SECURONIX™

CASE STUDY

Using Cloud-Based SIEM to Safeguard Real Estate Firm

The Challenge: Massive Data Spread Among Several Solutions

This organization gathers a huge amount of data from both cloud applications (such as Google Apps, CrowdStrike, PingFederate, and others) and on-premises solutions (such as Windows, Proofpoint/Proxy, Firewalls, CyberArk, Cylance, and others). With data spread across multiple environments, performing meaningful analytics is extremely difficult and the cost and operational overhead needed to maintain their data was excessive.

Another challenge for this organization was that, while they are a mid-sized company, they only have a small security team. The ideal security solution for them was one that provided next-generation capabilities, but required minimal operational overhead. The less time their security team needed to spend managing their security solution, as opposed to investigating and remediating threats, the better.

Additionally, in order to comply with the organization's cloud-first initiative, the customer required that any new solution needed to be a single end-to-end, cloud-based platform for information storage and analytics. Securonix took up the challenge to integrate everything onto a single platform using a seamless SIEM and data analytics solution.

The Solution: Massive Data, Extensive Analytics, Reduced Manual Effort

Securonix Next-Generation SIEM met the organization's need for a single end-to-end solution. This cloud-based SIEM platform is an all-in-one solution that can ingest a wide variety of data sets, store the data in its centralized data storage, and apply advanced artificial intelligence and machine learning analytics in order to detect cyber threats.

Leveraging Securonix API connectors to ingest data from the cloud, and syslog forwarding techniques using remote ingestion nodes for the on-premises data, Securonix Next-Gen SIEM successfully integrated the organization's scattered data sources into one multi-tenant infrastructure.

Due to Securonix Next-Generation SIEM's rapid implementation and its completely managed infrastructure, the organization experienced decreased time to value. The organization also now also has access to Securonix's cutting-edge knowledgebase, containing the latest threats discovered by Securonix researchers. The organization can quickly implement new threat models, or create customized threat models to address various use cases.

> "SECURONIX CLOUD HAS SAVED US MONTHS OF DEPLOYMENT TIME AND 60-70% OF RESOURCE TIME IN CONFIGURATION AND ONGOING MONITORING OF THE SYSTEM."
>
> REAL ESTATE FIRM

Company Profile

This organization is a premier real estate firm that wants their customers to have a seamless online experience when living in properties managed by them, including maintenance scheduling, payments, security, and so on. To do so, they have multiple cloud-based applications available to assist property owners and tenants. Overall, property owners and tenants are satisfied with the services and the ease with which they can access them. However, the real estate firm is relying on on-premises security solutions to secure their cloud applications, which is not working.

The Business Impact: Improved Focus on Security

The organization not only realized cost savings by switching to Securonix Next-Generation SIEM, but now that less time was required to manage the organization's security infrastructure, employees could instead focus primarily on responding to cyber threats.

By integrating and actively monitoring all of the organization's data, the organization was able to use Securonix to detect and respond efficiently to a major phishing campaign threatening the organization. Using Office 365, malicious entities were attempting to exfiltrate sensitive data at all levels of the organization. This had previously gone undetected due to siloed data and inefficient analytics. However, with Securonix Next-Generation SIEM running on the SNYPR Cloud Platform's best in class data analytics, the customer was able to identify, detect, and respond to the threat effectively.

About Securonix

Securonix is redefining the next generation of security monitoring using the power of machine learning and big data. Built on Hadoop, the Securonix solution provides unlimited scalability and log management, behavior analytics-based advanced threat detection, and intelligent incident response on a single platform. Globally, customers use Securonix to address their insider threat, cyber threat, cloud security, fraud, and application security monitoring requirements. For more information visit www.securonix.com.

SECURONIX™

LEARN MORE
www.securonix.com

LET'S TALK
+1 (310) 641-1000

14665 Midway Rd. Suite #100, Addison, TX 75001 | ©2018 Securonix