Elevate Security

Elevate Identity

Identify and Safeguard Your Riskiest Users

Research finds that a small percentage of employees contribute to the majority of an organization's security incidents. Amplifying the problem, identity management teams have no reliable method to pinpoint these users in order to better protect them and strengthen their access to sensitive systems and data.

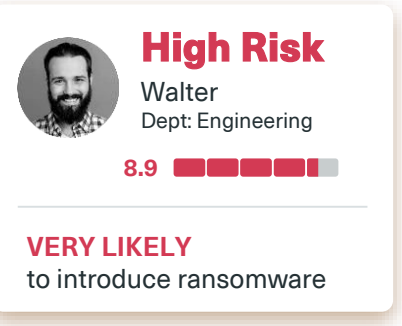
Without visibility into a user's risk profile at the time of authentication, the chances of an adversary entering and gaining persistence dramatically increase.

Elevate Security solves this problem by helping you identify who is most 'at-risk' and automating your response and controls to reduce account takeover attacks, and slash the amount of time an adversary can maintain persistence in your environment.

The **Identity** package of Elevate helps you make smarter access decisions by enforcing conditional access policies and reviews based on verified user risk behaviors. Let's look closer!

Strengthening Identity Management for 'High-Risk' Users

Elevate ingests & aggregates data from your enterprise to identify and score individual risk based on behaviors and attack history



USE CASE:

Walter—a very risky user!

- Developer w/source code access
- Recently downloaded malware
- Browsed to sites he shouldn't
- Clicked on phishing links

Elevate injects user risk data into identity systems to automate conditional access policies, revoke access based on verified threat signals, and enhance access governance reviews

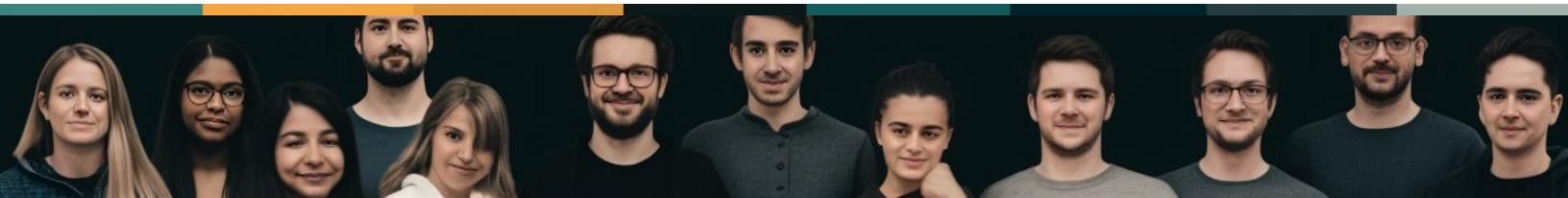
Elevate Identity helps you better protect employees like Walter. Given his role and actions that exceed his risk threshold, Elevate automatically adds him to a 'High-Risk' DevOps group where he'll be subject to conditional access policies the next time he authenticates, including:

Require Phishing Resistant MFA

Login from a Trusted Location

Use Company Compliant Device

OR, break glass and lock down the account!

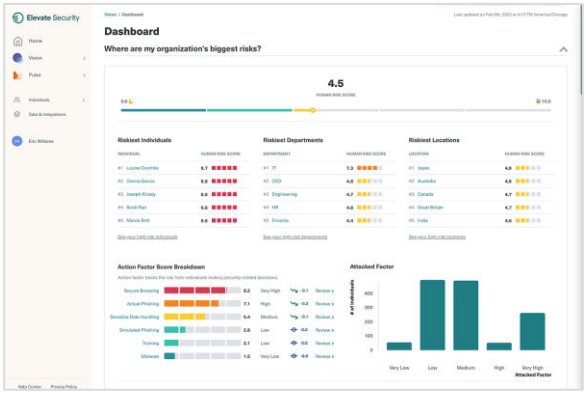


Elevate Security

Elevate works with Identity & Access Management (IAM) and Identity Governance & Administration (IGA) systems to automate conditional access policies, real-time access evaluations, and intelligent entitlement review workflows. Context and insights are built through API integrations with core security technologies such as email security, endpoint, web gateways, and other tools, to generate high-confidence risk signals based on user behavior and patterns of attacks.

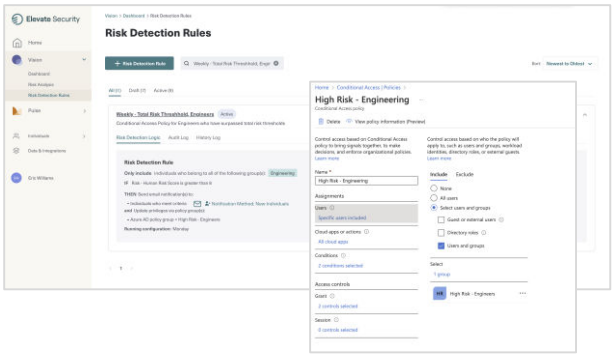
The Elevate Dashboard

The Elevate Vision Dashboard details riskiest individuals, departments, locations, as well as the factors driving each user's risk



Automating conditional access for high-risk users

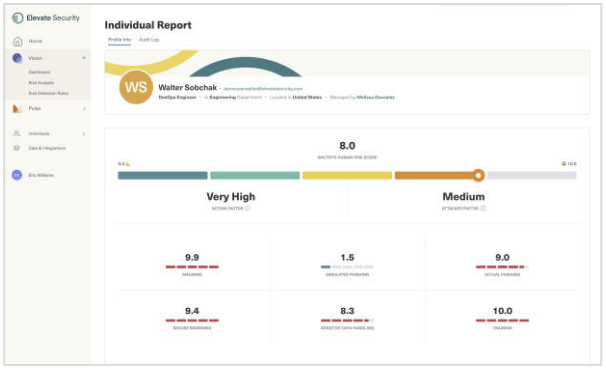
Easily create conditional access policies dynamically mapped & tailored to user risk levels, enabling granular control such as imposing enhanced MFA, device restrictions, or trusted location requirements



Intelligent access reviews

Inject user risk data into access governance workflows to ensure the right level of approval scrutiny

BOOK A DEMO



Elevate Identity enables dynamic access policies, continuous access evaluations, and smarter access reviews. High-risk users receive strict protections, resulting in reduced incidents, lower cybersecurity risk, and fewer events requiring costly triage and response.

Visit us at elevatesecurity.com

0423 v1