CrowdStrike White Paper

CROWDSTRIKE

CROWDSTRIKE SOLUTIONS FOR FEDERAL AGENCIES

Move forward with endpoint protection, Zero Trust and threat intelligence

Breaches in federal agency cybersecurity — like those caused by the SUNBURST supply chain attack, the Microsoft Exchange breach, the Colonial Pipeline ransomware attack and the Log4Shell zero-day exploit — have been making headlines all too frequently.

Agencies must advance their cybersecurity programs in these three areas at a minimum to protect their agency from today's modern attackers:

- **Endpoint detection and response (EDR).** Federal agencies must be able to continuously evaluate everything that is happening on endpoints to improve threat detection and mitigation of cybersecurity incidents.
- **Zero Trust.** Adopting a Zero Trust approach to cybersecurity — trust nothing, verify everything, anticipate the breach — provides for better security, especially given the accelerated adoption of cloud services.
- **Shared threat intelligence.** Collecting and maintaining information from network and system logs enables the sharing of cybersecurity intelligence for investigation and remediation.

Powered by the CrowdStrike Security Cloud — one of the world's largest unified, threat-centric data fabrics — the CrowdStrike Falcon® platform enables federal agencies to rapidly advance on all three of these fronts by leveraging real-time indicators of attack (IOAs), threat intelligence, knowledge about evolving adversary tradecraft and enriched telemetry across their entire digital estate.

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

STRENGTHEN YOUR ENDPOINT PROTECTION

How do you detect and respond to threats when endpoints are numerous and distributed across on-premises and cloud environments? By adding advanced next-generation antivirus protection, powerful endpoint detection and response, USB device security for device control, and incident response and advisory services to maximize your organization's ability to prepare for and respond to a breach.

CROWDSTRIKE FALCON PREVENT™ NEXT-GENERATION ANTIVIRUS (NGAV)

In protecting endpoints from malware, CrowdStrike offers an advanced antivirus (AV) solution that improves threat identification. CrowdStrike Falcon Prevent, the next-generation antivirus (NGAV) module of the CrowdStrike Falcon platform, combines the most effective prevention technologies with full attack visibility and simplicity. CrowdStrike Falcon Prevent protects against all types of attacks — from known malware signatures to the most sophisticated attacks that involve fileless and zero-day malware, exploitation of known vulnerabilities, encrypted malware or credential theft — all with one solution, even when offline.

CROWDSTRIKE FALCON INSIGHT™ ENDPOINT DETECTION AND RESPONSE (EDR)

CrowdStrike Falcon Insight is the endpoint detection and response (EDR) module of the CrowdStrike Falcon platform. Because the CrowdStrike Falcon platform is purpose-built in the cloud and leverages cloud-scale artificial intelligence (AI), Falcon Insight can offer real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network.

CrowdStrike delivers industry-leading automated detection and remediation to stop threats through continuous, comprehensive endpoint visibility that spans detection, response and forensics. CrowdStrike ensures nothing is missed and potential breaches are stopped.

- **Know exactly what's happening and where.** Continuous monitoring captures endpoint activity, from a threat on a single endpoint to an attack threatening the entire organization.
- **Automatically detect and stop breaches.** CrowdStrike Falcon delivers visibility and in-depth analysis to automatically detect suspicious activity and stop stealthy attacks and breaches.
- **Accelerate security operations.** CrowdStrike allows security teams to spend less time handling alerts so they can investigate and respond to attacks more rapidly.

CROWDSTRIKE FALCON XDR™ EXTENDED DETECTION AND RESPONSE

CrowdStrike Falcon XDR takes CrowdStrike's industry-leading EDR capabilities to the next level, delivering real-time detection and automated response across the entire security stack. Falcon XDR seamlessly ingests data from across the broadest range of third-party data sources — including network security, email security, infrastructure as a service (IaaS), platform as a service (PaaS), software as a service (SaaS) and cloud access security broker (CASB) — and correlates it with industry-leading threat intelligence from the CrowdStrike Security Cloud.

CROWDSTRIKE FALCON USB DEVICE SECURITY

CrowdStrike Falcon USB Device Security™ helps mitigate risks associated with USB devices by providing the visibility and granular control required to enable their safe usage across your organization.

- Gain automatic visibility of USB device usage to monitor how the devices are used in your environment.
- Control device usage by determining precisely which devices are allowed or restricted and the granular level of access granted to each device.
- Implement and manage device control policies with ease, with no additional endpoint software installation or hardware to manage.

CROWDSTRIKE INCIDENT RESPONSE AND ADVISORY SERVICES

CrowdStrike Services delivers a comprehensive suite of **Incident Response and Advisory Services** that help you prepare for an attack, respond to a breach and enhance your cybersecurity practices and controls to maximize your endpoint protection.

- **Incident response, investigation and endpoint recovery** help you understand if a breach has occurred and how to respond and recover from a breach with speed and precision to remediate the threat.
- **Compromise assessments** identify ongoing or past attacker activity in your environment.
- **Cybersecurity maturity assessments** evaluate your organization's security posture in terms of prevention, detection, response, governance, security foundations and threat intelligence.
- **Tabletop and adversary emulation exercises** proactively help train and prepare your organization for when a security incident occurs.
- **Red Team/Blue Team exercises and penetration tests** help your team understand how to identify, stop and prevent a breach resulting from a targeted attack.
- **Cloud security services** help you respond to a breach in your cloud environment, prepare for an advanced attack on your cloud resources and enhance the security posture of your cloud platforms.

ENFORCE ZERO TRUST AS YOU ADOPT CLOUD SERVICES

As federal agencies increasingly adopt cloud services like IaaS, PaaS and SaaS, their attack surface expands exponentially, including the trust relationship between on-premises systems and cloud services.

Agencies are being urged from the top to adopt a Zero Trust model to protect themselves in this increasing dynamic and broadly distributed digital estate. Enforcing Zero Trust means giving only the right people or resources the right kind of access to the right data and services, from the right device, under the right circumstances.[1] Zero Trust should be holistic, applied across the enterprise to devices, identities, data, networks and workloads, both on-premises and in the cloud.

To enable this, the CrowdStrike Security Cloud correlates trillions of security events per day with real-time IOAs, the industry's leading threat intelligence and enterprise telemetry from across customer endpoints, workloads, identities, DevOps, IT assets and configurations.

CrowdStrike's cloud security modules provide adversary-focused Cloud Native Application Protection Platform (CNAPP) capabilities, including cloud security posture management (CSPM) and real-time, continuous evaluation of the security of IaaS, PaaS and SaaS instances across the major cloud service providers. This includes the security of their respective containers and associating continuous integration/continuous delivery (CI/CD) workflows.

---

1 Definition of Zero Trust from **Preventing insider threats, data loss and damage through zero** trust quoted in eBook.

The CrowdStrike Falcon Identity Threat Protection component of the CrowdStrike Falcon platform enables frictionless Zero Trust security with real-time threat prevention and IT policy enforcement using identity, behavioral and risk analytics. CrowdStrike offers Active Directory security visibility with insights and analytics into all account types, and detects identity-based attacks or anomalies by comparing live authentication traffic against baseline behaviors and attack patterns.

- **Spot weaknesses.** CrowdStrike Falcon provides visibility into the service and privileged accounts on your network and cloud, with full credential profiles and discovery of weak authentication across every domain in your organization. Analyze each of them for potential vulnerabilities from stale credentials and weak or stale passwords. Identify weak authentication protocols used in service connections.
- **Identify suspicious behavior.** CrowdStrike Falcon monitors authentication traffic on domain controllers on-premises and in the cloud via API. CrowdStrike Falcon creates a baseline for entities and compares current behavior to identify unusual lateral movement, Golden Ticket attacks, Mimikatz traffic patterns and other related threats. CrowdStrike Falcon can also help you identify escalation of privilege and anomalous service account activity.
- **Reduce time to detect.** CrowdStrike Falcon lets you view live authentication traffic, expediting the finding and resolving of incidents. During authentication, you can see real-time events and potential incidents by rogue users of any type. Falcon offers curated traffic feeds to enrich the "what" of identity protection events with the "who" of credential identification.

In multi-directory environments, CrowdStrike enforces frictionless Zero Trust security with real-time threat prevention and IT policy enforcement using identity, behavioral and risk analytics.

- **Gain actionable insights.** Falcon enables unified visibility and control of user access to applications, resources and identity stores, providing actionable insights into user behavior and risks, and eliminating security blindspots across hybrid environments.
- **Move faster without using logs.** Falcon shortens the mean time to detect and resolve incidents by eliminating the need for complex, error-prone log analysis, improving efficiencies for security operations center (SOC) analysts.
- **Reduce alert fatigue.** False positives create a huge amount of work that can bog down investigations, create alert fatigue and lead to missed alerts. In comparative testing by leading **independent third parties**, CrowdStrike Falcon's automated protection and remediation has been shown to excel in stopping malware and ransomware attacks while minimizing false positives.
- **Enforce Zero Trust security with zero friction.** Falcon lets you put in place consistent risk-based policies to automatically block, allow, audit or step up authentication for every identity, while ensuring a frictionless login experience for genuine users.

MEETING FEDERAL STANDARDS

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

Trusted Internet Connection (TIC) 3.0

FedRAMP

Enterprise Security Solution (ESS)

Comply-to-Connect (C2C)

LEVERAGE AND SHARE THE BEST THREAT INTELLIGENCE

Threat intelligence is data that is collected, processed and analyzed to help security teams understand a threat actor's motives, targets and attack behaviors. Threat intelligence enables agencies to make faster, more informed, data-backed security decisions and change their behavior from reactive to proactive in the fight against threat actors.

Responding to sophisticated attacks requires a mix of automation and human expertise in the form of elite threat hunting, reviewing content and adding context to detections — a mix of art and science that cannot be completely solved by machine learning.

CrowdStrike Threat Graph® is the brains behind the cloud-native CrowdStrike Falcon platform. 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. Threat Graph puts this body of knowledge at the responder's fingertips in real time, empowering responders to understand threats immediately and act decisively.

Threat Graph offers a comprehensive platform for preventing breaches and delivers instant value on Day One, without costly consulting services and with zero maintenance overhead. Threat Graph predicts, investigates and hunts at a fraction of the cost, enabling 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.

Threat Graph maintains a wide range of data for you in the cloud, where it is secure from tampering and data loss. This ensures you are armed with the knowledge you need to effectively understand the current threat landscape.

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 HELPS FEDERAL AGENCIES OVERCOME CONSTRAINTS

Implementing advanced EDR, enforcing Zero Trust, and leveraging and sharing threat intelligence are actions you can take today. But federal agencies also must work within a number of constraints, including cost, ease of deployment, regulatory compliance and purchasing and logistics complexities.

As the leading cybersecurity solution used by the public sector leveraging the trusted AWS GovCloud (U.S.), the CrowdStrike Falcon platform enables federal agencies to make rapid advances on all of these fronts. Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon platform leverages real-time 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.
- **Offloads the burden of updates and maintenance.** CrowdStrike assumes responsibility for all components leveraging the Falcon platform and CrowdStrike Security Cloud, driven by the needs of federal agency customers. The CrowdStrike Falcon platform agent is unobtrusive: no pop-ups and no reboots, and all updates are performed silently and automatically. You can monitor and manage your environment using a web console. In addition, thanks to our machine learning approach and focus on indicators of attack, CrowdStrike updates our on-device machine learning 3-4 times a year, each one roughly 50MB in size — meaning no daily 110MB downloads.
- **Extends your ROI in existing security solutions.** CrowdStrike integrates with all of the security solutions essential to federal agencies.

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 program requirements
- Department of Defense Impact Level 4 (IL-4)
- Criminal Justice Information Services (CJIS) Ready
- EU-U.S. and Swiss-U.S. Privacy Shield Frameworks
- Service Organization Control 2 (SOC 2)

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

- Exceeds U.S. FedRAMP program requirements with U.S. administrators and NIST 800-171 **compliance**.
- Provides coverage for all five certification levels of the Cybersecurity Maturity Model Certification (CMMC).

CROWDSTRIKE SOLUTIONS FOR FEDERAL AGENCIES

- Addresses the system protection and monitoring controls identified in NIST SP 800-53 Rev. 4 with eight separate NIST control families covering 23 separate controls.
- 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** and **AWS Marketplace - GovCloud**

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, FedRAMP authorized and 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 Moderate

Selected by FedRAMP JAB: 1 of 12 companies

Actively pursuing FedRAMP High

Achieved Impact Level 4

Actively pursuing Impact Level 5

SOC2 compliance

NIST compliance

For more information, please visit **https://www.crowdstrike.com/why-crowdstrike/crowdstrike-compliance-certification/**

WANT TO LEARN MORE?

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

Contact us: **https://www.crowdstrike.com/public-sector/request-information/**

RESOURCES

Crowdstrike Falcon Has You Covered with the White House Cybersecurity EO

eBook: How Federal Agencies Can Build Their Cybersecurity Momentum

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, 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/**