Elevate Security

# Unintentional Insider Risk Mitigation: How Elevate Security Protects the Enterprise From the Inside Out

# Table of Contents

# Executive Summary

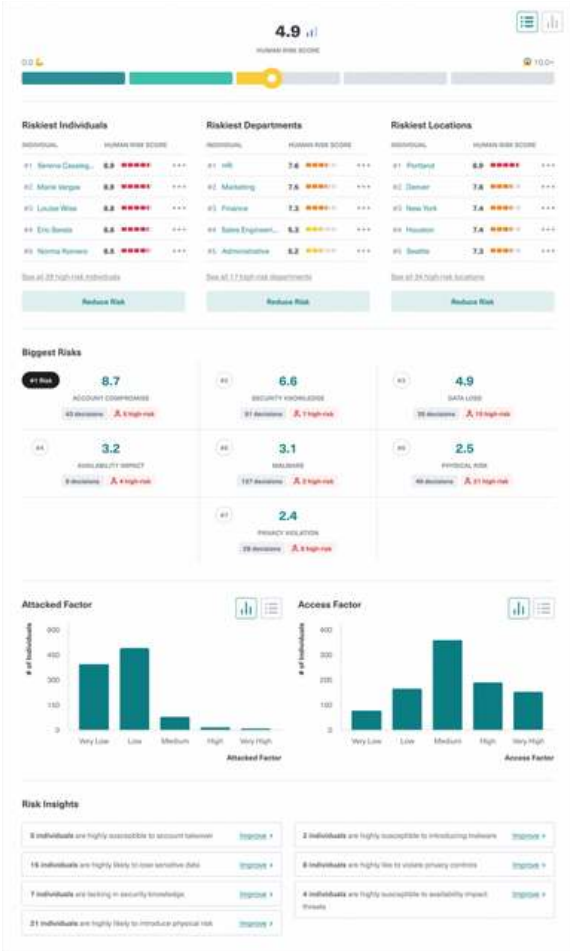
Unintentional insider risk refers to the potential of each worker within an organization to trigger a security breach. This form of risk is recognized as one of the most pressing issues for security professionals to address. Data now shows that only a small fraction of your workers represent the vast majority of this risk:

- 4% of users generate 82% of phishing incidents (some clicking twice per month)
- 3% of users generate 92% of malware events
- 12% of users are responsible for 71% of secure browsing incidents

It's no surprise that **76% of cybersecurity leaders believe that having a dedicated program to manage insider risk would improve their organization's overall security posture.** However, training and simulation alone won't solve for unintentional insider risk. The most effective programs require risk measurement and active, individualized mitigation.

The question is, how can you safeguard high-risk users, and your business, if you don't know who they are? The answer is simple: **data**.

By leveraging data captured from various technologies (SIEM vendors, HR systems, IAM products, etc.) to track user actions and attackability, measuring and quantifying unintentional insider risk is easier than ever before. **This is where Elevate Security comes into play.**




[1] Elevate Security

Elevate Security is a comprehensive workforce cyber risk monitoring, management, and mitigation platform that identifies and responds proactively to your organization's highest risk users.

With deep visibility into each individual's user risk level, including the actions they take and the frequency they are attacked, Elevate Security provides security teams with the visibility and risk scoring necessary to zero in on the most likely source of the next security incident, and stop it before it starts.

Let's dive deeper into the Elevate Security Platform and uncover the benefits of unintentional insider risk mitigation.

# Introduction

According to Gartner, companies spent $150 billion globally on information security and risk management services. This is a 12% increase from the global security spending in 2020. While cybersecurity measures are a necessary expense, many organizations tend to use a majority of their cybersecurity budget to address risks outside of the company.

The reality is — 43% of data breaches involve internal users, such as employees or third-party vendors.

**Users represent a critical risk factor by unintentionally triggering a security breach that may leave your organization vulnerable to malware, data loss, or account takeover.** Common cybersecurity tools focus on detection and remediation, without providing preventative measures to stop attacks before they occur. These tools don't provide visibility of the internal risks on an individual, departmental, and company-wide scale.

Elevate Security provides insights on unintentional insider risk to:

Tailor security controls appropriate to each individual's risk

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

Reduce manual effort with automated workflows and playbooks

Share near real-time and personalized feedback on internal risks

By getting to the root of the issue and identifying the riskiest users within your organization, you can reduce the risk of account breaches, data loss threats, and ransomware.

# Unintentional Insider Risk: The State of the Industry

**74%** of companies believe insider risk management is of greater concern now than before the pandemic.

**82%** of decision-makers are looking for tools and ways to better protect company data.

Today, there's an increasing concern over unintentional insider risk. In its wake, the pandemic has left organizations to face cybersecurity challenges due to users working remotely, the increasing number of third-party partners, and the migration to the cloud. Failing to address these new ways of working and their associated security risks renders organizations vulnerable to security breaches and data loss.

**82% of breaches involve the human element.**

*-Verizon's 2022 Data Breach Investigations Report*

To better protect their data, customers, and reputation, organizations today must address unintentional insider risk head-on. This means adopting the technology and strategies that:

Mitigate unintentional insider risk

Strengthen an organization's overall security posture

Don't impede the productivity of the business

# What is Proactive Insider Risk Management?

Proactive insider risk management refers to a company's ability to use data and preventative actions to protect both the organization and workers against unintentional insider risk. This involves identifying users that take actions that put themselves and the organization at risk, such as clicking on suspicious links, visiting questionable sites, or downloading malware.

66% of companies say that they experience data leaks due to insiders at least monthly.

With the right proactive insider risk management tools, you can identify risky users *before* damages can occur. Proactive insider risk management can help prevent:

### Account Takeovers

When threat actors access a user's account and have access to all the account data, including credentials and confidential information.

### Ransomware Attacks

When a user accidentally downloads malicious software (typically by clicking a suspicious link or opening an unsafe file). This allows the threat actor to gain control over the user's computer and encrypt data.

### Data Loss

When threat actors gain a foothold within a system, they can use the user's identity to find and exfiltrate data.

With a deeper understanding of a user's attackability level, security teams can make adjustments to their accounts, effectively lowering their chances of becoming a victim of a scam or cybersecurity attack.

# Elevate Security's Predictive Risk-Based Mitigation & Management

Risk-based protection enables security teams to have:

- Wide and targeted security controls that can tailor to each user or department
- The ability to quantify internal user risk
- The ability to predict who's going to start the next incident
- The capability to measure the effectiveness of current programs

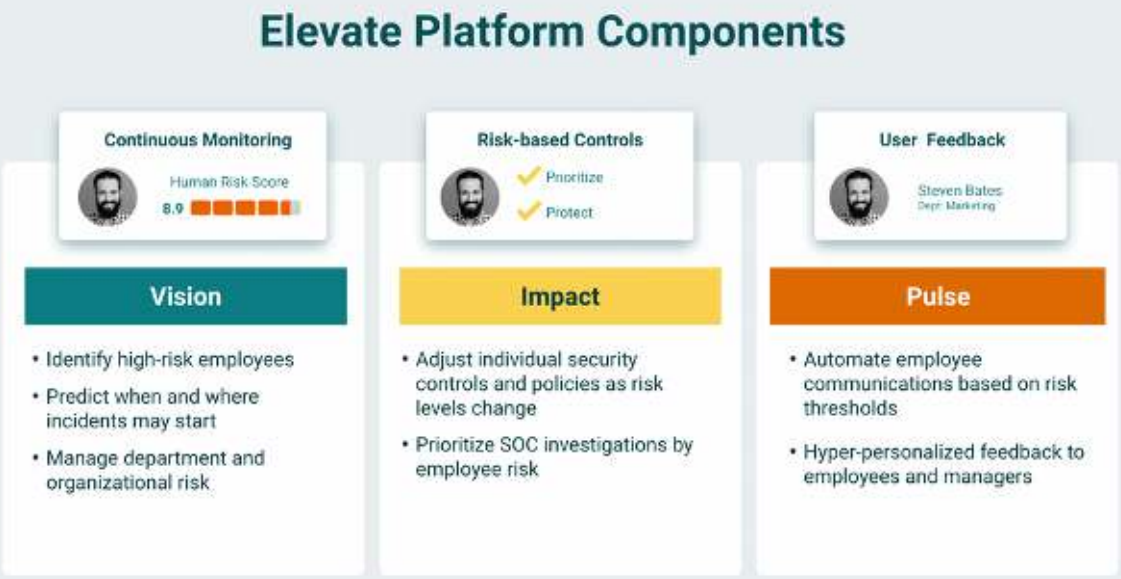

Elevate Security's platform integrates with leading SIEM vendors, HR systems, IAM products, and many other popular enterprise security technologies. This deep data integration ecosystem contextually quantifies your workforce risk by building Human Risk Scores based on an individual's likelihood of causing an incident and the potential impact.

Elevate's risk-based protection benefits each level of the business:

# How Elevate Security Works

To assess your organization's highest security vulnerabilities, it's vital that you have access to data analytics that provide you with information on your organization's riskiest users. Trying to identify high-risk users without data analytics is like searching for a needle in a haystack, especially if your organization has a multitude of users and departments. With three core components, the Elevate Security Platform:

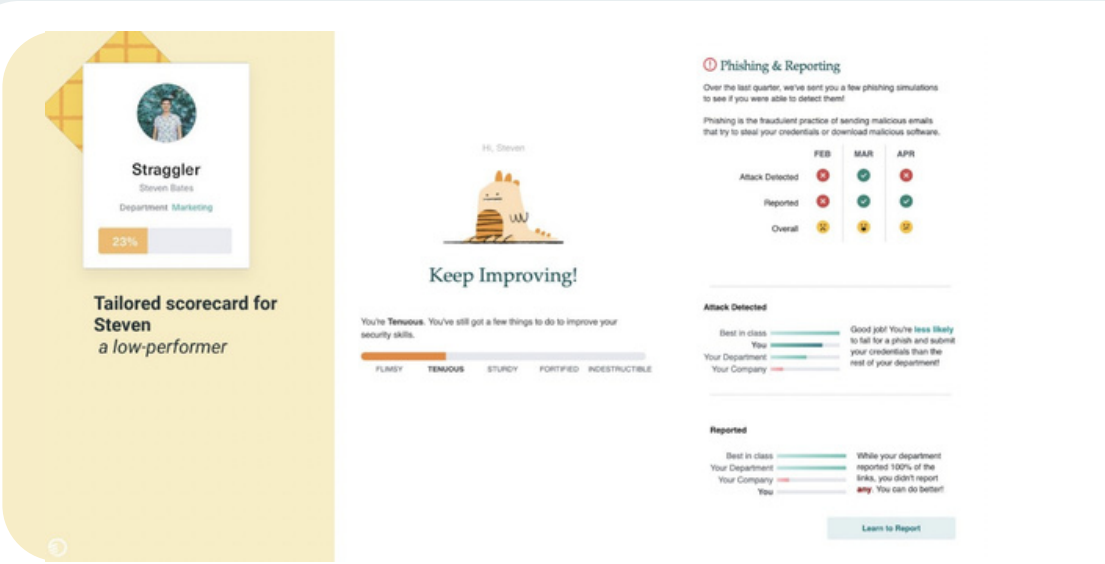
- **Identifies** risky users & **predicts** when and how attackers will go after them
- **Applies** risk-based controls to protect them and the organization
- **Automates** personalized feedback to users and managers




The Elevate Security Platform provides you with a "Heat Map" of your riskiest users that pulls data from their existing identity, email, web, device, and other security tools. With this data, security teams can fortify their organization's security measures and proactively orchestrate their existing tooling to develop user risk profiles.

A user risk profile compiles data on a user's actions and attackability to determine their level of risk. Think of it like a scorecard that tracks a user's previous actions, including clicking on phishing links or reporting suspicious emails, to determine how likely they are to be the victim of a scam or cyberattack.

Check out this user risk profile that demonstrates a low-risk score:



## The 5 Tenants of Elevate Security

With the Elevate Security Platform, you can identify the vulnerabilities that each of your users represents and take action to protect your organization. Here are the 5 main tenets of Elevate Security:

### Unprecedented Visibility

Identify your riskiest users by reviewing each employee's historical actions and likelihood of being attacked.

### Risk-Adjusted Security Controls

Adjust security controls to ensure that each user's identity, endpoint, and email controls align with their risk profile.

### Automated Playbooks

Help security teams to adjust Elevate Security controls (i.e. raising an alarm about risks and pinpointing where security controls can be tighter).

### Customized Feedback

Communication workflows provide near real-time feedback on user actions to share the impact their actions have on the company's security posture.

### User Risk Intelligence

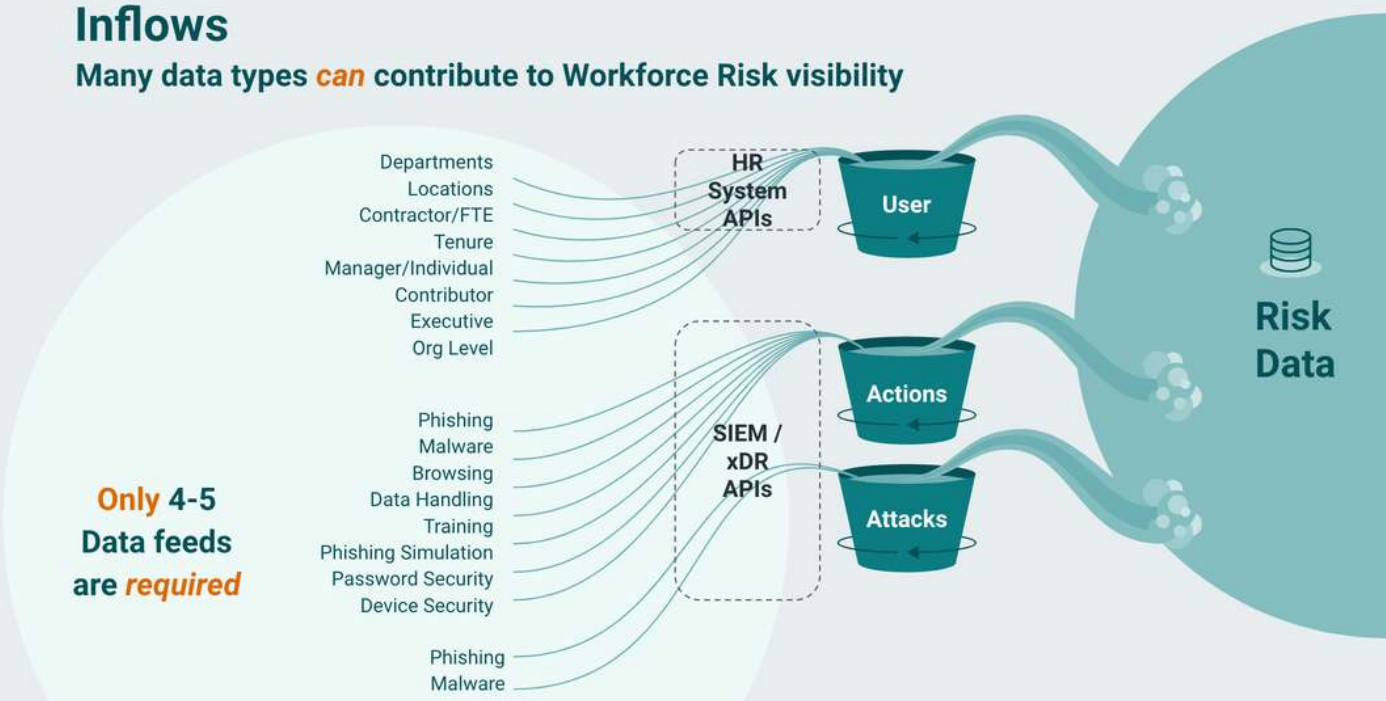
A dataset is drawn from security product telemetry, and offers the broadest and largest set of internal risk signals available. This enables security teams to compare their data and analytics to industry trends.

# Inflows and Outcomes

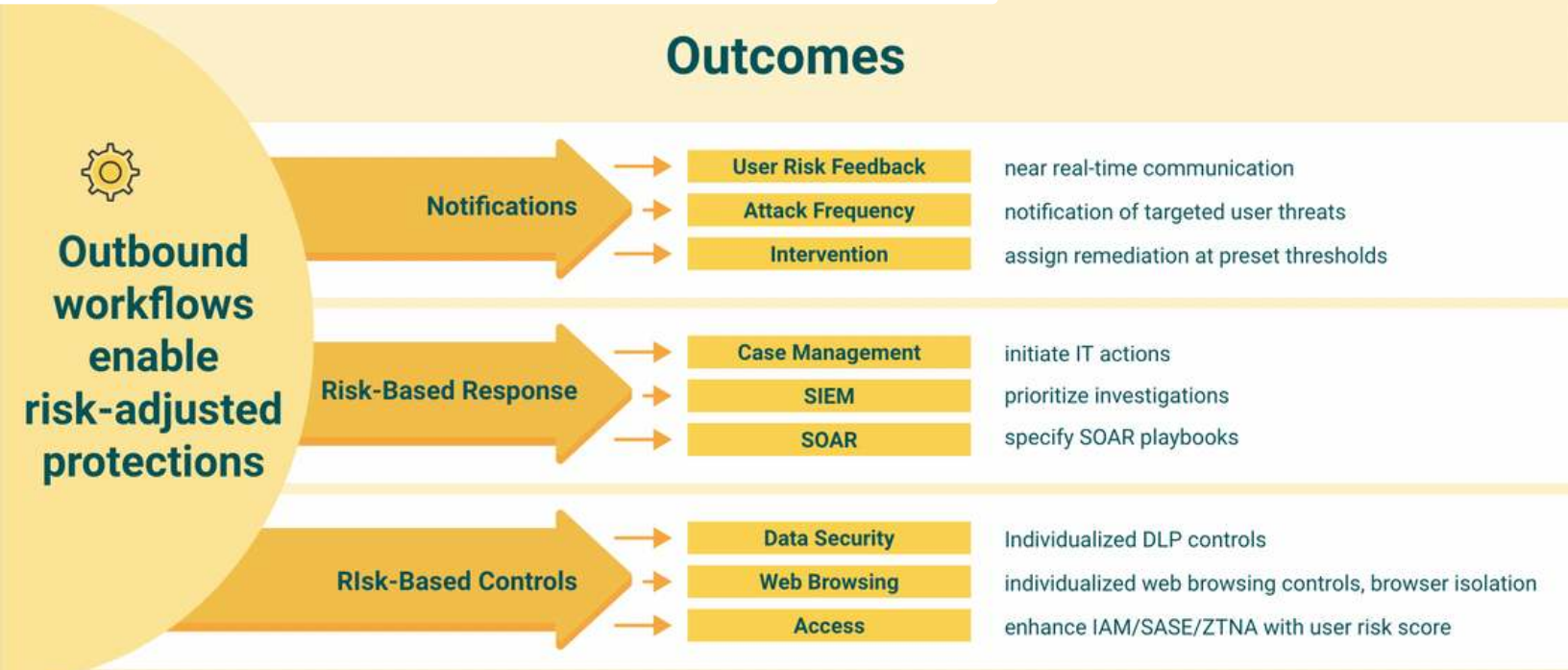
Simple and effective, the Elevate Security Platform has many inflows — the data types that can contribute to workforce risk visibility — and, as a result, has significant outcomes.

Take a look below at the graphic detailing all the potential inflows that inform Elevate Security about:

- Your riskiest users to help you identify those most vulnerable to an attack
- The riskiest actions that are most likely to trigger a security incident
- The number of times your users and organization is attacked




**The outcome of all these inflows? Risk-adjusted protections:**



# How Elevate Security Calculates Human Risk Scores

A Human Risk Score is a rating that helps security teams identify an organization's riskiest users. Companies can leverage Human Risk Scores to determine which users may require targeted controls to lower their risk.

Components that impact a user's Human Risk Score include:

## Actions

A user's actions involve any task that they complete online that contributes to their risk. When a user logs online and opens their email, do they click on suspicious links? This would be an action that influences their Human Risk Score.

Downloading unsafe software or mishandling sensitive data can also have a negative impact on Human Risk Scores. On the other hand, some tasks can increase a Human Risk Score, like reporting phishing emails or refraining from clicking on suspicious links.

## Attackability

Does one user at your organization get way more phishing emails than the rest? That user has a high level of attackability, and it's likely that their Human Risk Score is pretty low.

Attackability refers to the frequency at which an individual becomes the target of a phishing scam or malware attack. Performing risky actions can increase a user's attackability, making them more susceptible to data loss threats and account breaches.

The Elevate Security Platform communicates Human Risk Scores using dashboards, reports, and visibility tools at four levels, which include the following:

## Individual

Security teams calculate a user's Human Risk Score by reviewing their actions and attackability to determine the likelihood that they will be the victim of a cyberattack.

## Department

Security teams can find a specific department's Human Risk Score by calculating the true average of all individuals' Human Risk Scores within a certain department.

## Location

Security teams calculate the true average of Human Risk Scores for all individuals within a specific location, such as the city, state, country, or region, to see which locations pose the biggest risk.

## Company

Security teams can find Human Risk Scores for each individual at the company. All risk actions are weighted equally for each department, member of management, and employee to produce valid Human Risk Scores.

# Elevate Security in Action [Case Study]

Recently, we worked with a Fortune 500 company in the Financial industry that has a large, global workforce including a mix of full-time, contract, and subcontractor roles. The company handles particularly sensitive financial data and has a sophisticated security program, maturing it over the last two decades. This organization has hundreds of millions of customer records and, at an average of $388 per record paid out in a recent financial industry breach — this is no small task to defend against. This led to a partnership with Elevate Security.

## The Challenge

The company found they had a high volume of alerts and a high number of incidents to address. This problem became even more challenging, as the various security technologies were often disconnected from each other, making correlating data and connecting the dots between the different systems labor intensive. Upon review, the security team felt they were too focused on clean-up and response without a good way to address the root cause of the incidents.

## The Solution

One of the goals of rolling out the Elevate Security Platform was to help the team get in front of incidents and protect the sensitive financial data of its customers. The reality of addressing a constant stream of alerts forced the team to follow a reactive approach.

In two weeks, Elevate Security had ingested data sets across their identity platform, email security gateway, web gateway, endpoint and endpoint management solutions to build organizational, departmental, and individual risk profiles for the organization. These profiles provided deep visibility into their organizational risks around ransomware, account takeover and data loss based on the actions users took, the access they have, how frequently they are attacked, and the controls that were in place.

The core of this work fell into three categories:

1. Automating notifications to employees, managers and the security team around current and emerging risks to them and the organization
2. Sharing user risk intelligence with other systems to enable better decision making of security team analysts and other systems like identity solutions
3. Tailoring application controls and policies based on workforce risk profiles to build precision policies based on an individual's risk

## The Results

Elevate Security helped the Fortune 500's security team shine in their Board communications. With deep visibility across key business risks, internal and external benchmarking and beautiful dashboards and reports, the team now has a key tool in their arsenal when presenting their journey.

Plus, with Elevate Security, this organization experienced:

- An 82% reduction in malware/ransomware and account takeover incidents
- A 55% improvement in risky security decisions being made
- A 47% increase in the detection of attacks targeting employees

# Final Thoughts

Without a reliable method for identifying the riskiest users and the actions within the organization, businesses are exposed to potential security threats and attacks such as:

- Account takeover
- Data loss
- Ransomware

Just as we expect the rate of insider risk to increase in organizations that don't prioritize insider risk mitigation, we expect the adoption of unintentional insider risk mitigation technology to increase exponentially within the next few years. Elevate Security is here to help.

Have questions? Let's talk.

Get in touch with us here.

## About Elevate Security

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 automated playbooks. Elevate Security's SaaS platform integrates with leading SIEM vendors, HR Systems, Identity products, and other popular security technologies to provide a Human Risk Score which allows security teams 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, please visit elevatesecurity.com.

Elevate Security