Beyond the Perimeter 2023

Context-Driven Security for Enhanced Protection

The Challenge

Fluid, hybrid global workforces present an increasingly complex access and authorization landscape for enterprise security teams.

The flexible, remote or hybrid workforce is here to stay. But for many enterprises, enabling users to quickly and easily access any resources they need—from anywhere, at any time, on any device—has introduced some sobering security challenges.

In today's competitive business environment, workforce access to enterprise apps and assets needs to be safe and frictionless. Securing that access, however, is exponentially more difficult than it was just a few years ago. Today's dynamic global teams are logging in from all over the globe, using a dizzying array of connected devices (both sanctioned and unsanctioned), using an ever-expanding set of identities with constantly morphing roles and permissions.

For companies built around traditional perimeter security, it can be hard to close that gap quickly to provide the unfettered access today's workforces need while keeping enterprise apps and assets safe from threat actors. Too often, the quick fix has been over-provisioning, providing team members more access rights than they need. This introduces serious security risks that threat actors are adept at exploiting. Essentially, over-provisioning leaves a back door open, inviting cyberattacks and data breaches.

Overburdened security and IT teams have to make real-time access decisions, in this complex, dynamic, ever-expanding permissions landscape. And what's become clear is that granting permissions based on user credentials alone is no longer safe. Enterprise teams need to know where users are located, what device is in play, what network they're utilizing, and many other details, so they can make deeply informed real-time access decisions. This is context-aware security, and it's the essential tool cloud-first businesses need to keep their enterprises safe from the next security breach.

©2023 Zscaler, Inc. All rights reserved.

The Solution

Context-aware security lets organizations confidently fine-tune access decisions in real time and at scale, securing company assets without sacrificing usability.

Context-aware security looks beyond basic user credentials when assessing access requests, providing admins with deep, informative supporting insights, at scale and in real time. By leveraging shared telemetry from endpoint, network, and cloud applications, teams can dynamically assess every user device, its location, what network the user is connected to, and other crucial contextual details, for smarter decisions.

The Zscaler and CrowdStrike integration makes context-aware security a reality, enabling organizations to effortlessly combine and interpret threat intelligence data so they can minimize the risk of lateral movement, prevent data loss, and deliver fast detection and rapid remediation in the face of emerging threats. This shared information helps customers establish context-driven security controls that work across devices, servers, the public cloud, and cloud applications.

Context-aware security lets any organization provide reliable, secure, frictionless access for a mobile, global workforce, improve access control over third parties, simplify internal architecture, and close security gaps to keep opportunistic threat actors at bay. Enabling deep visibility into granular user- and device-specific context, this deep integration informs faster, smarter access decisions, hardening defenses against even the most sophisticated ransomware threats and cyberattacks.

The integration supports a strong Zero Trust security posture, helping companies confidently connect genuine, authenticated users directly to the applications they need without unnecessary friction. Zscaler and CrowdStrike can enable secure, seamless access to essential business applications in the data center or in the cloud, all while hardening enterprise defenses by denying threat actors a foothold to exploit.

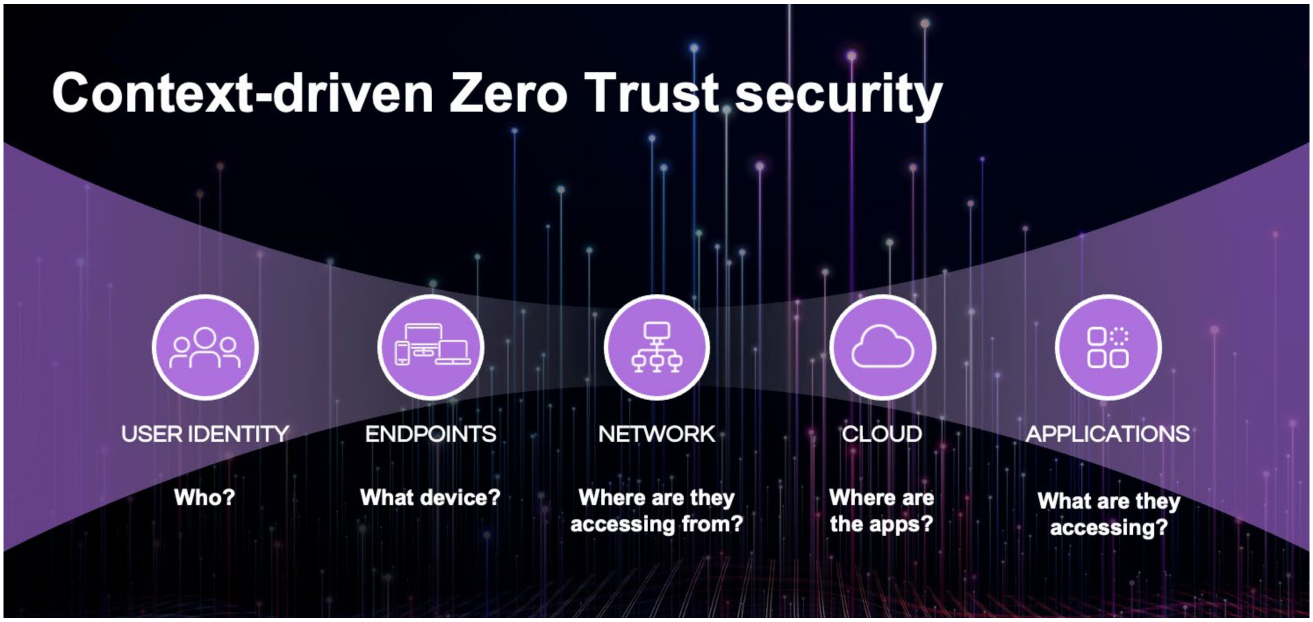
Key Benefits of the Zscaler + CrowdStrike Integration

- Give enterprise teams real-time visibility into critical context through high-fidelity telemetry sharing
- Leverage artificial intelligence (AI) and machine learning to stop known and unknown threats in real time
- Automate your workflow for faster investigation and threat hunting with extended detection and response (XDR)
- Identify compromised users and prevent lateral movement by automating remediation or quarantine
- Secure your enterprise with deeply integrated, industry-leading platforms, backed by best-of-breed platforms

©2023 Zscaler, Inc. All rights reserved.

What context really means when it comes to access requests

Context is broadly used to describe additional details that help convey deeper understanding of a situation. In the world of hybrid work and remote access, context means supplying security and IT teams with additional qualifying information for access requests, so they can make more informed decisions. Additional data points can include identity (Is this person an employee or a contractor? What's their role and group status?), device (Is this a managed or unmanaged device?),location (Is the request coming from a restricted region or IP address?), request (What security policies govern the resources in question? Is the requester looking for full overwrite/ delete powers, or read-only access?), what applications they are trying to access, where these applications are and more.



Context-driven Zero Trust security

USER IDENTITY
Who?

ENDPOINTS
What device?

NETWORK
Where are they accessing from?

CLOUD
Where are the apps?

APPLICATIONS
What are they accessing?

Together, CrowdStrike and Zscaler bring that context to bear across the enterprise. With the joint solution in place, access becomes more than just a policy enforcement point—it's effectively a new perimeter, fed by a continuous integrated data stream that permits fluid real time and continuous verification that adapts to changes in the enterprise ecosystem as they happen, keeping the enterprise safe without impeding efficiency.

How enterprises can leverage context to harden security

Here's how Zscaler and CrowdStrike's products, deeply integrated into a customer's tech stack and across devices, work together to provide game-changing visibility into the critical context behind every access request.

CrowdStrike monitors user and device activity, while Zscaler manages access traffic and issues direct application access. The CrowdStrike Falcon® platform produces the context, for example by synthesizing endpoint data to

©2023 Zscaler, Inc. All rights reserved.

produce device posture scores in real time. This context is added to access requests which then proceed through Zscaler's Zero Trust Exchange, where policies are enforced for app access. The added visibility reduces the burden on case-by-case investigation, supporting quicker, safer, and more decisive responses. Finally, this context-aware security establishes a solid basis for continuous, automated enforcement, such as a new policy of automatically quarantining users whose identity seems to be compromised.

CrowdStrike and Zscaler: Leveraging context-aware security to make smarter, safer access decisions

The expanding challenge of securing a modern, fast-evolving corporate ecosystem isn't slowing down anytime soon. Some organizations may continue to prioritize the efficiency of frictionless access over growing security concerns, and may accept the risks of providing over-privileged access. But as the accelerated pace of recent breaches demonstrates, this is an increasingly dangerous path. Zscaler and CrowdStrike have a better way.

Shared intelligence brings a wealth of critical context to bear in real time. Smart tools let enterprise teams compare anomalous situations against known and emerging threats. A clearer picture of what's really going on enables fast, reliable access decisions and automated remediation (including user quarantine) by policy. For Zscaler and CrowdStrike's joint customers, this deep integration maximizes access efficiency and minimizes risk, reduces their attack surface, prevents lateral movement by threat actors, and provides rapid response and remediation, so organizations can focus on growing and prospering.

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.

©2022 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, and ZPA™ are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

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.

Learn more: https://www.crowdstrike.com/

Follow us: Blog | 🐦 | in | f | ◎

Start a free trial today:
https://www.crowdstrike.com/free-trial-guide/

© 2023 CrowdStrike, Inc. All rights reserved.