Modernize Security Operations for Financial Services

With Splunk and Adarma

Financial institutions safeguard some of their customers' most sensitive information and data, and that makes them a prime target for their adversaries. At the same time, their attack surface constantly expands as they digitize to meet rising customer expectations, such as online services and open banking that introduce hundreds of application programming interface (API) calls into the mix.

Maintaining high levels of security is key to maintaining customer trust — which is particularly critical in the highly competitive financial services industry. When it's easy for customers to switch banks, loyalty is hard to build and harder to keep.

Across the globe, regulation continues to influence security strategy as financial services organizations navigate new mandates, including the Digital Operational Resilience Act (DORA) in the EU, T+1 in the U.S., and the global push toward open banking.

Banking on resilience in financial services

The race to innovate must be met with a similar dedication to digital resilience. To get there, Adarma and the Splunk platform help financial services institutions extend visibility across their entire technology landscape to detect, investigate, and respond to threats faster.

The financial services sector is focused on building the security operations center (SOC) of the future, so they can:

Detect threats at scale

Unify security operations

Empower security innovation

> Compared to other industries, financial services leaders are optimistic about their ability to keep up with cybersecurity requirements. In fact, 50% of respondents to a recent survey say it was easier to keep up this year, versus 41% across industries.

1

Detect threats at scale

To meet customer expectations, organizations are coming to market with more consumer-friendly financial management features. They're convenient for users but introduce more security risks by creating additional points of contact where data changes hands.

We're already seeing the impacts: API attacks are rising dramatically in financial services with a 65% increase over last year.*

That's why financial institutions are working to get end-to-end visibility across their entire tech stack so they can detect threats at scale.

Core to this effort is the work to:

Analyze all sources across a complex landscape

Gain context into new threats

Proactively address risks

> By reinforcing and modernizing the SOC to automatically deal with many of these types of threats, organizations can free analyst teams to focus on emerging, novel threats (rather than spending time on mundane or routine investigations).
>
> **Matt Swann,**
> Strategic Advisor, Splunk

*CSO, "Web app, API attacks surge."

2

Unify security operations

The financial services industry is working to unite teams and systems across the enterprise in the fight against fraud and financial crime.

However, most financial services organizations are used to working in rigid silos, which can break down across different lines of business and often reflect decades of M&A activities. These silos often create visibility gaps that financial criminals can exploit — while making it harder for the organization to work together to solve issues effectively.

That's why the financial services industry is embracing the concept of "fusion centers." By offering 360-degree visibility and consistent work processes, fusion centers can help spot and solve cybersecurity problems faster.

These fusion centers will require:

Unifying threat detection, investigation, and response (TDIR) workflows

Automating SOC processes

Finding new ways to govern, comply, and measure

> We're due for a return to the fundamentals of cybersecurity. With so much at stake, I think it's now more important than ever for financial services institutions to protect their systems and data from the core cyberattacks that pose a threat to their customers, the banks, and overall reputation.
>
> **Matt Swann,**
> Strategic Advisor, Splunk

3

Fraudsters and financial criminals won't stop innovating in pushing valuable financial data. However, the industry can hold them off by accelerating their own path to security innovation.

For instance, AI and machine learning (ML) have broadened the threat landscape for financial crimes and fraud. But these tools are also becoming a key part of the solution — giving financial institutions enhanced visibility and controls to effectively fight fraud.

Splunk and Adarma help financial services institutions elevate digital resilience to prevent major issues that threaten the security and reliability of their digital infrastructure and quickly remediate issues that do occur — helping them focus on innovations that advance SOC practices, strengthen their business, and keep customers happy.

With the Splunk platform, financial services institutions can experience:*

90%

faster identification of root cause and remediation

50%

increase in alert fidelity

30%

increase in operational efficiency

> In Splunk's 2024 State of Security report, 76% of financial services leaders said that they don't have enough education to fully understand the implications of generative AI — and 39% listed AI-powered attacks as a top concern. Yet respondents were also hopeful about AI's role in alleviating the talent gap.

*ESG Economic Summary, *Analyzing the Economic Benefits of Splunk Security.*

Together, Adarma and Splunk guide financial services organizations on a journey toward improved digital resilience. With our security solutions, organizations gain an unmatched breadth of technology, expertise, and community to reduce risks, modernize the SOCs, and propel ongoing innovation.

> Digital resilience is a catalyst, driving SOC enhancements that address challenges head-on. Organizations are building towards the SOC of the future, where unified threat detection, investigation, and response drive critical outcomes.

splunk>
a CISCO company

Learn more: www.splunk.com/asksales

www.splunk.com

ADARMA
TOGETHER WE'VE GOT THIS

Learn more:
Adarma.com