



Elevate Engage

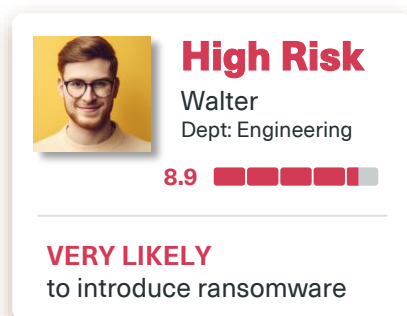
Identify Your Human Risk & Drive Measurable Behavior Change

Research finds that a small percentage of employees contribute to the majority of an organization's security incidents. These users routinely demonstrate unsecure computing behaviors that open the door to worst-case cyber scenarios, and burden security operations teams with costly clean up cycles. Amplifying the problem, there's no reliable way to pinpoint these users in order to provide the interventions and protections needed to mitigate their cyber risk.

Elevate Security solves this problem by helping you identify who is most 'at-risk' and automating your response, allowing you to drive smarter behaviors and defend against real-world threat actors.

The **Engage** package of Elevate uses individual scorecards, targeted training, and personalized feedback when employees go off course to measure and motivate behavior change that builds a strong security culture. Let's look closer!

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



USE CASE: Walter, a risky user

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

Armed with deep visibility into behaviors and patterns that define an individual's risk profile, you're ready for the cool part—*engagement*

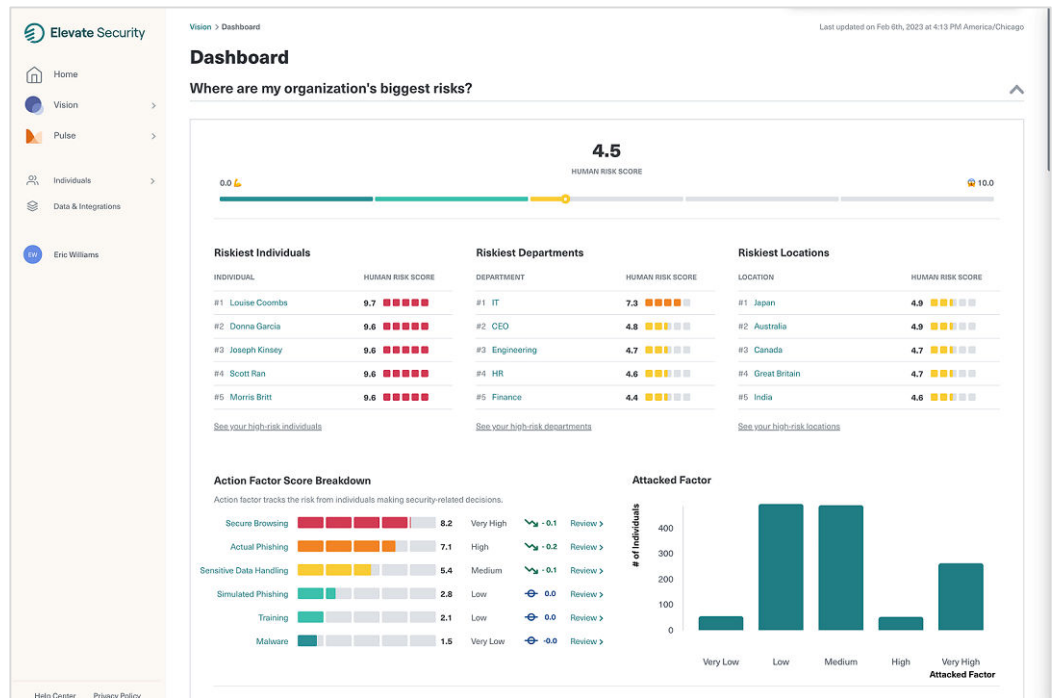
Given his role and actions that exceed his risk threshold, Elevate Engage will automate the right-touch response, at the right time, to get Walter back on track. From assignment of specialized training to **'nudges'** in Slack or MS Teams alerting of policy violations and tips for improvement, you'll proactively course correct employees like Walter.

DYNAMIC RISK RESPONSE

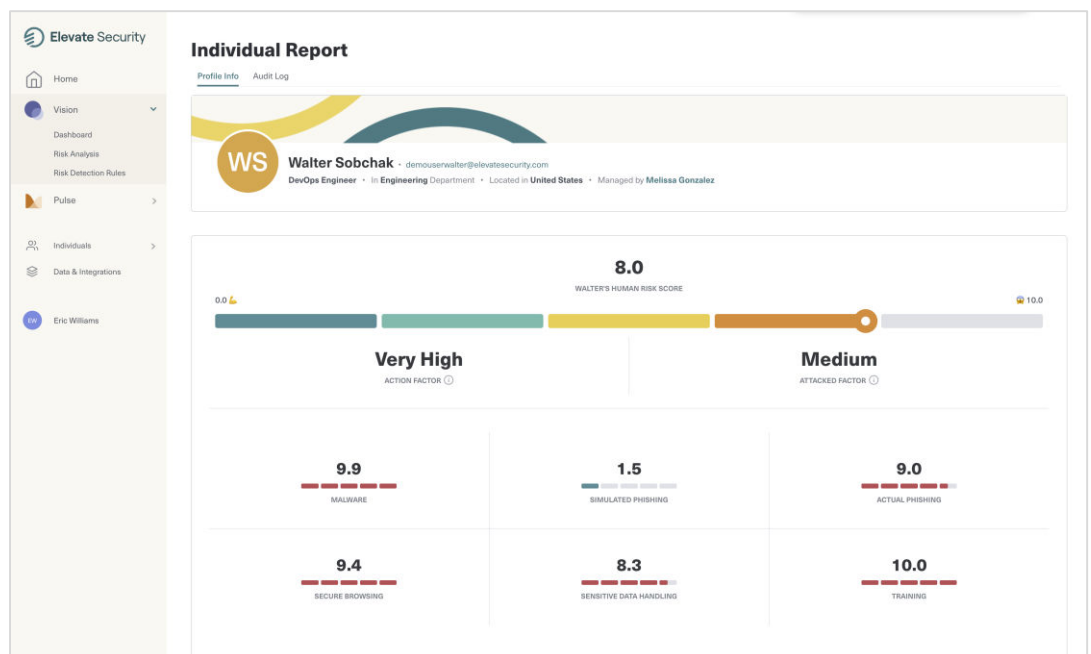
- **Improve security behavior & awareness**
 - Assign phishing recognition training
 - Deliver policy violation alerts
 - Deliver tailored guidance for security improvements
- **Enhance & streamline security operations (SecOps)**
 - Add to 'High-Risk' watch list; share with other security functions
 - Integrate risk profile data into Help Desk/SecOps
- **Strengthen critical asset defense with [Elevate Identity](#)**

A positive security culture starts with measurable behavior change. By deeply understanding the risks of each individual, Elevate Engage helps you make better decisions for protecting your organization and fostering a culture of security accountability and awareness. In turn, you'll flip the segment of people most likely to create worst-case security incidents into your best defenders.

The Elevate Vision Dashboard details riskiest individuals, departments & locations, as well as the factors driving human risk



Individual risk profiles detail verified threat signals that drive unique user risk scores and inform corrective measures



DYNAMIC RISK RESPONSE

Change awareness & behaviors through personalized education, gamification, and friendly touch points to reinforce good security judgement

Employee communications provide tailored feedback and guidance

Phishing & Reporting

Over the past few months, we've sent you a few phishing simulations to see if you were able to detect them!

Phishing is the fraudulent practice of sending malicious emails that try to steal your credentials or download malicious software.

	MAR	APR	MAY
Attack Detected	✘	✘	✘
Reported	✘	✘	✔
Overall	😞	😞	😞

Attack Detected

Best in class: [Progress bar]

Your Department: [Progress bar]

Your Company: [Progress bar]

You: [Progress bar]

Oh no! You are **much more likely** to fall for a phish and submit your credentials than people in your department. You can do better!

Reported

Best in class: [Progress bar]

You: [Progress bar]

Your Company: [Progress bar]

Your Department: [Progress bar]

Nice work! You're **more likely** to report than your department!


Reported Bad: [Icon] You earned a badge!

! Heads up! You can do better.

Our security tools detected you navigated to a site that was blocked because it posed a security threat. Often these sites attempt to introduce malicious software or are disguised with the intent to fraudulently capture sensitive data (i.e., credentials, credit card or personal information).

Additionally, our security tools detected you recently tried to access a site that was blocked because it was known to have malicious or suspicious content. Often these sites host harmful software, spam, or provide unauthorized file sharing that can pose a security risk.

We've detected this risky browsing activity numerous times. In fact, you are 3.7x more likely to browse to a dangerous site than others in your department.



Almost There!

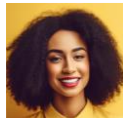
You're **Fortified!** Keep improving on the behaviors below and you will be an expert soon enough.

FLIMSY TENUOUS STURDY **FORTIFIED** INDESTRUCTIBLE

[SEE A DEMO](#)

Right-touch response, at the right time, to the right people

Engage your people to become your best defenders



Low Risk

Sally
Dept: Finance

1.8 [Progress bar]

NOT LIKELY
to fall for phishing exploit

USE CASE: Sally

- Junior Accountant
- Completes assigned training
- Reports suspected phishing
- Good browsing judgement

➔ **Recognize & celebrate good cyber citizens**

- Share social proof affirmation of good cyber awareness
- Celebrate with kudos from management
- Reward with bonus for achieving cyber awareness goals



Elevate Engage allows you to move beyond “check-the-box” training to a personalized communication approach with your riskiest people. The result? You’ll drive behavioral change that builds a stronger security culture and improved cyber outcomes.