Elevate Security

Elevate Identity

Identify and Safeguard Your Riskiest Users

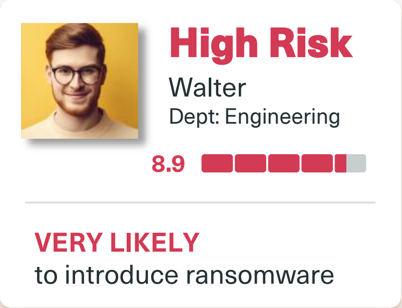
Research finds that a small percentage of employees contribute to the majority of an organization's security incidents. These users routinely demonstrate unsecure computing behaviors that expose sensitive resources to worst-case cyber scenarios. Amplifying the problem, there's no reliable way to pinpoint these users in order to provide the protections needed to strengthen their access to 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 risky users and their actions. In turn, this 'human risk intelligence' may be applied as a condition of access to reduce account takeover attacks.

The **Identity** package of Elevate helps you make smarter access decisions by automating enforcement of conditional access policies based on verified user threat signals. Let's look closer!

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

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



High Risk

Walter

Dept: Engineering

8.9

VERY LIKELY

to introduce ransomware

USE CASE: Walter, a risky user

Developer w/source code access

Recently downloaded malware

Browsed to sites he shouldn't

Clicked on phishing links

Elevate Identity helps you identify and 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—along with proactive engagement for improvement.

DYNAMIC RISK RESPONSE

→ Improve security behavior & awareness

— *Assign phishing recognition training; Deliver policy violation alerts and tailored security improvement guidance*

→ Enhance & streamline security operations (SecOps)

— *Add to 'High-Risk' watch list; share with other security functions*

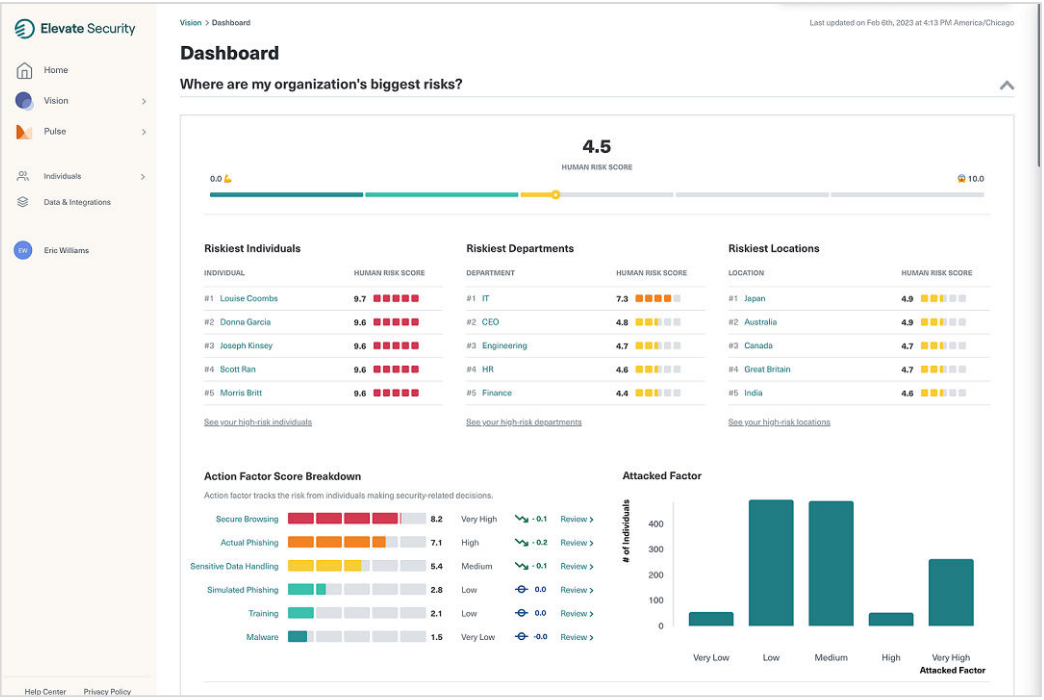
— *Integrate risk profile data into Help Desk/SecOps*

→ Strengthen critical asset defense

— *Require enhanced multi-factor authentication; login from trusted device & location: initiate access governance review*

Elevate Identity strengthens protection of critical assets by providing human risk as a conditional access control in identity and access governance workstreams. Now, in addition to an organization's use of strong authentication such as something an employee has (*token*) or something they are (*fingerprint*), you can apply 'something they are doing' (*threat signals*) as context for access decisions.

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



Last updated on Feb 6th, 2023 at 4:13 PM America/Chicago

Dashboard

Where are my organization's biggest risks?

4.5 HUMAN RISK SCORE

0.0 💪 — 10.0

Riskiest Individuals

INDIVIDUAL	HUMAN RISK SCORE
#1 Louise Coombs	9.7
#2 Donna Garcia	9.6
#3 Joseph Kinsey	9.6
#4 Scott Ran	9.6
#5 Morris Britt	9.6

See your high-risk individuals

Riskiest Departments

DEPARTMENT	HUMAN RISK SCORE
#1 IT	7.3
#2 CEO	4.8
#3 Engineering	4.7
#4 HR	4.6
#5 Finance	4.4

See your high-risk departments

Riskiest Locations

LOCATION	HUMAN RISK SCORE
#1 Japan	4.9
#2 Australia	4.9
#3 Canada	4.7
#4 Great Britain	4.7
#5 India	4.6

See your high-risk locations

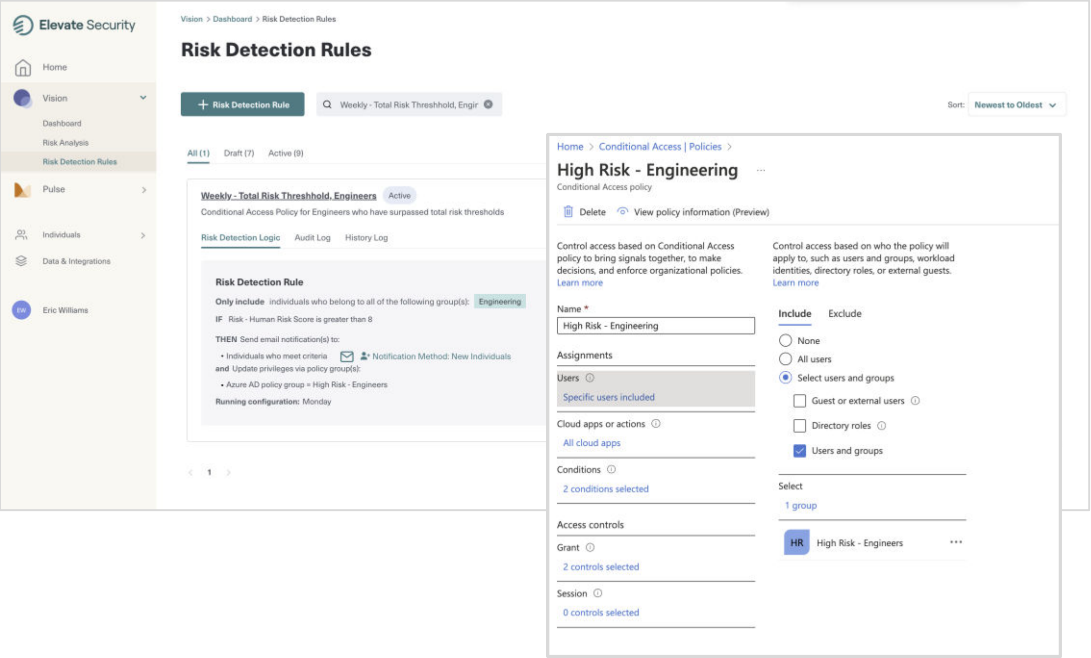
Action Factor Score Breakdown

Action factor tracks the risk from individuals making security-related decisions.

Secure Browsing	8.2	Very High	-0.1	Review ›
Actual Phishing	7.1	High	-0.2	Review ›
Sensitive Data Handling	5.4	Medium	-0.1	Review ›
Simulated Phishing	2.8	Low	0.0	Review ›
Training	2.1	Low	0.0	Review ›
Malware	1.5	Very Low	-0.0	Review ›

Attacked Factor

Easily create conditional access policies mapped to user risk levels, enabling granular control such as enforcing enhanced MFA, device restrictions, or access from trusted locations



Risk Detection Rules

+ Risk Detection Rule

Weekly - Total Risk Threshhold, Engir

Sort: Newest to Oldest

All (1) Draft (7) Active (9)

Weekly - Total Risk Threshhold, Engineers — Active

Conditional Access Policy for Engineers who have surpassed total risk thresholds

Risk Detection Logic Audit Log History Log

Risk Detection Rule

Only include individuals who belong to all of the following group(s): Engineering

IF Risk - Human Risk Score is greater than 8

THEN Send email notification(s) to:

- Individuals who meet criteria ✉ Notification Method: New Individuals

and Update privileges via policy group(s):

- Azure AD policy group = High Risk - Engineers

Running configuration: Monday

‹ 1 ›

Home > Conditional Access | Policies >

High Risk - Engineering ···

Conditional Access policy

Delete View policy information (Preview)

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

High Risk - Engineering

Assignments

Users ⓘ

Specific users included

Cloud apps or actions ⓘ

All cloud apps

Conditions ⓘ

2 conditions selected

Access controls

Grant ⓘ

2 controls selected

Session ⓘ

0 controls selected

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests. Learn more

Include Exclude

○ None

○ All users

● Select users and groups

☐ Guest or external users ⓘ

☐ Directory roles ⓘ

☑ Users and groups

Select

1 group

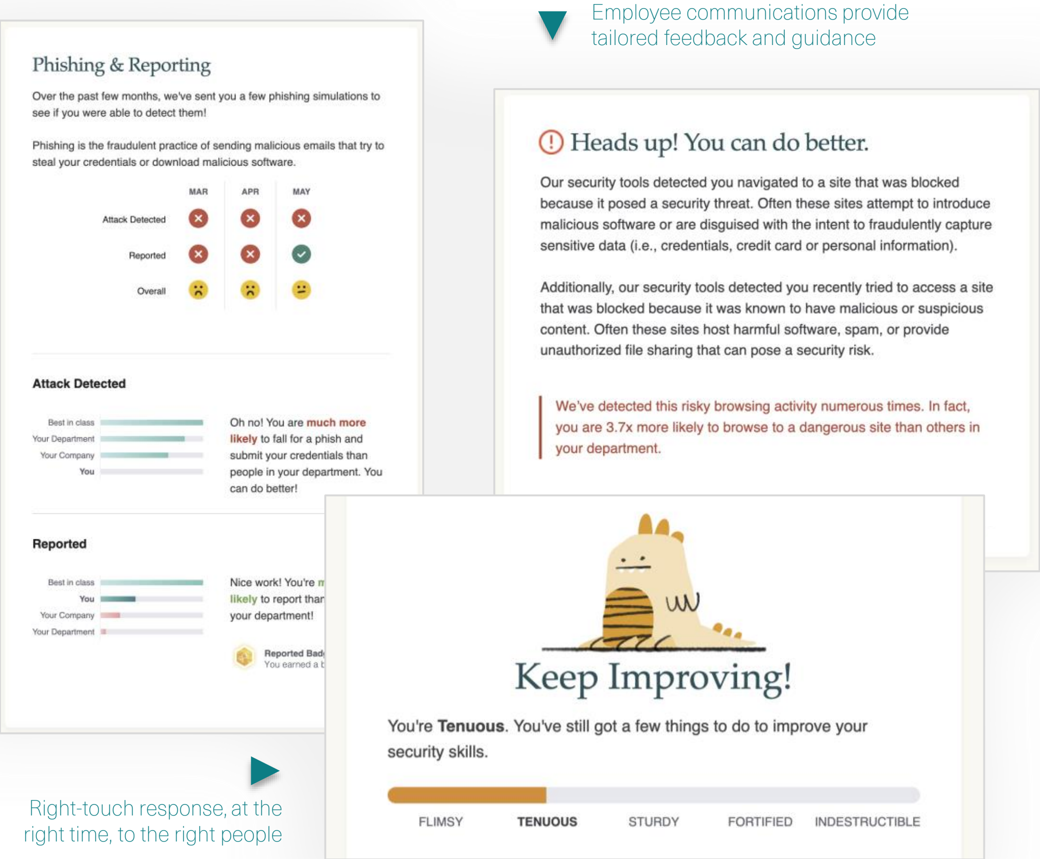
HR High Risk - Engineers ···

Elevate Security

PRODUCT BRIEF

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

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

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

Reported Bad
You earned a b

ⓘ 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.

Keep Improving!

You're **Tenuous**. You've still got a few things to do to improve your security skills.

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

SEE A DEMO

Typically, identity and access management protections are generalized based on job function and sensitivity of assets being accessed. This one-size-fits-all approach lacks visibility to disparities between good cyber citizens and those individuals engaged in unsecure behaviors or in high-risk workgroups.

Identify human risk patterns and trends to proactively protect vulnerable user groups

New Hires

Attack Targets

Sys Admins w/elevated privilege

Low risk behaviors, but focus of targeted attacks. Protect with conditional access safeguards.

Elevate Identity allows you to defend against the unpredictability of often hidden behaviors that create unintentional security gaps by applying human risk as a powerful new control factor in securing access.

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

Visit us at elevatesecurity.com