securonix | Alberta Health Services

CASE STUDY

Alberta Health Services Reduces False Positives by 90% with Securonix

CASE STUDY

Alberta Health Services Reduces False Positives by 90% with Securonix

Alberta Health Services

Alberta Health Services is part of Canada's first and largest provincewide, fully integrated health system and is responsible for delivering health services to more than 4.4 million people living in and around Alberta. They offer programs and services at more than 900 facilities throughout the providence.

> "We've cut down on a huge number of false positives which has resulted in massive time savings. We've saved hundreds of thousands in labor, we used to have 3 FTE employees dedicated to closing false positives who now have time to focus on incident response"
>
> – Cyber Security Operations Manager, Alberta Health Services

The Challenge: Reduce False Positives and the Time Spent on Maintenance

Prior to adopting Securonix, Alberta Health Services (AHS) leveraged the on-prem solution from RSA, NetWitness. This solution relied on a large amount of hardware, making maintenance expensive and time-consuming for their SOC. AHS spent 2-3 hours a day just on maintenance and struggled to get adequate support from their vendor. On top of dealing with constant tuning issues, they also faced alert fatigue and a highly manual investigation process.

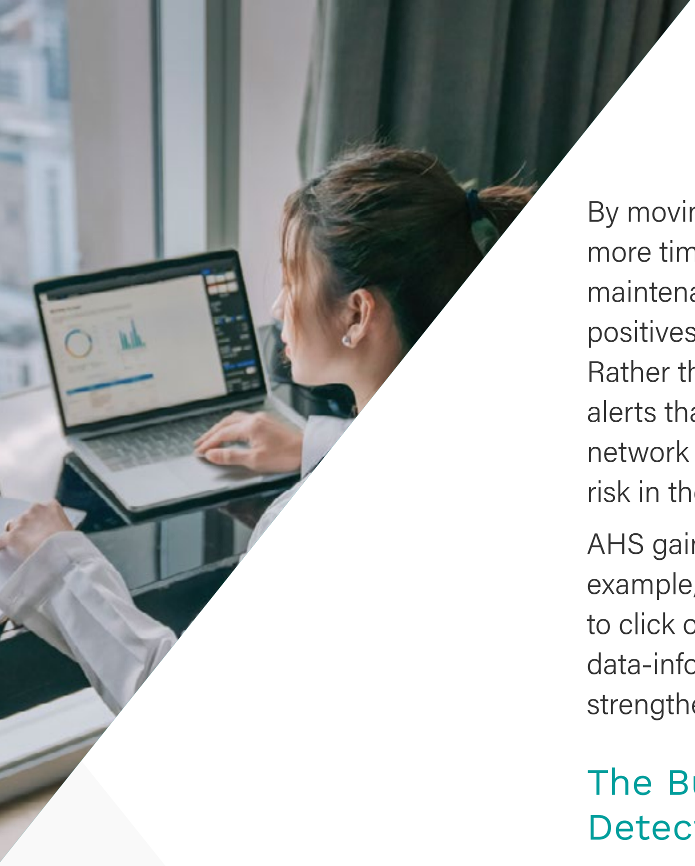
They needed to streamline incident case management with advanced analytics and offload the burden of maintenance with a cloud-based solution.

Key Challenges

- Unburden their team from tuning and maintenance issues
- Reduce false positives and detect threats faster
- Partner with a vendor who could provide consistent support

The Solution: Securonix Provides Continuous Security Monitoring in a Cloud-Native Solution

When searching for a Next-Gen SIEM solution to meet their unique needs, AHS ultimately chose Securonix Next-Gen SIEM due to the solution's industry-leading behavior analytics and cloud-native platform that offers log management, security analytics, and a security data lake in a single solution.



By moving to a cloud-native solution, AHS analysts were able to devote more time to critical detection and response tasks instead of SIEM maintenance and tuning. The Securonix Next-Gen SIEM reduced false positives by transforming raw events into meaningful insights in real-time. Rather than chasing down and investigating an incident, analysts received alerts that were already enriched with information around identity, assets, network activities, and more, giving them a more complete picture of cyber risk in their organization.

AHS gained a better understanding of their user trends and activity. For example, they learned that the night staff were almost 10X more likely to click on a phishing link. This level of visibility allowed them to make data-informed decisions to recommend additional security training and strengthen their overall security posture.

The Business Impact: One Platform for Security Detection and Response

By adopting Securonix, AHS now has a cloud-native platform with better visibility and security insights. Benefits of Securonix Next-Gen SIEM include:

- **Fast Time-to-Value:** Received more value in their first 6 months with Securonix than in 8 years with their previous solution.
- **Reduced False Positives:** 3 full-time employees who solely worked on reducing false positives now focus on more critical detection and response tasks.
- **Zero Infrastructure to Manage:** Gained 2-3 hours a day back by offloading maintenance to Securonix.
- **Massive Time Savings:** A 90% reduction in false positives compared to their previous solution reduces manual investigation times.

Ultimately, AHS found a partner they can trust to partner with them as they scale.

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