securonix

Cloud SIEM Saves Regional Financial Institution 50% of an FTE Over On-premises Solution

CASE STUDY

Cloud SIEM Saves Regional Financial Institution 50% of an FTE Over On-premises Solution

Large Regional US Bank

This large, regional U.S. bank was recognized in the top 10 on Forbes' World's Best Banks award in 2020. They believe their customers, communities, and employees make them a great business to work with for personal and business banking. The bank offers all types of financial products including personal loans, home loans, CDs, and other types of investments and always like to buy the 'best-in-breed' technologies for security.

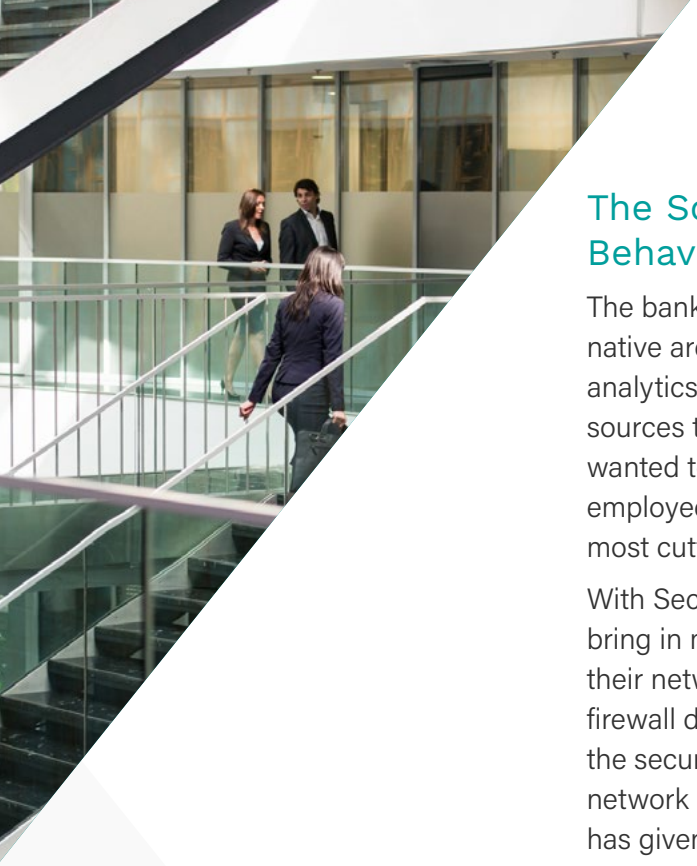
The Challenge: Moving from On-premises to an Advanced Analytics Cloud SIEM

A regional bank knew it was time to upgrade their SIEM. Their on-premises LogRhythm SIEM solution was experiencing stability issues causing their security team to spend time maintaining the solution instead of investigating threats. Additionally, their SIEM solution had limited contextual enrichment and analytics capabilities only covering basic use cases, which made the security team worry they were missing threats in their environment.

Preferring a cloud solution for their security operations center (SOC), the bank's security team sought out information on top software-as-a-service (SaaS) SIEM solutions. They looked at Exabeam, Splunk, and Securonix. The bank wanted to ensure the chosen next-generation SIEM could detect advanced threats, ingest more of their environment's data, and was easy to customize for specific use cases. Cloud-native SIEM solutions, like Securonix, were seen as strong contenders to replace LogRhythm because of their increased scalability and cost efficiency.

Key Challenges

- Lack of visibility into employees' and contractors' behavior
- Lack of behavioral insights to detect insider threats and external threats
- Lack of customization for specific use cases
- Lack of ability to handle and ingest huge volumes of data from multiple sources



The Solution: Securonix for Increased Visibility and Behavioral Insights

The bank chose the Securonix Next-Gen SIEM solution due to its cloud-native architecture, strong advanced analytics for user and entity behavior analytics (UEBA), and the ability to customize and ingest more data sources than their previous LogRhythm deployment. The security team wanted to gain increased visibility and understand the behaviors of their employees versus their contractors. They always tried to work with the best, most cutting-edge technology in their SOC, and Securonix fit the bill.

With Securonix Next-Gen SIEM and UEBA in place, the SOC was able to bring in more data sources, from physical security, like badge reads, to their network segmentation logs with Guardicore and their web application firewall data with Signal Science. The advanced analytics and UEBA give the security team a better understanding of how entities behave on their network and the deviations from what is normal in their environment. This has given the team increased insight into entities and users, such as the behavior of employees and contractors.

The Business Impact: Fast Time to Value and Saving 50% of an FTE for Detection and Response

The large regional bank achieved fast time to value since they were able to gain parity with their previous SIEM solution in only a few months, while ingesting over twenty data sources. Additionally, due to the switch from an on-premises SIEM to a SaaS SIEM, the security team was able to save half of a full time employee's time, moving them from managing the solution to detecting and responding to threats. Allocating more time to investigations gives their security operations team the agility needed to reduce the bank's risk of cyber threats.

About Securonix

Securonix is redefining SIEM for today's hybrid cloud, data-driven enterprise. Built on big data architecture, Securonix delivers SIEM, UEBA, XDR, SOAR, Security Data Lake, NDR and vertical-specific applications as a pure SaaS solution with unlimited scalability and no infrastructure cost. Securonix reduces noise and prioritizes high fidelity alerts with behavioral analytics technology that pioneered the UEBA category.

For more information visit securonix.com