Elevate Security

4 Steps to Achieve Smarter Identity & Access Management

During 2021-2022, **84% of organizations experienced an identity-related security breach**. According to CrowdStrike's 2023 Global Threat Report, in 2022, 80% of cyberattacks utilized identity-based techniques to compromise login credentials and deceive security teams. Today, adversaries are refusing to back down on stealing credentials.

Identity-related cyberattacks are on the rise.

As such, the demand for effective identity and access management (IAM) technologies and support is also increasing. Already in 2023, there's been a 112% year-over-year increase in advertisements for access-broker services.

Plus, **the global cloud IAM market size is projected to reach US$ 13.42 Billion by 2027**, at a CAGR of 22.71%.

Why Traditional IAM Solutions are Insufficient Today

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.

Smarter Identity and Access Management

Security teams today need **an IAM solution that provides a 360° profile of the human risk behind each access attempt.** By enhancing IAM with user risk data, security teams can make better decisions during the authentication process. As a result? Organizations experience reduced incidents of unauthorized access and minimized post-incident cleanup.

With Elevate Security...

High-risk users can receive more stringent protections that would be unacceptable if applied across the entire user population.

Lower-risk users can receive 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.

4 Steps to Achieving Smarter IAM with Elevate Security

Step 1: Users

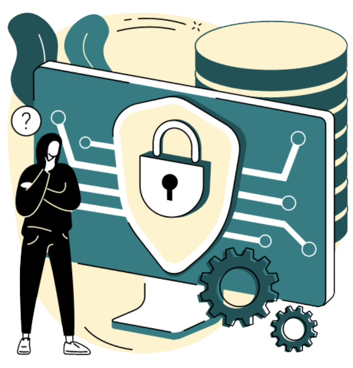
The user initiates access to corporate data and resources, including Okta, Duo, Microsoft, and more.

okta DUO

Microsoft

Step 2: Identity Providers & Authentication Data

The identity provider runs basic checks on credentials, device, location, and network to authenticate data.



Step 3: User Risk

Elevate authenticates and vets the real user risk behind each access request for potential issues, such as:

- Phishing
- Ransomware
- Data theft
- Targeted attacks
- Blast radius

Step 4: Policy Options, Data & Applications

Conditional policies are assigned based on a comprehensive user risk profile. Policy options might include:

- Allow access
- Block access
- MFA prompt
- Policy controls
- more...

Improve your cyber defense at the point of access—enhance your IAM policies and protocols with Elevate's user risk data.

Book your demo

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 elevatesecurity.com.