

# Healthcare Technology Provider

## Active Threat Analytics – Essential



Cisco® Active Threat Analytics Essential helped this healthcare company manage the taxing effects of growth and technological innovation on its in-house security team.

### Customer Profile

- An American healthcare provider
- Experienced company growth and increased demand for innovative technologies
- Lacked internal resources necessary to effectively manage the secure adoption of new technologies

### Solution

- Cisco Active Threat Analytics Essential
- Provided management for the company's security technologies
- Cisco Security Operations Center supplemented the company's security team with added expertise to analyze security events

### Key Takeaways

- Faster and more accurate detection of threats in the customer's network
- Time and resources saved by Active Threat Analytics network management
- Room for the health care company to scale its security operations Enhanced and Premier Cisco offerings

### Security Challenge

This U.S.-based international healthcare company is known for the innovative and reliable medical devices, software, and solutions that it sells to hospitals worldwide. The company is subject to the privacy demands both of the hospitals and the patients who interact with their products. Strict healthcare regulations, sensitive patient information, and increasingly sophisticated cyber threats culminated in the company's need for advanced network security.

To respond to these needs, this healthcare company established its own security operations center. However, continued growth increased demand for the company's products and drove innovation in new technologies, and its security team became overwhelmed with the level of work stemming from this added connectivity. The healthcare company sought a solution to streamline its day-to-day threat monitoring operations to unburden its security team and more effectively manage its growth and adoption of disruptive security technologies.



## Cisco Solution

Because this healthcare company needed to improve its security operations with limited internal resources, Cisco met this challenge with Active Threat Analytics Essential – the first tier of its Active Threat Analytics portfolio. This service met the security needs of a company facing difficulties with growth and the subsequent increase in threat detection responsibilities.

The company needed help managing its expanding range of devices, and Essential had the capability to seamlessly incorporate and monitor the healthcare company's new and existing third party devices, products, and software. Active Threat Analytics Essential security technologies installed on the healthcare company's premises made this holistic network management possible. Furthermore, Active Threat Analytics Essential provided an existing security operation center, adding expertise to supplement the health care company's still expanding security team.

Even while incorporating more technologies into its analyses, Essential reduced the number of false-positive security alerts with continuous management, log collection and event correlation, and threat intelligence backing remediation recommendations.

## Business Outcomes

Active Threat Analytics Essential reallocated time and resources for the health care company's security team from tedious threat monitoring to a focus on core business initiatives.

Essential provided speedy and accurate threat detection with a constant focus on the customer's network. These capabilities equipped the hospital's security team to securely incorporate a wide range of state-of-the-art technologies into its portfolio.

The healthcare company is still growing and adopting increasingly advanced security capabilities from Cisco. Active Threat Analytics Essential was first step in maturing the company's security operations. As the company grows and its security needs continue to evolve, Cisco will be able to provide increasingly efficacious and beneficial solutions through more advanced (Enhanced and Premier) levels of Active Threat Analytics.

## 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](http://www.cisco.com/go/securityservices)