

# Overview

## Elevate Security Bridges the Gap between Firefighting Incidents and Proactively Protecting against Ransomware, Data Loss, and Account Takeover.

One of the most challenging aspects of building a security program is balancing the need to secure the business while maintaining a productive workforce. Elevate Security solves this challenge for enterprise security leaders by enabling deep and predictive visibility into business risks such as ransomware, data loss, and account takeover. Our innovative platform gives your security team playbooks to proactively protect individuals based on our adaptive risk profiling. Using Elevate Security, CISOs can fundamentally transform from a reactive incident response approach to proactively managing them.

With deep visibility into each individual's user reputation (i.e. the actions they take, access they have, and frequency they are attacked), security teams enjoy clear benchmarking on their biggest risks, share real-time and personalized feedback, automate business workflows such as case management, and tailor security controls appropriate to each individual's risk.

Security teams can now take proactive measures to defend their organization with just the right amount of security appropriate to the risk.



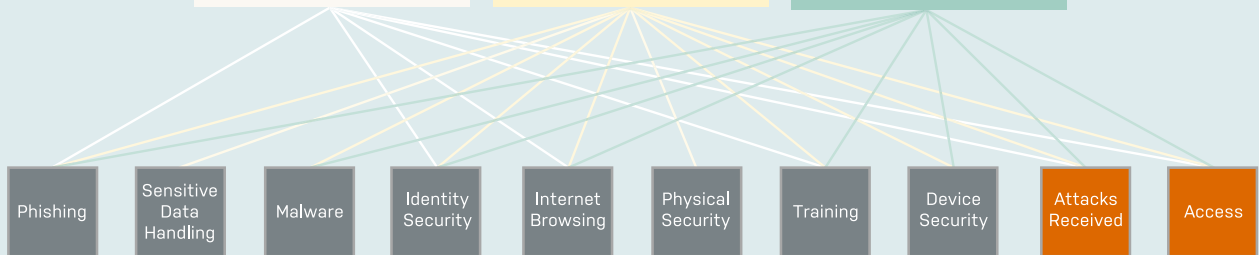
Susie's **Risk Score** Predicts How Risky Her Actions are, and Helps Address that Risk

7.2

"How much risk of **Account Takeover** does this person represent?"  
5.2

"How much risk of **Data Loss** does this person represent?"  
7.6

"How much risk of **Ransomware** does this person represent?"  
8.9



# Take Action on Predictive Risk

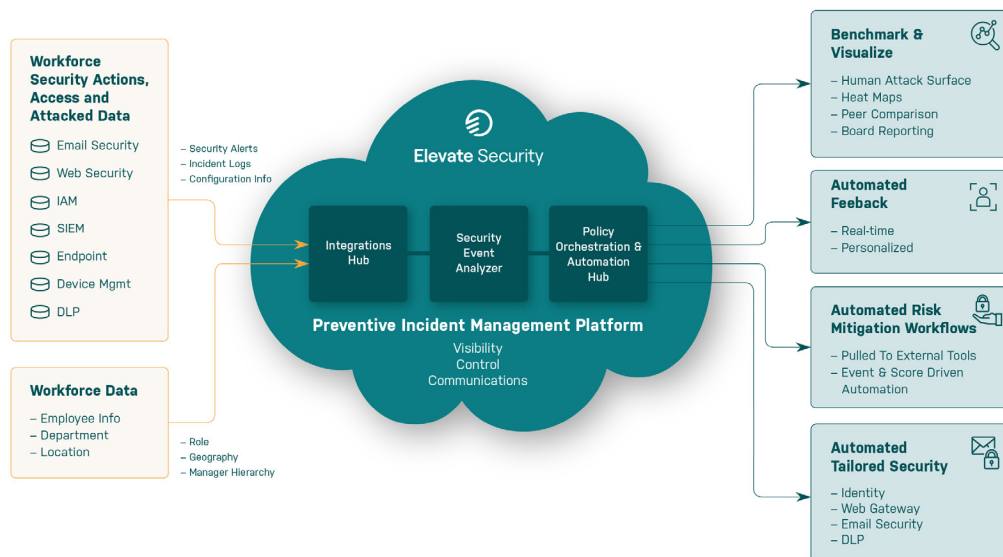
Our industry's approach to managing security incidents for the last decade has been reactive. Something or someone did something wrong, and we've relied on our incident detection to identify it and our incident response process or technology to clean it up. These alerts, notifications, logs, controls, and access details however give deep insights and an historical timeline... if we begin to stitch them together.

The best predictor of future behavior is past behavior. Elevate Security Platform enables your teams to not only understand historical risks, but predictively identify those users most likely to cause future incidents.

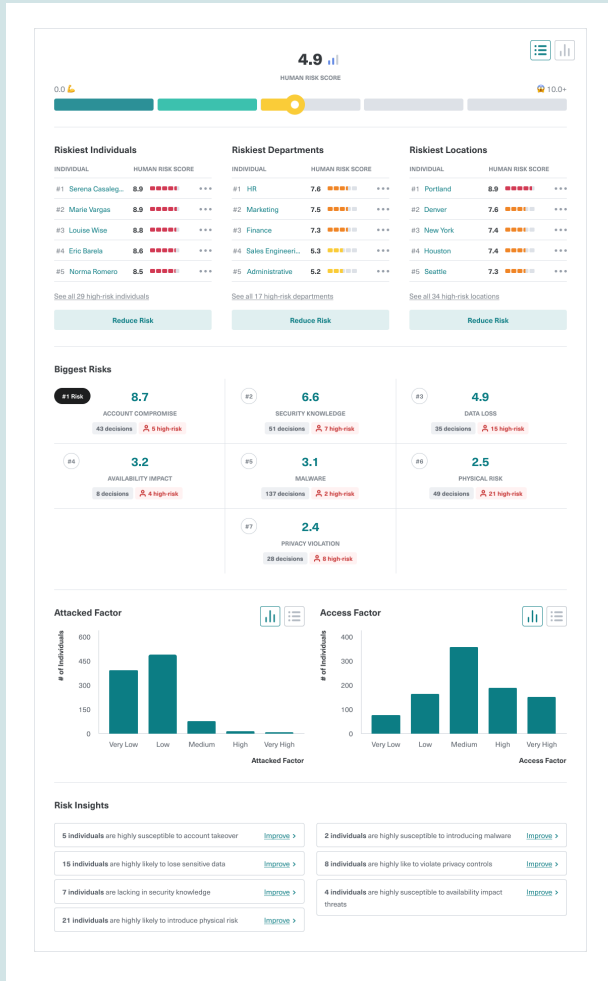
Furthermore, these insights are actionable directly in Elevate Security Platform using NIST-based playbooks that help you automate feedback, business workflows, and tailored controls - all of which are adaptive to your environment and optimized to keep your highest risk users secure and your business more frictionless.

# Proactively Protect Your Workforce

Elevate Security's cloud-based platform integrates with leading SIEM vendors, HR systems, IAM products, and 100+ other popular enterprise security technologies. This deep data integration ecosystem contextually quantifies your workforce risk by building Human Reputation Scores based on an individual's likelihood of causing an incident and the potential impact. Armed with this high fidelity score, security teams are in a great position to defend their organization by proactively orchestrating the technology stack they already have in place today utilizing Elevate's NIST-based playbooks.



# Benchmarking Your Workforce Risk



Gain deep visibility and dashboards which benchmark your organization across key business risks such as:

- Ransomware
- Data Loss
- Account Takeover

Elevate Security Platform allows you to predictively understand riskiest users across your workforce in your organization and gives you deep analytics across historical and point in time threats.

Benchmarking and insights are available across your industry peers, organizational departments, and at the individual level.

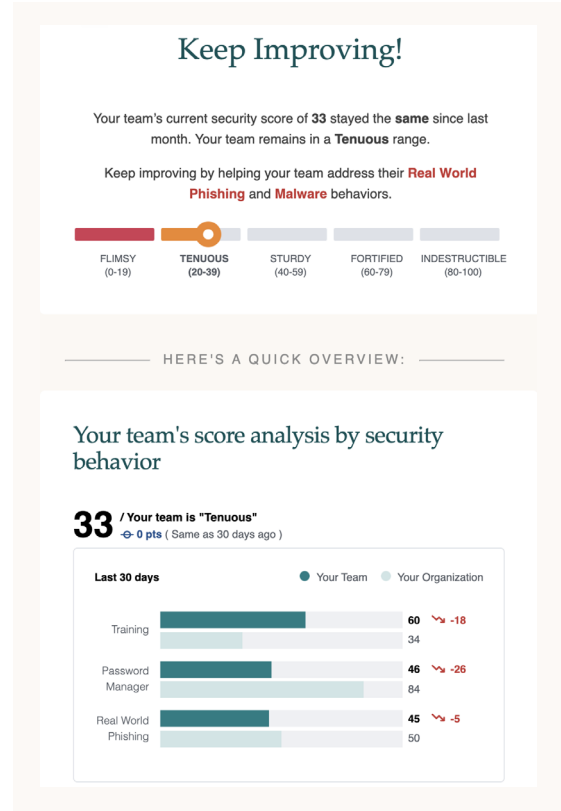
**“Elevate Security risk analytics provides our management with “Heat Map” visibility to high-risk users with the ability to drill down to specific business risks. This level of actionable insight is extremely valuable in assessing security risk and defining our corporate strategy.”**

~ VP, Global Security Risk Operations

# Real-Time Feedback & Notifications

Deliver feedback and communications as new insights arise. This gives you the ability to notify staff, managers, and security teams to provide feedback in areas such as:

- **Feedback to all user types (employees, contractors, suppliers, etc.) on poor decisions such as mishandling sensitive data**
- **Notifications to users with high levels of access when attacks against them are increasing**
- **Communication to managers when individuals on their team need course correction**
- **Alerts to security team when an individual's risk posture is out of compliance**



# Workflow Automation To Reduce Manual Effort

**For affected individuals...**

**IF** Risk - Account Compromise is greater than 5.9 for 2 months  
**and** Access is High or Very High

**OR** Risk - Account Compromise is greater than 5.9 for 2 months  
**and** Access is Medium  
**and** Attacked is High or Very High

**THEN** Send email notification(s) to:

- Individuals who meet the criteria

**and** update privileges via policy group(s):

- Authentication Policy Group > High Risk


Create workflow automation to proactively address critical business risks identified by Elevate Security Platform. With our NIST-based playbooks and over 100 integrations available, security teams have the power to automate security processes right out of the box. This gives teams the power to reduce and remove manual and error-prone steps and free up valuable resource time.

# Adaptive Controls With Tailored Security


Elevate Security Platform allows security teams to take automation one step further by putting guard rails in place around your riskiest users (and reducing friction for the rest), enabling you to:

- Add additional policies in technology you already have for your riskiest users
- Deploy additional logging for those with critical risk and access
- Roll out licenses of heavy friction technology to those you are most concerned about

## Tailored Security Controls



**Straggler**  
Steven Bates  
Department: Marketing


8.9 

---


**VERY LIKELY** to introduce ransomware

- ✓ Limit unknown software execution
- ✓ Increase email filtering
- ✓ Most restrictive browsing settings
- ✓ Feedback on how to improve

## Enable the Business



**Top Performer**  
Josie Brown  
Department: Recruiting

0.8 

---

**VERY LIKELY** to report phishing

- ✓ Auto-approve access requests
- ✓ Relax browsing restrictions
- ✓ Training opt-out
- ✓ Recognition for great performance

## About Elevate Security

One of the most challenging aspects of building an enterprise security program is gathering enough context and knowledge to apply the right resources and technology to the right user at the right time. Elevate Security helps enterprise security leaders gain deep visibility into their biggest workforce security risks. Using Elevate Security, CISOs can fundamentally transform beyond simply managing incidents on a day-to-day basis into proactively addressing their riskiest users with our NIST-based playbooks. Elevate Security's cloud-based platform integrates with leading SIEM vendors, HR Systems, Identity products, and other popular security technologies to provide a User Reputation Score which allows security team's a deep understanding of each and every individual's risk and potential "blast radius" if they were breached. Elevate Security counts leading enterprises in industries such as financial services, technology, healthcare, and more as customers who have benefited from this forward-looking approach to strengthening their workforce security posture.

For more information, visit: <https://elevatesecurity.com/>