# Zscaler and CrowdStrike

## Extending zero trust to modernize the security operations center (SOC)

Solution Brief

### Key Highlights

- Zscaler collects and analyzes active security incident signals occurring on the endpoint from the CrowdStrike Falcon platform, adding a rich layer of context to its adaptive access control policy engine and making device posture driven zero trust access control even more robust.
- Zscaler Risk360 service integrates with CrowdStrike to provide insights into risk contributing factors within your organization, categorizes it under Risk360 attack stage categories, and quantifies each risk factor according to its risk weight.
- Zscaler's Data Fabric for Security enriches and correlates CrowdStrike's CVE data with concurrent data streams to provide contextualized, real time insights into vulnerabilities and exposures across your entire IT estate.
- Natively developed by CrowdStrike, the Falcon Foundry Zscaler application serves as a foundation for Zscaler's integration with CrowdStrike's next-gen security incident and event management (NG-SIEM) platform. The pre-built offering automates and orchestrates threat intel sharing and enables coordinated policy actions for rapid and effective response to security threats.

## The Challenge

Hybrid work has dissolved the perimeter and continues to reinvent the business landscape leaving organizations with the complex task of securely enabling a distributed workforce  from any location and on any device while protecting their business from cyber attacks.

The paradigm shift in how work gets done has led to an exponential growth in the number of devices connected to corporate networks today. Each connected device represents a potential entry point for cyber attacks, further complicating security efforts.

Amidst industry challenges, IT and security teams struggle with maintaining secure access to applications across diverse multi-cloud environments and fluctuating threat landscapes. They need visibility and control to scale security across the vast ecosystem of endpoints and applications to secure all potential attack surfaces.

Security operations teams face their own unique challenges. Saddled with detecting advanced threats and monitoring risks from high volumes of disjointed data, they are expected to respond to security incidents in the shortest possible time. All while superlatively coordinating response strategies across multiple tools and platforms. Compounding these challenges is the rift between IT security and security operations that often delays incident resolution, weakening the organization's overall security posture.

## Zscaler and CrowdStrike: An Unmatched Defense-in-Depth Approach

Zscaler and CrowdStrike deliver an integrated zero trust security solution that simplifies endpoint to application security in a hybrid world. Expanding on core zero trust capabilities, the solution offers a suite of powerful new integrations that transform the security operations center (SOC).

Zscaler's cloud-delivered Zscaler Zero Trust Exchange™ platform serves as an intelligent switchboard securely connecting millions of users, devices, and applications across any network and location. Zscaler has further extended the power of its platform with new capabilities for risk quantification and data contextualization to help solve the day-to-day difficulties faced by security operations in detecting and responding to threats.

By integrating Zscaler's industry-leading zero trust security and AI-powered risk management with CrowdStrike's advanced endpoint protection, threat intelligence, and next-generation SIEM capabilities, the integrated solution streamlines the entire risk management, detection and response lifecycle, effectively closing the loop between IT security and security operations.

## The Zscaler and CrowdStrike integration is multi layered and supports multiple use cases:

- **Adaptive Zero Trust Access:** Zscaler leverages CrowdStrike Falcon Zero Trust Assessment (ZTA) device scores and security incident signals to enable adaptive access controls, ensuring only secure devices gain access to applications.
- **Threat Intelligence Sharing:** CrowdStrike's indicators of compromise (Iocs) feed into Zscaler's threat intelligence engine, enhancing its custom block lists for proactive threat prevention.
- **Advanced Zero-day Threat Detection and Quarantine:** Zscaler Cloud Sandbox integrates with CrowdStrike Falcon telemetry to detect zero day malware and facilitate rapid quarantine actions on impacted endpoints.
- **Decoys for Early Threat Intelligence:** Zscaler Deception deploys decoys on endpoints, networks, cloud, and identity systems to provide high-fidelity alerts on early indicators of attack (IOAs) and share this high-confidence threat intel with CrowdStrike.
- **Holistic Cyber Risk Visibility, Risk Assessment, and Management:** Zscaler Risk360 and Data Fabric for Security ingest unique risk factors across the attack chain and CVE data respectively from CrowdStrike to quantify risk and prioritize critical vulnerabilities into automated remediation workflows.
- **Cross-Platform Telemetry Sharing and Correlation:** Zscaler integrates with CrowdStrike to share relevant Zscaler logs for improved end-to-end visibility with telemetry from endpoints, networks and cloud applications to maximize cross-platform effectiveness for accelerated investigations.
- **Cross-Platform Detection and Response:** CrowdStrike Falcon Next-Gen SIEM now integrates with Zscaler via the Falcon Foundry for Zscaler app, and provides full closed-loop remediation between ZIA's advanced sandboxing, CrowdStrike's next generation SIEM, and ZIA's policy enforcement engine.

## The latest integrations from Zscaler and CrowdStrike support the following new use cases:

Use Case 1

### Context-Aware Adaptive Access Policy Enforcement

Expanding the scope of adaptive access capabilities, Zscaler now leverages real-time context from CrowdStrike enabling superior risk assessment and policy enforcement decision making. The new integration goes beyond enforcing access control policy based on the Falcon ZTA device health scores, and now incorporates detailed security incident data from CrowdStrike to evaluate risks in real time.

Zscaler collects and analyzes active security incident signals occurring on the endpoint from CrowdStrike, adding a rich layer of context to its adaptive access control policy engine and making device posture driven zero trust access control even more robust.

The continuous flow of security incident data from CrowdStrike provides a dynamic and responsive security posture from the endpoint to the application, significantly broadening Zscaler's adaptive access capabilities, and allowing for more granular and context-aware access controls.

With this new capability, Zscaler admins can now set security incident thresholds and grant application access to endpoints that meet both the Falcon ZTA compliance and the specified security incident threshold criteria.

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

Use Case 2

## Holistic Cyber Risk Quantification and Visualization

Zscaler Risk360 is a powerful risk quantification and visualization framework for remediating cybersecurity risk. It ingests real data from external sources, the customer's Zscaler environment, and security research from ThreatLabz to generate a detailed profile of the organization's risk posture. The framework spans across the four stages of attack i.e. external attack surface, compromise, lateral propagation, and data loss—and all the entities in your environment, including assets, applications, users, and third parties.

The Risk360 service integrates with CrowdStrike to provide insights into risk contributing factors within your organization. Once set up, Zscaler pulls risk-related information from the Falcon platform, categorizes it under Risk360 attack stage categories, and quantifies each risk factor according to its risk weight.

This integration allows customers to take action on policies to update or amend them. It also includes guided investigative workflows that allow for deeper drill downs to investigate specific issues.

Use Case 3

## Security Data Contextualization and Unified Vulnerability Management

Security teams currently leverage a myriad of technologies and solutions to protect their businesses from an expanding attack surface. Each of these tools produces massive amounts of valuable data. However, this data is often siloed and duplicative across tools. As a result, security teams struggle with information overload, opaque workflows, and increasing difficulty in defending their cybersecurity posture.

Zscaler's Data Fabric for Security aggregates data from disparate tools making it more actionable and useful. It transforms how security operations manage and respond to security threats by seamlessly aggregating data from over 150 sources, including common vulnerabilities and exposures (CVEs) detected at the endpoint by CrowdStrike. The Data Fabric enriches and correlates CrowdStrike's CVE data with concurrent data streams to provide contextualized, real time insights into vulnerabilities and exposures across your entire IT estate.

Armed with this knowledge, security analysts can dynamically connect the dots between vulnerabilities, threats, findings, incidents, assets, software components, and users and lean on cross referenced, actionable intelligence to efficiently prioritize and address the most critical vulnerabilities and risks first.

Use Case 4

## Coordinated Threat Sharing, Detection and Response

Natively developed by CrowdStrike, the Falcon Foundry Zscaler application serves as a foundation for Zscaler's integration with CrowdStrike Falcon Next-Gen SIEM. The pre-built application automates and orchestrates threat intel sharing and enables coordinated policy actions for rapid and effective response to security threats.

Available in the CrowdStrike Marketplace, the pre-built app enables licensed, mutual customers to enhance their perimeter security through advanced monitoring and threat detection by utilizing indicators of compromise (IoCs) sourced from CrowdStrike's threat intel repositories. Additionally, it enables customers to develop and deploy custom workflows tailored for specific threat detection, investigation, and response use cases.

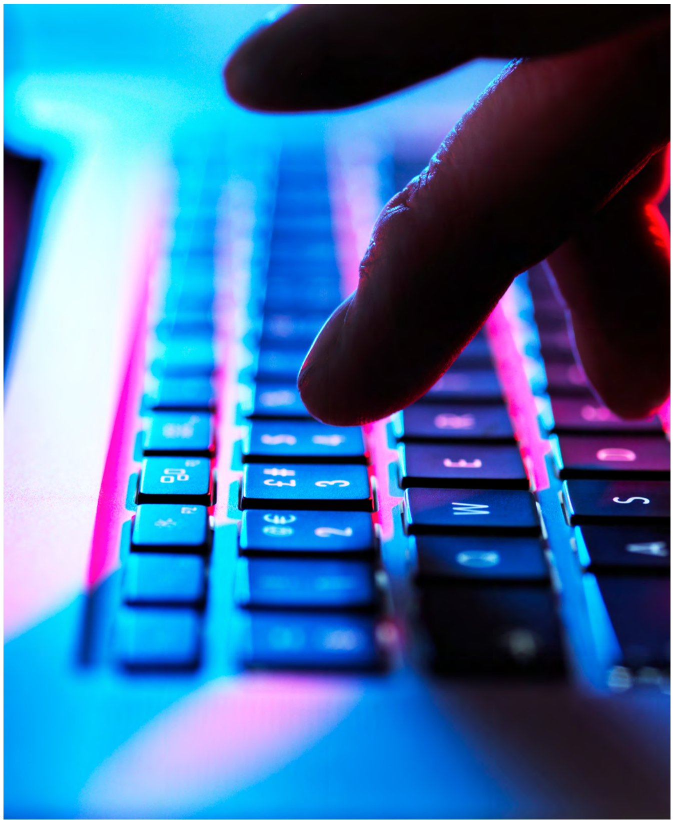
By creating a continuous feedback loop and coordinated response mechanism between ZIA's advanced sandboxing, Falcon Next-Gen SIEM, and ZIA's policy enforcement engine, the ready to use application streamlines security workflow automation and orchestration to accelerate security operations.

## Better Together Benefits

- **Context Rich Adaptive Access Policies:** Improve your endpoint-to-application security posture by enforcing zero trust policies that adapt dynamically to changing conditions.
- **Holistic Visibility into the Cyber Risk Landscape:** Gain an accurate view of risk exposure across the four stages of attack and leverage consolidated risk score across multiple sources for a complete understanding of cyber risk.
- **Contextualized Security Data for Improved Risk Assessment:** Aggregate and contextualize security data to prioritize your biggest risks and automate workflow for remediation.
- **Out-of-the-Box SOAR Integration:** Get up and running with pre-built Foundry app for Zscaler for threat intel sharing. Build custom Falcon Fusion SOAR workflows quickly, to automate detection, investigation, and response from end-to-end.
- **Rapid Detection and Coordinated Response:** Speed up mean time to detect (MTTD) and mean time to respond (MTTR) with coordinated response and policy enforcement actions that bridge gaps between IT security and security operations.

## Strengthen Security Operations with Zscaler and CrowdStrike

Zscaler and CrowdStrike are on a mission to augment zero trust enforcement and strengthen security operations with powerful complementary capabilities. Our newest integrations seamlessly work together to elevate your security operations to the next level. Together, we expand on cutting-edge zero trust enforcement to usher in the age of the modern SOC.



CROWDSTRIKE

**About CrowdStrike**
CrowdStrike has redefined security with the world's most advanced cloud-native platform that protects and enables the people, processes and technologies that drive modern enterprise. CrowdStrike secures the most critical areas of risk — endpoints and cloud workloads, identity, and data to keep customers ahead of today's adversaries and stop breaches. Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence on 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 — all through a single, lightweight agent. With CrowdStrike, customers benefit from superior protection, better performance, reduced complexity and immediate time-to-value. Learn more at crowdstrike.com.

LEARN MORE AT
zscaler.com/partners/crowdstrike

**Download our Zscaler + CrowdStrike Deployment Guide**

zscaler™ | **Experience your world, secured.™**

**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 SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.