

Duo and Elevate Security

Adding User Risk Intelligence to your Zero Trust Strategy

Your 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.

Our Solution:

Elevate Security transforms your Duo security framework by adding 'user risk' as a factor in making conditional access decisions. Elevate generates a high-confidence risk score for each user based on their past decisions and behaviors, allowing Duo to block or grant access based on individual risk levels along with traditional factors such as device, location, connection, etc. This transformation allows security teams to protect high-risk workers while maintaining the productivity of the majority population of lower-risk users.

Elevate Security and Duo Integrated Solution:

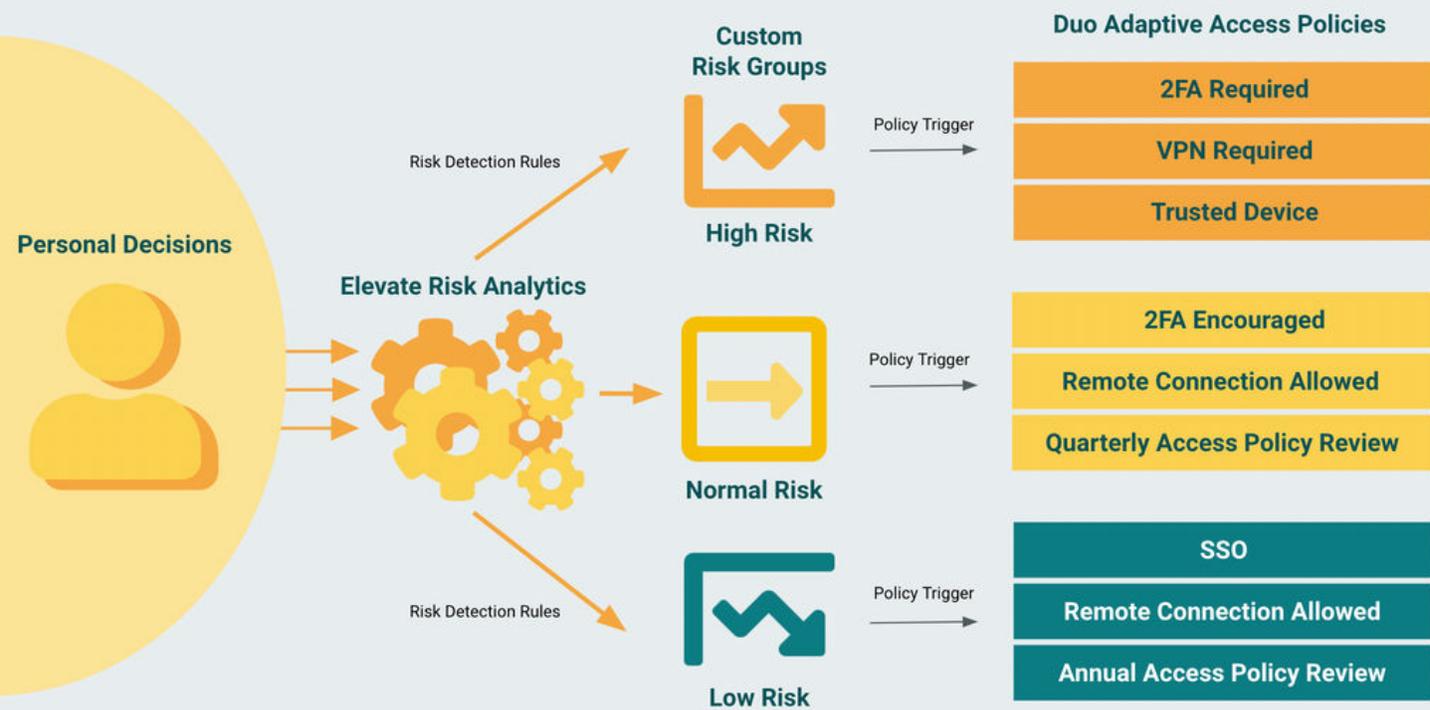
Duo and Elevate work together, via automated bi-directional API data flows, to increase the effectiveness of your Zero Trust and Conditional Access strategies. Duo feeds login and device intelligence, including device type, OS, browser, and many more data points to Elevate where it is incorporated into user risk score analysis. The Elevate platform, in return, provides comprehensive individual risk data back to Duo, empowering Duo's Adaptive Access Policies to be custom tailored to an individual's broad spectrum risk level and pattern.

Better Together.

By incorporating Elevate risk intelligence into an integrated Duo solution, customers gain the confidence to implement automated adaptive access policies that are highly tuned to the needs of each individual user. High-risk users can be afforded more stringent protections than would be acceptable across the entire user population, while those who have proven themselves to be lower risk are afforded policies that enable high productivity and worker satisfaction. The security team benefits from a best-practice approach to individual user risk management with lower incident rates, lower organization-wide risk, and less user-generated incidents requiring triage and response.

Use Case Example: Tailored Protections for a High-Risk Developer

Elevate / Duo Adaptive Human Protection



- DevOps Engineer, Walter, takes actions that increase his risk—visiting questionable websites, refusing training, and downloading malware.
- 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 workers is unaffected.

About 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.

About Elevate Security:

Elevate is a leading provider of cyber risk intelligence that helps organizations radically improve how they make and apply security decisions and better protect workers from targeted attacks. The Elevate Platform combines advanced risk analytics, decision modeling, and data science in an open and extensible platform that allows organizations to visualize and reduce workforce risk, enable risk-based safeguards, and understand and apply risk trends.