Netsurion™ | EventTracker®

Case Study

Co-Managed SIEM - Insurance Company

INSURANCE

About the Customer:

This U.S. based insurance company has 55+ years of experience supporting agents and clients as a trusted advisor. As a high-value target to hackers, the insurance firm is committed to protecting sensitive personally identifiable information (PII), maintaining compliance, and retaining customer trust. They sought a security solution that would strengthen security defenses, rapidly detect new and emerging threats, control security costs, and optimize their existing team's capabilities.

"We built our security processes around Netsurion's EventTracker co-managed security. We want to be proactive versus reactive and adopt advanced cybersecurity features to add coverage beyond our three-person IT team"

- Cybersecurity Manager, U.S. Insurance Company

The Challenge

As a financial services vendor that processes credit card payments, they faced increasing security and compliance mandates, starting in 2014. "PCI DSS was the initial catalyst to select a Security Information and Event Management (SIEM) solution to increase visibility and log correlation," said the cybersecurity manager at the insurance company. The insurance company's small IT team was already stretched with day-to-day operating responsibilities, so it was clear that a managed SIEM solution with a Security Operations Center (SOC) would be crucial. "Netsurion's co-managed security solution with strong compliance and incident investigation provides 24/7 monitoring and peace of mind," said the cybersecurity manager. The insurance company continues to advance its cybersecurity capabilities in light of today's accelerating data breaches.

Prior to a co-managed SIEM, their team faced:

- Finite IT and security resources despite ever-increasing threats
- Lack of 24/7 visibility and challenges identifying remediation recommendations
- Difficulty maintaining PCI DSS compliance
- Uncertainties in implementing File Integrity Monitoring (FIM) for data protection

"Event monitoring and log management were previously done on an ad hoc basis. We were searching for a security partner that could grow with us over time. Netsurion's EventTracker SIEM provided the foundation for our security infrastructure," said the long-time cybersecurity manager for the insurance company.

Solution - Why Netsurion's Co-Managed SIEM

"We considered many SIEM solutions such as SolarWinds, Splunk, and EventTracker. We shortlisted Netsurion's EventTracker SIEM based on a co-worker's previous successful experience. After doing research and viewing demos from all the vendors, we selected EventTracker by Netsurion that can be tailored to our unique requirements," said the insurance company's cybersecurity manager.

Smaller organizations face enterprise-scale threats but operate with finite IT resources. It can be challenging to deploy, manage, and use an effective combination of experts and tools for early detection of advanced attacks and insider threats. Comprehensive 24/7/365 monitoring and real-time log correlation were crucial to the organization's IT and security team. "We wanted a managed SIEM to do it right, otherwise SIEM would just be a boat anchor weighing us down," said their security leader.

Netsurion's co-managed SIEM solutions are purpose-built for small-to-medium-sized businesses (SMBs) with ease-of-use and affordability at its core. For example, real-time alerting and reporting are essential capabilities for the SOC-as-a-Service insurance customer. "We selected Netsurion's daily report option. We need full 24/7 coverage so that we don't overlook any security threats," said the insurance firm's cybersecurity manager. "The EventTracker SOC keeps an eye on systems and our network. I like the color-coded cybersecurity reports that pinpoint areas for action

and increase productivity by arming me with remediation recommendations."

Onboarding and Security Effectiveness

Every organization's security needs are different. "Netsurion has always been flexible and open to tailoring the onboarding meeting and content to our needs and questions," said the insurance company executive. "The Knowledge Pack (KP) team has been very responsive in creating new software integrations for us in just a few weeks. During the vendor evaluation process, other SIEM vendors said custom integrations with our existing applications could take 6-8 weeks to complete."

The insurance company's initial implementation of EventTracker SIEM occurred in 2014. Advances in the portfolio motivated them to adopt EventTracker v9.1 to capitalize on advanced search and threat investigation capabilities. "We liked the Elasticsearch capabilities to monitor and investigate cloud security and alerts built around Office 365," said the insurance company's cybersecurity manager. "We did have to procure different hardware for v9.1, but in the grand scheme, it was a worthwhile expense to advance our security maturity."

Accelerate Security with EventTracker EDR

"Today's biggest threats take advantage of endpoint gaps," noted the insurance company's cybersecurity manager. An Endpoint Detection and Response (EDR) solution integrated with SIEM and backed by a managed service was crucial for effective remediation and automation. As a complement to their co-managed SIEM solution, they selected EventTracker EDR from Netsurion in 2019 to correlate data and provide contextual visibility into potential attacks that span multiple endpoints and networks.

Netsurion's EventTracker EDR met all their needs:

- Catch threats that traditional anti-malware tools miss
- Block suspicious processes in real-time
- Reduce dwell time at all stages of the threat chain, including lateral movement

"We were happy with our anti-virus software, but dropped our anti-malware subscription after purchasing EventTracker EDR from Netsurion, which helped offset the cost," said the insurance company's security expert. The console's single pane of glass visibility also increased the IT team's efficiency.

"It made sense to let EventTracker manage EDR - it leverages the same sensor as Netsurion's co-managed SIEM," said the cybersecurity manager for the financial services organization.

Results

Netsurion's co-managed security predicts, prevents, and detects while the EventTracker Security Operations Center (SOC) analysts help organizations of all sizes and industries respond quickly and appropriately. "We look closely at the daily reports produced by Netsurion," said the insurance company's cybersecurity manager. "I use them for my weekly meetings with the chief information officer (CIO) to outline any incidents, assess insider and external threats, and provide actionable information to cross-functional teams and executives."

The co-managed SIEM's built-in behavior analysis detects suspicious activity and provides real-time alerting for rapid investigation and mitigation. "Our EventTracker SOC analyst detected some suspicious events inside our insurance organization," noted the cybersecurity manager. "We investigated and found that an insurance company employee had circumvented internal company policy regarding flash drives, which we do not allow. This rapid notification enabled us to take quick action with the rogue employee who may be downloading sensitive data."

Benefits to the insurance company included:

- Achieved real-time 24/7/365 security monitoring and actionable threat intelligence
- Delivered a straightforward, cost-effective solution tailored to organizational needs
- Improved compliance with PCI DSS and FIM
- Enhanced security posture with a small IT team

An integrated SIEM + EDR + SOC solution was the crucial step for the insurance organization's maturing IT infrastructure.

"I am impressed with the co-management and the level of expertise that EventTracker SOC brings to the table. I connect daily with our EventTracker SOC Analyst. I know EventTracker's cybersecurity experts will help us defend our network and sensitive data," summarized the insurance company's long-standing Cybersecurity Manager.