Elevate Security

PRODUCT BRIEF

Smarter Identity and Access Management

Your Problem:

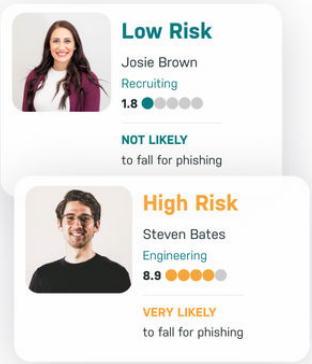
Today, you don't know the user risk behind an attempt to access your systems. Basic Identity data – user credential, location, network, and device - doesn't offer insight into the risk profile of the person behind the access attempt. Without visibility into user risk at the time of authentication and authorization, your chances of overprovisioning access to a high risk user, or worse, letting an adversary in and allowing them to achieve persistence, increase dramatically.

Our Solution:

The Elevate Security platform adds comprehensive user risk information that enriches traditional Identity data, providing a 360° profile of the human 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 avoid post-incident clean up.

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.



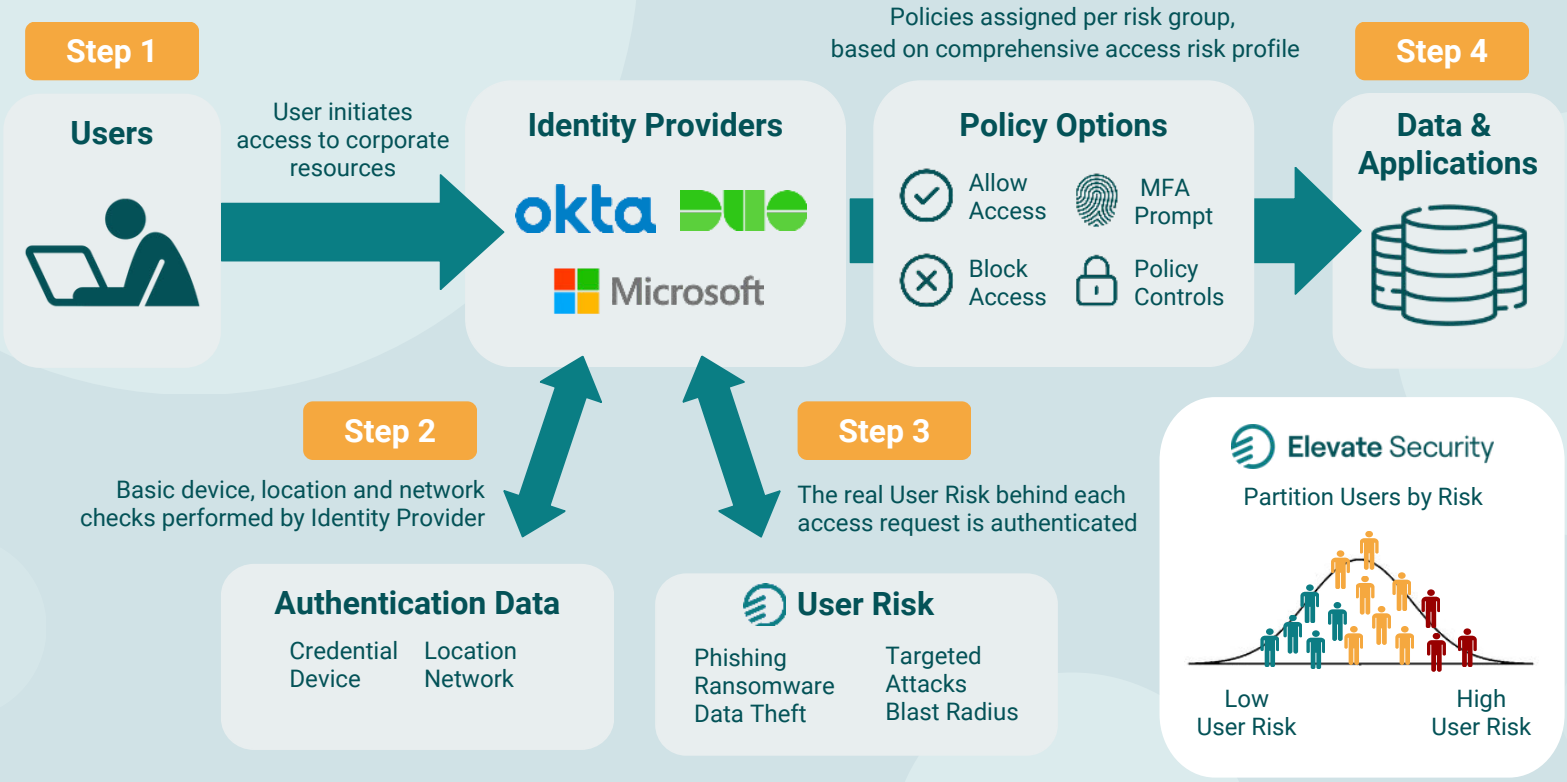
User Risk Partitioning

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, DevOps 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 intelligence into an integrated Identity Management solution, customers can confidently implement adaptive access policies tuned to the risk of each group. 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: 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

By segmenting users by risk during the authentication and authorization process, security teams can frustrate adversaries attempting to gain unauthorized access, with less likelihood of an adversary 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.

Quantify risk across the organization, and identify areas where increased controls and processes are needed to reduce your aggregate risk profile.

Book a Demo

Elevate Security

0223 V3