Securing Work Beyond the Perimeter

With Zscaler™ and CrowdStrike

zscaler™

CROWDSTRIKE

The Challenge

Today's workforce is no longer limited by the bounds of a physical office. Employees and partners are working from anywhere, and their devices are regularly moving off the network and back on again. Simultaneously, applications that were once hosted in data centers are now moving to public clouds or are being replaced by SaaS applications. The corporate network is now less relevant as more work takes place off of it. Therefore, gateway appliances designed to build a hard perimeter around it have become obsolete.

Traditional solutions emphasized network security and often did not consider device posture prior to allowing access to network resources. However, the prevalence of cloud adoption means IT can no longer control the network for application access when relying on the castle-and-moat architectures of the past. Since IT does not control the network, they cannot secure access to applications either. Moreover, without evaluating device posture, the chance of a dirty device connecting to your network could increase the attack surface.

In light of this, there is a need to protect user-to-application connectivity from end-to-end, irrespective of where the users are connecting from. This requires security beyond the perimeter.

The Solution: Securing work beyond the perimeter, with zero trust

To secure work beyond the perimeter, most IT teams have begun adopting a zero trust model.

Zero trust consists of three key criteria: user identity, device posture, and access policies. These three criteria are used to establish zero trust based on context, and then adapting access rights as the context changes.

Together, Zscaler and CrowdStrike have been simplifying the adoption of zero trust for IT teams at companies such as Cushman & Wakefield and Paychex. The joint innovation between Zscaler and CrowdStrike provides an end-to-end security solution—from endpoint to application. These integrations ensure that administrators have a real-time view of a device's security posture, and that access to critical applications is based on granular access policies. By sharing data between the CrowdStrike sensor at the endpoint and the Zscaler Zero Trust Exchange™, access can automatically adapt based on the context of the user, device health, or updated access policies from Zscaler.

CrowdStrike Falcon Zero Trust Assessment (ZTA) provides continuous, real-time security and compliance checks for endpoints, making sure that the authentication and authorization is granted only to devices whose security posture complies with the organization's policy.

The Zscaler cloud architecture , which has points of presence (PoPs) in 150 locations worldwide, uses policy to securely connect users to SaaS, internet, or private apps. By leveraging CrowdStrike device posture score and CrowdStrike threat intelligence, Zscaler not only applies access policy to ensure only the compliant devices can access highly sensitive data and private apps, but can also block malicious IP and domains inline via custom block list.

KEY BENEFITS

- Real-time device health metrics used to enforce access policy to private apps
- ZPA has the ability to enforce access policy based on the changing device posture
- Enables convergence of user, device, and network visibility to IOCs and automated workflow as a holistic system strengthening security posture
- Ability to trigger device quarantining to prevent malware propagation
- Shared intelligence increases visibility and enables stronger reporting and remediation and maximizes an organization's ability to respond to increasing volumes and sophistication of attacks

In addition, Zscaler Advanced Cloud Sandbox detects zero-day malware inline and block malicious files from being downloaded. Additional quarantine action can be triggered from Zscaler to CrowdStrike platform, isolating other at-risk endpoints which has gotten the file from another means, such as via USB or near-field file transfer.

This gives a security administrator the option to trigger a quarantine action from Zscaler to CrowdStrike Falcon and stop malware from spreading from the offending device.

This bi-directional sharing of threat intelligence, increased visibility, and automatic workflow across platforms, helps organizations improve the timeliness and effectiveness of threat defense, detection, and remediation.

The benefits from the joint solution are not just limited to IT security alone. As businesses look to enable work-from-anywhere strategies, our joint solution with CrowdStrike 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

Zero trust access to private apps

Step 1: CrowdStrike Falcon evaluates device posture with ZTA

CrowdStrike Falcon collects OS and sensor settings from an endpoint device and calculates its Zero Trust Assessment (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 is able to measure the health of the user's device relative to the organization's baseline and recommended best practices over time.

Step 2: ZPA implements access policies

Zscaler Private Access™ (ZPA™) implements zero trust access policies in two layers. First, Zscaler Client Connector checks if the CrowdStrike 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 selective private applications. If these conditions are met, access to applications is granted. If not, then access is revoked. Access policies on the Zscaler dashboard can be adjusted to change the threshold of the score based on the organization's requirements.

Zero-day detection and remediation

Step 1: Zscaler Cloud Sandbox correlates zero-day malware detection with CrowdStrike Telemetry

The Zscaler Cloud Sandbox sits inline at the cloud edge to detect zero-day threats. Unknown files are detonated in the sandbox. If found malicious, the file hash is correlated with the endpoint data from CrowdStrike. This ties the threat detected at the network edge with endpoint data.

Step 2: Quarantine and remediate threats with a cross-platform workflow

The correlation automatically identifies the impacted endpoints within the entire environment and facilitates a one-click trigger to the Falcon platform for rapid quarantine action. Administrators can pivot from the Zscaler Insight Log to the Falcon Console with automatically populated data for endpoint investigation.

Augmenting Zscaler inline blocking with CrowdStrike threat intelligence

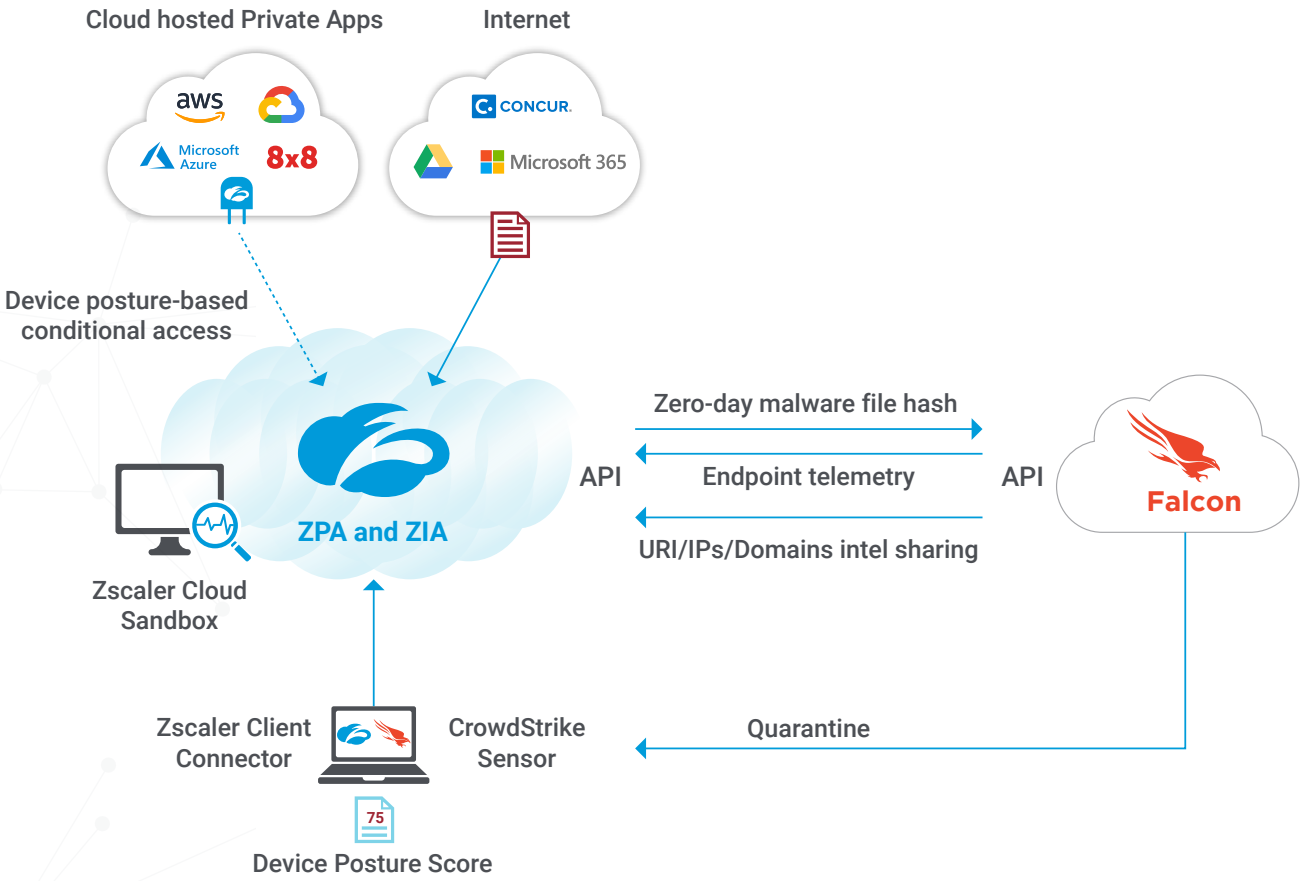
Step 1: Zscaler ingests a custom blocklist

Zscaler has the capability of retrieving the CrowdStrike threat intelligence that's already available within a specific customer environment and automatically ingests high-confidence threat data such as URLs/IPs/domains to a custom block list. These shared IOC (Indicators of Compromise) in the custom block list are in addition to the Zscaler global threat feeds and are specific to a customer's own environment. Attempts to access such URLs/IPs/domains are blocked as a result of the IOC sharing. ZIA (Zscaler Internet Access) and CrowdStrike ensure the same threat vector is blocked inline by Zscaler before it can infect other endpoints.

Step 2: Evaluating the severity of activity

The Zscaler Zero Trust Exchange connects to CrowdStrike APIs to retrieve high confidence IOCs for a specific customer, and automatically adds this to the custom block list. ZIA can then block threats based on this continuous update of IOCs, enabling faster threat prevention across cloud applications and endpoints.

Architecture diagram



Key Capabilities:

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

Moreover, 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, Zscaler and CrowdStrike enable access to applications and the internet with maximally adaptive access control, without hindering user productivity.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that 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 SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com