securonix

AmerisourceBergen®

CASE STUDY

AmerisourceBergen Uses Securonix Next-Gen SIEM to Reduce Cyber Risk by 80%

securonix

AmerisourceBergen

CASE STUDY

AmerisourceBergen Uses Securonix Next-Gen SIEM to Reduce Cyber Risk by 80%

About AmerisourceBergen

AmerisourceBergen is one of the world's largest pharmaceutical distributors. They are based in the United States and have over 150 global offices in more than 50 countries worldwide. It was founded over 100 years ago and is ranked in the top 10 of the Fortune 500.

The Challenge: Detect Internal and External Threats Across a Huge IT Environment

AmerisourceBergen, one of the world's largest pharmaceutical distributors, needed to find a cybersecurity solution to detect threats that was reliable, adaptable, open, and cost-effective to serve as the backbone of their security operations center (SOC). The organization needed a solution that could ingest and analyze all the data across their large IT environment of over 100 devices and detect potential threats. Overall, AmerisourceBergen needed to boost their cyber threat detection, mitigation, hunting, and response skills to make better and more informed decisions about what violations analysts should investigate.

In addition to increasing their security posture, a major concern for this organization was the storage and retrieval of data over a large period of time – which may span several years – for compliance purposes. AmerisourceBergen needed a solution that would support compliance efforts including the United States' Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), and the European Union's General Data Protection Regulation (GDPR).

Key Challenges

- Enough scalability to ingest huge volumes of data from over 100 devices and with over 100 billion events
- Need for advanced analytics for threat detection, hunting, investigation, and response to take informed decisions against cyber and insider threats
- Require enough data storage and retrieval to cover a large period for compliance – which can span several years
- Lack of a unified platform for security monitoring, detection, response, remediation, and compliance

The Solution: Securonix Next-Gen SIEM Scales to Improve Security Operations and Compliance

AmerisourceBergen evaluated several products and chose Securonix Next-Gen SIEM for its scalability and advanced analytics with UEBA, over Splunk and IBM QRadar. The organization uses Securonix Next-Gen SIEM as their central security monitoring solution to mitigate risk posed by external and internal threats, handling over 100 billion events from over 100 devices.

The organization uses Securonix as a security data lake to collect and analyze all of their data across technical solutions, like email security and data loss prevention, but also non-technical systems like those used by Human Resources. Using Securonix Next-Gen SIEM, the security team works with data from across AmerisourceBergen to detect possible cyber and insider threats, such as connections to external sites, with entity behavioral analytics. Additionally, security now has visibility into the kill chain in order to identify threats at various stages of progression and prioritize which to investigate. Securonix Next-Gen SIEM also covers compliance mandates for HIPAA, PCI DSS, and GDPR to help the organization meet its compliance goals.

The Business Impact: Reduced Insider Threats by 80% Within One Month

AmerisourceBergen was pleased that, within one month, 80%, or 400 of their insider threats, were resolved. AmerisourceBergen was also able to reduce the potential reputational and financial risks that could be caused by an external attack resulting in the theft of business-critical information or disruption of the organization's critical services.

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