Elevate Security

CASE STUDY - FINANCIAL SERVICES

Proactively Reduce Incidents to Prevent Account Take-Over, Data Loss, and Ransomware

The Elevate platform helps me quickly identify and support my riskiest users. It lets the security team feel good that we've put the right guardrails in place to protect our organization.

VP, Security Engineering and Architecture

The Challenge

With a layered defense strategy and security technology investments spanning two decades, this institution had built a world class security organization. Increasingly, however, the company found they had a high volume of alerts and a high number of incidents to address.

This problem was made even more challenging as the various security technologies were often disconnected from each other and correlating data and connecting the dots between the different systems was 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.

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.

Project Goals

- Protect sensitive customer data at all costs
- Benchmarking for security executive and board level conversations
- Proactively automate time intensive and error prone manual steps

Why Elevate

- Predictive visibility into ransomware, account takeover and data loss risks across the company, departments and individuals
- The only solution that helps them proactively stay ahead of threats
- Fast time to value; highly customizable

The Organization

This Fortune 500 company in the Financial industry with a large, global workforce that included 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.

Note: *Elevate respects that some of our customers prefer not to publicly state which security vendors they use. As such, we have removed the client's name and anonymized specific details in this case study.*

The Solution

From Reactive to Proactive

The reality of addressing a constant stream of alerts forced the team to follow reactive approach. The existing security tool set primarily focused on the detect, response and recovery stages of the NIST Cybersecurity Framework. The team realized that these efforts, while useful, had two major issues:

> **They weren't using the learnings from these alerts and incidents to protect their organization**
>
> **They weren't addressing the root cause of the incidents**

This led to a partnership with Elevate Security. In two weeks Elevate had ingested data sets across their identity platform, email security gateway, web gateway, endpoint and endpoint management solutions to build organizational, department 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,

Building Business Workflows

Using multiple security tools that were disconnected from each other, the security team had to coordinate many manual tasks to implement controls. The Elevate platform provided effective policy orchestration via the Elevate policy risk engine.

The core of this work fell into three categories:

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

From the Key Success Metrics – Reducing Incidents

At the beginning of the partnership, the key metric identified was a reduction in bad actions the organization as a whole were taking that led to incidents. Elevate was very quickly able to benchmark the organization and together we began to see improvements in all areas we focused on. Below is a sample of the types of issues we've seen across this customer and others like them:

82%

Reduction in malware/ransomware and account takeover incidents

55%

Improvement in risky security decisions being made

47%

Increase in the detection of attacks targeting employees

Benchmarking to the Board

Elevate helped the 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.

The biggest compliment any partner can get is that we've helped them look good internally with the Board, their executives and their users. That plus real metrics showing a decrease in risk is a beautiful union.