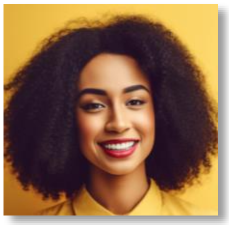
Elevate Security

Dynamic Risk Response

Drive measurable human risk mitigation

Elevate Security ingests and aggregates data from across your enterprise to identify and score individual cyber risk based on behaviors and attack history.

Identify and baseline user risk



Sally
Low Risk

Junior accountant
Completes assigned training
Reports suspected phishing
Good browsing judgement

Walter
High Risk

Developer w/access to source code
Recently downloaded malware
Clicked on phishing links
Bad browsing habits

New Hires
Attack Targets

Sys Admins w/elevated privilege
Good behavior, *but. . .*
Focus of targeted attacks
Vulnerable to false work requests

But, quantifying workforce risk is just the start. Armed with deep visibility into the people, behaviors, and patterns that define your organization's current risk profile, you're ready for the really cool part—dynamic risk response.

What is dynamic risk response?

Dynamic risk response allows you to easily apply policies and automated actions to match the right response, to the right person/group, at the right time, to drive measurable behavioral changes and strengthen security protections. Consider:

Match response to individual risk needs

Sally, a good cyber citizen — *Celebrate!*

- Recognize her efforts with management and social proof affirmation

Walter, a very risky user — *Course Correct!*

- Add to 'high-risk' watch list; enforce use of strong authentication

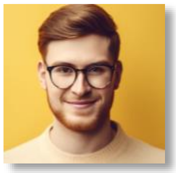
New Hire Sys Admins, vulnerable attack targets — *Protect!*

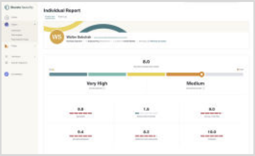
- Alert of attack status; provide best practice guidance and tailored training

Dynamic risk response—How it works

Response to workforce risk is driven by rules managed within the Elevate Security Risk Engine. Risk response rules automate the process of analyzing, identifying, and responding to unique user risk—and are fully customizable. The Elevate Risk Engine works with your specific integrations to inform, notify and take action on an individual's unique risk signals. Let's explore!

USE CASE: Solving for Walter, a 'high-risk' user





BOOK A DEMO

Walter's Risk Signals:

Downloaded malware
Clicked on phishing links
Browses insecure sites

DYNAMIC RISK RESPONSE ACTIONS

→ **Improve security behavior & awareness**

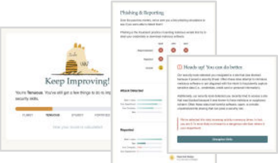
- *Assign phishing recognition training*
- *Deliver policy violation alerts*
- *Deliver tailored guidance for security improvements*

→ **Enhance & streamline security operations (SecOps)**

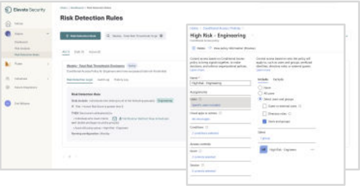
- *Add to 'High-Risk' individual watch list; share with other security functions*
- *Integrate risk profile data into Help Desk/SecOps*

→ **Strengthen system & resource access**

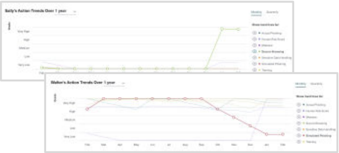
- *Require Multi-Factor Authentication*
- *Require login from trusted location*
- *Require use of company device*
- *Initiate quarterly access reviews*



Modify behaviors & awareness



Better protect critical assets



Report & Track Progress

Dynamic risk response interventions work to significantly reduce security incidents and the likelihood of a breach. Elevate analyzes customer data to identify trends that drive successful outcomes—here's a Fortune 500 customer's recent findings:

Drive measurable behavior change and security improvements

⌄ 73%	⌄ 70%	⌃ 373%
Reduction of **Sensitive Data Handling Incidents**	Reduction of **Phishing Clicks**	Increase of **Phishing Reporting**

Dynamic risk response enables use of interventions that drive real improvements to your overall security posture—and help turn your people into your greatest defenders! Contact us to learn more.

Visit us at elevatesecurity.com