CROWDSTRIKE

CROWDSTRIKE FALCON™ FOR THE PUBLIC SECTOR

SECURE YOUR ENTERPRISE WITH A SOLUTION THAT PROVIDES UNRIVALED PROTECTION, SECURITY EXPERTISE, AND OPTIMAL SCALABILITY

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 the enterprise. Unfortunately, this reactive approach to threat detection and prevention leaves enterprises 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.The Verizon Data Breach Investigations Report (DBIR) states that after financial and healthcare organizations, the public sector is the third highest breach victim in the United States, with almost 240 reported breaches in 2016 alone. 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

KEY BENEFITS

» Fulfill compliance requirements for your enterprise

» Stop breaches and keep your data safe with a lightweight, unified solution

» Ensure comprehensive enterprise coverage with a solution that scales with you

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.

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 meet the challenge of today's sophisticated adversaries, CrowdStrike focused on revolutionizing endpoint protection by creating an entirely new platform and architecture from the ground up. Protecting endpoints is critical because they are distributed and serve as users' interface to the enterprise environment. They also frequently store sensitive data and historically have been difficult to secure. Once the endpoint is breached, 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.

To reinvent endpoint protection, CrowdStrike became the first and only company to unify five crucial elements: next-generation AV, endpoint detection and response (EDR), IT hygiene, 24/7 managed hunting services, and threat intelligence. This entire platform is uniquely delivered via the cloud in a single integrated solution. This innovative combination of solutions stops breaches by preventing and responding to all attack types — both malware and fileless.

CROWDSTRIKE FALCON — HELPING THE PUBLIC SECTOR MEET TODAY'S CHALLENGES

REGULATORY COMPLIANCE

CHALLENGE

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

SOLUTION

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

- 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 your large-scale industry and enterprise-size organization.

PROACTIVELY STOP INFILTRATORS WITH CROWDSTRIKE SERVICES

Breaches are not a hypothetical threat to the public sector, they are a harsh reality. Enterprises 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. Powered by an elite team of security consultants, Crowdstrike offers a portfolio of proactive services ranging from tactical to strategic. Leveraging the rich intelligence collected from security events across the entire CrowdStrike user base, law enforcement and industry collaboration, and other services engagements, CrowdStrike Services emulate attacker activity to provide high-fidelity, tailored recommendations to improve your security preparedness.

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

COMPROMISE ASSESSMENT — 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 enterprise. 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.

SECURITY

CHALLENGE

Public sector enterprises struggle to adequately protect their endpoints against increasingly sophisticated TTPs employed by adversaries.

SOLUTION

Falcon is designed with your security needs in mind and a solution arsenal to protect against all attack types:

- Falcon blocks known and unknown malware as well as non-malware-based threats.
- Its continuous monitoring of the endpoint allows for rapid detection and response to malicious activity.
- 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 enterprises to stop breaches and keep your data safe.

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.

WHY CROWDSTRIKE

CrowdStrike Falcon provides a cloud-delivered solution that safeguards your organization while satisfying your mission requirements. 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 enterprise and a dedicated team of security professionals, CrowdStrike protects your enterprise with a solution designed to stop the breach and evolve with you.

DEPLOYMENT

CHALLENGE

As enterprises 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 enterprise 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.

ABOUT CROWDSTRIKE

CrowdStrike® is the leader in cloud-delivered next-generation endpoint protection. The CrowdStrike Falcon® platform offers instant visibility and protection across the enterprise and prevents attacks on endpoints on or off the network. CrowdStrike Falcon deploys in minutes to deliver actionable intelligence and real-time protection from Day One. Falcon seamlessly unifies next-generation AV with best-in-class endpoint detection and response, backed by 24/7 managed hunting. Its cloud infrastructure and single-agent architecture take away complexity and add scalability, manageability, and speed. CrowdStrike Falcon protects customers against all cyberattack types, using sophisticated signatureless artificial intelligence/machine learning and indicator of attack (IOA) based threat prevention to stop known and unknown threats in real time. Powered by the CrowdStrike Threat Graph™, Falcon instantly correlates over 60 billion security events from across the globe to immediately prevent and detect threats.

LEARN HOW CROWDSTRIKE STOPS BREACHES:

VISIT WWW.CROWDSTRIKE.COM

Speak to a representative to learn more about how CrowdStrike can help you prepare for and defend against targeted attacks.

1.888.512.8906

PUBLICSECTOR@CROWDSTRIKE.COM

WWW.CROWDSTRIKE.COM