CrowdStrike Technology Partner

Solution Brief

CROWDSTRIKE FALCON AND CLOUDFLARE

Connect to corporate resources safer, faster and more seamlessly with enriched device-based Zero Trust access policies

CHALLENGES

Today, users, devices and applications largely exist outside of the traditional corporate perimeter. Traditional tools that connect employees to corporate applications (e.g., VPNs and IP-based controls) grant excessive trust, potentially exposing users to malicious threats like phishing and malware, potentially resulting in the loss of data. They can also increase an organization's attack surface, limit visibility and frustrate end users.

SOLUTION

Combining Cloudflare Zero Trust Network Access (ZTNA) and Cloudflare Secure Web Gateway (SWG) with CrowdStrike Falcon® enriched endpoint data and security posture details helps provide a safer, faster and easier way to ensure secure access for increasingly distributed workforces.

The Cloudflare and CrowdStrike integration delivers defense-in-depth, ensuring employees have secure access to applications from anywhere. Cloudflare's Zero Trust platform protects critical resources by granting users conditional access after verifying the identity, context and policy adherence for each access request. By combining Cloudflare's capabilities with the CrowdStrike Falcon platform's enriched endpoint data, powered by the CrowdStrike Security Cloud and world-class artificial intelligence (AI), it's easy for your organization to secure access, from devices and identities to applications.

The integration enables you to seamlessly build in the Cloudflare interface Zero Trust policies that are based on the CrowdStrike Falcon Zero Trust Assessment (ZTA) score — a continuous real-time security posture assessment across all endpoints in your organization. This device posture provides important contextual signals to help your security team enforce conditional access policies based on device health and compliance checks, mitigating risks posed by compromised or malicious devices. As these policies work across Cloudflare's Zero Trust platform, your organization can build powerful rules invoking Browser Isolation, Tenant control, Anti-virus or any part of your Cloudflare deployment.

The integration between Cloudflare and CrowdStrike, in addition to the existing **CrowdXDR Alliance** partnership, empowers customers to rapidly identify and respond to threats, strengthening Zero Trust security posture to help you thwart adversaries.

KEY BENEFITS

Comprehensive security: Identify, investigate and remediate threats quickly, and ensure security for external, public-facing web properties and internal resources.

Simple Zero Trust policies: Easily enforce device-aware access policies enabled by Falcon Zero Trust Assessment (ZTA) with a few clicks in the Cloudflare dashboard.

Compromise mitigation: Prevent lateral movement of infected devices, restricting them from accessing sensitive data (e.g., account credentials).

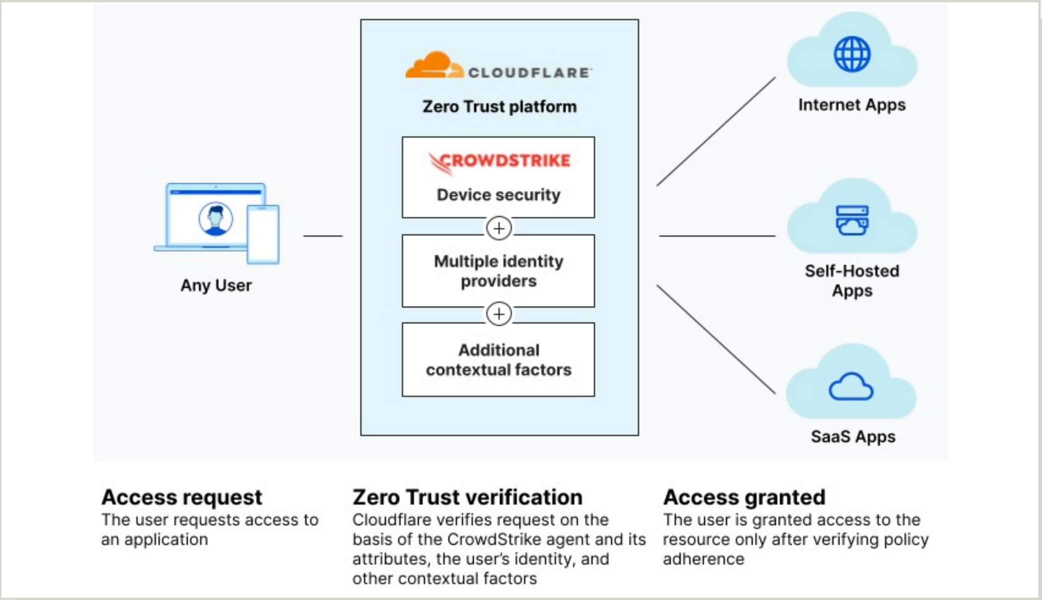
Accelerated network control: Cloudflare's lightning-fast network for enforcement decisions provides access within 50ms for 95% of the world's internet-connected population.

BUSINESS VALUE

Use Case	Solution	Benefits
Zero Trust Network Access (ZTNA)	Cloudflare's ZTNA solution secures applications with identity, device and context-driven rules, and integrates with the CrowdStrike Falcon platform to help teams build conditional access policies. These policies can be configured to require a minimum Falcon ZTA score to be met before a user is granted access.	Enable dynamic and adaptive secure conditional access to applications from any endpoint based on a Zero Trust framework, regardless of the user or location.
Secure Web Gateway (SWG)	Cloudflare SWG protects users and data safe from threats on the internet, with no backhauling required. Through the integration with CrowdStrike, organizations can leverage the device context from the Falcon ZTA score to influence various mitigation or protection measures.	Mitigate risks that stem from compromised or malicious devices and gain visibility of device health and compliance checks within the organization.
Incident Response	CrowdStrike is an incident response partner of Cloudflare. During an incident or attack, CrowdStrike works with Cloudflare to help get an organization's web properties and networks back online.	Get rapid support in attack situations and ensure systems get back online quickly to mitigate operational friction and user hindrance in the event of an incident.

TECHNICAL SOLUTION

The integration between CrowdStrike and Cloudflare allows organizations to build on their existing Cloudflare access and gateway policies to ensure that a minimum Falcon ZTA score is met before a user is granted access. If a user does not meet the threshold ZTA score, the administrator can choose to block, isolate and run other checks. In addition, Cloudflare customers can build Zero Trust policies based on the presence of a CrowdStrike Falcon agent at the endpoint and its ZTA score. This score delivers continuous, real-time security posture assessments across all endpoints in an organization regardless of location; enables the enforcement of conditional access based on device health and compliance checks to mitigate risks; and is evaluated each time a connection is requested, enabling conditional access to adapt to the evolving condition of the device.



Access request
The user requests access to an application

Zero Trust verification
Cloudflare verifies request on the basis of the CrowdStrike agent and its attributes, the user's identity, and other contextual factors

Access granted
The user is granted access to the resource only after verifying policy adherence

> "We've been working with CrowdStrike since we launched our Zero Trust platform, and have heard repeatedly from customers about the power of combining the insights from Cloudflare's global network with those from the CrowdStrike Security Cloud. With this integration, we're making it easy for joint customers of Cloudflare and CrowdStrike to benefit from the insights from our respective platforms and create seamless Zero Trust protection from the network to the device."

Alex Dyner, *Senior Vice President, Special Projects at Cloudflare*

CrowdStrike Technology Partner

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

ABOUT CLOUDFLARE

Cloudflare Zero Trust is a security platform that increases visibility, eliminates complexity, and reduces risks as remote and office users connect to applications and the Internet. In a single-pass architecture, user traffic is verified, filtered, inspected, and isolated from Internet threats; and performance never suffers, as users connect through data centers near them in 250+ cities and 100+ countries around the world.

Other Zero Trust providers offer multiple point products to protect from every threat vector, but leave customers to manage their own attack surface. The Cloudflare platform stops more attacks by isolating applications and endpoints from the attack surface by shifting it to our edge, and applies threat defenses to shield that edge.

Learn more at **cloudflare.com/products/zero-trust**.

ABOUT CROWDSTRIKE

CrowdStrike Holdings, Inc. (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**

Learn More
in the CrowdStrike Store

Learn more **www.crowdstrike.com**