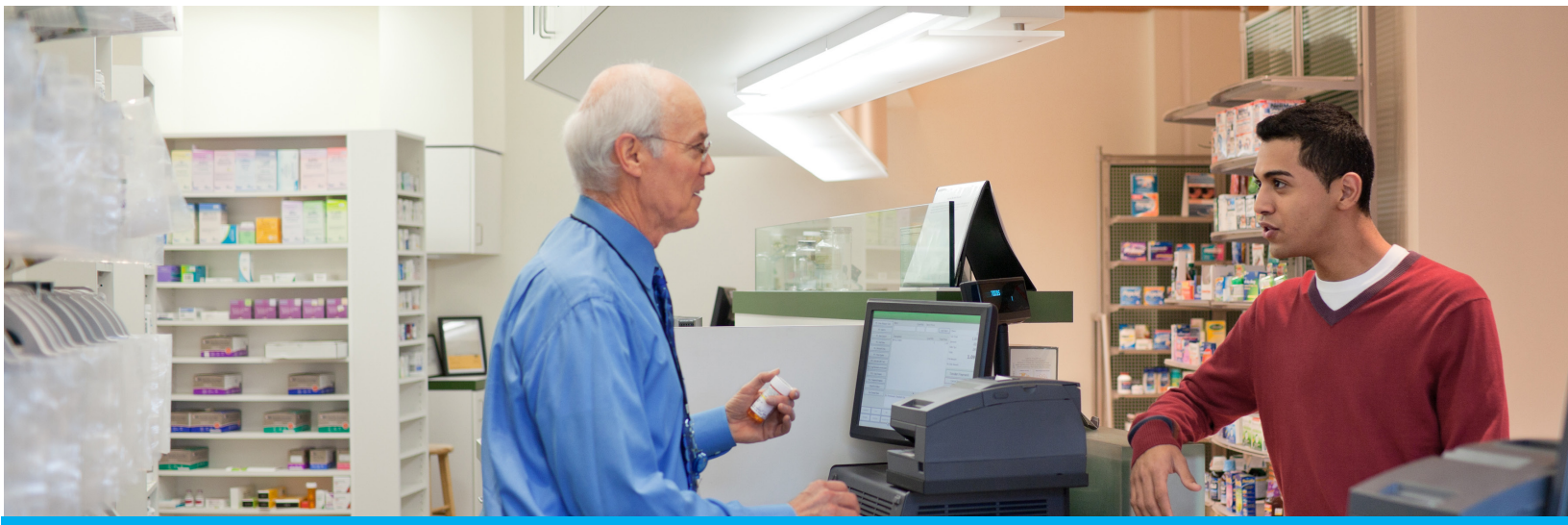
Healthcare Provider

Active Threat Analytics – Premier



Cisco Active Threat Analytics Premier helped this hospital protect sensitive client information while adopting and securing innovative medical technologies connected to their network.

Customer Profile

- U.S. hospital
- Famous, privacy-sensitive customers
- Enthusiastic about new technology and the possibility to position as a security leader in the healthcare industry

Solution

- Active Threat Analytics Premier pilot
- Big data capabilities to enable proactive threat hunting
- Secured connections between innovative medical technologies

Key Takeaways

- New ability to approach customers a security leader in healthcare
- Saved resources by securing technology with proven Premier methodologies
- Increased security capabilities: proactive threat hunting, full-packet capture for detailed visibility into specific threats

Security Challenge

This U.S. hospital, subject to the needs of high-profile, privacy-sensitive customers, was interested in branding itself as a security leader in the medical industry. By positioning as innovatively secure, the hospital would both improve its brand and decrease its risk of a breaches that incur monetary expenses and other damages for a healthcare industry already under extreme regulatory scrutiny.

However, the hospital's current capabilities were reactive, and its leadership wanted to get ahead of the attacks it was experiencing. Because the reactive security operations were relatively immature, the hospital struggled to deal with the cyber attacks it encountered.

The hospital's medical staff members were also early-adopters of new medical technologies. Not only does the Internet of Everything increase connectivity between people, process, data, and things but also increased attack vectors for cybersecurity threats. Therefore, the challenge for this hospital included adopting innovative new technologies while effectively securing a greater number and variety of connections.

Cisco Solution

Due to the inherent sensitivity of the medical data handled by this hospital, the extra privacy needed for its notable clients, and the desire to position as a security-leading hospital, Active Threat Analytics Premier was the clear solution.

Active Threat Analytics Premier uses advanced analytics approaches to proactively hunt threats, which resolve the hospital's struggle to become less reactive. Specifically, big data analytics, along with full-packet capture and expert security personnel, enables the collection of huge amounts of device agnostic network telemetry. Active Threat Analytics then manipulates and interprets this data to proactively identify potential cyber attacks and other security risks.

Furthermore, Active Threat Analytics Premier solves the hospital's challenge of securing multiple technologies by readily aggregating and analyzing information from all customer technologies in the Cisco OpenSOC platform. In this platform, expert Cisco threat analysts and investigators review the hospital's security events and escalate if necessary.

Business Outcomes

Because Active Threat Analytics Premier uses big data for proactive threat hunting, the hospital evolved from its former reactive capabilities. Furthermore, the next-generation, cutting-edge capabilities of Active Threat Analytics Premier enabled the hospital to position itself as a trustworthy company to high-profile clients.

The hospital received the advanced accuracy and speed of threat detection offered by Active Threat Analytics. The service provides a 24-hour focus on the hospital's network that, when supplemented with its threat detection capabilities, offers the most reliable managed threat service available on the market.

Active Threat Analytics constantly filters thousands of security events, alerting users of only pertinent incidents and providing customized, rapid remediation recommendations. This filtration provided focused and complete visibility to the hospital's security posture, while saving time and resources that its analysts and investigators could instead use to focus on initiatives more central to the business. Furthermore, this full visibility enables the hospital to proactively improve its program and stay ahead of emerging threats.

About Active Threat Analytics

Cisco Active Threat Analytics (ATA) integrates deep expertise with cutting-edge technology, leading intelligence, and advanced analytics to detect and investigate threats with great speed, accuracy, and focus. Our expert investigators monitor customer networks 24x7 from our global network of state-of-the-art security operations centers, providing constant vigilance and in-depth analysis as a comprehensive security solution.

www.cisco.com/go/securityservices