CrowdStrike White Paper

CROWDSTRIKE

SIMPLIFYING THE ZERO TRUST JOURNEY FOR HEALTHCARE ORGANIZATIONS

CrowdStrike's Frictionless Approach to Stopping Healthcare IT Threats

EXECUTIVE OVERVIEW

Healthcare organizations are adopting cloud-based applications and services to simplify IT operations, increase clinician productivity and improve patient care and outcomes. As these healthcare organizations adopt cloud applications, they still have inscribed in their IT architecture numerous on-premises and legacy applications that they have been using for years. Together, the cloud and mix of legacy applications have fundamentally transformed the way healthcare organizations deliver and consume applications, creating new opportunities for threat actors and new challenges for security teams.

Cyberattacks can impair patient care, damage a hospital's reputation and result in costly compliance fines, legal settlements and loss of revenue. Traditional perimeter-based security architectures, designed to control access to conventional on-premises IT infrastructure and trusted enterprise networks, are ill-suited for the digital era — especially when applications transform to the cloud. In today's digital world, healthcare organizations host applications in both public and private clouds, as well as in on-premises data centers. And clinicians and other users access Electronic Health Record (EHR) systems and other healthcare applications and business tools from any place, any device and at any time.

Going forward, healthcare organizations must take a fresh look at security systems, frameworks[3] and best practices for the world of cloud workloads and mobile users. Many are looking at Zero Trust frameworks to stop security breaches and ransomware attacks, safeguard protected health information (PHI), and improve compliance with HIPAA and other patient privacy regulations.

This paper reviews digital healthcare security challenges and explains how CrowdStrike's frictionless Zero Trust approach helps healthcare organizations take full advantage of all the benefits of digital transformation quickly and cost-effectively — without compromising security, impairing user experience or hindering IT staff productivity.

A 2020 ransomware[1] attack against Universal Health Services, for example, impacted 250 separate healthcare facilities, resulting in an estimated $67 million USD[2] in lost revenue.

1 Cyberattack hobbles major hospital chain's US facilities

2 Universal Health Services lost $67 million due to Ryuk ransomware attack

3 A Guide to Frictionless Zero Trust for Modern Enterprises

PERIMETER SECURITY SOLUTIONS CAN'T MEET DIGITAL HEALTHCARE AGILITY AND SCALABILITY REQUIREMENTS

Today, many healthcare organizations are constrained by outdated perimeter-based security solutions designed to protect traditional on-premises IT systems and workloads. Most organizations rely on a disjointed collection of discrete security products and technologies (e.g., firewalls, VPNs, VLANs, NAC solutions) with distinct administrative interfaces to segment networks and isolate traffic. These siloed security implementations are inherently rigid and fundamentally difficult to manage and scale, and ill-suited for the world of cloud services and mobile users. Challenges and limitations include:

AGILITY

Configuring firewall rules, VLAN ACLs and NAC policies is a manually intensive, time-consuming and piecemeal proposition that can lead to security gaps and open the door for cybercriminals. Sophisticated threat actors can exploit security vulnerabilities to disrupt critical healthcare IT systems or steal PHI. How will the security posture change when healthcare IT accommodates more remote workers and third-party contractors who log in from unmanaged devices and from previously unknown remote locations? This dynamic behavior cannot be hard-coded into traditional security solutions in order to maintain a consistent security posture.

MANAGEABILITY

Siloed security implementations are notoriously costly and complex to administer. Configuring security policies and remediating threats across an extended healthcare network takes time and effort, and diverts valuable staff from other critical tasks.

VISIBILITY

A fractured security approach introduces blind spots, making it difficult to detect and isolate suspicious behavior in real time. Attackers can breach defenses, escalate privileges, traverse healthcare networks and evade detection for weeks or even months. To make matters worse, many healthcare organizations lack visibility into service accounts: the non-human privileged accounts used to invoke applications and to initiate virtual machine instances, automated services and other processes. Because Windows, UNIX and Linux service accounts are difficult to track — an individual service account is often accessed by many applications and processes — they are a common target for malicious attackers. Yet many organizations don't have complete visibility into what those service accounts are up to, such as how many are active or stale and whether they are suddenly being invoked by a malicious user or application.

VERSATILITY

Traditional perimeter-based security models, conceived to protect on-premises infrastructure and hospital-owned endpoints, are ill-suited for today's digital world, where physicians, lab technicians and others access on-prem and cloud-based solutions from any location, using hospital-owned and personal devices. Physicians now routinely access EHR systems, prescribe medications and perform other functions from outside the hospital using home computers or personal mobile devices. In addition, many employees and contractors access healthcare networks and services from inside the hospital using their own devices (BYOD). Further, the pandemic has found nonessential hospital employees often working from home using their own computers and devices, a situation that will likely continue after the pandemic passes. Bad actors often target inadequately secured, unmanaged devices and compromised credentials to steal PHI or launch malicious attacks like ransomware.

EXTENSIBILITY

Most hospitals rely on legacy medical imaging systems (e.g., CT scanners, ultrasound systems, x-ray machines) and other specialized medical devices (aka special-purpose or fixed-function systems) that often run outdated, unpatched or even unsupported software releases like Windows XP and Windows 7, creating significant security vulnerabilities and risk. Access to legacy devices is often loosely controlled via Active Directory and single-factor authentication methods, opening the door for savvy attackers.

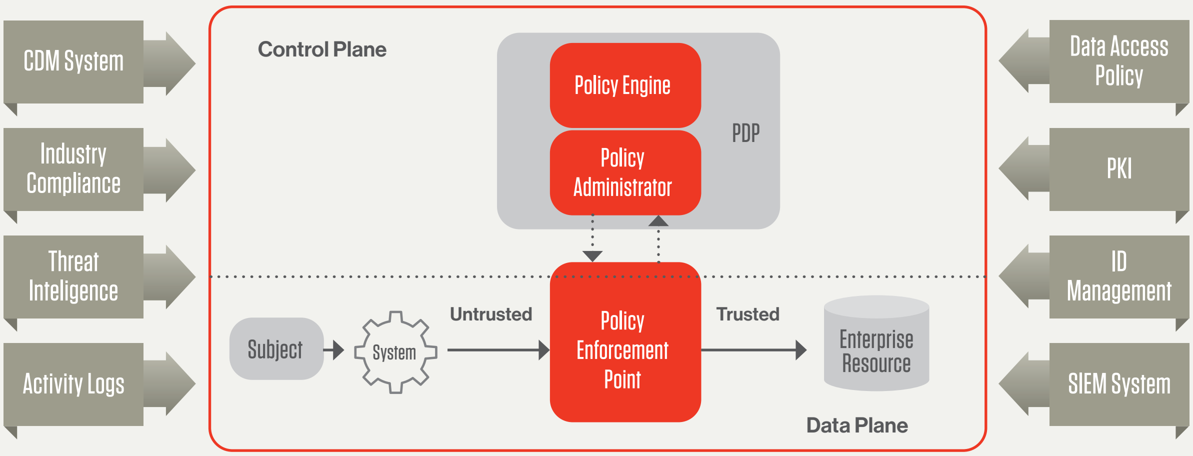
Modern threats like ransomware don't necessarily follow the traditional attack chain in a linear manner; they don't necessarily begin with malicious emails, websites or phishing schemes. Ransomware can originate from compromised endpoints, identities or workloads. In fact, according to a 2021 Ponemon Institute study, compromised credentials are the most common initial attack vector and cost an average of $4.37 million USD per breach.[4] Going forward, healthcare organizations must revamp their security architectures to protect against today's threats and vulnerabilities.

4 Cost of a Data Breach Report 2021, Ponemon Institute and IBM Security, July 2021.

A ZERO TRUST FRAMEWORK FOR THE DIGITAL ERA

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207 defines Zero Trust framework for the era of mobile devices and public, private, hybrid and multi-cloud infrastructure. In a Zero Trust security model, users are authenticated, authorized and validated independently of network borders. The Zero Trust model is intended to reduce attack surfaces and restrict lateral movement if a resource is compromised. It assumes all users, endpoints and workloads are inherently untrusted, wherever and whenever they try to access enterprise resources or applications.

NIST 800-207 CONCEPTUAL FRAMEWORK



The NIST SP 800-207 framework includes a control plane with a Policy Decision Point (PDP) and a data plane with a Policy Enforcement Point (PEP). The PDP includes a Policy Engine (PE) that maintains business rules and a Policy Administrator (PA) that governs a communication path between a subject and an enterprise resource. The PEP establishes, monitors and terminates connections between a subject and resource, based on policy.

CROWDSTRIKE ZERO TRUST SOLUTION FOR HEALTHCARE

The CrowdStrike Zero Trust solution secures the modern healthcare enterprise with its cloud-delivered approach to stop breaches in real time on any endpoint, cloud workload or identity, wherever they are. CrowdStrike does all of the heavy lifting for enterprise security teams to enforce frictionless Zero Trust with its industry-leading Security Cloud. The CrowdStrike Security Cloud processes trillions of events per week, enabling high-fidelity attack correlation, real-time threat analytics and threat response at scale. The solution protects multi-cloud and hybrid cloud implementations and supports modern web applications as well as legacy and proprietary applications.

The CrowdStrike Zero Trust solution follows the NIST SP 800-207 Zero Trust framework, helping healthcare organizations ensure strong security for today's cloud-based applications and mobile users. The NIST framework outlines privacy risks and mitigation strategies that will possibly align with existing federal guidance and compliance programs such as the Health Insurance Portability and Accountability Act (HIPAA).

The NIST Zero Trust framework is guided by the following key principles:

- **Understand behavioral data.** Are users accessing EHR systems to steal PHI (e.g., VIP patient snooping, coworker snooping) or to commit identity theft, fraud or abuse? If someone tries to access a patient record in an application or server, how will the healthcare organization detect and stop this activity if it is done with malicious intent?
- **Limit the attack surface with segmentation.** Use identity-based segmentation to tightly control which IT resources can be accessed by users (nurses, doctors, residents, students, technicians, contractors, vendors, business and IT professionals) and applications (service accounts). Apply the principles of least privilege and dynamic risk assessment to reduce the attack surface.
- **Automate security tied to context.** Use signals from users, devices, networks and workloads to gain unified visibility, improve analytics, enforce policies and automate security — all tied to context to improve the fidelity of alerts and incident response.
- **Continuously verify access attempts with the least friction.** Verify every attempt to access healthcare applications, EHR systems and business tools without impairing clinician workflows or hindering user productivity.

KEY CROWDSTRIKE ZERO TRUST SOLUTION ADVANTAGES

Rapid Deployment. Falcon sensors/agents can be deployed at scale — in hours, not days.

Frictionless Operations. The CrowdStrike Security Cloud provides security automation and analytics to intelligently enforce policies with the least friction for clinicians, business users, and healthcare IT and security teams.

Advanced Protection. With industry-leading sets of endpoint, workload, container and identity telemetry, threat intelligence, and AI-powered analytics, healthcare security teams can automatically predict and prevent PHI data exfiltration, malware and other sophisticated threats in real time.

Cloud Economics and Agility. CrowdStrike's cloud-native approach lets healthcare security teams achieve Zero Trust protection while avoiding infrastructure and operations expense and complexity.

Cybersecurity Cost Containment. CrowdStrike can help healthcare organizations reduce cybersecurity insurance premiums by demonstrating they have in place strong security systems and practices to defend against ransomware attacks and other threats.

MAKING ZERO TRUST FRICTIONLESS

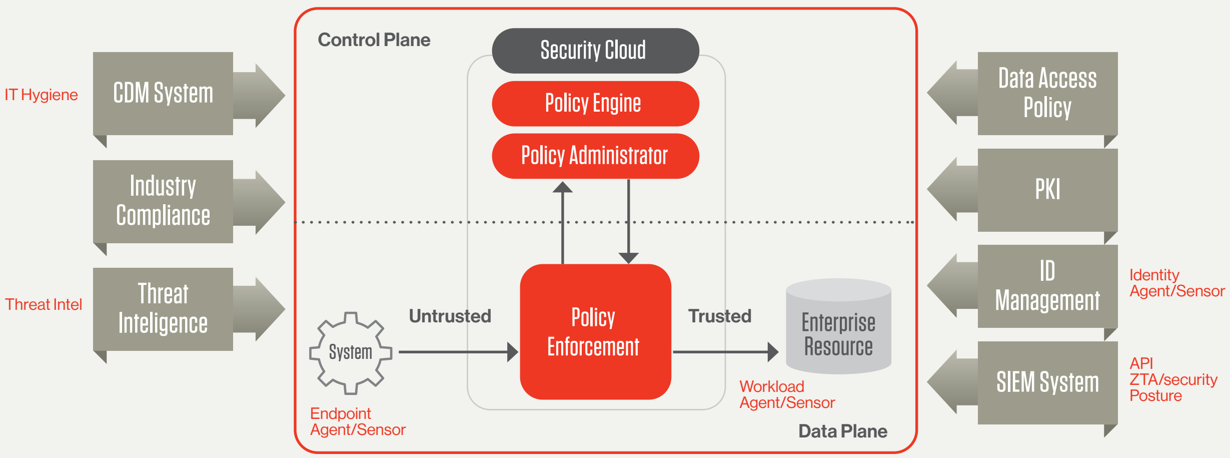
Rolling out a Zero Trust security model can be costly, lengthy and disruptive if implemented incorrectly. Architecting and deploying new security solutions and instituting new operational procedures takes time and budget, and new authentication and authorization controls can adversely affect user experiences and hinder adoption.

Forward-looking healthcare IT organizations are turning to cloud-delivered Zero Trust security solutions to accelerate time-to-value and simplify operations. A frictionless Zero Trust approach lets organizations quickly take full advantage of all the functional and economic benefits of digital transformation without compromising security or user experience.

FRICTIONLESS ZERO TRUST ELIMINATES IMPLEMENTATION, SCALABILITY AND OPERATIONS BARRIERS

The CrowdStrike Zero Trust solution is easy to deploy, scale and administer. The solution includes only two components: a lightweight CrowdStrike Falcon® sensor/agent and the CrowdStrike Security Cloud.

CROWDSTRIKE FALCON AGENT AND CROWDSTRIKE SECURITY CLOUD IN A NIST 800-207 ARCHITECTURE



CROWDSTRIKE FALCON AGENT

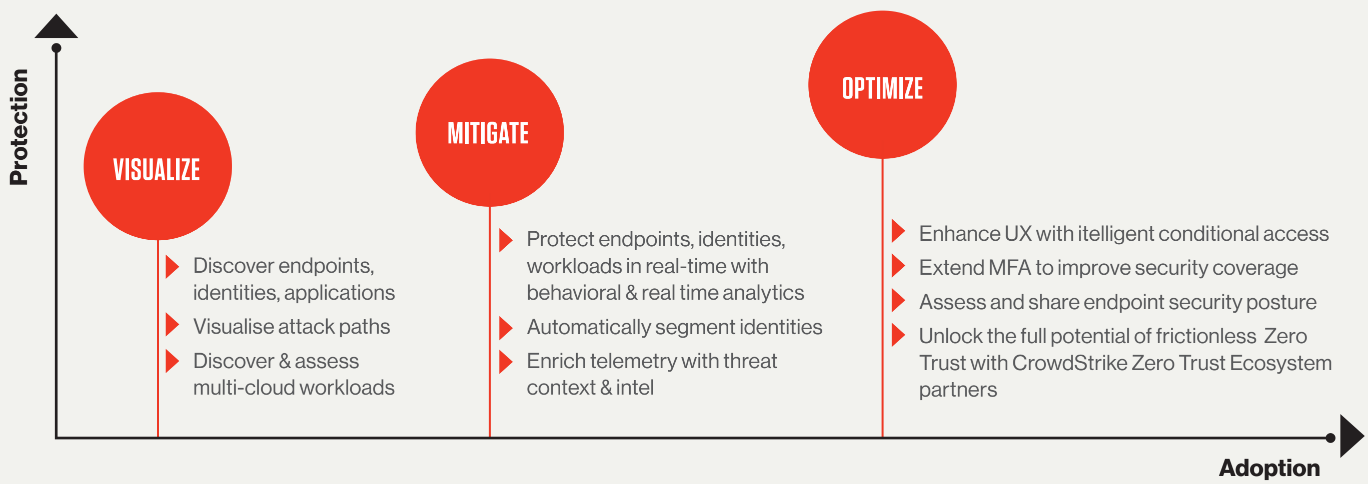
The intelligent CrowdStrike Falcon agent blocks malware, ransomware and sophisticated attacks, and captures and records endpoint and user activity for accurate risk posture assessments. It runs on a variety of endpoints and operating systems including workstations, servers, containers, virtual machines and desktops, and Domain Controllers (DC). Designed for today's cloud-centric organizations, the Falcon agent requires no enterprise network or VPN connectivity, and supports traditional devices like PCs and bare-metal servers as well as cloud workloads. The cloud-delivered agent is easy and non-disruptive to install, with no reboot required. Large healthcare systems can deploy tens of thousands of agents per day with little or no help desk intervention.

CROWDSTRIKE SECURITY CLOUD

The CrowdStrike Security Cloud is a next-generation, cloud-native security platform that uses artificial intelligence (AI) and machine learning (ML) to defend against modern cyberattacks. The solution takes full advantage of cloud scale, speed and agility, processing over 6 trillion events per week, making more than 140 million indicator of attack (IOA) decisions every second.

CROWDSTRIKE STREAMLINES THE ZERO TRUST JOURNEY

Healthcare organizations can introduce CrowdStrike Zero Trust functionality in phases to accelerate time-to-value and address their most urgent requirements as quickly as possible. Customers begin by using CrowdStrike to gain a holistic view of all users and assets, including all on-premises and cloud-based workloads. Next, they deploy advanced threat detection and prevention capabilities to defend against ransomware attacks, PHI theft and other malicious activity. Over time, customers can add capabilities to cover legacy applications or extend identity verification (multifactor authentication, or MFA) to desktops not covered by cloud-based MFA solutions, and also on tools like PowerShell and protocols like RDP over NTLM to reduce the attack surface and optimize security.



VISUALIZE

The CrowdStrike Zero Trust solution provides full visibility into all endpoints, identities and workloads to help healthcare organizations eliminate blind spots and thoroughly and proactively assess threats and risks. The solution is also ideal for heterogeneous healthcare IT networks that have been cobbled together over time through mergers and acquisitions.

With CrowdStrike, healthcare IT and security teams can:

- **Discover all endpoints, identities and applications.** Discover managed (hospital-owned) and unmanaged (personal, or third-party/contractor) endpoints and identify potentially risky devices. Gain visibility into privileged account credential management and access. Identify privilege escalation, compromised passwords and other activity symptomatic of fraud, theft or abuse.
- **Get full attack visibility across endpoints, identity stores, workloads and container environments.** Gain unified visibility into user identities and access privileges across diverse directory services such as Microsoft Active Directory [AD] and Azure AD, and integrate with cloud single sign-on [SSO] and federation solutions like Okta, AD FS and PingFederate. In addition to tightening AD security and hygiene, get insights into cloud workloads and containers with the ability to identify images, registries and libraries, and understand file access, network communications and process activity.
- **Discover and assess multi-cloud workloads.** Automatically discover cloud workloads. Gather real-time information about workloads including system configuration, networking and security group information for AWS, GCP and Azure.

MITIGATE

The CrowdStrike Zero Trust solution uses AI, ML and behavioral analytics to automatically identify and remediate suspicious activity in real time. The solution helps healthcare organizations safeguard PHI and defend against ransomware, malware and malicious attacks.

With CrowdStrike, healthcare IT and security teams can:

- **Protect endpoints and workloads from malicious attacks.** Protect Windows, Windows Server, macOS and Linux endpoints from ransomware, malware and fileless attacks. Safeguard cloud workloads and containers against malware. Prevent attacks on container-based applications by uncovering hidden threats in open-source packages and third-party images.
- **Detect and respond to incidents without manual threat correlations.** Automatically detect and prioritize malicious activity with IOAs. Use intelligent endpoint detection and response functionality to contain and investigate compromised devices. Use advanced cloud-based analytics and correlation to detect and prevent reconnaissance, lateral movement and persistence.
- **Automatically segment identities.** Automatically classify identities into hybrid and cloud-only identities. In addition, automate segmentation of accounts into human, service, shared and privileged categories.

OPTIMIZE

Healthcare organizations can deploy additional Zero Trust capabilities over time to extend coverage and boost security.

With CrowdStrike, healthcare IT and security teams can:

- **Enhance the user experience with intelligent, conditional access.** Define and enforce access policies with simple rules based on authentication patterns, behavior baselines and individual risk scores. Remove login hassles for genuine users (e.g., minimize MFA challenges) while still providing strong security.
- **Extend MFA to legacy applications and on-prem systems.** Protect and extend previous investments and reduce attack surfaces by adding MFA controls to traditional applications and systems. Reduce security risks associated with legacy medical devices that are running unpatched or unsupported operating systems, or are not integrated with existing enterprise authentication services.
- **Assess and share endpoint security posture.** Determine endpoint health across the enterprise with real-time security posture assessment scores. Enforce real-time conditional access to resources from compliant endpoints by sharing CrowdStrike Zero Trust Assessment (ZTA) scores with CrowdStrike Zero Trust ecosystem partners including Zscaler, Okta, Proofpoint and Netskope.
- **Monitor and control access to any type of account.** CrowdStrike protects workloads and on-premises/SaaS applications distributed across hybrid environments with continuous identity verification when users or applications attempt to access any type of account — regular, privileged or service.

CONCLUSION

Traditional perimeter-based security solutions, designed to protect conventional IT systems, are ill-suited for the cloud-first, work-from-anywhere world of healthcare IT. The NIST SP 800-207 defines the Zero Trust framework for the digital era as assuming that all users are implicitly untrusted, wherever and whenever they try to access enterprise resources.

The CrowdStrike Zero Trust solution provides real-time, continuous visibility and security across all healthcare IT assets — on-premises and in the cloud — following the NIST SP 800-207 Zero Trust framework. The solution improves visibility, detects and mitigates threats, and reduces risk.

The CrowdStrike Zero Trust solution helps healthcare IT and security organizations:

- Stop ransomware, malware and other sophisticated threats in real time from any endpoint, workload or identity.
- Safeguard PHI and improve compliance with HIPAA and other patient privacy mandates.
- Streamline security operations, slash incident detection and response times, and reduce risks with cloud-based automation and behavioral analytics.
- Accelerate time-to-value with a frictionless Zero Trust approach that minimizes cost and operational complexity.

To learn how the CrowdStrike Zero Trust solution can help your organization improve visibility and strengthen security in the digital era, visit **www.crowdstrike.com/zero-trust/**.

ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint and workload protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints and workloads on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates upward of 1 trillion endpoint-related events per day in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: **We stop breaches.**

Related Resources

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

© 2021 CrowdStrike, Inc. All rights reserved.