

securonix



CASE STUDY

# Simeio Uses Securonix Next-Gen SIEM on AWS for Advanced Threat Detection





securonix

simeio™

## CASE STUDY

# Simeio Uses Securonix Next-Gen SIEM on AWS for Advanced Threat Detection

### About Simeio

Simeio is an identity and access management (IAM) solution provider that leverages AWS cloud infrastructure to deliver integrated IAM solutions such as access governance, privileged identity management, and identity administration. Simeio, with its end-to-end identity management solution offering, protects over 150 million identities across on-premise and cloud infrastructure for its customers across the globe.

### The Challenge: Detect Data Exfiltration and Data Theft

Simeio needed the ability to detect and respond to advanced threats within their product and to protect sensitive company information. The Simeio solution handles confidential data in the form of customer personally identifiable information (PII) which includes customer identity data and account information. Additionally, Simeio, being a software company, has proprietary intellectual property (such as software code) that it needs to protect against internal and external compromise and misuse. Cloud security was also of importance since their environment includes AWS and Microsoft Office applications in the cloud.

### Key Challenges

- Require cloud security monitoring for the company's sensitive data, including PII, from data exfiltration and misuse
- Need behavioral analytics to detect and respond to insider threats
- Need the ability to detect advanced cyber threats

### The Solution: Security Monitoring with Securonix

Simeio chose Securonix Next-Gen SIEM because of the solution's flexibility and software-as-a-service deployment strategy. Securonix runs on AWS infrastructure and monitors security events in a secure and dependable manner.

Securonix Next-Gen SIEM detects and responds to advanced insider threats and cyber threats using its cutting-edge machine learning-driven technology. Securonix monitors Simeio's on-premises and cloud logs from data sources such as Microsoft Office 365, AWS CloudTrail, Windows Active Directory, firewalls, and endpoints, among others. Their top use cases include insider threat monitoring, cloud security monitoring, and cyber threat monitoring.



## The Business Impact: Detect and Prioritize Unknown Threats

Simeio was able to save thousands of dollars in capital expenditures, time, and resource cost due to minimal operational overhead, rapid deployment, and no associated hardware infrastructure costs with the Securonix Next-Gen SIEM. The low rate of false positives and full visibility into cloud infrastructure and apps helped Simeio overcome their initial challenges to detect threats no matter if they originated internally or externally. Finally, the Securonix Next-Gen SIEM ensures compliance of the AWS environment and provides cloud security monitoring of sensitive data to prevent data exfiltration and misuse.

The Securonix cloud-native platform is SOC2 Type 2 certified. Securonix provides Simeio with a highly secure deployment that meets the company's security and compliance requirements by leveraging the security capabilities of the AWS infrastructure and built-in security and privacy controls with Securonix.

### 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](https://securonix.com)



Visit Securonix in [AWS Marketplace](#)

