



Solution Brief

CROWDSTRIKE AND ZSCALER INTEGRATION

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

CHALLENGES

Hybrid work is increasingly becoming the normal way of doing business. Employees are working from anywhere, partners and their devices are moving on and off the office network, and many applications once hosted in data centers are now moving to a public cloud or being replaced with software as a service (SaaS). The corporate network is becoming less relevant as more work takes place off of it, and gateway appliances designed to build a hard perimeter around it 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 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.

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.

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 the Zscaler Zero Trust Exchange™, access policies can automatically be adapted according to user context, device health and newly detected 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.

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

The integrations enable 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 malware from propagating 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

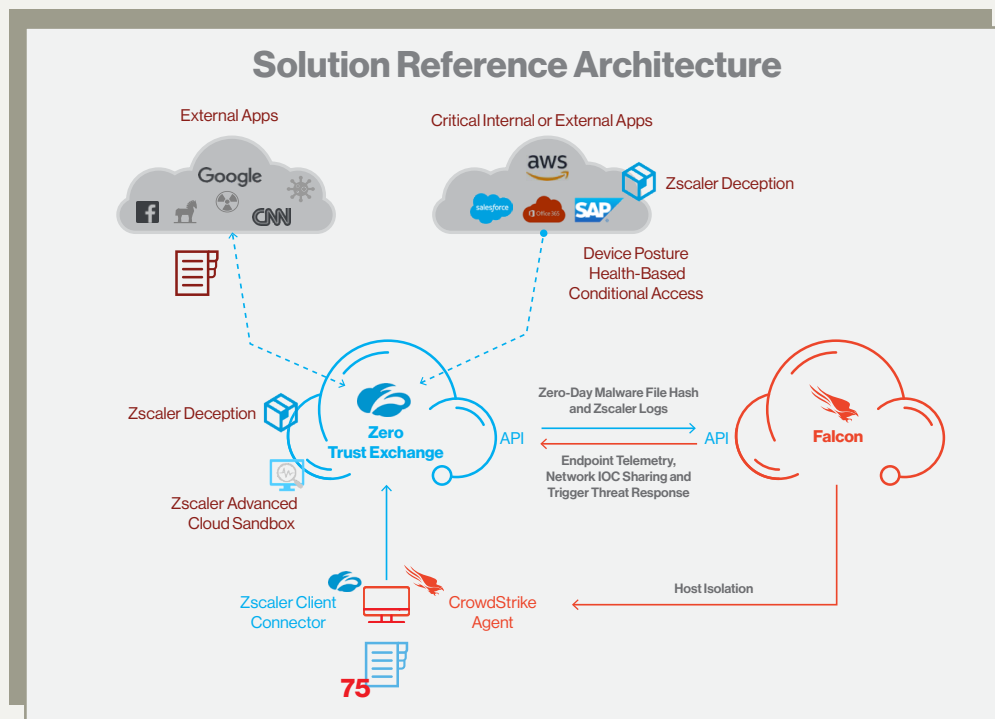
Zscaler Zero Trust Exchange uses policy to securely connect users to the internet, SaaS or private apps. CrowdStrike provides a ZTA score, which is the device posture score, and also provides the ability to use threat intelligence so Zscaler can adaptively enforce policy to access applications or to block malicious URLs, IP addresses or domains inline via a custom blocklist. This enables a security administrator 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 automatic 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 can trigger cross-platform response workflow, enabling Zscaler Zero Trust Exchange to adapt flexible access policies with speed and efficacy.

In addition, Zscaler Deception deploys decoys on endpoints, networks, cloud and identity systems to provide high-fidelity alerts and telemetry of targeted attacks. It also provides dynamic attack scoring and enables administrators to initiate both orchestrated and manual containment requests to the CrowdStrike Falcon platform to prevent lateral movement from a compromised host in real time.

The benefits from the joint solution are not just limited to IT security alone. As businesses look to enable work-from-anywhere strategies, this joint solution makes it easier to provide users with safe, seamless and secure access to essential business applications for day-to-day employee activity. All of this can now be achieved on a foundation of Zero Trust.

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 ZERO TRUST ASSESSMENT (ZTA)

The CrowdStrike Falcon platform collects OS and sensor settings from an endpoint device and calculates its ZTA score. Any changes in settings will automatically trigger a recalculation of the ZTA score. By comparing the 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 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.

AUGMENTING ZSCALER INLINE BLOCKING WITH CROWDSTRIKE THREAT INTELLIGENCE

STEP 1: CROWDSTRIKE ADDS INDICATORS OF COMPROMISE (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 delta is then automatically added to the customer's Customer Block List in the Zscaler platform. These include high-confidence threat data such as URLs, IP addresses and domains. These shared indicators of compromise (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/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.

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.

The integration provides the ability to monitor device health and compliance via 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.

CROWDSTRIKE HUMIO LOG MANAGEMENT INCREASES VISIBILITY

STEP 1: CROWDSTRIKE HUMIO CONSUMES ZSCALER LOGS

CrowdStrike Humio ingests various Zscaler logs into the Falcon platform, gaining network visibility.

STEP 2: CROWDSTRIKE HUMIO PERFORMS DATA CORRELATION AND ANALYTICS

The CrowdStrike Humio platform 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 EXTENDED DETECTION AND RESPONSE (XDR)

STEP 1: GET COMPREHENSIVE VISIBILITY ACROSS APPLICATIONS AND ENDPOINTS

Falcon XDR offers purpose-built XDR integration with Zscaler logs to funnel relevant security data at scale, achieving network and cloud applications visibility.

STEP 2: CUT THROUGH THE NOISE AND DETECT ADVANCED THREATS

Falcon XDR can leverage these security events from Zscaler to generate meaningful and actionable security insights, speed up proactive threat hunting and respond decisively to stop cyberattacks.

Zscaler is a trusted **CrowdStrike Technology Partner**, offering innovative integrated solutions based on CrowdStrike's rich open APIs, extending the Falcon platform with Zscaler's Zero Trust capabilities.

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](https://twitter.com/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.**

Follow us: [Blog](#) | [Twitter](#) | [LinkedIn](#) | [Facebook](#) | [Instagram](#)

© 2022 CrowdStrike, Inc. All rights reserved.

