CROWDSTRIKE

CROWDSTRIKE FALCON FOR THE PUBLIC SECTOR

Secure your most critical areas of enterprise risk to stay ahead of today's threats and stop breaches

YESTERDAY'S SOLUTIONS CAN'T SOLVE TOMORROW'S PROBLEMS

Despite regulatory and administrative requirements, the public sector continues to be attacked and exploited by sophisticated threat actors. The fragmentation of security resources leaves federal, state and local agencies constantly fighting fires throughout their organizations. Unfortunately, this reactive approach to threat detection and prevention leaves organizations exposed, particularly once adversaries breach your agency's outer defenses. While agencies are retaining more critical and sensitive information than ever before, vulnerable legacy security solutions are still widely employed in public sector organizations, applying yesterday's solutions to tomorrow's problems.

The existence of these legacy security solutions, combined with a massive human capital deficit, has exposed the public sector as a particularly attractive target for threat actors. Highly resourceful adversaries — often nation-state sponsored or affiliated and equipped with an arsenal of advanced tactics, techniques, and procedures (TTPs) — continue to overwhelm security teams that are already pushed to the brink. As a result, bad actors continuously slip through agency infrastructure cracks, resulting in dwell times averaging well over a year.

To counter this trend, federal, state, and local governments have increasingly mandated that public sector organizations modernize their IT infrastructure, as well as their overall approach to cybersecurity risk management. Although this push will greatly enhance protection measures, evolving this framework and protecting against vulnerabilities remains a daunting task.

KEY BENEFITS

Fulfill compliance requirements for your agency

Stop breaches and keep your data safe with a light-weight, cloud-native, unified solution

Ensure comprehensive coverage of your organization with a solution that scales with you

NEXT-GENERATION ENDPOINT PROTECTION FOR THE PUBLIC SECTOR

The nature of cybersecurity problems facing the public sector has changed radically, but the solutions in place to solve these problems have not. Standard security providers still rely on outdated architecture models, while myopically focusing on stopping malware alone. Yet,

the problem is no longer just about malware. In fact, malware is only responsible for five out of every 10 attacks. What about the other 50 percent? This is where adversaries leverage TTPs that move beyond malware — such as exploiting features of a legitimate application or operating system. Adversaries are extremely skilled, well-funded, and relentless, able to outsmart and bypass malware-based defenses. Clearly, a new approach is needed — one that not only addresses malware more effectively, but goes a step beyond to stop fileless, malware-free attacks.

To To stop advanced attacks and address adversaries' evolving tradecraft, CrowdStrike is focused on the most critical areas of enterprise risk and friction: endpoints and cloud workloads, identities and data. Protecting these assets is critical because they are distributed and serve as users' interface to the local environment. Endpoints and cloud workloads also frequently store sensitive data and historically have been difficult to secure. Once Once a breach occurs, be it through an endpoint, workload or identity, adversaries can move laterally within your network with relative ease, quietly exfiltrating your valuable data and compromising your intellectual property for months, sometimes years, without fear of detection. This is critical for an industry where dwell times average over a year.

CrowdStrike has redefined security with the world's most advanced cloud-native platform that protects and enables the people, processes and technologies that drive modern enterprise.

Powered by the CrowdStrike Security Cloud, 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, customers benefit from unmatched scalability, superior protection and performance, reduced complexity and immediate time-to-value.

ENABLING NEXT GENERATION PROTECTION WITH CROWDSTRIKE

REGULATORY COMPLIANCE

CHALLENGE

Compliance is the foundation for accountability as the public sector looks to modernize its security strategy . Organizational requirements vary based on agency scope and focus, and your organization has new obligations that you must meet in order to safeguard your stakeholders.

SOLUTION

CrowdStrike satisfies compliance requirements across several focus areas for the public sector:

- CrowdStrike Falcon on GovCloud is FedRAMP authorized, Impact Level Moderate
- CrowdStrike Falcon is approved to deliver critical cyber capabilities in support of the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation Program (CDM).
- CrowdStrike Falcon ® is the ideal solution for addressing the system protection and monitoring controls in NIST 800-53 Rev. 4.
- The Falcon platform helps healthcare organizations achieve HIPAA compliance.
- CrowdStrike meets all elements of PCI DSS v 3.2 requirement 5, and provides assistance with meeting four additional requirements.

BENEFIT

CrowdStrike provides a solution that assists with meeting the compliance requirements of public sector organizations of all sizes.

PROACTIVELY STOP INFILTRATORS WITH CROWDSTRIKE SERVICES

Breaches are not a hypothetical threat to the public sector, they are a harsh reality. Agencies are constantly under attack as adversaries seek to exfiltrate sensitive material. Breaches like that of the Office of Personnel Management in 2015, left millions of stakeholders' most sensitive information exposed, leading to far-reaching national security implications and serious political consequences. While investments in security tools and infrastructure are critical, their value cannot be fully realized without a security plan, including policies and procedures that have been vetted and tested before an attempted intrusion occurs.

CrowdStrike Services has helped identify and remediate intrusions against some of our most high-profile political organizations as well as key members of the Defense Industrial Base. The CrowdStrike Security Cloud correlates trillions of security events per day with indicators of attack, the industry's leading threat intelligence and enterprise telemetry from across customer endpoints, workloads, identities, DevOps, IT assets and configurations.

Using cloud-scale AI and machine learning, the CrowdStrike Security Cloud creates actionable data, identifies shifts in adversarial tactics, and maps tradecraft in the patented Threat Graph to automatically prevent threats in real time across CrowdStrike's global customer base.

CrowdStrike's five key services offerings help your agency stay one step ahead of sophisticated adversaries:

COMPROMISE ASSESSMENT: This identifies whether outside attackers have previously or currently breached your network, and if so, who they are and what they have accessed.

NEXT-GENERATION PENETRATION TESTING: The CrowdStrike Red Team emulates attackers that are relevant to your organization. Using the actual TTPs employed by the adversaries most likely to target you, CrowdStrike conducts a simulated attack and mock-compromises your organization, before providing recommendations on how you can improve your security.

PROGRAM DEVELOPMENT: The Service team's expertise allows them to guide change in each of three crucial areas: general information security, incident response planning, response and security operations center (SOC) development. Regardless of your organization's level of maturity, CrowdStrike develops a roadmap to make sure you continue to improve over time.

TABLETOP EXERCISES: These are designed to provide realistic, scenario-based training opportunities that identify gaps in cybersecurity and incident response processes. Tabletop exercises are also a highly valuable internal training tool.

COUNTER THREAT ASSESSMENT: CrowdStrike provides a highly customized evaluation that identifies the threats and attack groups most likely to negatively impact your organization, allowing you to prioritize investments based on applicable risk.

CrowdStrike's emulation of adversaries shows the creative vectors that these bad actors take in order to disrupt your mission. By leveraging this expertise, you stay one step ahead of the adversaries targeting your organization by proactively addressing gaps in your security posture.

SECURITY

CHALLENGE

Public sector organizations struggle to adequately protect their endpoints against adversaries' advanced techniques and evolviing tradecraft.

SOLUTION

The Falcon Platform is the world's most advanced cloud-native security platform that protects and enables the people, processes and technologies that drive modern enterprise.

- Falcon blocks known and unknown malware as well as non-malware-based threats.
- Its continuous monitoring of the most critical areas of enterprise risk – endpoints and cloud workloads, identity, and data – allows for rapid detection and response, providing unparalleled protection in today's security landscape.
- Falcon OverWatch™ provides proactive 24x7 managed hunting for adversary activity so operators can detect and block attacks before they can wreak havoc on the enterprise.

BENEFIT

CrowdStrike provides a single, powerful, unified solution that is focused on enabling agencies to stop breaches and keep your data safe.

FALCON FOR THE PUBLIC SECTOR

WHY CROWDSTRIKE

CrowdStrike is redefining security and delivering superior protection and performance with the Falcon platform and world-leading Security Cloud. The threats the public sector faces are constantly evolving and you require a solution that proactively detects and prevents these events from occurring. CrowdStrike has built its solutions around the ability to detect and prevent breaches by even the most sophisticated adversaries. With a platform that seamlessly deploys and scales with your agency and a dedicated team of security professionals, CrowdStrike protects your organization from the most advanced attacks - now and in the future.

ABOUT CROWDSTRIKE

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

Powered by the CrowdStrike Security Cloud, 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 enables customers to benefit from 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 | Twitter | LinkedIn | Facebook | Instagram**

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

DEPLOYMENT

CHALLENGE

As organizations grow and become more distributed, an increasingly broad attack surface is provided for sophisticated adversaries targeting your data and IT infrastructures. The success of such attacks has been well documented in recent years, showing the inherent vulnerabilities in conventional on-premises, network- and malware-centric defenses.

SOLUTION

Crowdstrike protects your agency as you scale by deploying across all IT environments and operating systems:

- With a lightweight agent that deploys in minutes, the Falcon platform ensures comprehensive protection with immediate time-to-value.
- CrowdStrike Falcon deploys across all endpoint and data environments, including on-premises, virtual and cloud-based servers.
- Supplemented by CrowdStrike's rich threat intelligence and managed hunting, the Falcon platform protects, detects, and responds to all threat vectors that impact your mission, from the mundane to the sophisticated.
- Falcon streamlines your operational efficiency with a security solution that requires no new installs, reboots, or scans.

BENEFIT

CrowdStrike provides an industry-leading solution that scales with your IT environment, providing comprehensive threat prevention and detection without impacting system performance.

Start Free Trial
of Next-Gen AV

Learn more at **www.crowdstrike.com**