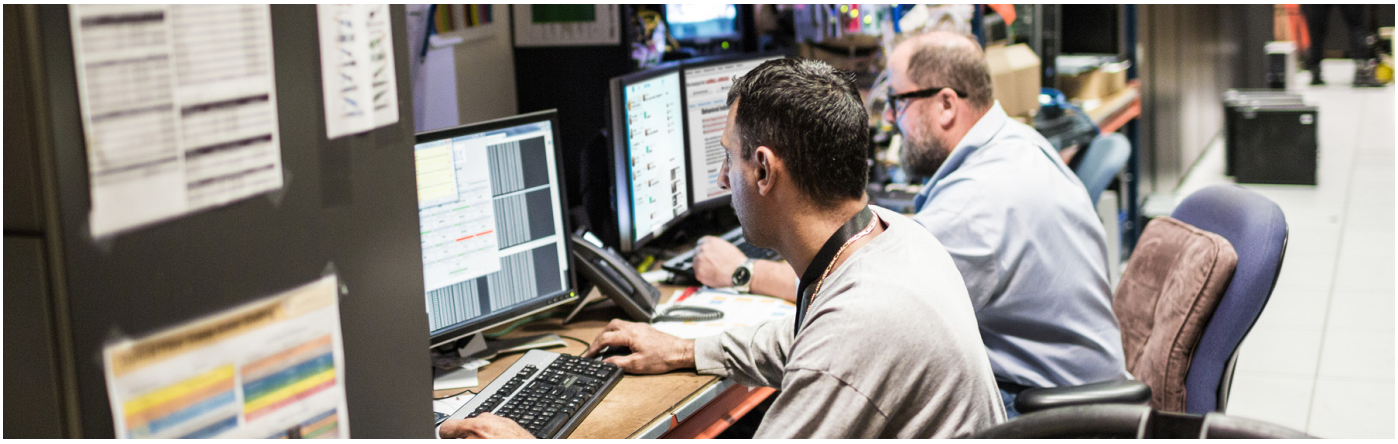
Case Study

Improving Visibility and Security with Cisco Stealthwatch



EXECUTIVE SUMMARY

Customer Name: Erie Insurance

Location: Erie, Pennsylvania

Number of Employees: More than 5,000 (plus 12,000 independent agents)

"Stealthwatch has provided us insight into areas of our network that we did not previously have."

"Whenever I do an investigation, one of the first stops I make is to pull the flows for the assets in question from Stealthwatch."

Jamison Budacki
Senior Information Security Architect, Erie Insurance

Challenge – Lack of Network Visibility

Erie Insurance is a publicly held company based in Erie, Pennsylvania, offering auto, home, life, and business insurance. The company was founded in 1925 with the goal of putting customer service above all else. Today, Erie Insurance is a Fortune 500 company with over 5,000 employees, 12,000 independent agents, and 5 million insurance policies in place with customers across 12 states and the District of Columbia.

As a result of several audits, penetration tests, and self-assessments, Erie's IT team realized that it needed better network visibility to accelerate threat detection and incident response.

"We needed improved situational awareness on our network as a whole, especially insight into our remote branch locations," said Jamison Budacki, Senior Information Security Architect at Erie.

He explained that his team's previous toolset had led to a number of challenges, including:

- Slower threat detection and response due to having too many disparate tools, too much information, and the need for a lot of manual correlation to find the right data
- Limited data retention capabilities
- No compatibility with other technologies

Expanded Network Insight and Improved Response

Erie Insurance turned to the Cisco Stealthwatch™ solution to address these issues. By collecting and analyzing NetFlow data from Erie's existing network infrastructure, Stealthwatch delivers end-to-end visibility and security intelligence.

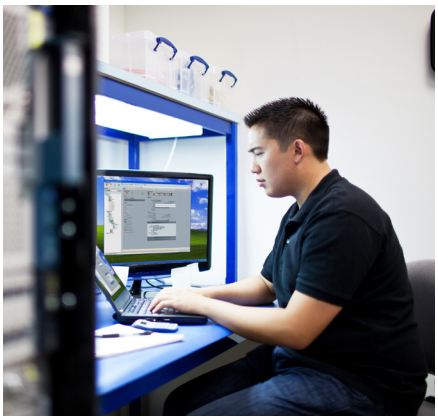
Today, Stealthwatch is monitoring the company's campus, data center, various demilitarized zones (DMZs), and all 25 branch locations, and is used by its security analysts on a daily basis.

Stealthwatch is one of the main tools used by Erie's security team when doing any type of investigation – whether it's for a DDoS attack, malware infection, data exfiltration, policy violations, and so on.

The company uses both the CIS Critical Security Controls and NIST Cybersecurity Framework as part of its security strategy. Stealthwatch has improved Erie's self-assessment scores against each respective framework.

"We had numerous penetration tests that had similar themes and underscored our need to improve in areas such as network segmentation and monitoring and detection capabilities," said Budacki. "The analysis and capabilities that Stealthwatch offers had a significant impact on our self-assessment scores."

He added, "Aside from greatly improving our self-assessment scores, Stealthwatch has reduced our mean time to know (MTTK) and our mean time to respond (MTTR). Stealthwatch has also been integrated with other investigation tools for greater operational insight into incidents and visibility into all areas of our network."



Product Integration for Comprehensive Security

Erie has integrated Stealthwatch with other tools including its SIEM, Gigamon infrastructure, and several Cisco® ASA firewalls for more seamless security. The company has also integrated Stealthwatch with the Cisco Identity Services Engine (ISE) to obtain user attribution for network activities.

"This integration gives us the ability to easily search for a user within Stealthwatch," said Budacki. "The integration of ISE and Stealthwatch has been extremely helpful in user attribution as well as obtaining deeper insight into the devices on the network."

In the future, Erie plans to expand its Stealthwatch and ISE integration by automating some remediation decisions. For example, if Stealthwatch detects anomalous user behavior, it can send a command to ISE to quarantine that user.

Added Benefits of Stealthwatch

Additional benefits of the Stealthwatch deployment for Erie include:

Greater collaboration between the security and networking teams

"When I started at Erie Insurance, there wasn't a lot of collaboration between the two teams and that was something I really wanted to change right away," said Budacki. "We did that, and now with our great relationship, we make use of their technology, they make use of our technology, and it makes things operate a lot smoother. The network team makes use of Stealthwatch as a replacement for a legacy tool that was no longer being utilized. They also use Stealthwatch for capacity planning, QoS policy development, and looking for top talkers during congestion."

Long-term data retention for improved forensics

Erie's goal was to get at least 120 days of flow data retention, and with Stealthwatch, they can now retain over a year's worth of data.

Products

Security

- Cisco Stealthwatch
- Cisco Identity Services Engine (ISE)
- Cisco ASA 5525-X and 5545-X Adaptive Security Appliances

NAT stitching for extended visibility

"Stitching takes the public Internet IP address and our internal IP address and combines it into a single flow record," said Budacki. "This enables us to see the actual host in question and not just a NAT address."

Effective customer support and training

According to Budacki, the Stealthwatch support team is very willing to go out of their way to help Erie get an answer or a fix to a problem. He also said that the training provided for Stealthwatch customers has made it easier for Erie to onboard new employees.

With Cisco Security, Erie Insurance is better equipped to continue offering exemplary service to its millions of customers. "Stealthwatch has provided us insight into areas of our network that we did not previously have," said Budacki. "Whenever I do an investigation, one of the first stops I make is to pull the flows for the assets in question from Stealthwatch."

For More Information

This case study is based on a longer Q&A conducted by the SANS Institute. Access the full interview here: http://www.cisco.com/c/dam/en/us/products/collateral/security/stealthwatch/cisco-erie.pdf.

Find out more about Cisco Stealthwatch and ISE at http://www.cisco.com/go/stealthwatch and http://www.cisco.com/go/ise.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices**.

C36-738691-00 03/17