

CrowdStrike Solutions for Public Sector

The CrowdStrike Falcon Platform Approach to Strengthen CISA and DoW Zero Trust Maturity

High-profile cyber incidents targeting the United States' critical infrastructure — such as the [MOVEit ransomware attack in 2023](#), the [February 2024 ransomware assault on U.S. water treatment facilities](#), and [state-sponsored malicious activity in July 2024](#) — underscore the pressing need for robust and proactive cybersecurity measures to protect against evolving threats.

The Office of the National Cyber Director (2024) released the 2024 Report on the Cybersecurity Posture of the United States, which identified five key trends driving change within Public Sector environments. These trends require ongoing vigilance and strategic adaptation to ensure a robust cybersecurity posture.

- 1. Evolving Risks to Critical Infrastructure:** Nation-state adversaries increasingly targeted critical infrastructure systems, even those without clear espionage value, to advance their broader strategic goals.
- 2. Ransomware:** Ransomware remained a significant danger to national security, public safety, and economic prosperity. Ransomware groups continually developed sophisticated methods to evade defensive and disruptive countermeasures.
- 3. Supply Chain Exploitation:** Complex, interconnected software and IT service supply chains enabled malicious actors to compromise multiple victims simultaneously, exploiting these intricate networks.
- 4. Commercial Spyware:** A growing market emerged for advanced cyber-surveillance tools, sold by private vendors to nation-states. These tools could remotely access devices, extract content, and manipulate components without user awareness.
- 5. Artificial Intelligence:** AI, one of the most powerful and accessible technologies of our time, continued to evolve. This evolution presented both opportunities and challenges for large-scale cyber risk management.

(Office of the National Cyber Director, 2024)

To defend against today's sophisticated cyberattackers, agencies must strengthen their cybersecurity programs across these seven critical areas:

- **Securing Endpoints, Identities, and Workloads:** Integrate identity, endpoint, and workload security to detect and stop modern identity-based attacks in real time. Leverage advanced threat prevention to safeguard user accounts, ensuring seamless protection across your environment without compromising efficiency.
- **Advanced Threat Detection and Analytics:** Utilize advanced analytics and threat intelligence to identify malicious activity and streamline incident response.
- **Comprehensive Visibility and Response:** Ensure real-time monitoring and proactive management of endpoints, networks, and systems to detect and respond to threats efficiently.
- **XIoT Security:** Implement comprehensive visibility and protection for operational technology (OT), Internet of Things (IoT), SCADA, Internet of Medical Things (IoMT), industrial control systems (ICS), and building management systems (BMS), collectively known as the Extended Internet of Things (XIoT). Discover all of your XIoT assets, protect against malware, ransomware, and identity-based attacks, and manage vulnerabilities without disrupting operations.
- **Cloud Security:** Leverage at-scale visibility, runtime protection, workload vulnerability management, and posture monitoring to secure cloud workloads, applications, and services. Integrate security into the DevOps lifecycle to detect and mitigate threats during development, ensuring comprehensive protection without hindering innovation.
- **Data Protection and Compliance:** Secure sensitive information by enforcing access controls, monitoring data movement, and supporting compliance with regulatory standards.
- **Zero Trust Alignment:** Implement a security model that enables verification and validation for every user, device, application, and access request, with a focus on least-privilege access principles.

The CrowdStrike Falcon® platform empowers organizations to secure critical assets with centralized capabilities for real-time visibility, threat detection, and control across endpoints, cloud workloads, and IT infrastructure, all while supporting compliance with enterprise standards. Its lightweight, cloud-native architecture delivers unparalleled protection, rapid deployment, and instant actionable insights to enhance operational efficiency.

Purpose-built in the cloud with a single lightweight-agent architecture, the CrowdStrike Falcon platform enables customers to benefit from rapid and scalable deployment, reduced complexity, and immediate time-to-value.

Meeting Federal Standards

Establishing Zero Trust controls can help meet standards and use cases such as:

- DoD Zero Trust Reference Architecture
- CISA Zero Trust Maturity Model
- Trusted Internet Connection (TIC) 3.0
- FedRAMP
- Federal Information Security Management Act (FISMA)
- Cybersecurity Maturity Model Certification (CMMC)
- Enterprise Security Solution (ESS)
- Comply-to-Connect (C2C)

Building Resilient Cybersecurity for Modern Threat Landscapes

How do highly complex, critical environments build resiliency against today's sophisticated cyber threats? With comprehensive, real-time visibility and proactive management across all systems and environments, organizations can detect and respond to emerging risks rapidly. Advanced cloud security solutions, including runtime protection, workload vulnerability management, and posture monitoring, safeguard critical assets and address vulnerabilities effectively. These measures strengthen an organization's defenses, ensuring that threats are mitigated before they can disrupt operations.

Resiliency is further enhanced by adopting a Zero Trust architecture that dynamically validates every user, device, and application to enforce least-privilege access and minimize attack surfaces. Unified platforms like CrowdStrike Falcon provide centralized capabilities to manage endpoint security, identity protection, and data governance, while integrated threat intelligence enables real-time policy enforcement and adaptive controls. Together, these strategies allow organizations to maintain a resilient, adaptive security posture, meeting the demands of today's complex threat landscape while ensuring operational agility and supporting compliance.

CrowdStrike Falcon Identity Protection

CrowdStrike Falcon® Identity Protection redefines identity security by providing continuous monitoring, real-time threat detection, and advanced analytics to defend against identity-based attacks. By enhancing visibility into user accounts and privileges, it proactively safeguards against credential theft, lateral movement, and privilege escalation. With features such as risk-based authentication and conditional access enforcement, Falcon Identity Protection empowers organizations to strengthen identity security without adding complexity to their security operations. Its seamless integration with existing environments ensures that your security remains agile and adaptive to evolving threats.

Falcon Identity Protection is a key component of the CrowdStrike platform, working in unison with solutions like CrowdStrike Falcon® Insight XDR and CrowdStrike Falcon® Fusion SOAR. This deep integration enables security teams to detect, investigate, and respond to identity threats more effectively, all from a single console and agent. By unifying identity protection with endpoint protection, Falcon Identity Protection simplifies operations and accelerates threat response, making it an essential tool for modern enterprises striving to secure their most critical assets: their identities.

Greater ROI from Security Tools

CrowdStrike enables customers to realize increased ROI from other security solutions by consuming data from them and fusing it with raw CrowdStrike threat intelligence to detect IOAs across solutions.

CrowdStrike Falcon Next-Gen SIEM

CrowdStrike Falcon® Next-Gen SIEM transforms security operations by delivering index-free data ingestion, real-time search, and advanced analytics for accelerated threat detection and response. Built to unify and correlate data across diverse sources, Falcon Next-Gen SIEM empowers security teams with full visibility to detect complex threats at scale. With automated workflows and seamless integration into existing environments, Falcon Next-Gen SIEM reduces operational complexity and enhances the speed and efficiency of security operations, making it an essential solution for modern threat landscapes.

Falcon Next-Gen SIEM offers exceptional performance, scalability, and user-friendly interfaces, with deeper integration into other CrowdStrike products such as CrowdStrike Falcon® Adversary Intelligence, Falcon Insight XDR, Falcon Identity Protection, and Falcon Fusion SOAR. All of these capabilities are available on one platform and accessible from one user console, providing a seamless experience for security teams.

CrowdStrike Falcon for IT

CrowdStrike Falcon® for IT unifies IT and security operations by providing real-time visibility across all endpoints, enabling teams to efficiently manage assets, monitor compliance standards, and implement automation at scale. By leveraging native support for osquery, Falcon for IT empowers enterprise teams to perform precise, environment-wide queries, extract actionable insights in real time, and execute tasks at scale.

The platform streamlines the management of complex device fleets and compliance monitoring, proactively addressing vulnerabilities and fortifying endpoint security. Its robust architecture supports granular control and advanced automation, reducing operational complexity and enabling rapid responses to emerging threats and infrastructure challenges. Seamless integration with existing systems ensures Falcon for IT aligns IT and security workflows to foster collaboration and operational efficiency.

Whether managing a sprawling fleet of devices, helping to meet compliance requirements across endpoints, or addressing vulnerabilities, Falcon for IT equips organizations with the technical precision and scalability necessary to automate repetitive processes, maintain a hardened security posture, and confidently operate in dynamic, critical environments.

CrowdStrike Falcon for XIoT

CrowdStrike Falcon® for XIoT enhances operational technology protection by providing comprehensive visibility and protection across all XIoT assets. By unifying device discovery, classification, and vulnerability assessment, and endpoint and identity protection, it enables organizations to identify and mitigate risks swiftly, ensuring robust security measures throughout their connected IT and XIoT infrastructure. Its non-disruptive approach simplifies XIoT security management, allowing teams to secure critical operational assets without impacting productivity or requiring additional infrastructure deployment.

CrowdStrike Falcon Cloud Security

CrowdStrike Falcon® Cloud Security elevates cloud protection by delivering comprehensive visibility and real-time threat detection across all cloud workloads, containers, and Kubernetes environments. By unifying security posture management and workload protection, Falcon Cloud Security enables organizations to detect and respond to threats swiftly, ensuring robust defense mechanisms are in place throughout the cloud infrastructure.

With seamless integration into existing cloud platforms, Falcon Cloud Security facilitates the identification of vulnerabilities and misconfigurations, providing actionable insights to help maintain compliance and enhance security posture. The unified Falcon platform simplifies cloud security management, allowing security teams to focus on strategic initiatives while ensuring continuous protection against evolving cyber threats.

CrowdStrike Falcon Data Protection

CrowdStrike Falcon® Data Protection redefines data security by integrating advanced data loss prevention (DLP) capabilities into the Falcon platform to safeguard sensitive information. By leveraging deep content inspection and contextual analysis, it monitors and secures data across endpoints and USB devices in real time. Falcon Data Protection helps ensure organizations can detect unauthorized data exfiltration, prevent accidental data leakage, and support compliance with regulatory standards, all from a single unified platform.

Built on CrowdStrike's lightweight agent and centralized management architecture, Falcon Data Protection simplifies deployment and operational oversight. It integrates seamlessly with existing security infrastructures, enabling organizations to scale protection across thousands of endpoints without disrupting productivity. With automated policy enforcement, real-time alerts, and actionable insights, Falcon Data Protection empowers security teams to safeguard critical information assets, address data breaches proactively, and navigate today's evolving compliance and threat landscapes with confidence.

Enforce Zero Trust with Advanced Security Architecture

Zero Trust is a modern cybersecurity framework that assumes no implicit trust for users or devices, whether inside or outside the network. Instead, it requires continuous validation of every access request based on user identity, device health, and context to ensure only authorized entities can interact with critical resources. By implementing Zero Trust principles, organizations can reduce the attack surface, prevent lateral movement, and mitigate risks associated with compromised credentials or unauthorized access ([NIST.gov](https://nist.gov)).

The CrowdStrike Falcon platform empowers organizations to achieve both Target and Advanced level outcomes of the DoD Zero Trust Reference Architecture as well as optimal and advanced maturity levels prescribed by the CISA Zero Trust Maturity Model during its implementation of Zero Trust strategies. Zero Trust implementation is delivered through a unified solution that integrates advanced endpoint, identity, workload, and application protection. By correlating telemetry across endpoints, networks, identities, and cloud environments, Falcon provides real-time visibility, continuous risk assessments, and adaptive, context-aware access controls. Modules like Falcon Identity Protection and Falcon Insight XDR enable the proactive mitigation of credential-based attacks, prevention of lateral movement, and enforcement of dynamic least-privilege access policies. Together with other CrowdStrike capabilities supporting Zero Trust across devices, users, cloud, and applications — and leveraging over 400 integrations — the Falcon platform equips organizations with the tools needed to achieve Zero Trust architectures, ensuring comprehensive and resilient protection for critical assets in today's rapidly evolving threat landscape.

CrowdStrike Helps Federal Agencies and the DoD Overcome Constraints

Actions you can take today include ensuring real-time visibility and control, advanced threat detection and analysis, and data protection and compliance; enforcing Zero Trust; and leveraging and sharing threat intelligence. But federal agencies also must work within a number of constraints, including cost, ease of deployment, regulatory compliance, and purchasing and logistics complexities.

Powered by the CrowdStrike Security Cloud and world-class intelligence, the CrowdStrike Falcon platform leverages real-time indicators of attack (IOAs), threat intelligence, knowledge about evolving adversary tradecraft, and enriched telemetry from across the entire agency infrastructure.

- **Fully operational in seconds:** CrowdStrike's design enables the industry's fastest deployment and instant operationalization. Only CrowdStrike enables customers to deploy tens of thousands of agents at once with no reboots needed to install or change security settings. CrowdStrike eliminates the need for signatures, fine-tuning, and costly infrastructure for faster time-to-value.
- **Near-zero impact on the endpoints:** The Falcon platform provides full, automated protection across endpoints without impacting endpoint performance and end-user productivity, from initial deployment through ongoing day-to-day use.
- **No large upfront acquisition or deployment costs:** Capabilities are subscription-based, with no on-premises controllers to be installed or configured.
- **Extends your ROI in existing security solutions:** CrowdStrike integrates with security solutions essential to federal agencies.

CrowdStrike Falcon® on GovCloud provides the industry's first cloud-delivered endpoint security and IT hygiene solution. Each component is tailored for securing the U.S. public sector, is FedRAMP and DoD IL5 authorized, and is delivered from AWS GovCloud (U.S.). Falcon on GovCloud enables customers to prevent modern attacks and significantly reduces the cost of operating security infrastructure.

Falcon on GovCloud meets these federal agency needs:

- FedRAMP High Authorized
- Achieved Impact Level 5
- CSA STAR compliance
- SOC2 compliance
- NIST compliance

Partnership with CrowdStrike ensures you have access to the expertise and knowledge you need:

- Access to expert threat hunters, minimizing the need to hire full-time staff
- The option for fully managed protection and remediation
- Through the CrowdStrike Security Cloud, access to threat intelligence from public agencies and the private sector as well as crowd-sourced intelligence from a large customer base

CrowdStrike meets the following compliance requirements:

- U.S. FedRAMP High Authorization
- Department of Defense Impact Level 5 (IL-5) Authorization
- Criminal Justice Information Services (CJIS) EU-U.S. and Swiss-U.S. Privacy Shield Frameworks
- Service Organization Control 2 (SOC 2)

In addition to being an endpoint protection platform, the CrowdStrike Falcon platform:

- Supports customer compliance needs pertaining to NIST 800-171
- Provides **coverage for** Level 2 of the Cybersecurity Maturity Model Certification (CMMC) 2.0
- Addresses the system protection and monitoring controls identified in NIST SP 800-53
- Enables agencies to meet the requirements of the Federal Financial Institutions Examination Council (FFIEC)
- Helps agencies comply with the Health Insurance Portability and Accountability Act (HIPAA)
- Is one of only 12 organizations accredited by the National Security Agency for National Security Cyber Assistance Program (NSCAP) Cyber Incident Response Assistance (CIRA)

For ease of purchasing, CrowdStrike federal agency customers can access CrowdStrike solutions through a variety of Government-Wide Acquisition Vehicles (GWACs), Blanket Purchase Agreements (BPAs), Indefinite Delivery Indefinite Quantity Contracts (IDIQ), the AWS Enterprise Discount Program (EDP) and Federal Supply Schedules (FSS). Below are a few highlights:

- **GSA Schedule 70**
- **National Aeronautics and Space Administration (NASA) Solutions for Enterprise-Wide Procurement (SEWP)**
- **Department of Defense (DoD) Enterprise Software Initiative (ESI)**
- **Chief Information Officer-Commodities and Solutions (CIO-CS)**
- **Continuous Diagnostics and Mitigation (CDM) Approved Product List (APL)**
- **AWS Marketplace**

Want to learn more?

Visit: <https://www.crowdstrike.com/public-sector/federal-government>

Resources

[FedRAMP Marketplace - CrowdStrike Falcon Platform for Government](#)

[CrowdStrike Provides Target and Advanced DoD Zero Trust Activities](#)

[CrowdStrike Falcon Identity Protection](#)

[CrowdStrike Falcon Next-Gen SIEM](#)

[CrowdStrike Falcon for IT Data Sheet](#)

[CrowdStrike Falcon Cloud Security](#)

[CrowdStrike Falcon Data Protection Data Sheet](#)

[CrowdStrike Falcon Platform for CMMC 2.0](#)

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/>