Elevate Security

SOLUTION GUIDE

Smarter Identity and Access Management

Your Problem:

Today, you don't know the real risk behind attempts to access your systems. Basic identity data – user credentials, location, network, and devices aren't a comprehensive risk profile.

If you're not authenticating real user risk during access, your chances of an adversary gaining persistence increase.

Without user risk, Access Reviews are burdensome, complex, and often result in managers approving broad entitlements to avoid user denial of service.

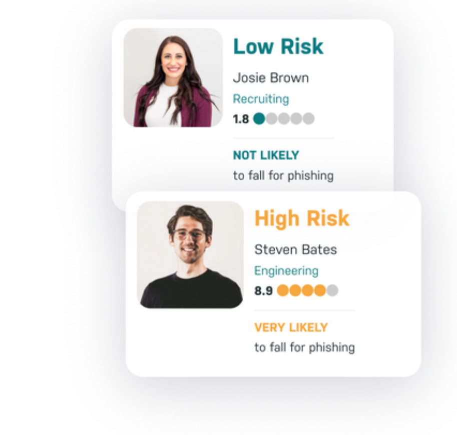
Our Solution:

Elevate provides a 360° profile of the human risk behind each access attempt. By enhancing Identity Access Management (IAM) with Elevate user risk data, security teams can make better decisions during the authentication process, leading to reduced incidents of unauthorized access, and helping minimize post incident clean up.

With user risk data, Access Reviews are triggered by changes in risk profile, reducing overall AR burden, while increasing focus on (a small number of) high risk users.

Identity Management Made Smarter with Elevate

Elevate works with IAM systems to increase the effectiveness of your Conditional Access strategies by gathering context from across the estate, including email security, Endpoint Detection and Response (EDR), web gateways, SIEMs, and other technologies. This current, high-confidence risk signal is based on user decisions, behavior, and attacks already targeting them.



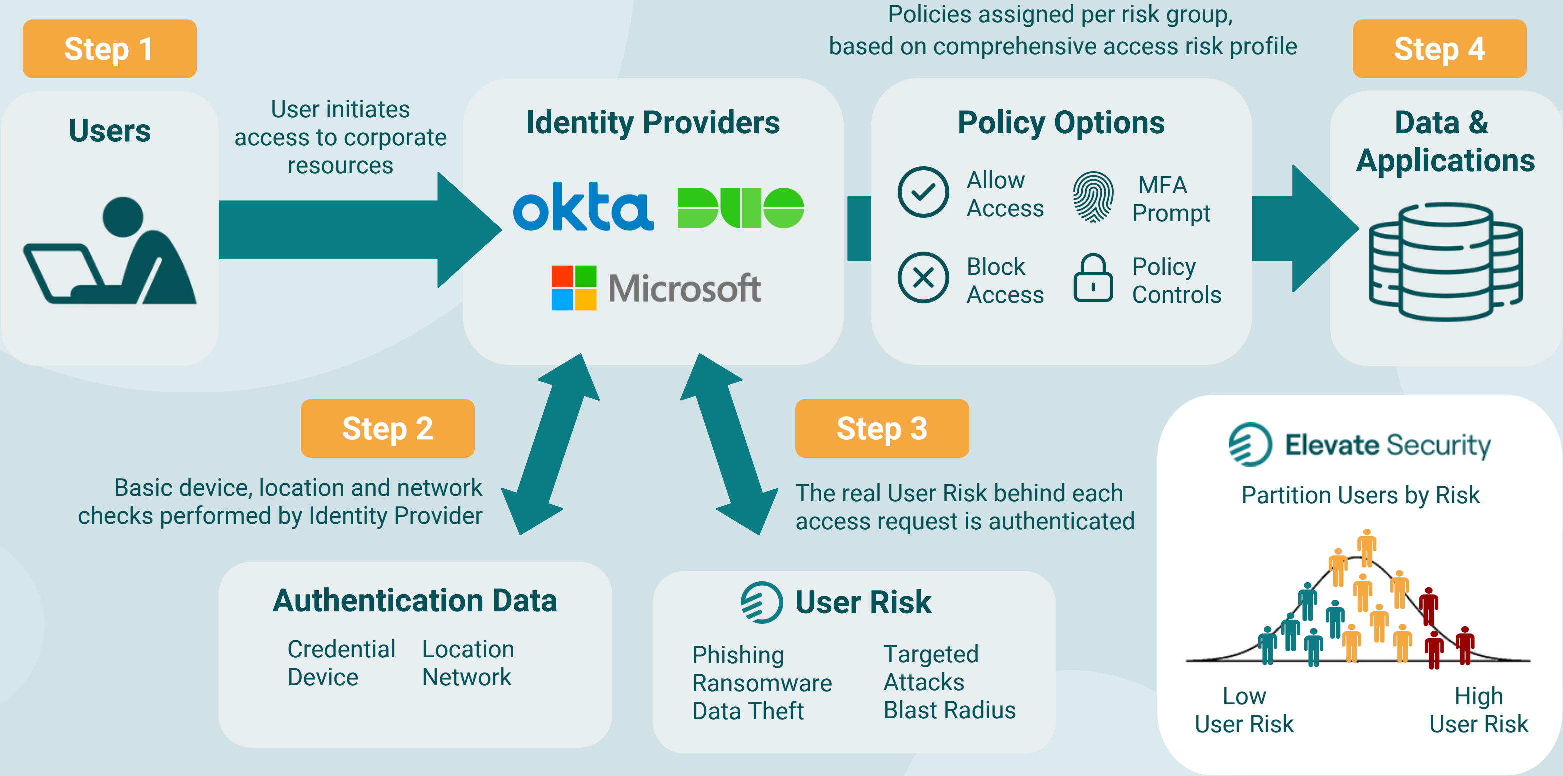
User Risk Partitioning

Leveraging detailed, full-spectrum risk data, Elevate partitions users into specific risk groups. Integrating directly with Microsoft Active Directory, Elevate continuously updates individual group membership as risks evolve. For example, dev/ops engineers with rising malware risk factors might be added to a risk group entitled, 'High Risk - Malware'. Inclusion in any particular risk group subjects the individual to that group's policies, i.e., limiting access, requiring MFA, applying additional policy controls, kicking off an risk-based access review, etc.

Better Together

By incorporating Elevate risk data into an integrated Identity Management solution, customers can confidently implement adaptive access policies tuned to the risk of each user. High-risk users can be afforded more stringent protections that would be unacceptable if applied across the entire user population. At the same time, lower risk users can be afforded policies that balance their risk with the benefits of high productivity and worker satisfaction. The security team gets a best practice approach to IAM with lower incident rates, lower organization-wide risk, and less user generated incidents requiring triage and response.

Smarter IAM with Elevate Authenticated User Risk



Step 1

Users

User initiates access to corporate resources

Identity Providers

okta DUO Microsoft

Policies assigned per risk group, based on comprehensive access risk profile

Policy Options

Allow Access

MFA Prompt

Block Access

Policy Controls

Step 4

Data & Applications

Step 2

Basic device, location and network checks performed by Identity Provider

Step 3

The real User Risk behind each access request is authenticated

Authentication Data

Credential
Device
Location
Network

User Risk

Phishing
Ransomware
Data Theft
Targeted Attacks
Blast Radius

Elevate Security

Partition Users by Risk

Step 1: User initiates a request to access corporate applications and data
Step 2: Identity provider runs basic checks on credentials, device, location, and network
Step 3: Elevate authenticates the true risk of the user behind the request
Step 4: Better informed and smarter policy decisions are made during the authorization process

Partitioning users by risk during the authentication and authorization process, lets security teams frustrate adversaries attempting unauthorized access, with less likelihood of successfully establishing persistence and performing lateral movement. Also, because Elevate integrates directly into core security automation and triage tools (SIEM, Case Management, and SOAR) security teams can prioritize, triage, and drive additional security workflows based on user risk.

Why Add User Risk to Identity and Access?

Without User Risk Data	With Elevate User Risk Data
Access decisions are limited (e.g., auth or block)	Access policies are adjusted dynamically according to each user's risk
When an insider threat appears, the organization is vulnerable during slow manual investigation and intervention	Increases in a user's risk profile automatically trigger **mid-session** reevaluation / revocation (e.g., MS CAE) often before a threat materializes
Access Reviews across the general population are burdensome, complex, and often result in broad entitlements to avoid user denial of service	Access Reviews are triggered by risk profile, reducing overall burden, while increasing focus on (a small number of) high risk users

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 AI 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.
Learn more at https://elevatesecurity.com/