splunk>

CASE STUDY

Orrstown Bank Invests in Splunk® Cloud for Security and Business Intelligence

ORRSTOWN BANK

Executive summary

With more than $1.2 billion in assets, Orrstown Financial Services, Inc. and its wholly-owned subsidiary, Orrstown Bank, provide a full range of financial services through 22 locations throughout Pennsylvania and Maryland. With a need to comply with demanding security regulations, Orrstown Bank wanted a security solution that could provide visibility into its complex hybrid IT infrastructure, identify and resolve threats, and provide required uptime and compliance. Since deploying Splunk Cloud, the bank has seen benefits including:

- Improved operational efficiency and customer satisfaction
- Estimated 50 percent reduction in fraud losses
- Enhanced security posture

Why Splunk

Initially, Orrstown Bank relied on a security services provider that delivered basic security information and event management (SIEM) functionality around the bank's security devices. Unfortunately, the security service could not offer enough intelligence for the bank's security team to rapidly identify incidents or respond to requests from regulators.

"Our security provider is a one-size-fits-all solution designed for community banks, which did not give us long-term trending and analytics," says Andrew Linn, SVP, chief information security officer, Orrstown Bank. "We needed to augment its monitoring to properly defend the bank against threats and fraud. We wanted greater visibility to detect both internal and external threats and to collect forensic evidence to understand and neutralize them. But our business is banking, not running a datacenter, so we want as little on-premises infrastructure as possible."

Prior to Orrstown, Linn and his colleagues had worked for some of the world's largest financial institutions and were familiar with Splunk Enterprise. Splunk Cloud, which delivers all the functionality of Splunk Enterprise as a cloud service, eliminated the need for an onsite deployment. Another important factor was Splunk Cloud's 100 percent uptime SLA and its SOC2 Type II certification.

Industry

- Financial services

Splunk Use Cases

- Security and fraud
- Business analytics
- IT operations

Challenges

- Protect the bank and its customers from the growing threat of debit and credit card fraud
- Needed to identify and respond to internal and external security threats
- Obtain the maximum value for IT spend by using as much cloud-based or off-site services as possible
- Consolidate operational and security analytics into one platform

Business Impact

- Faster detection of potential fraud, malware or anomalous behavior
- Estimated 50 percent reduction in fraud losses and improved operational efficiency
- Bolstered security posture thanks to cost-effective SIEM functionality
- Business value gained from improved security, performance and financial oversight of ATMs
- Able to meet regulatory compliance mandates
- Enhanced customer experience

Data Sources

- ATM devices
- Debit card transaction history
- Perimeter firewalls and VPN servers
- Internet proxy
- IDS/IPS systems and routers
- On-premises and AWS servers
- Microsoft Azure, web servers and Active Directory

Splunk Products

- Splunk Cloud

"Rather than buy a dedicated SIEM solution and numerous monitoring solutions, we deployed the Splunk Cloud platform, which slashed our administrative overhead," says Linn. "We're aggregating data from over 60 sources, mostly on-premises servers and security systems, and are constantly discovering new use cases for Splunk software."

Centralized visibility into security and business processes

Splunk Cloud took just two weeks to deploy at Orrstown Bank and is providing the bank with real-time, centralized visibility into its security, network and business operations. Administrators and security specialists now use the platform to establish baseline performance metrics to assess the health of systems, proactively monitor and receive alerts, and quickly investigate and resolve any issues. "Rather than pore over thousands of lines of transactions, we use Splunk Cloud dashboards to visualize patterns and trends," says Linn. "We can observe login anomalies, detect questionable activities and behaviors, and promptly take measures to remediate them."

Fraud reduction yields far-reaching benefits

Orrstown has experienced an increase of more than 400 percent in debit card fraud over the past three years. To combat this, the bank integrates an anomaly detection solution in its Splunk Cloud deployment. This joint solution rapidly identifies the first instance of fraud and then prevents subsequent fraudulent transactions. The solution uses statistical modeling to discover abnormal activities, incorporating transaction characteristics such as the location, amount, time of transaction, as well as the risk profile of the vendor.

The combination of these dimensions determines a risk score for each transaction. Based on the severity of the score, Orrstown is able to take appropriate action, such as disabling the debit card or issuing a proactive customer notification. By incorporating anomaly detection into Splunk Cloud, the bank estimates it cut debit card fraud losses by over 50 percent.

"We initially applied Splunk Cloud for security use cases, but we're developing more and more business-focused use cases where we use the visibility and analytics provided by the Splunk platform to improve our operations and customer satisfaction. We're enjoying security, IT and business value from a single, cost-effective solution."

Andrew Linn, SVP, CISO
Orrstown Bank

Security intelligence improves ATM operations

With Splunk Cloud, Orrstown gains real-time fraud and business analytics across its network of ATMs. The bank indexes data from the ATMs and displays the information in Splunk dashboards, providing near real-time insight into potentially fraudulent activities.

Thanks to Splunk Cloud, the bank also derives business intelligence from its ATMs. By baselining the flow of money in and out of each ATM, for instance, it ensures the devices are neither under nor over-provisioned, efficiently making funds available to customers.

Linn concludes, "These innovative Splunk use cases allow us to further monetize our ATM system. We initially applied Splunk Cloud for security use cases, but we're developing more and more business-focused use cases where we use the visibility and analytics provided by the Splunk platform to improve our operations and customer satisfaction. We're enjoying security, IT and business value from a single, cost-effective solution."