securonix

CASE STUDY

Real Estate Firm’s Small Security Team Gains Efficiency with Cloud SIEM

CASE STUDY

Real Estate Firm’s Small Security Team Gains Efficiency with Cloud SIEM

About Real Estate Firm

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 Challenge: Massive Amount of Data for Threat Detection and Response

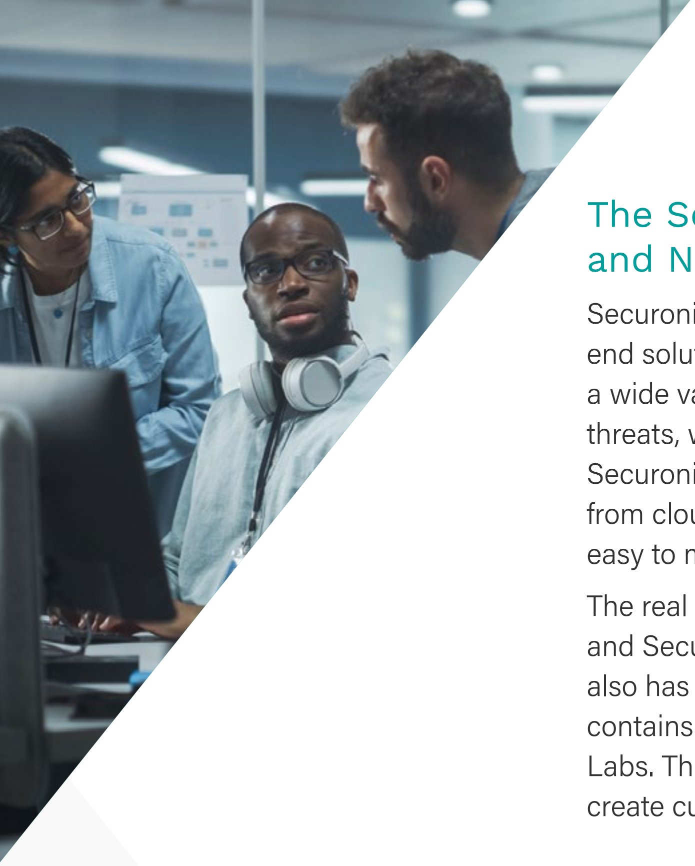
A real estate firm was gathering a huge amount of data from both cloud applications (e.g., Google Apps, CrowdStrike, PingFederate, etc.) and on-premises solutions (e.g., Windows, Proofpoint/proxy, firewalls, CyberArk, Cylance, etc.). With data spread across multiple environments, performing meaningful security analytics for detection and response was extremely difficult and the cost and operational overhead needed to maintain their data was excessive.

Another challenge the real estate firm faced was that, as a mid sized company, they only have a small security team. The ideal security solution would need to provide advanced analytics but require minimal operational overhead. The organization needed a next-generation SIEM that demanded less management so their security team could focus on investigating and remediating threats.

Finally, to comply with the organization’s cloud-first initiative, the real estate firm prescribed that any new solution needed to be a cloud-based platform and include security analytics.

Key Challenges

- Lack of unified platform for monitoring, detection, response, and remediation
- Employ a small security team and needed more efficient detection capabilities
- Need advanced analytics to detect threats more effectively



The Solution: Cloud SIEM With Advanced Analytics and No Infrastructure To Manage

Securonix Next-Gen SIEM met the organization's need for a single end-to-end solution. The cloud-based SIEM is an all-in-one solution that can ingest a wide variety of data sets and apply advanced analytics to detect cyber threats, which improved the real estate firm's cybersecurity effectiveness. Securonix successfully integrated the organization's scattered data sources, from cloud and on-premises, into one multi-tenant infrastructure that was easy to manage.

The real estate firm realized fast time to value due to rapid implementation and Securonix Next-Gen SIEM's managed infrastructure. The organization also has access to Securonix's cutting-edge knowledge base, which contains content to detect the latest threats discovered by Securonix Threat Labs. The security team can quickly implement new threat models or create customized threat models to address various use cases.

The Business Impact: Improved Detection and Response Catches Phishing

The real estate firm saved money by switching to Securonix Next-Gen SIEM because the solution took less time to manage. Now the security team could focus primarily on responding to cyber threats.

The organization started receiving strong value from Securonix by efficiently detecting and responding to a major phishing campaign. Using Office 365, malicious entities were attempting to exfiltrate sensitive data at all levels of the organization. This phishing attempt had previously gone undetected due to siloed data and inefficient analytics. However, with Securonix Next-Gen SIEM, the security team was able to detect, and respond to the threat effectively.

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