their threat landscape.
-

- **Asset Identification and Alert Correlation:** Ensures all assets are identified and correlated with alerts, providing security teams with accurate and detailed information to expedite incident response. This process also enhances vulnerability assessments, supporting better risk management.
- **Establishment of User Behavior Baselines:** Develops baselines for user and role behaviors to serve as benchmarks in identifying and responding to abnormal or potentially malicious activities. These baselines help differentiate normal patterns from potential threats, improving the overall security posture.

7.3 Common Security and Risk Analytics

- **CrowdStrike Falcon Identity Protection** provides actionable insights into identity-based threats, enabling organizations to analyze user behavior patterns and deviations effectively. This solution addresses the need for standardized analytics tools capable of supporting visibility across key operational areas. By implementing robust tools to analyze data across diverse pillars, organizations can develop a unified analytics environment that delivers comprehensive intelligence, driving informed decision-making and improving security postures. Establishing baselines for user behavior and identifying deviations empowers security teams to rapidly detect and mitigate identity-related risks, ensuring adherence to organizational objectives.
- **Mapped Outcomes:**
 - **7.3.1 Implement Analytics Tools, 7.3.2 Establish User Behavior Pattern**
 - **Development of Analytic Environment Requirements:** Supports the establishment of minimum requirements for analytics tool capabilities, ensuring compatibility with broader visibility and risk management objectives.
 - **Procurement and Implementation of Analytics Tools:** Facilitates the acquisition and deployment of tools designed to deliver actionable insights and intelligence across all operational areas.
 - **User Behavior Pattern Analysis:** Enables the analysis of user behavior to establish baselines and identify deviations from normal patterns, strengthening detection and response capabilities.
 - **Differentiation of Normal and Abnormal Activities:** Provides methodologies to define and distinguish standard behaviors from potential threats, improving overall risk analysis.

7.4 User and Entity Behavior Analytics

- **CrowdStrike Falcon Identity Protection** empowers organizations to identify and assess user and device risks by leveraging user/role baselines to develop detailed threat profiles. These profiles are extended to unmanaged and nonstandard devices — including IoT and OT devices — enabling enhanced monitoring and detection capabilities. This approach ensures seamless integration of analytics across various operational pillars, prioritizing risky entities and streamlining detection and response processes.
-

- **CrowdStrike Falcon Prevent** extends detection capabilities to unmanaged devices — such as IoT and OT devices — by using standardized attributes and outputs for profiling. This enables the prioritization of risky users and devices for increased monitoring while integrating detection and response across operational areas to ensure comprehensive and effective security.
- **CrowdStrike Falcon Insight XDR** empowers organizations to build and refine threat profiles for users and devices to assess and manage risks effectively. It expands profiling to unmanaged and nonstandard devices — including IoT and OT devices — and integrates these profiles into comprehensive analytics frameworks. These capabilities ensure enhanced monitoring and prioritization of risky entities while enabling seamless integration of detection and response functions across operational pillars.
- **Mapped Outcomes:**
 - **7.4.1 Risk Profiling, 7.4.2 Baseline and Profiling, 7.4.3–7.4.4 UEBA Baseline Support**
 - **Identification of User/Role Threat Profiles:** Establishes baselines for users and roles to develop comprehensive threat profiles, enabling the assessment of risks and strengthening the security posture of individual entities. These profiles provide a foundation for detecting deviations and mitigating risks effectively.
 - **Expansion to IoT and OT Devices:** Extends baselines and threat profiles to unmanaged and nonstandard devices, including IoT and OT devices, by utilizing standardized attributes and monitoring outputs. This ensures visibility across diverse device types and addresses evolving security challenges.
 - **Prioritization of Risky Users and Devices:** Automatically identifies and prioritizes high-risk users and devices for enhanced monitoring, ensuring targeted allocation of security resources. This prioritization supports quicker response and mitigates the impact of potential threats.
 - **Integration of Detection and Response Across Pillars:** Aligns monitoring outputs with detection and response systems across operational areas, facilitating improved coordination and enhancing the overall efficiency of security measures. This synchronization supports seamless threat management.
 - **Development and Extension of Analytics:** Refines analytics frameworks by incorporating outputs from expanded baselines and profiles, enabling precise detection and response strategies for complex and evolving threat landscapes. These updates ensure continuous improvement of security capabilities.

7.5 Threat Intelligence Integration

- **CrowdStrike Counter Adversary Operations and Falcon Adversary Intelligence** empower organizations to integrate threat intelligence effectively by building robust CTI programs. These solutions facilitate the development of CTI teams, ensuring collaboration among critical stakeholders and extending their capabilities to include actionable insights across enforcement points. By centralizing intelligence from approved feeds and adapting strategies over time, organizations can enhance visibility, improve coordination and enforce security measures across operational domains.
-

- **Mapped Outcomes:**
 - **7.5.1-7.5.2 Cyber Threat Intelligence Program**
 - **Establishment of CTI Teams:** Supports the creation of CTI teams that include key mission and task stakeholders to ensure effective intelligence gathering and utilization.
 - **Utilization of Approved CTI Feeds:** Aggregates controlled, DoD-approved threat intelligence feeds into centralized monitoring systems, enhancing the visibility and efficiency of security operations.
 - **Expansion of Stakeholder Collaboration:** Encourages the inclusion of additional stakeholders as necessary, fostering collaboration and expanding the scope of threat intelligence integration.
 - **Centralized Intelligence Aggregation:** Consolidates intelligence data from various feeds into a unified system, supporting comprehensive analysis and actionable insights.
 - **Integration with Enforcement Points:** Aligns threat intelligence outputs with enforcement mechanisms across operational areas, ensuring effective implementation of security controls.
 - **Strategic Adaptation Over Time:** Promotes the continuous refinement of threat intelligence strategies, aligning with program maturity and evolving security landscapes.

7.6 Automated Dynamic Policies

- **CrowdStrike Falcon Identity Protection** enhances access control by leveraging environment analytics and existing rules to enable adaptive decision-making. It integrates JIT and just-enough-access controls to ensure secure and efficient resource allocation. By continuously refining access strategies based on real-time analytics, it supports risk-informed adjustments to network and access controls.
 - **CrowdStrike Falcon Insight XDR** utilizes environment analytics and existing rules to improve access control decisions. It incorporates JIT and just-enough-access controls, ensuring secure and efficient resource management. By updating access strategies based on analytics, it aligns decision-making with evolving operational requirements.
 - **CrowdStrike Falcon Next-Gen SIEM** enhances access control strategies through robust data retention and analysis capabilities, allowing organizations to centralize and correlate extensive data from various sources. These capabilities provide visibility into enterprise environments, ensuring data-driven resource management decisions. By analyzing historical data and trends, it facilitates informed, scalable and context-aware resource allocation aligned with operational needs.
 - **CrowdStrike Falcon Fusion SOAR** refines access control strategies by orchestrating security workflows and analyzing data from diverse sources. It integrates with JIT and just-enough-access frameworks to ensure secure and efficient resource management. By automating responses and enhancing decision-making through continuous analysis, it supports scalable, adaptive and context-aware access controls.
-

– **Mapped Outcomes:**

- **7.6.1 AI-Enabled Network Access, 7.6.2 AI-Enabled Dynamic Access Control**
 - **Environment Analytics Integration:** Leverages insights from environment analytics to inform and refine access control decisions, ensuring alignment with organizational security and operational objectives. These analytics provide a foundation for dynamic and responsive adjustments to access policies.
 - **Support for Dynamic Access Policies:** Establishes and continuously refines rule-based frameworks for dynamic access policies, enabling responsive, context-aware access controls. This adaptability ensures that access decisions remain aligned with evolving organizational requirements and environmental changes.
 - **Implementation of JIT and Just-Enough-Access Controls:** Incorporates JIT and just-enough-access frameworks into access policy enforcement, minimizing unnecessary exposure while maintaining operational efficiency. These controls enhance security by restricting access to only what is needed, when it is needed.
 - **Policy Refinement for Broader Decision-Making:** Continuously updates and expands access policies to support more comprehensive and adaptive decision-making frameworks. This approach ensures scalability and flexibility in managing diverse resource control needs across operational environments.
 - **Risk-Informed Access Adjustments:** Aligns access decisions with real-time risk assessments derived from aggregated and analyzed data. This integration improves response accuracy, reduces vulnerabilities and supports secure, data-driven resource management.
 - **Automation of Response Mechanisms:** Streamlines enforcement and response processes by automating adjustments to access controls based on real-time analytics. Automation ensures timely and precise reactions to changing operational needs and security threats.
 - **Alignment with Operational Objectives:** Ensures that all access control decisions are informed by comprehensive data analysis and aligned with enterprise security profiles and evolving operational priorities. This alignment promotes consistent and auditable resource management across the organization.

4. Capability Recommendations and Activity Outcomes

1. User Pillar Capabilities

ID #	Capability	Capability Description	Capability Outcome	Impact to Zero Trust	CrowdStrike Product Mapping
1.1	User Inventory	Regular and privileged users are identified and integrated into an inventory supporting regular modifications. Applications, software and services that have local users are all part of the inventory highlighted.	System owners have control (visibility and administrative rights) of all authorized and authenticated users on the network.	Users not on the authorized user list will be denied access by policy.	Falcon Identity Protection Falcon Insight XDR
1.2	Conditional User Access	Through maturity levels, conditional access works to create a dynamic level of access for users in the environment. This starts with traditional role-based access controls across a federated ICAM, expands to include application-focused roles and ultimately utilizes enterprise attributes to provide dynamic access rules.	Eventually, organizations control user, device and non-user entity DAAS access by dynamically changing user risk profiles and fine-grained access control to include the use of user risk assessments.	Users not known to the system and users who present an unacceptable degree of risk will be denied access with greater accuracy.	Falcon Identity Protection Falcon Insight XDR
1.3	Multifactor Authentication	This capability initially focuses on developing an organization-focused MFA provider and IdP to enable the centralization of users. Retirement of local and/or built-in accounts and groups is a critical part of this capability. At the later maturity levels, alternative and flexible MFA tokens can be used to provide access for standard and external users.	DoD organizations require users and non-user entities to authenticate using at least two of the following three attributes to access DAAS: knowledge (user ID/password), possession (CAC/token) or something inherent to them (e.g., iris/fingerprints).	Users not presenting multiple forms of authentication will be denied access to DAAS.	Falcon Identity Protection
1.4	Privileged Account Management	This capability focuses on removing permanent administrator/elevated privileges by first creating a PAM system and migrating privileged users to it. This capability is then expanded by using automation with privilege escalation approvals and feeding analytics into the system for anomaly detection.	DoD organizations control, monitor, secure and audit privileged identities — e.g., through password vaulting, JIT/JEA with PAWS — across their IT environments.	Critical assets and applications will be secured, controlled, monitored and managed through limits on admin access.	Falcon Identity Protection Falcon Insight XDR
1.5	Identity Federation and User Credentialing	The initial scope of this capability focuses on standardizing ILM processes and integrating with the standard organizational IdP/IDM solution. Once completed, this capability shifts to establishing an enterprise ILM process/solution either through a single solution or identity federation.	DoD organizations manually issue, manage and revoke credentials bound to DoD person, device and NPE identities. Identity information is developed and shared across entities and trust domains providing “single sign-on” convenience and efficiencies to identified (authenticated and authorized) users and devices.	Visibility and accuracy of user authentication information is increased, to include DoD users and users managed by other agencies. Users lacking sufficient credentials will be denied access according to established policies.	Falcon Identity Protection

1.6	Behavioral, Contextual ID and Biometrics	Utilizing the enterprise IdP, UEBA is enabled with basic user attributes. Once completed, this is expanded into organization-specific attributes using organizational IDPs as available. Finally, UEBA is integrated with the PAM and JIT/JEA systems to better detect anomalous and malicious activities.	DoD organizations utilize behavioral, contextual and biometric telemetry to enhance risk-based authentication and access controls.	Behavioral, contextual and biometric telemetry enhance MFA.	Falcon Identity Protection
1.7	Least Privileged Access	DoD organizations govern access to DAAS using the absolute minimum access required to perform routine, legitimate tasks or activities. DoD application owners identify the necessary roles and attributes for standard and privileged user access. Privileged access for all DoD organization DAAS is audited and removed when unneeded.	DoD organizations govern access to DAAS using the absolute minimum access required to perform routine, legitimate tasks or activities.	Users on the network will only have access to the DAAS for which they are authorized and authenticated over a specific time frame.	Falcon Identity Protection
1.8	Continuous Authentication	The DoD organizations and overall enterprise will methodically move toward continuous attribute based authentication. Initially, this capability focuses on standardizing legacy single authentication to an organizationally approved IdP with users and groups. The second stage adds in based rule based (time) authentication and ultimately matures to continuous authentication based on the application/software activities and privileges requested.	DoD organizations continuously authenticate and authorize users' access to DAAS within and across sessions using MFA.	Critical assets and aUsers not continuously presenting multiple forms of authentication will be denied access to DAAS.	Falcon Identity Protection
1.9	Integrated ICAM Platform	DoD organizations and overall enterprise employ enterprise-level identity management and public key infrastructure (PKI) systems to track user, administrator and NPE identities across the network and ensure access is limited to only those who have the need and the right to know. Organizations can verify they need and have the right to access via credential management systems, identity governance and administration tools, and an access management tool. PKI systems can be federated but must either trust a central root certificate authority (CA) and/or cross-sign standardized organizational CAs.	DoD organizations employ enterprise-level identity management systems to track user and NPE identities across the network and ensure access is limited to only those who have the need and the right to know; organizations can verify they need and have the right to access via credential management systems, identity governance and administration tools, and an access management tool.	Identities of users and NPEs are centrally managed to ensure authorized and authenticated access to DAAS resources across platforms.	Falcon Identity Protection

2. Device Pillar Capabilities

ID #	Capability	Capability Description	Capability Outcome	Impact to Zero Trust	CrowdStrike Product Mapping
2.1	Device Inventory	DoD organizations establish and maintain an approved inventory list of all devices authorized to access the network and enroll all devices on the network prior to network connection. Device attributes will include technical details such as the PKI (802.1x) machine certificate, device object, patch/vulnerability status and others to enable successor activities.	DoD organizations establish and maintain a trusted inventory list of all devices authorized to access the network and enroll all devices on the network prior to network connection	By default policy, devices will be denied network access; the only devices permitted access to the network shall be known, authorized and listed in the device inventory.	Falcon Spotlight Falcon Discover Falcon Exposure Management Falcon for IT
2.2	Identity Device Detection and Compliance	DoD organizations employ asset management systems for user devices to maintain and report on IT and Cybersecurity compliance. Managed devices (enterprise and mobile) attempting to connect to a DoD network or access a DAAS resource is detected and has its compliance status confirmed (via C2C).	DoD organizations employ asset management systems for user devices to maintain and report on IT compliance. Any device (including mobile, IOT, managed, and unmanaged) attempting to connect to a DoD network or access a DAAS resource is detected and has its compliance status confirmed (via C2C)	Any device attempting to connect to the network will be detected; only devices that are compliant (e.g., antivirus is up-to-date, approved configuration) will receive access to requested DAAS.	Falcon Discover Falcon Exposure Management
2.3	Device Authorization w/ Real Time Inspection	DoD Organizations conduct foundational and extended device tooling (NextGen AV, AppControl, File Integrity Monitoring (FIM), etc.) integration to better understand the risk posture. Organizational PKI systems are integrated to expand the existing Enterprise PKI to devices as well. Lastly Entity Activity Monitoring is also integrated to identify anomalous activities.	DoD organizations establish processes (e.g., Enterprise PKI) and utilize tools to identify any device (including unmanaged devices, infrastructure devices, and endpoint devices) attempting to access the network, and make a determination if the device should be authorized to access the network. Maturation of this capability monitoring and detection of this activity on endpoints and IT infrastructure in real time	Components can use policies to deny devices by default and explicitly allow access to DAAS resources only by devices that meet mandated configuration standards. Identified security threats are remediated faster through continuous activity inspection enables faster remediation of security threats.	Falcon Prevent Falcon FileVantage Falcon Insight XDR
2.4	Remote Access	DoD organizations govern access to DoD organizations audit existing device access processes and tooling to set a least privilege baseline. In phase 2 this access is expanded to cover basic BYOD and IOT support using the Enterprise IDP for approved applications. The final phases expand coverage to include all BYOD and IOT devices for services using the approved set of device attributes.	DoD organizations establish policies to allow authorized users and devices access to the network or a device from a geographical distance through a network connection	Enables properly authorized users and authenticated users and NPEs to access DAAS from remote locations.	Falcon Identity Protection Falcon Discover Falcon Exposure Management Falcon for XIoT

2.5	Partially & Fully Automated Asset, Vulnerability and Patch Management	DoD organizations establish processes to automatically test and deploy vendor patches for connected devices; hybrid patch management (both human and automated) is employed.	DoD organizations establish processes to automatically test and deploy vendor patches for connected devices; hybrid patch management (both human and automated) is employed	Risk is minimized by automatically deploying vendor patches to all network devices.	Falcon Spotlight Falcon Discover Falcon Exposure Management Falcon for IT
2.6	Unified Endpoint Management and Mobile Device Management (MDM)	DoD organizations establish a centralized UEM solution that provides the choices of agent and/or agentless management of computer and mobile devices to a single console regardless of device location. DoD-issued devices can be remotely managed and security policies are enforced.	DoD organizations establish a centralized UEM tool that provides the choices of agent and/or agentless management of computer and mobile devices to a single console. DoD-issued mobile devices are remotely managed and security policies are enforced.	DAAS resources are protected through agent and agentless management, IT is able to manage, secure and deploy resources and applications on any device from a single console to provide redress of cybersecurity threats. Security vulnerabilities are mitigated, and policy enforcement measures are received through IT remote management of DoD-issued mobile devices	Falcon for IT
2.7	Endpoint & Extended Detection & Response (EDR and XDR)	DoD organizations use endpoint detection and response (EDR) tooling to monitor, detect, and remediate malicious activity on endpoints. Expanding the capability to include XDR tooling allows organizations to account for activity beyond the endpoints such as cloud and network as well.	DoD organizations use EDR tools to monitor, detect, and remediate malicious activity on endpoints as a baseline. Upgrading to XDR tools allows organizations to account for activity beyond the endpoints.	Threats originating from network-connected endpoints are initially reduced through active investigation and response. Maturation focuses on forensics, and faster threat detection and remediation are enabled by correlating data across multiple security layers (e.g., email, cloud, endpoint).	Falcon Insight XDR Falcon Next-Gen SIEM Falcon Prevent Falcon Identity Protection

3. Application and Workload Pillar Capabilities

ID #	Capability	Capability Description	Capability Outcome	Impact to Zero Trust	CrowdStrike Product Mapping
3.1	Application Inventory	System owners ensure that all applications and application components are identified and inventoried; only applications and application components that have been authorized by the appropriate authorizing official/CISO/CIO shall be utilized within the system owner's purview	System owners ensure that all applications and application components are identified and inventoried; only applications and application components that have been authorized by the appropriate authorizing official/CISO/CIO shall be utilized within the system owner's purview	Unauthorized applications and application components are not used on or within the system.	Falcon for IT Falcon Discover Falcon Exposure Management Falcon Cloud Security
3.2	Secure Software Development and Integration	Foundational software and application security processes and infrastructure are established following Zero Trust principles and best practices. Controls such as code review, runtime protection, secure API gateways, container and serverless security are integrated and automated.	Organization-defined security controls and practices are integrated, to include Zero Trust security controls and virtualization, into the software development lifecycle and DevOps toolchain. Custom software development teams use DevSecOps to integrate static and dynamic application security testing into software delivery workflows in accordance with the organization's requirements (policies, technologies, and processes).	Zero Trust security concepts, processes and capabilities are accepted and integrated across the DevOps toolchain, to include static and dynamic application security testing necessary for the discovery of weaknesses and vulnerabilities during application development.	Falcon Cloud Security

3.3	Software Risk Management	DoD organizations establish software/application risk management program. Foundational controls include Bill of Materials risk management, Supplier Risk Management, approved repositories and update channels, and vulnerability management program. Additional controls include Continual validation within the CI/CD pipelines and vulnerability maturation with external sources.	DoD establishes policies and procedures to secure supply chain cybersecurity for code components within DoD and DIB systems by evaluating and identifying supplier sourcing risk for approved sources, creating repositories and update channels for use by development teams, creating Bill of Materials for applications to identify source, supportability and risk posture, and establishing industry standard (DIB) and approved vulnerability databases for use in DevSecOps	The code used in DAAS and associated components of the supply chain is secure, vulnerabilities are reduced and the DoD is aware of potential risks.	Falcon Exposure Management Falcon Cloud Security Falcon Next-Gen SIEM
3.4	Resource Authorization & Integration	DoD establishes a standardized resource authorization gateway for authorizations via the CI/CD pipelines in a risk approach that reviews the User, Device and Data security posture. Authorizations utilize a programmatic (e.g., Software Defined) approach in a live/production environment. Attributes are enriched utilizing other pillar activities and the API and Authorization gateway. Approved enterprise APIs are micro-segmented using authorizations.	DoD establishes a standard approach managing the authorizations of resources in a risk approach that reviews the User, Device and Data security posture.	Resource authorization enables the ability for limited access to those resources and in a programmatic way in later stages. This improves the ability to remove access when it is not needed.	Falcon Next-Gen SIEM Falcon Insight XDR Falcon Identity Protection
3.5	Continuous Monitoring and Ongoing Authorizations	DoD organizations employ automated tools and processes to continuously monitor applications and assess their authorization to operate	DoD organizations employ automated tools and processes to continuously monitor applications and assess their authorization to operate	Near real-time visibility into the effectiveness of deployed security controls.	Falcon Cloud Security

4. Data Pillar Capabilities

ID #	Capability	Capability Description	Capability Outcome	Impact to Zero Trust	CrowdStrike Product Mapping
4.1	Data Catalog Risk Alignment	Data owners ensure that data is identified and inventoried and any changes to the data landscape are automatically detected and included within the catalog. The data landscape must then be reviewed to identify potential risks related to data loss, attack, or any other unauthorized alteration and/or access	Data owners ensure that data is identified and inventoried and any changes to the data landscape are automatically detected and included within the catalog. The data landscape must then be reviewed to identify potential risks related to data loss, attack, or any other unauthorized alteration and/or access	Data assets are known and can therefore be collected, tagged and protected according to risk levels in alignment with a prioritization framework, and encrypted for protection.	Falcon Data Protection
4.2	DoD Enterprise Data Governance	DoD establishes enterprise data labeling/tagging and DAAS access control/sharing policies (e.g., SDS policy) that are enforceable. Developed enterprise standards ensure an appropriate level of interoperability between DoD Organizations.	DoD establishes enterprise data labeling/tagging and DAAS access control/sharing policies (e.g., SDS policy) that are enforceable at the field level	Decision rights and the accountability framework ensure appropriate behavior in the valuation, creation, consumption and control of data and analytics.	Falcon Data Protection DoD Process/Policy
4.3	Data Labeling and Tagging	Data owners label and tag data in compliance with DoD enterprise governance on labeling/tagging policy. As phases advance automation is used to meet scaling demands and provide better accuracy.	Data owners label and tag data in compliance with DoD enterprise governance on labeling/tagging policy	Establishing machine-enforceable data access controls, risk assessment and situational awareness require consistently and correctly labeled and tagged data.	Falcon Data Protection Falcon Next-Gen SIEM
4.4	Data Monitoring and Sensing	Data owners will capture active metadata that includes information about the access, sharing, transformation, and use of their data assets. Data Loss Prevention (DLP) and Data Rights Management (DRM) enforcement point analysis is conducted to determine where tooling will be deployed. Data outside of DLP and DRM scope such as File Shares and Databases is actively monitored for anomalous and malicious activity using alternative tooling.	Data owners will capture active metadata that includes information about the access, sharing, transformation, and use of their data assets	Data in all states is detectable and observable.	Falcon Cloud Security

4.5	Data Encryption and Rights Management	DoD organizations establish and implement a strategy for encrypting data at rest and in transit using Data Rights Management (DRM) tooling. The DRM solution utilizes data tags to determine protection and lastly integrates with ML and AI to automate protection	DoD organizations establish and implement a strategy for encrypting data at rest and in transit	Encrypting data in all states reduces the risk of unauthorized data access and improves data security.	Does Not Meet
4.6	Data Loss Prevention (DLP)	DoD organizations utilize the identified enforcement points to deploy approved DLP tools and integrate tagged data attributes with DLP. Initially the DLP solution is put into a "monitor-only" mode to limit business impact and later using analytics is put into a "prevent" mode. Extended data tag attributes are used to feed the DLP solution and lastly integrate with ML and AI.	DoD organizations have identified enforcement points, deployed approved DLP tools at those enforcement points, and integrate tagged data attributes with DLP	Data breaches and data exfiltration transmissions are detected and mitigated.	Falcon Data Protection
4.7	Data Access Control	DoD organizations ensure appropriate access to and use of data based on the data and user/NPE/device properties. Software Defined Storage (SDS) is utilized to scale manage permissions to DAAS. Lastly the SDS solution(s) is integrated with DRM tooling improving protections.	DoD organizations ensure appropriate access to and use of data based on the data and user/NPE/device properties	Unauthorized entities — or any entity on an unauthorized device — cannot access data. Zero Trust cybersecurity will be sufficiently strong to separate community of interest data access for data in the same classification.	Falcon Cloud Security

5. Network and Environment Pillar Capabilities

ID #	Capability	Capability Description	Capability Outcome	Impact to Zero Trust	CrowdStrike Product Mapping
5.1	Data Flow Mapping	DoD organizations reconcile data flows by gathering, mapping, and visualizing network traffic data flows and patterns to ensure authorized access and protection for network and DAAS resources specifically tagging programmatic (e.g., API) access when possible.	DoD organizations reconcile data flows by gathering, mapping, and visualizing network traffic data flows and patterns to ensure authorized access and protection for network and DAAS resources	Sets the foundation for network segmentation and tighter access control by understanding data traffic on the network.	DoD Process/Policy
5.2	Software-Defined Networking (SDN)	DoD organizations define API decision points and implement SDN programmable infrastructure to separate the control and data planes and centrally manage and control the elements in the data plane. Integrations are conducted with decision points and segmentation gateway to accomplish the plane separation. Analytics are then integrated to real time decision making for access to resources.	DoD organizations define API decision points and implement SDN programmable infrastructure to separate the control and data planes and centrally manage and control the elements in the data plane	Allows the control of packets to a centralized server, provides additional visibility into the network and enables integration.	Falcon Platform Integrations Falcon Identity Protection Falcon Insight XDR Falcon Next-Gen SIEM
5.3	Macrosegmentation	DoD organizations establish network boundaries and provide security against networked assets located within an environment by validating the device, user, or NPE on each attempt of accessing a remote resource prior to connection.	DoD organizations establish network perimeters and provide security against devices located within an environment by validating the device, user, or NPE on each attempt of accessing a remote resource prior to connection	Network segmentation is defined by a large perimeter to enable resource segmentation by function and user type.	Falcon Platform Integrations Falcon Identity Protection Falcon Insight XDR Falcon Firewall Management
5.4	Micro Segmentation	DoD organizations define and document network segmentation based on identity and/or application access in their virtualized and/or cloud environments. Automation is used to apply policy changes through programmatic (e.g., API) approaches. Lastly where possible organizations will utilize host-level process micro segmentation	DoD organizations define and document network segmentation based on identity and/or application access in their virtualized cloud environments	Network segmentation is narrower and specific segmentation in a virtualized environment via identity and/or application access, allowing for improved protection of data in transit as it crosses system boundaries (e.g., in a coalition environment, system high boundaries) and supported dynamic, real-time access decisions and policy changes.	Falcon Platform Integrations Falcon Identity Protection Falcon Insight XDR Falcon Firewall Management Falcon Next-Gen SIEM

6. Automation and Orchestration Pillar Capabilities

ID #	Capability	Capability Description	Capability Outcome	Impact to Zero Trust	CrowdStrike Product Mapping
6.1	Policy Decision Point (PDP) and Policy Orchestration	Data owners label and tag data in DoD organizations initially collect and document all rule based policies to orchestrate across the security stack for effective automation; DAAS access procedures and policies will be defined, implemented, and updated. Organizations mature this capability by establishing PDPs and PEPs (including the Next Generation Firewall) to make DAAS resource determinations and enable, monitor, and terminate connections between a user/device and DAAS resources according to predefined policy.	DoD organizations initially collect and document all rule based policies to orchestrate across the security stack for effective automation; DAAS access procedures and policies will be defined, implemented, and updated. Organizations mature this capability by establishing PDPs and PEPs (including the Next Generation Firewall) to make DAAS resource determinations and enable, monitor, and terminate connections between a user/device and DAAS resources according to predefined policy	PDPs and PEPs ensure proper implementation of DAAS access policies to users or endpoints that are properly connected (or denied access) to requested resources.	Falcon for IT Falcon Next-Gen SIEM Falcon Insight XDR Falcon Identity Protection Falcon Exposure Management
6.2	Critical Process Automation	DoD organizations employ automation methods, such as RPA, to address repetitive, predictable tasks for critical functions such as data enrichment, security controls, and incident response workflows according to system security engineering principles.	DoD organizations employ automation methods, such as RPA, to address repetitive, predictable tasks for critical functions such as data enrichment, security controls, and incident response workflows according to system security engineering principles	Response time and capability is increased with orchestrated workflows and risk management processes.	Falcon Fusion SOAR Falcon Next-Gen SIEM Falcon for IT Falcon Insight XDR
6.3	Machine Learning	DoD organizations employ ML to execute (and enhance execution of) critical functions such as incident response, anomaly detection, user baselining, and data tagging.	DoD organizations employ ML to execute (and enhance execution of) critical functions such as incident response, anomaly detection, user baselining, and data tagging	Response time and capability is increased with orchestrated workflows and risk management processes.	Does Not Meet
6.4	Artificial Intelligence	DoD organizations employ AI to execute (and enhance execution of) critical functions - particularly risk and access determinations and environmental analysis	DoD organizations employ AI to execute (and enhance execution of) critical functions - particularly risk and access determinations and environmental analysis	Response time and capability is increased with orchestrated workflows and risk management processes.	Falcon Insight XDR Falcon Identity Protection Falcon Next-Gen AV

6.5	Security Orchestration, Automation and Response (SOAR)	DoD organizations achieve initial operational capability of security technologies to orchestrate and automate policies (e.g., PEPs and PDPs) and rulesets to improve security operations, threat and vulnerability management, and security incident response by ingesting alert data, triggering playbooks for automated response and remediation.	DoD organizations achieve IOC of security technologies to orchestrate and automate policies (e.g., PEPs and PDPs) and rulesets to improve security operations, threat and vulnerability management, and security incident response by ingesting alert data, triggering playbooks for automated response and remediation	Predefined playbooks for everything from collection and incident response to triage enable initial process automation that accelerates a security team's decision and response speed.	Falcon Fusion SOAR
6.6	API Standardization	DoD establishes and enforces enterprise-wide programmatic interface (e.g., API) standards; all non-compliant APIs are identified and replaced.	DoD establishes and enforces enterprise-wide API standards; all non-compliant APIs are identified and replaced	Standardizing APIs across the department improves application interfaces, enabling orchestration and enhancing interoperability.	DoD Process/ Policy
6.7	Security Operations Center and Incident Response	In the event a computer network defense service provider (CNDSP) does not exist, DoD organizations define and stand up security operations centers (SOC) to deploy, operate, and maintain security monitoring, protections and response for DAAS; SOC's provide security management visibility for status (upward visibility) and tactical implementation (downward visibility). Workflows within the SOC are automated using automation tooling and enrichment occurs between service providers and technologies.	In the event a CNDSP does not exist, DoD organizations define and stand up SOC's to deploy, operate, and maintain security monitoring, protections and response for DAAS; SOC's provide security management visibility for status (upward visibility) and tactical implementation (downward visibility)	Organizations will have standardized, coordinated and accelerated incident response and investigative efforts.	Falcon Identity Protection Falcon Cloud Security Falcon Exposure Management Falcon Insight XDR Falcon Next- Gen SIEM Falcon for IT Falcon Prevent Falcon Firewall Management Falcon Device Control Falcon FileVantage Falcon Discover Falcon for Mobile Falcon Fusion SOAR

7. Visibility and Analytics Pillar Capabilities

ID #	Capability	Capability Description	Capability Outcome	Impact to Zero Trust	CrowdStrike Product Mapping
7.1	Log All Traffic (Network, Data, Apps, Users)	DoD organizations collect and process all logs including network, data, application, device, and user logs and make those logs available to the appropriate Computer Network Defense Service Provider (CNDSP) or security operations center (SOC). Logs and events follow a standardized format and rules/analytics are developed as needed.	DoD organizations collect and process all logs including network, data, application, device, and user logs and make those logs available to the appropriate Computer Network Defense Service Provider (CNDSP) or SOC	All traffic is logged, which is foundational to the development of automated threat hunting and incident response playbooks	Falcon Exposure Management/ Falcon for XIoT Falcon Identity Protection Falcon Next-Gen SIEM Falcon for IT
7.2	Security Information and Event Management	Computer Network Defense Service Provider (CNDSP) or security operations centers (SOC) monitor, detect, and analyze data logged into a security information and event management (SIEM) tool. User and device baselines are created using security controls and integrated with the SIEM. Alerting within the SIEM is matured over the phases to support more advanced data points (e.g., Cyber Threat Intel, Baselines, etc.)	CNDSPs/SOCs monitor, detect, and analyze data logged into a security information and event management (SIEM) tool	Processing and exploiting data in the SIEM solution enables effective security analysis of anomalous user behavior as well as alerting and automated incident response to common threat events.	Falcon Next-Gen SIEM Falcon Identity Protection
7.3	Common Security and Risk Analytics	Computer Network Defense Service Provider (CNDSP) or security operations centers (SOC) employ data tools across their enterprises for multiple data types to unify data collection and examine events, activities, and behaviors.	CNDSPs/SOCs employ big data tools across their enterprises for multiple data types to unify data collection and examine events, activities, and behaviors	Analysis is integrated across multiple data types to examine events, activities and behaviors.	Falcon Identity Protection
7.4	User and Entity Behavior Analytics	DoD organizations initially employ analytics to profile and baseline activity of users and entities and to correlate user activities and behaviors and detect anomalies. Computer Network Defense Service Provider (CNDSP) or security operations centers (SOC) mature this capability through the employment of advanced analytics to profile and baseline activity of users and entities and to correlate user activities and behaviors, and detect anomalies.	DoD organizations initially employ analytics to profile and baseline activity of users and entities and to correlate user activities and behaviors, and detect anomalies. CNDSPs/SOCs mature this capability through the employment of advanced analytics to profile and baseline activity of users and entities and to correlate user activities and behaviors, and detect anomalies	Advanced analytics support detection of anomalous users, devices, NPE actions and advanced threats.	Falcon Identity Protection Falcon Prevent Falcon Insight XDR

7.5	Threat Intelligence Integration	Computer Network Defense Service Provider (CNDSP) or security operations centers (SOC) integrate threat intelligence information and streams about identities, motivations, characteristics, and tactics, techniques and procedures (TTPs) with data collected in the SIEM.	CNDSPs/SOCs integrate threat intelligence information and streams about identities, motivations, characteristics, and tactics, techniques and procedures (TTPs) with data collected in the SIEM	Integrating threat intelligence into other SIEM data enhances monitoring efforts and incident response.	CrowdStrike Counter Adversary Operations Falcon Adversary Intelligence
7.6	Automated Dynamic Policies	DoD organizations define API DoD Organization ML & AI solutions dynamically and automatically update security profiles and device configuration through continuous security posture monitoring, risk and confidence scoring, and automated patch management.	CNDSPs/SOCs dynamically and automatically update security profiles and device configuration through continuous security posture monitoring, risk and confidence scoring, and automated patch management	Users and NPEs are denied access based on automated, real-time security profiles. These profiles are based on external conditions and evolving risk and confidence scores.	Falcon Identity Protection Falcon Insight XDR Falcon Next-Gen SIEM Falcon Fusion SOAR

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: <https://www.crowdstrike.com/>

Follow us: [Blog](#) | [X](#) | [LinkedIn](#) | [Facebook](#) | [Instagram](#)

Start a free trial today: <https://www.crowdstrike.com/free-trial-guide/>