CrowdStrike Solution Brief

CROWDSTRIKE

CROWDSTRIKE SOLUTIONS FOR HEALTHCARE ORGANIZATIONS

Move forward with endpoint protection, Zero Trust and threat intelligence

CYBERSECURITY CHALLENGES IN HEALTHCARE ORGANIZATIONS

Healthcare organizations today increasingly depend on new, interconnected solutions to deliver quality care to more patients — for example, by integrating with clinical partners and third-party service providers. Meanwhile, many of these organizations rely on legacy antivirus (AV) products that are increasingly vulnerable to adversaries trying to compromise protected health information (PHI).

Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon® platform enables healthcare organizations to defend against modern threats. By leveraging cloud-native, behavior-based solutions that are driven by machine learning (ML) and integrate threat intelligence and real-time indicators of attack (IOAs), healthcare organizations can protect their vital data as well as their patients.

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

MAXIMIZE ENDPOINT PROTECTION ACROSS THE ORGANIZATION

How do you detect and respond to threats when tens of thousands of endpoints are distributed across on-premises and cloud environments and third-party partners and services? Today's healthcare organization must integrate new medical and personal devices — including those that provide patient self-service — and endpoints at clinical partners and other third-party organizations that may not be as rigorous in securing those devices.

Financially motivated organized criminal groups continue to target the healthcare sector, with the deployment of ransomware being a favored tactic given the high value of healthcare data and the dire consequences of it not being available.[1]

In today's threat environment, on-premises legacy AV solutions fall short. This antiquated technology can neither detect fileless and zero-day malware, nor prevent the exploitation of known vulnerabilities, encrypted malware and credential theft. Legacy AV provides little attack information across multiple devices and the entire network. Most important, there is no inclusive growth path for increasing or broadening security.

The World's Most Advanced Cloud-Native Platform

Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon platform leverages real-time indicators of attack (IOAs), threat intelligence and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

1 Source: "Protecting Healthcare Systems Against Ransomware and Beyond," p. 5, CrowdStrike

CROWDSTRIKE FALCON INSIGHT™ ENDPOINT DETECTION AND RESPONSE (EDR)

CrowdStrike Falcon Insight is the endpoint detection and response (EDR) module of the Falcon platform. Because the 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 healthcare organization, preventing attacks on endpoints on or off the network.

CrowdStrike Falcon delivers industry-leading automated detection and remediation to stop threats through continuous, comprehensive endpoint visibility that spans detection, response and forensics. CrowdStrike Falcon 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 Falcon allows security teams to spend less time handling alerts so they can investigate and respond to attacks more rapidly.
- **Eliminate bloat.** Unlike legacy AV, there are no on-premises controllers to be installed, configured, updated or maintained. CrowdStrike Falcon eliminates the bloat and performance issues of increasingly ineffective scheduled scans associated with legacy AV, consolidating endpoint agents into a single, lightweight agent automatically maintained by CrowdStrike .
- **MITRE ATT&CK score:** **CrowdStrike achieved 100% prevention** in a recent MITRE Engenuity ATT&CK evaluation .

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 Falcon platform, combines the most effective prevention technologies with full attack visibility and simplicity. 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 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 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.

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.

ENFORCE ZERO TRUST AS YOU INTEGRATE MORE ENDPOINTS AND CLOUD SERVICES

As healthcare organizations increasingly expand the number of endpoints to be protected and adopt cloud services like IaaS, PaaS and SaaS, their attack surface expands exponentially, including the trust relationship between on-premises environments and these cloud services.

Bad actors have more targets for attacks. Work-from-anywhere (WFA) initiatives have pushed machines and staff outside the network boundary. Skills needed for cloud management differ significantly from those used in on-premises operations, creating opportunities for misconfiguration and security exposure. Churn of staff also presents challenges to identity security.

Healthcare organizations are being urged 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. 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 SOLUTIONS FOR HEALTHCARE ORGANIZATIONS

CrowdStrike Falcon'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.

The CrowdStrike Falcon Identity Threat Protection component of the 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. 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. Falcon can also help you identify escalation of privilege and anomalous service account activity.
- **Reduce time to detect.** 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.
- **Limit the attack surface.** CrowdStrike lets you limit the scope of what applications can do. Control where regular users, third-party contractors and privileged users can go and limit which service accounts can access with segmentation. Apply the principles of least privilege and dynamic risk assessment to reduce the attack surface.

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.

LEVERAGE AND SHARE THE BEST THREAT INTEL

Security staff in healthcare organizations need access to the most comprehensive, up-to-date collection of security data available: global in scope, gleaned from both private industry and the public sector.

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 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.

POWERED BY THE CROWDSTRIKE SECURITY CLOUD, THE FALCON PLATFORM DELIVERS:

- **Hyper-accurate detections.** Using IOAs, Falcon provides insight earlier in the attack cycle to help determine the intent and ultimate goals of the attack, compared to indicators of compromise (IOCs), which flag events as they are happening.
- **Automated protection and remediation.** Falcon automatically investigates incidents and accelerates alert triage and response, including killing processes, deleting/blocklisting files, modifying registries, quarantining networks, and preemptively shutting down command-and-control (C&C) communications.

Greater ROI from Security Tools

Only 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.

- **Elite threat hunting.** Falcon combines automated analysis with human intelligence to predict, investigate and hunt for threats happening in your environment. CrowdStrike Intelligence gathers data on 28+ sophisticated threat actors that regularly set their sights on the healthcare industry and the tactics they use to conduct attacks.
- **Prioritized observability of vulnerabilities.** Falcon accelerates and simplifies threat investigations and streamlines SOC, IR and CTI teams.

CrowdStrike Falcon Intelligence Recon™ monitors potentially malicious activity across the open, deep and dark web to enable organizations to better protect their brand, employees and sensitive data. CrowdStrike Falcon Intelligence Recon+ adds further capabilities that reduce the time, skills and effort required for you to battle sophisticated adversaries.

CROWDSTRIKE HELPS HEALTHCARE ORGANIZATIONS OVERCOME CONSTRAINTS

Healthcare organizations also need to work within a number of constraints: a security workload that far outstrips the bandwidth and, in some cases, expertise of existing staff driving toward rapid response; difficulty hiring and retaining experts that fit an organization's security requirements and budget; and not enough staff to react to critical vulnerabilities on equipment owned and managed both internally and on vendor-managed equipment.

ADDITIONALLY, THERE IS THE BURDEN OF MEETING REGULATORY COMPLIANCE.

The Falcon platform has enabled over 100 healthcare organizations to make rapid advances in implementing advanced endpoint detection and response, enforcing Zero Trust, and leveraging and sharing threat intelligence. CrowdStrike safeguards over 1 million healthcare endpoints and counting across the U.S.

- **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.

CROWDSTRIKE HELPS HEALTHCARE ORGANIZATIONS COMPLY

HITRUST and Health Insurance Portability and Accountability Act **(HIPAA)** requirements

Affordable Care Act

U.S. Department of Health and Human Services Federal Health Care **Fraud and Abuse Laws**

Regulations that are state-specific regarding security — e.g., the California Consumer Privacy Act (CCPA) and New York's "Stop Hacks and Improve Electronic Data Security" (SHIELD) Act

Non-healthcare specific requirements like:

- Gramm-Leach-Bliley Act (GLBA)
- Payment Card Industry Data Security Standard (PCI DSS)
- General Data Protection Regulation (GDPR)
- Freedom of Information Act (FOIA)

Achievement of a new standard in healthcare cybersecurity through adoption of a "**1-10-60 Security Posture.**" This framework provides guidance for stopping breaches faster by overcoming common hurdles to establishing an effective incident response (IR) process.

CROWDSTRIKE SOLUTIONS FOR HEALTHCARE ORGANIZATIONS

- **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 our healthcare customers. The Falcon platform agent is unobtrusive: no pop-ups, no reboots, and all updates performed silently and automatically. Monitor and manage your environment using a web console.
- **Extends your ROI in existing security solutions.** CrowdStrike integrates with all of the security solutions essential to healthcare organizations.
- For organizations with greater security maturity and staffing, the CrowdStrike Falcon platform is flexible and extensible with components designed to protect endpoints, identity and cloud workloads against today's sophisticated threats.

For institutions who need more, **Falcon Complete with Identity Protection for Healthcare**, CrowdStrike's managed detection and response service, handles all aspects of endpoint and identity protection, freeing your staff to focus on your own mission and providing 24/7/365 security focus with established response times.

Regulatory compliance is critical to healthcare organizations, and CrowdStrike can assist with satisfying a broad range of compliance requirements.

CrowdStrike healthcare customers associated with state agencies may be able to access CrowdStrike solutions through a variety of Cooperative Purchasing Agreements, Blanket Purchase Agreements (BPAs), and Federal Supply Schedules (FSS), including California's Software Licensing Program (SLP) Plus; New York's Office of General Services (OGS); Texas' Department of Information Resources (DIR) and the Interlocal Purchasing System (TIPS), to name just a few.

WANT TO LEARN MORE?

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

RESOURCES

Read the report: **Healthcare IoT Security Operations Maturity**

Download the article: **Navigating Today's Healthcare Threat Landscape**

Look through the eBook: **Digital Health Innovation Requires Cybersecurity Transformation**

Read the eBook: **Protecting Healthcare Systems Against Ransomware and Beyond**

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, 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/**