

CASE STUDY

How an Insurance Giant Found Visibility

INTRODUCTION

The Director of Information Security oversees the cybersecurity program end-to-end including GRC, operations, and architecting solutions within the national insurance company. She, along with her team of eight, are also charged with securing the critical, rich data of their customers.

The company's business goals focus on growth, delivering the right product for the right target market, and expanding into new spaces. The security team's goals were to be at the table for those conversations, to find the right solutions to move better faster, and to secure customer data as the company grows into these new markets.

With a previous vendor, the Director did not have 100% access to her own systems and had very little visibility throughout the organization. The vendor's solution could not handle all devices or logs.

THE PROBLEM

Securing a Data-rich environment

The Director sought a log management solution to customize and increase her visibility. Since the company handles a significant amount of customer data, she understands that one breach could affect the company's national image and customer retention.

In order to succeed, the Director of Information Security needs to find a partner and SIEM solution that can handle log intake on all of the company's relevant sources and help with detection and response to events and incidents.



"Data security affects our company's national brand and image. I needed someone who could nip an incident in the bud."

-Director of Information Security

LIMITED VISIBILITY	INCOMPLETE LOG COVERAGE	CUSTOMER DATA EXPOSURE
THE PREVIOUS VENDOR PROVIDED LIMITED ACCESS TO SYSTEMS AND VISIBILITY ACROSS THE ORGANIZATION.	THE EXISTING SOLUTION COULD NOT HANDLE ALL DEVICES OR LOGS.	A BREACH COULD AFFECT THE COMPANY'S NATIONAL IMAGE AND CUSTOMER RETENTION.

Business & Security Goals

- **Be at the decision table:** The company's goals to expand into new markets would require the security team to adapt to business growth.
- **Secure customer data:** As one breach could compromise rich customer-data nationwide, the security team looked to comprehensive solutions.
- **Increase visibility:** With a disappointing managed security solution previously, the security team looked for a new partner and SIEM solution.

WHY REDLEGG

RedLegg's co-managed approach allowed the Director of Information Security to have personal contact with the CEO, sales, and architects, building a stronger co-managed relationship.

Both teams challenge each other, and her security team is learning along the way. RedLegg provides weekly conversations and monthly reporting. RedLegg's partnership also created touchpoints up and down the line from RedLegg's CEO to sales and to the security architects.

The insurance company found security in an engaging partnership and a cornerstone solution: SIEM.

SOLUTION: GROWTH-MINDED SOC & ENTERPRISE VISIBILITY

The security team worked with RedLegg to install and co-manage LogRhythm SIEM.

By installing a SIEM, the Director's team gained deep and broad visibility into their environment, and with a co-managed model, the security team partnered with RedLegg to handle complications.

LOG INGESTION

LogRhythm SIEM supports log intake from relevant enterprise sources.

EVENT CORRELATION

Correlation tools provide visibility into events across the enterprise.

24X7 VISIBILITY

The SIEM and SOC solution provides around-the-clock visibility.

DETECTION & RESPONSE

The solution supports the company's detection and response strategy.

REPORTING & COLLABORATION

Timely reports, security event updates, weekly conversations and monthly reporting.

IMPLEMENTATION

The security team worked with RedLegg to install and co-manage LogRhythm SIEM.

Starting from scratch with SIEM allowed the firm to customize and tweak the SIEM, providing depth and breadth. Correlation tools helped the security team oversee events nation-wide.

The firm received correlation tools, timely reports, and security event updates.

RedLegg provides weekly conversations and monthly reporting. RedLegg's partnership also created touchpoints up and down the line from RedLegg's CEO to sales and to the security architects.

THE BENEFITS

More visibility

Starting from scratch with SIEM allowed the firm to customize and tweak the SIEM, providing depth and breadth. Correlation tools helped the security team oversee events nation-wide.

Personal communications

RedLegg's co-managed approach allowed the Director of Information Security to have personal contact with the CEO, sales, and architects, building a stronger co-managed relationship.

“**With this solution, I have multiple eyes on our systems. It's collective, correlative, and over-arching.**” -Director of Information Security

HOW IT WAS DELIVERED

CO-MANAGED LOGRHYTHM SIEM

RedLegg and the internal security team installed and co-managed LogRhythm SIEM.



ENTERPRISE-WIDE VISIBILITY

Correlation tools supported broad visibility and security event monitoring across the enterprise.



COLLABORATIVE SECURITY MANAGEMENT

Weekly conversations, monthly reporting and direct access to RedLegg teams supported the co-managed relationship.

CONCLUSION

Competitive Advantage

RedLegg aided the firm's competitive advantage. The insurance company is now more confident to expand into new markets and protect customer data. The security team continues to innovate and grow their SOC in order to be at the table and help fulfill business goals.

With a SIEM and SOC solution, the insurance company's security team feels confident that they have the visibility to handle risks. The business can move forward confidently knowing that customer data is better protected, and the security team has a more mature posture.

“When I sleep, someone is still watching critical company assets.”

-Director of Information Security

IMPACT

- Achieved 24x7 visibility into the environment
- Installed key security solution for the enterprise
- Ability to see across the entire enterprise and correlate logs on a large scale. The firm received correlation tools, timely reports, and security event updates.
- The SIEM solution is a cornerstone of the security program that provides protection in scale. It helps with the detect and response strategy the company utilizes to protect rich customer-data and extends business life, growth opportunities.
- The insurance company is now more confident to expand into new markets and protect customer data.

FOR MORE INFORMATION REACH OUT:



312.757.4941



dotell@redlegg.com



redlegg.com