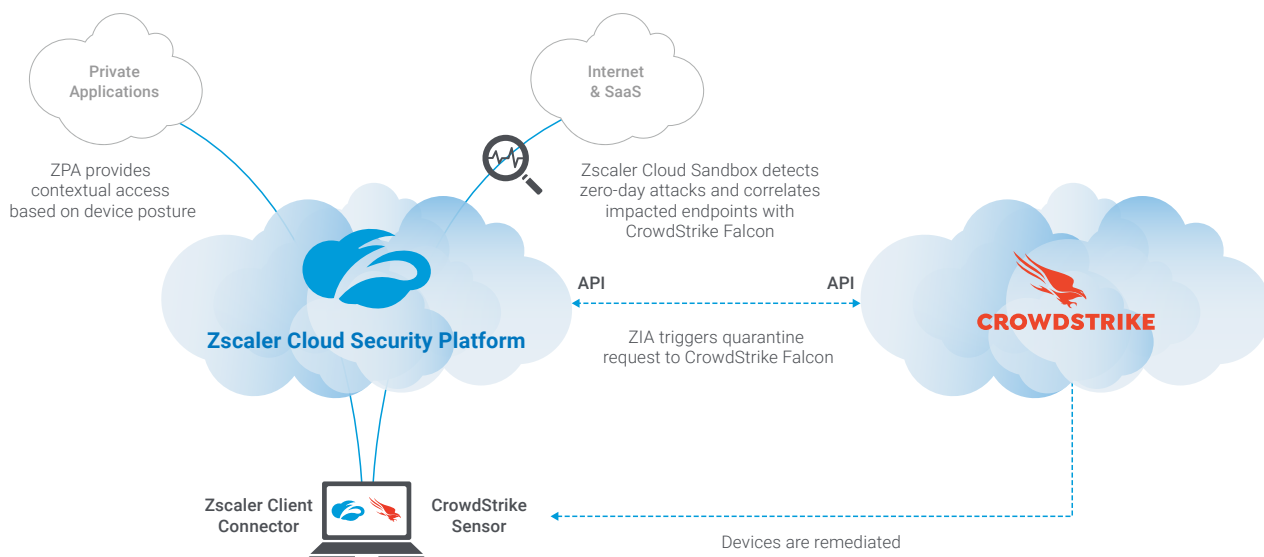


Modernizing Security from the Endpoint to the App

The Zscaler™ Cloud Security Platform integrates with the CrowdStrike Falcon Platform to provide end-to-end protection from device to network to app, including device posture-driven access control, cross-platform data correlation, and the ability to identify threat impact and respond faster.

The Problems

Users are increasingly working from remote locations and applications are moving to the cloud. The internet is the new corporate network. Traditional security models, built for the on-premises, data center era, can no longer keep up. First, on-premises security solutions are complex to deploy, manage and maintain. They require training IT and security experts to configure correctly and cannot scale dynamically. Appliance-based hardware has different refresh cycles, which require upfront CapEx investment and cause constant distraction to the core business during their upgrade process. Secondly, with remote users connecting to the cloud directly, risk to business increases due to lack of visibility to these activities. The traditional VPN approach impacts the user experience as users are repeatedly connected and disconnected from the VPN to balance productivity and the required secure access to business-critical applications. A bring-your-own-device (BYOD) approach introduces unmanaged devices onto corporate networks, thus increasing the risk of compromise and data leakage. Worst of all, traditional security solutions cannot detect advanced threats effectively and timely. While the volume of attacks grows daily and tactics become more sophisticated, organizations cannot hire security professionals fast enough to respond.



To address these issues, we need transformation. To make this transformation easy for companies, Zscaler and CrowdStrike have offered our security services as 100-percent cloud-native, security-as-a-service platforms. The partnership of our two market-leading solutions helps make your transition easier, faster, more effective and manageable.

The Zscaler and CrowdStrike Integration

Zscaler Private Access™ (ZPA™) and CrowdStrike Falcon Platform

Conditional access based on device posture: Zscaler ZPA allows conditional access to business-critical internal applications only via endpoint devices running CrowdStrike. This prevents non-compliant or rogue endpoints from accessing sensitive applications and data. Instead of traditional all-or-nothing access control solely based on authentication, this integration implements zero trust access control by taking device posture into consideration, and administrators can define which applications to protect based on this policy.

Zscaler Internet Access™ (ZIA™) and CrowdStrike Falcon Platform

Correlating zero-day detection with the endpoint environment for faster response: Zscaler Cloud Sandbox sits inline at the cloud edge to detect zero-day threats. Through API integration, the resulting report is correlated with endpoint data from CrowdStrike to automatically identify the infected endpoints within the entire environment and facilitate a one-click trigger to the Falcon platform for rapid quarantine action. Furthermore, the administrator can pivot from the Zscaler Insight Log to the Falcon console with automatically populated data for endpoint investigation.

CrowdStrike Endpoint Hits

Sandbox File Properties (Zscaler)

Sandbox Category	Suspicious	MD5	2484300564d0599555c00caf5095b704
Sandbox Score	70	SHA-1	918c31f10c9d03727ea5fbd7585751677dc608d
File Type	Windows Executable	SHA-256	3e908243592e12cd4df46c903501c5d39efcb848d7cbba2da391c27463b
File Size	22016	SSDEEP	384:GKeRlorFBIFKx5v38y34Lp29Jub/mPkaVikvTMNokpkjUo160Df:79or1/

File Detected on 1 Endpoint (CrowdStrike)

CrowdStrike Agent ID	Hostname	Internal IP	OS Version	File Status	Last Seen	Endpoint Status
464ae5077de04600701	W10CLIENT03	10.10.10.84	Windows 10	Detected	02/19/2020, 12:04 PM	Normal Contain

BENEFITS

- **Enables zero trust access control** – Ensure that users are accessing business-critical private applications only from endpoints that have CrowdStrike installed and running; obfuscating HTTP ports reduces the attack surface; removing the need for VPN vastly improves user experiences while strengthening endpoint security.
- **More effective teams** – Comprehensive visibility from the network and endpoint platforms provides a more complete view of the threat landscape. One-click drill down and pivot between consoles as well as cross-platform workflow makes investigation and response faster and more efficient.
- **Reduced risk** – The Zscaler inline and integrated security stack, including SSL inspection, firewall, web proxy, cloud sandboxing, CASB and DLP protection, combined with CrowdStrike’s advanced endpoint protection and analytics, can significantly reduce dwell time and the business loss caused by security breaches and downtime.
- **Reduced complexity** – Zscaler and CrowdStrike are architected and implemented 100 percent in the cloud. Our combined offering is easy to implement, always up-to-date, cost-efficient, agile and can scale rapidly. Security policies are applied consistently for all users and all apps for all locations, vastly reducing the risk of misconfiguration of disparaging on-prem applications in multiple locations. There’s good reason that both companies are Gartner MQ Leaders in their fields.

For more information, please visit www.zscaler.com/crowdstrike

About Zscaler

Zscaler enables the world’s leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its services, Zscaler Internet Access™ and Zscaler Private Access™, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100-percent cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to match. Used in more than 185 countries, the Zscaler multitenant, distributed security cloud protects thousands of customers from cyberattacks and data loss, so they can embrace cloud agility, speed, and cost containment—securely. .

About CrowdStrike

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint 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 on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over two trillion endpoint-related events per week in real time from across the globe, fueling one of the world’s most advanced data platforms for security.

