



Enhance Your Zero Trust / SASE Strategy with Individualized Risk Data

The Problem

According to Forrester, 59% of security leaders recognize the need for a more holistic insider risk management program as part of their Zero Trust Strategy. Security leaders are challenged to protect higher-risk users, reduce the probability of a breach through proactive scaled responses, and maintain workforce productivity without adding additional burdens to security operations teams.

Through easy integrations with Zscaler and the other technologies in your defensive stack, Elevate creates a risk score similar to a credit score based on each individual's behaviors, decisions, data handling, and attack history. With Elevate's context of individual risk and its logic engine, these technologies can now make better decisions - either by managing authentication and authorization policies for applications, or by creating access recertification with the context of how risky an individual is.

With these capabilities, Elevate and Zscaler allow security teams to make better security decisions and automate responses to protect the business.

The Solution

Elevate Security provides a deep understanding of individual risk within your workforce. Integrating with Zscaler's rich telemetry and aggregating it with other indicators from your security stack, Elevate provides a detailed view of a user's activity, decisions, data handling, and threat history, enabling visibility to the organization's riskiest (and safest) users.

Elevate Security & Zscaler — An Integrated Solution

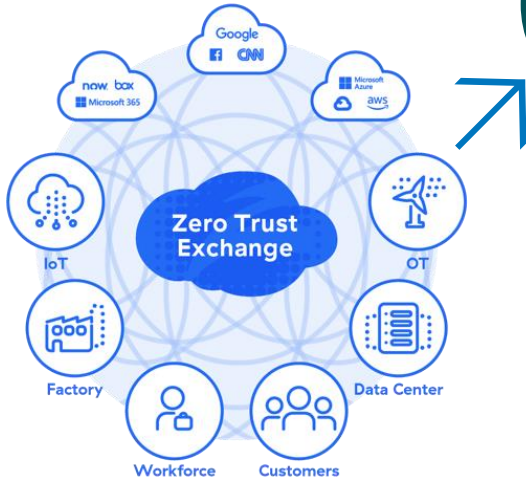
Together, Zscaler and Elevate increase the effectiveness of Zero Trust Network Access (ZTNA) and SASE strategies by adding user risk to existing identity traits. Elevate collects user information, device data, and employee behavior indicators across many vectors, including email security, Endpoint Detection and Response (EDR), web security, Security Information and Event Management (SIEM) tools, and other technologies, including Zscaler. With this information, automated conditional policies can better protect users, requiring Multi-Factor Authentication (MFA), limiting access to those on an approved device, limiting web access, and even driving specialized training and feedback.



Leverage Zscaler's high-resolution telemetry to gain deep actionable insights and attain a robust security posture infused with additional identity meta-data

Zscaler Cloud

Cloud NSS Data Feed — Push events from Zscaler Cloud to Elevate Security Platform via Cloud NSS data feed



Elevate Security Platform

Data Input Service — Facilitates data inputs to the Elevate Platform

Other Data Integrations



- Device Mgmt.
- DLP
- EDR
- Email Security
- Identity Mgmt.
- HR / Workforce Data
- SIEM
- Simulated Phishing
- Web Security

Better Together

Data is pushed from Zscaler Internet Access (ZIA) using Cloud Nanolog Streaming Service (NSS) in real-time to the Elevate Security Platform. Elevate Security's proprietary data science models automatically quantify the risk level of each individual in a credit-like risk score based on each individual's behavior, decisions, data handling, and attack history. Leveraging Zscaler's high-resolution telemetry along with Elevate's out-of-the-box and customizable playbooks, security teams can respond to user-based risks in near real-time with tailored responses in identity management and governance technologies based on each individual's risk levels.

For example, a developer with access to sensitive source control exhibiting other characteristics of account take-over can have their access modified, be required to present authentication factors that cannot be easily taken over such as hardware tokens, and have their existing sessions revoked—severely limiting an adversary's ability to achieve persistence. These decisions can be made on an individual basis, or to groups of employees as needed to appropriately manage the risk to critical data and systems without preventing employees from doing their jobs.

About Zscaler



Zscaler (NASDAQ: ZS) accelerates digital transformation so 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 in-line cloud security platform.