Elevate Security | CISCO DUO

Cisco Duo and Elevate Security

Adding User Risk Intelligence to your Zero Trust Strategy

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. They are challenged to protect higher risk users, reduce the probability of a breach through proactive scaled responses, and maintain workforce productivity without adding additional burden to the SecOps team.

The Solution

Elevate transforms your Duo security framework by adding 'user risk' as a factor when making access decisions. Elevate generates human risk scores based on verified threat signals, allowing Duo to grant or deny access based on risk, along with factors such as device, location, connection, etc. You protect risky users while maintaining the productivity of lower-risk users.

An Integrated Solution

Duo and Elevate work together via automated bi-directional API data flows to increase the effectiveness of your Zero Trust and conditional access strategies. Duo feeds login and device intelligence, including device-type, OS, browser, and many more data points, to Elevate where it is incorporated into user risk score analysis. In turn, Elevate provides comprehensive individual risk data back to Duo, empowering Duo's adaptive access policies to be tailored to an individual's broad spectrum risk level and patterns.

Identify and Safeguard Your Riskiest People

Human Risk Visibility

Elevate scores cyber risk at the employee level, allowing security teams to track overall organizational risk, and zero in on the most likely sources of the next security incident.

Smarter IAM

Elevate injects user risk data into authentication and access review workflows to enable conditional access to sensitive resources based on user risk profiles.

Better Defenders

Elevate uses personalized, near real-time feedback nudges to inform workers of poor behaviors along with tailored training assignments for security awareness.

Use Case:

Conditional Access for a High-Risk Developer

Walter

High-Risk

Developer w/access to source code

Recently downloaded malware

Clicked on phishing links

Bad browsing habits

Dynamic Response to Human Risk

→ Duo and other security tools, e.g., web gateway, email filter, and phishing simulation, feed data about Walter's decisions and actions to Elevate's deep analytics engines.

→ Elevate identifies that Walter's risk level has exceeded acceptable thresholds and implements Risk Detection Rules (RDR) that move Walter to a custom risk group called High-Risk Engineers. Note that Elevate RDRs can be integrated directly to apply Duo Adaptive Access Policies.

→ Duo Access responds by applying predetermined 'High-Risk Engineer' Conditional Access Policies to Walter, e.g., enforcing MFA, requiring a company-authorized device, limited application access, and ensuring only a verified connection.

→ Walter is provided exactly the access his risk level affords while the productivity of normal and lower-risk Employees are unaffected.

BETTER TOGETHER

Confidently implement automated adaptive access policies that are highly-tuned to the needs of each user.

Dynamically apply stringent access protections that would be unacceptable across the entire user population.

Drive lower incident rates, lower organization-wide risk, and less user-generated incidents requiring triage and response.

About Cisco Duo

Duo combines security expertise with a user-centered philosophy to provide two-factor authentication, endpoint remediation, and secure single sign-on tools for the modern era. It's so simple and effective, you get the freedom to focus on your mission and leave protecting it to us.

Book a demo to learn more about safeguarding your business, and your riskiest users!

BOOK A DEMO