



# Active Threat Analytics: Essential

## Today's dynamic threat landscape

The global average cost of a data breach is \$3.62 million, according to a 2017 report by Ponemon Institute.<sup>1</sup> Meanwhile the global cybersecurity workforce will have more than 1.8 million unfilled positions by 2022 according to a 2017 report from Frost & Sullivan.<sup>2</sup> This talent shortage, combined with an increase in incidents, has led to a generally weak security posture among most organizations. This shows that there is a dire need of a near real time threat analysis system that can analyze the everchanging, complex and fragmented business.

## Manage, detect and respond effectively

At Cisco, we partner with you to approach the challenges you face head on. We're experts in security and invest heavily in security talent, technology and intelligence. We've packaged these capabilities together to provide you with managed security services designed to help you maximize your investment, reduce complexity, and mitigate risk, allowing you to focus on growing your business with an improved security strategy, posture and threat coverage.

### Benefits



Increased network component utilization



Reduced operational management



Reduced deployment time



1,976 staff hours saved

Data based on Cisco analysis of customer experience results may vary. Learn more at [cisco.com](https://cisco.com)

<sup>1</sup> <https://www.ibm.com/security/infographics/data-breach/>  
<sup>2</sup> <https://iamcybersafe.org/wp-content/uploads/2017/07/N-America-GISWS-Report.pdf>

# Case Study

## American Healthcare Provider

### Challenges

- Strict healthcare regulations, sensitive patient information, and increasingly sophisticated cyber threats culminated in the company's need for advanced network security
- Inefficient day-to-day threat monitoring operations created a burden on the customer's security team
- Lacked internal resources necessary to effectively manage the secure adoption of new technologies

### Solution

- Provided management for the company's security technologies
- Cisco Security Operations Center (SOC) supplemented the company's security team with added expertise to analyze security events

### Outcome

- Accurate identification of threats in the customer's environment
- Time and resources saved by security device management
- Opportunities to scale security operations by adding other Cisco managed security offerings

## Active Threat Analytics: Essential

As a managed security service, the ATA Essential security team will monitor and manage your Cisco and third-party\* security devices 24/7/365 from a Cisco SOC. Our security investigators will monitor your security devices for security incidents and threats; and, our security engineers will manage the overall health and welfare of your investments by providing ITIL-based change and problem management services. Get started today, learn more, and contact your Cisco representative.



#### Policy Management

Create, deploy, test, and manage device configurations, signatures, and rule sets



#### Proactive Device Monitoring

Proactive, end-to-end performance and welfare monitoring



#### Holistic Architecture Management

Rule and signature tuning and optimization



#### Security Incident Analysis

Monitor and analyze security events and report validated network and system security incidents



#### Detailed Reporting

Device performance and security analysis reports



#### Device Support

Network/System Security, Identity & Access, Perimeter Security, Content Security, Security Management

\*Contact Cisco for list of supported third-party devices

## Next Steps

Visit [cisco.com/go/securityservices](https://cisco.com/go/securityservices) to connect with our advisors and protect your business today.