Strengthen Your Identity Governance with Human Risk Intelligence

Identity Governance and Administration (IGA) solutions enable user productivity, protect access to critical resources, and help demonstrate compliance with any number of data protection regulations.

- Users get the right access to the right assets at the right time
- Managers no longer need to contend with the complexities and confusion of manual access governance reviews that often result in compliance violations and weaker defense
- The business gains the many efficiency, cost saving, and defense-in-depth benefits that come from implementation of automated access governance policies and workflows

Further, when combined with complementary identity management tools such as Single Sign-On (SSO) and Multi-Factor Authentication (MFA), enterprise defense against adversaries strengthens dramatically.

Yet, despite deployment of world-class identity management, a persistent cybersecurity gap still exists—human risk. Let's explore.

Today's Biggest Cybersecurity Gap, Human Risk

The research is clear. Verizon's annual Data Breach Investigations Report consistently finds that the bulk of all enterprise breaches involve the human element. At Elevate Security, we've crunched the data. Elevate research—built upon 6 years of data analysis of billions of records across email gateways, web gateways, endpoint, data protection, and identity tooling for dozens of Fortune 500 enterprises—concludes that *people* have become the primary attack vector.

Since 2020, Elevate's analytics show adversaries hyper-targeting specific groups of individuals in an organization:

- 82% of delivered phishing emails go to only 5% of employees
- 92% of malware events come from 3% of employees
- 2022 saw a 2.5x increase in targeted attacks against engineers

Beyond the specter of threat actors, Elevate's analytics finds that 8% of employees contribute to 80% of all security incidents! When looking across your estate, consider—

- Who are your high-risk users? What factors contribute to their risk?
- What resources do they have access to and how frequently is their access reviewed?
- What is your risk exposure should their actions introduce an entry point for adversaries?

Today's Biggest Cybersecurity Gap, Human Risk *(Cont'd)*

Elevate Security works with organizations to quantify and make sense of individual human risk. In turn, this detail-rich intelligence can be embedded within existing identity and access management solutions to dynamically initiate additional safeguards and corrective measures before bad behaviors evolve into worst case security incidents—or allow adversaries to gain persistence! Let's dive deeper.

The Realities of Hidden Human Risk

Typically, identity and access management protections are generalized based on job function/business group and sensitivity of assets being accessed. However, in practice, each individual is different and represent a unique risk profile based on their knowledge of security, behaviors, and likelihood of being attacked. Applying a one-size-fits-all approach to identity governance lacks visibility to disparities between good cyber citizens and those individuals engaged in unsecure and risky activities—all subject to change based on factors not yet known or considered.

Elevate Security enables defense against the unpredictability of risky and often hidden behaviors that create unintentional security gaps by applying human risk as a powerful new control factor when provisioning and managing secure access.

Smarter Identity Governance Using Human Risk Intelligence

Building a smarter identity governance solution begins with understanding your organization's workforce risk profile and the cohorts you must embrace and course correct. Elevate Security's human risk management platform ingests and analyzes data from across your enterprise to identify and score individual risk based on behaviors and attack history resulting in near real-time human risk intelligence that may be applied as a condition of access.

Identify and safeguard your riskiest people with automated conditional access and entitlement reviews.

Smarter Identity Governance Using Human Risk Intelligence *(Cont'd)*

Imagine discovery of an employee with privileged access to sensitive data who recently downloaded malware, clicked on phishing links, and browsed unsecure sites. Based on verified threat signals, this newly flagged 'high-risk' user may now be subject to policies and automated workflows to ensure the greatest level of access safeguards. Here's a few ways:

Walter | Sr. Developer

High Risk Employee

8.9

Conditional Access Policies

Automatically apply stricter access requirements, e.g., login from trusted locations, and use compliant devices and/or phishing-resistant MFA.

Continuous Access Evaluation

Automatically revoke access to applications and sensitive resources based on verified risk signals.

Risk-Based Entitlement Reviews

Tie risk signals into identity governance processes to ensure managers and approvers are aware of risk prior to approving access, and/or initiate immediate access reviews.

Working Together: Human Risk Intelligence and IGA

The Elevate Security human risk platform provides an ever increasing number of out-of-box integrations with risk data sources and leading cybersecurity technologies to respond to human risk.

RISK DATA SOURCES

Workforce Data
Email Security
Web Security
IAM
SIEM
Endpoint
Device Mgmt.
DLP

Elevate Security

1 — Identify & Score User Risk

Benchmark & Visualize   Actionable Insights

HUMAN RISK MANAGEMENT

RISK RESPONSE for WALTER   3

2
→ Add to high-risk watchlist
→ Require phishing-resistant MFA
→ Require login from trusted device / location
→ Initiate immediate review of all entitlements
→ Increase frequency of access governance reviews
→ Assign phishing awareness training
→ Provide tailored cyber guidance

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

2 Elevate injects human risk data into identity management, identity governance, and user authentication workflows as a **powerful control factor** for approving or denying access

3 Through personalized feedback, guidance, and use of conditional access and governance requirements—you'll change Walter's behaviors and **drive improved cybersecurity outcomes**

Elevate Security and SailPoint Integration

Elevate partners with SailPoint to enhance defense of user access to critical business assets by providing human risk intelligence as a contextual factor when provisioning and reviewing employee access to enterprise resources.

Because not all employee risk is equal and certain roles are more vulnerable to targeted attack than others, Elevate continuously identifies individual risk and shares this intelligence with SailPoint to improve decision making in provisioning and access governance review workstreams.

Key capabilities:

Pinpoint Risky Employees

Elevate scores human risk across a spectrum of behaviors and attack history.

SailPoint uses this intelligence to strengthen provisioning and access approvals.
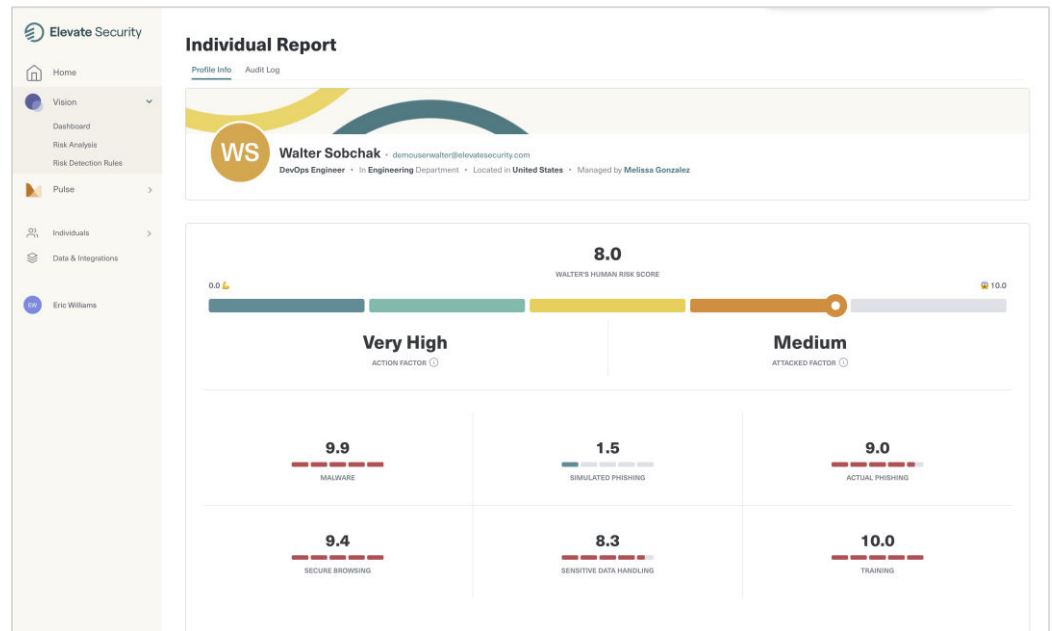
Continuous Access Evaluation

Contextual human risk intelligence may be used to automatically revoke access to applications based on verified threat signals.
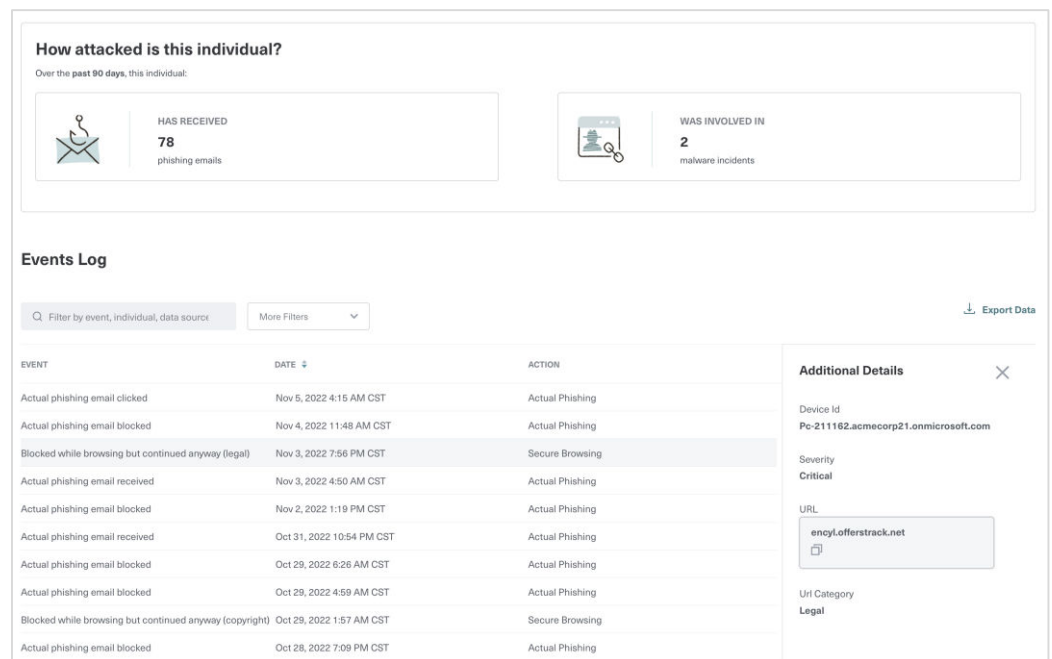
Elevate Security and SailPoint Integration *(Cont'd)*

Risk-Based Entitlement Reviews

Tie risk signals into your SailPoint identity governance processes to initiate immediate access reviews; ensure managers and approvers are aware of risk prior to approving access.

By embedding Elevate's human risk intelligence into your SailPoint identity and access governance workstreams, you'll enable smarter access decision making, strengthen defense of your most valuable assets from risky users, and increase the maturity of your identity capabilities.

Summary and Next Steps

The last few years have shown us that bad actors are targeting employees as the primary attack vector. By understanding this risk and its implications to your business, you can take a focused approach to your response to human risk.

With deep visibility across user attacks, behaviors, and workforce context, you'll have the intelligence needed to dynamically drive advanced human risk automation within your existing identity governance and administration investments—extracting greater value from your existing IGA investments.

Elevate is helping organizations like yours reduce the likelihood of an adversary gaining persistence in their environment, while helping drive measurable behavior changes and improved security outcomes. Contact us to learn more our platform capabilities and discuss how we can help you address and solve your specific human risk challenges.

Visit us at elevatesecurity.com

BOOK A DEMO