CrowdStrike Technology Partner

Solution Brief

CROWDSTRIKE AND ZSCALER INTEGRATION: POWERING HEALTHCARE CYBERSECURITY

Securing work beyond the perimeter with Zero Trust to modernize security across healthcare environments

CHALLENGE

As healthcare organizations undergo end-to-end digital transformation, it is critical to protect patient data and improve patient outcomes through repeatable best-in-class cybersecurity practices. An advanced strategy and smooth implementation is required when preventing ransomware supporting telehealth and investing in cybersecurity tools that prevent breaches and protect considerable investments into endpoints infrastructure and medical technology. Healthcare organizations are transitioning to a more effective, efficient and affordable way of providing patient care by combining in-office treatment with telehealth and remote monitoring. Employees are working from anywhere, on mobile devices that move with the staff from one patient to the next. Applications that were once hosted in data centers are now moving to a public cloud or are being replaced with software-as-a-service (SaaS) apps. The corporate network is becoming less relevant as more work takes place off of it, or between different networks and departments, and access to up-to-the-minute data from any location across multiple care teams is required more than ever before. Gateway appliances designed to build a hard perimeter around the entire network are now obsolete.

Traditional solutions emphasized network security and often did not consider device posture prior to allowing access to network resources. But the prevalence of cloud adoption means IT can no longer control secure application access when relying on the castle-and-moat architectures of the past. There is a need to protect the user-to-application connectivity from end to end, regardless of where users are connecting from. Security teams have access to more data now than ever and need tools that provide the right visibility into data with the right context at the right time. This requires security beyond the perimeter.

KEY BENEFITS

Real-time device health metrics are used to enforce access policy to private and SaaS apps

The capability to enforce access policy is based on the changing device posture over time

CrowdStrike and Zscaler's integration enables convergence of user, device and network visibility to indicators of compromise (IOCs) and automated workflow as a holistic system, strengthening security posture

The ability to trigger device quarantining helps prevent ransomware and malware propagation after a user accesses malicious files

Increased visibility enables stronger reporting and remediation and maximizes an organization's ability to respond to the increasing volume and sophistication of attacks

CROWDSTRIKE AND ZSCALER INTEGRATION: POWERING HEALTHCARE CYBERSECURITY

SOLUTION

To secure work beyond the perimeter, most IT teams have begun adopting a Zero Trust model that has three key criteria: identity, user device posture and access policies. These criteria are a means for establishing Zero Trust based on context and then adapting access rights as the context changes, no matter which unit the information originated from or if the access point is in an office, patient room, surgical facility or nursing station.

Together CrowdStrike and Zscaler are simplifying the adoption of Zero Trust for IT teams by providing an integrated end-to-end security solution — from endpoint to application — that gives administrators a real-time view of a device's security posture and bases access to critical applications on granular access policies. By sharing data between the CrowdStrike Falcon® sensor at the endpoint and Zscaler Zero Trust Exchange™, access policies can automatically be adapted according to user context, device health and newly detected indicators of compromise (IOCs).

CrowdStrike Falcon Zero Trust Assessment (ZTA) provides continuous, real-time security and compliance checks for endpoints, making sure that authentication and authorization are granted only to devices with security posture as approved by the organization.

Zscaler Zero Trust Exchange uses policy to securely connect users to the internet, SaaS or private apps. CrowdStrike provides a Falcon ZTA score, which is the device posture score, and also provides the ability to use threat intelligence so that Zscaler can adaptively enforce policy to access applications or to block malicious URLs, IP addresses or domains inline via a custom blocklist. This gives a security administrator the option to initiate a quarantine action from Zscaler to the CrowdStrike Falcon® platform and stop malware from spreading from the offending device. This bidirectional sharing across platforms of threat intelligence, increased visibility and automated workflow helps organizations increase the timeliness and effectiveness of threat defense, detection and remediation.

As a part of the CrowdXDR Alliance, Zscaler integrates with CrowdStrike to share relevant Zscaler logs for improved end-to-end visibility with telemetry from endpoints, networks and cloud applications. This sharing of intelligence maximizes cross-platform effectiveness for accelerated investigations. CrowdStrike Falcon® Fusion security orchestration, automation and response (SOAR) can trigger cross-platform response workflows, enabling Zscaler Zero Trust Exchange to adapt flexible access policies with speed and efficacy.

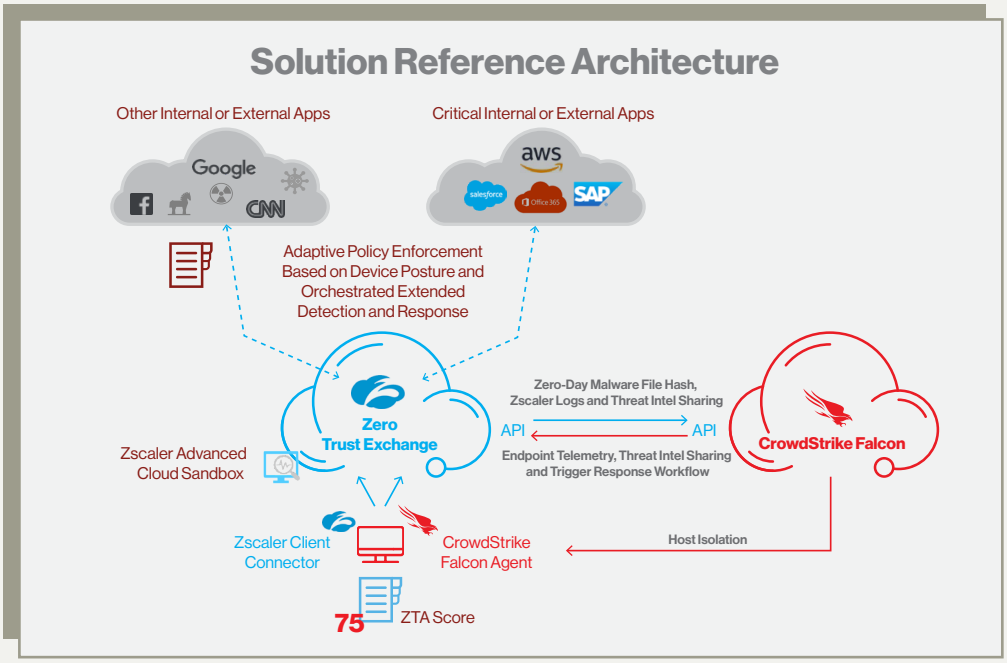
CrowdStrike Falcon® Insight XDR endpoint detection and response (EDR) now integrates with Zscaler Zero Trust Exchange to drive response actions from XDR detections or via automated Falcon Fusion SOAR workflows. These automated response actions include limiting or updating user access to applications with adaptive access control policies based on detection criticality, providing full closed-loop remediation across platforms.

The benefits from the joint solutions are not just limited to IT security. As businesses look to enable telehealth and care-from-anywhere strategies, these joint solutions make it easier to provide staff and administrators with safe, seamless and secure access to essential patient data and business applications for day-to-day staff activity. All of this can now be achieved on a foundation of Zero Trust.

CrowdStrike Technology Partner

CROWDSTRIKE AND ZSCALER INTEGRATION: POWERING HEALTHCARE CYBERSECURITY

HOW IT WORKS



** Third-party logos remain the property of their respective owners and are not meant to convey a relationship or endorsement.*

ZERO TRUST ACCESS TO ALL APPS

- **Step 1: The CrowdStrike Falcon platform evaluates device posture with Falcon ZTA**
  The Falcon platform collects OS and sensor settings from an endpoint device and calculates its Falcon ZTA score. Any changes in settings will automatically trigger a recalculation of the Falcon ZTA score. By comparing the Falcon ZTA score with the organization's baseline score, CrowdStrike can measure the health of the user's device relative to the organization's baseline and recommended best practices over time.

- **Step 2: Zscaler Zero Trust Exchange implements access policies**
  Zscaler Zero Trust Exchange implements Zero Trust access policies in two layers. First, Zscaler Client Connector checks if the CrowdStrike Falcon sensor is running on the endpoint device. Next, Client Connector reads the device's Falcon ZTA score and compares it against the policy threshold defined for selected business-critical applications. If these conditions are met, access to applications is granted. If not, then access is denied. Access policies on the Zscaler dashboard can be adjusted to change the threshold of the score based on the organization's requirements and changing conditions over time.

ZERO-DAY DETECTION AND REMEDIATION

- **Step 1: Zscaler Cloud Sandbox correlates zero-day malware detection with CrowdStrike Falcon telemetry**
  The Zscaler Cloud Sandbox sits inline at the cloud edge to detect zero-day threats. Malicious files are detonated in the sandbox, creating a report that is correlated with endpoint data from the Falcon platform. This ties the threat detected at the network edge with endpoint data.

- **Step 2: Administrators quarantine and remediate threats with a cross-platform workflow**
  The correlation automatically identifies impacted endpoints within the entire environment and facilitates a one-click trigger to the Falcon platform for rapid quarantine action. Alternatively, administrators can pivot from the Zscaler console to the Falcon console with automatically populated data for further in-depth investigation.

CrowdStrike Technology Partner

CROWDSTRIKE AND ZSCALER INTEGRATION: POWERING HEALTHCARE CYBERSECURITY

AUGMENTING ZSCALER INLINE BLOCKING WITH CROWDSTRIKE THREAT INTELLIGENCE

- **Step 1: CrowdStrike adds IOCs into Zscaler's Custom Blocklist**
  When CrowdStrike Intelligence identifies a threat within a specific customer environment, the threat is compared with Zscaler's threat database, and the resulting data is then automatically added to the Customer Block List in the Zscaler platform. These include high-confidence threat data such as URLs, IP addresses and domains. These shared IOCs in the custom blocklist are in addition to the Zscaler global threat feeds and are specific to a customer's environment.
- **Step 2: Zscaler uses new intel to block threat**
  Attempts to access such URLs, IPs and domains are proactively blocked inline by Zscaler as a result of the sharing of IOCs. Zscaler Internet Access (ZIA) and CrowdStrike Falcon ensure the same threat vector is blocked inline by Zscaler before it can infect other endpoints.

CROWDSTRIKE FALCON LOGSCALE LOG MANAGEMENT INCREASES VISIBILITY

- **Step 1: CrowdStrike Falcon® LogScale ingests Zscaler logs**
  Falcon LogScale ingests various Zscaler logs into the Falcon platform, gaining network visibility.
- **Step 2: Falcon LogScale performs data correlation and analytics**
  Falcon LogScale takes the telemetry from Zscaler to perform data correlation and analytics. This opens up a rich potential for threat hunting and investigation, as well as potential cross-platform triage and remediation.

EXTENDED DETECTION AND RESPONSE WITH CROWDSTRIKE FALCON INSIGHT XDR

- **Step 1: Get comprehensive visibility across applications and endpoints**
  Falcon Insight XDR offers purpose-built XDR integration with Zscaler logs to funnel relevant security data at scale, achieving visibility into network and cloud applications and maximizing cross-platform sharing for accelerated investigations and responses.
- **Step 2: Detect advanced threats and respond effectively**
  Falcon Insight XDR leverages security events identified from Zscaler logs to generate meaningful and actionable insights, speed up proactive threat hunting and respond decisively to stop cyberattacks. Based on a new detection, CrowdStrike Falcon can trigger Zscaler Zero Trust Exchange to move a user to a restrictive group, whereby adaptive access control policies can be applied — for example, restricting access to an app by browser isolation or network quarantine.

CrowdStrike Technology Partner

CROWDSTRIKE AND ZSCALER INTEGRATION:
POWERING HEALTHCARE CYBERSECURITY

KEY CAPABILITIES

The CrowdStrike integration with Zscaler shares threat intelligence and enables automatic workflows to help organizations reduce the number of security incidents — and, if an incident does occur, delivers quick time-to-detection and remediation critical to compliance with healthcare regulations.

The integration provides the ability to monitor device health and compliance via Falcon ZTA scores and quickly remediate gaps with Zero Trust access policy control and inline blocking based on CrowdStrike-detected IOCs. Together, CrowdStrike and Zscaler enable access to applications and the internet with maximally adaptive access control, without hindering user productivity.

Zscaler is a trusted CrowdStrike Technology Alliance Partner, offering innovative integrated solutions that ensure administrators have a real-time, end-to-end insight into the threat landscape to minimize attack surface, prevent lateral movement and deliver rapid threat detection and response. Zscaler is also a member of the CrowdXDR Alliance, a revolutionary security alliance that delivers unified XDR enterprise-wide.

ABOUT ZSCALER

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

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 and world-class AI, 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 delivers 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/**

Learn More about CrowdStrike for Healthcare