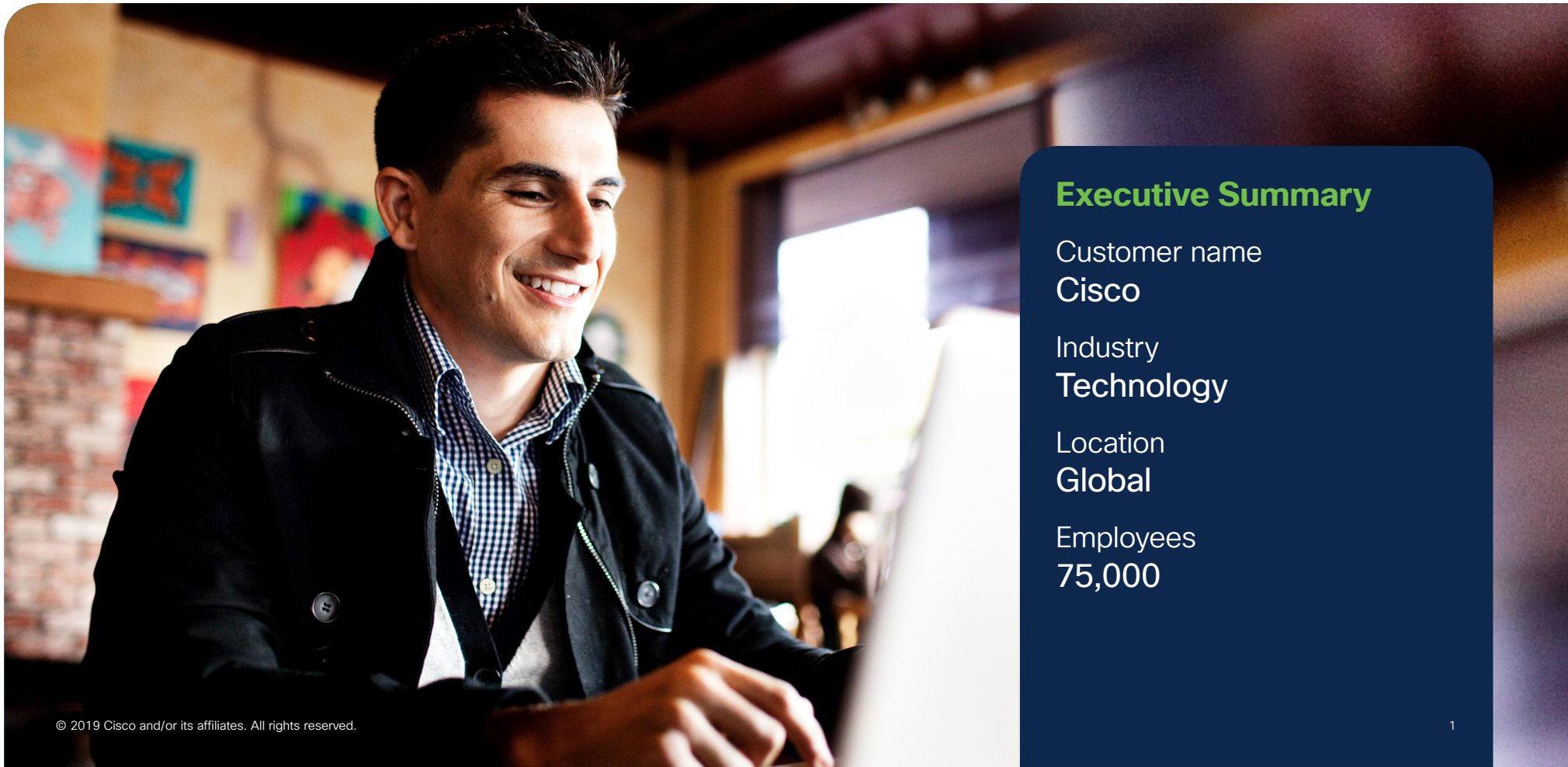
Endpoint Visibility = Better Security for Cisco

Combined Cisco and Splunk solution reduces investigation time from days to hours



Executive Summary

Customer name
Cisco

Industry
Technology

Location
Global

Employees
75,000

Challenges

- Needed additional visibility for endpoints on and off the network
- Wished to improve unknown and insider threat detection on the endpoint
- Wanted to shorten incident investigation time

Solution

- Cisco® Endpoint Security Analytics Built on Splunk:
  - Cisco AnyConnect Network Visibility Module (NVM)
  - Splunk Enterprise

Results

- Obtained in-depth visibility across 96,000 endpoints
- Reduced investigation time from days to hours
- Fortified overall security

In a company of roughly 75,000 employees, visibility is critical for the Cisco information security team. While confident in its ability to see and monitor network traffic, the team wanted to obtain better visibility into the endpoints and follow their activity when off the Cisco network.

To effectively secure the Cisco environment, the information security team wanted in-depth endpoint knowledge of: who was using its devices, which applications they were running, how much data they were transmitting, and so on. This way, anomalies such as insider threats, data hoarding, and malware could be quickly identified and remediated.

Cisco turned to its own technology, the AnyConnect Network Visibility Module (NVM), to obtain this insight. Still, it needed a way to quickly query and analyze the telemetry data provided by NVM. Having been a Splunk customer for a number of years, the Cisco security team felt that a combined solution of NVM and Splunk would be the best solution for the job. Today, the combined solution is known as Cisco® Endpoint Security Analytics Built on Splunk, and Cisco offers it to its customers as well.

> "Splunk makes accessing the data from NVM, writing queries, and analyzing the data very easy."

Imran Islam
Cisco CSIRT

Unique Endpoint Visibility

According to Imran Islam, the leader of Cisco's EMEA/APAC CSIRT team, there is no other product on the market that can profile an endpoint like NVM. Invented by Cisco, it provides a wide range of data on various facets of endpoint activity and attributes, such as:

- Which devices and operating systems are on the network?
- Who is using each device and what are they doing with them?
- Which endpoints have known bad files or applications?
- Which endpoints are talking to bad domains?
- Are any machines using unapproved applications or SaaS services?
- Is someone hoarding or exfiltrating data?
- Did any users' behavior change?

These are just a few examples of the insightful details that can be gleaned from NVM.

Today, Cisco is using the solution to analyze data across roughly 96,000 endpoints. Data can be continuously collected whether users/devices are on- or off-prem, and select variables within the data can be excluded if necessary to comply with privacy requirements.

Additionally, because it is part of Cisco AnyConnect, NVM was easy for Cisco's security team to deploy, and is simple for other companies to implement as well. Cisco AnyConnect is best known as Cisco's VPN client deployed to more than 130 million endpoints. With AnyConnect, customers do not have to worry about deploying yet another agent in their environment to obtain in-depth endpoint visibility.

Quick, Easy Data Analysis

NVM provides a rich set of endpoint data, but it needs to be analyzed by an equally powerful technology. Using Splunk Enterprise, the Cisco security team can collect and analyze IPFIX flows generated by NVM, pulling out context such as user, device, application, location, and destination for each flow.

At one point it became necessary for the Cisco security team to quickly determine which machines in its environment were running a specific, unsecure application. With only the "update server" domain name as a starting point, the security team was able to identify:

Cisco's security team estimates that roughly 80 percent of these use cases wouldn't be possible without the NVM and Splunk solution.

1. The application processes that were connecting to the update server.
2. The hostnames of the systems running the software.
3. The operating systems of the hosts.
4. Other (undocumented) domains with which the software was communicating.

Typically, this investigation would require a week's worth of requests and multiple systems to complete. With Cisco Endpoint Security Analytics Built on Splunk, the team was able to uncover which endpoints had the software installed in a matter of hours. The team could then immediately block the process using Cisco AMP for Endpoints, as well as Cisco Umbrella to stop any DNS lookups.

According to Imran Islam, “Splunk makes accessing the data from NVM, writing queries, and analyzing the data very easy.” He also said that it’s very simple to create a dashboard and share the data with others.

In a complex environment like Cisco’s, this flexibility is key. “For an advanced security team like ours, it’s important to be able to work with a rich command set so that we can look for exactly what we want across our endpoints and customize the output,” said Imran. For more novice users, Cisco also offers a free Splunk app for Cisco Endpoint Security Analytics that makes data visualization and analysis more turnkey, so the technology can be leveraged by a wide range of users.

Because Cisco Endpoint Security Analytics Built on Splunk is based on behavioral analysis and identifying changes in behavior, it provides a rich data source for threat hunters/analysts proactively looking for malicious or suspicious activity. It can provide early detection for threats that would be missed by antivirus and other endpoint solutions.

It is also important for detecting insider threats that cannot be mapped back to known attack behaviors, such as an employee sending confidential data to a competitor. The Cisco security team can set parameters for normal endpoint behavior, and get alerts for anything that deviates from these parameters to gain visibility into a wide range of potential threats.

Part of a Cohesive Solution

Endpoint visibility and analysis is just one piece of a comprehensive security strategy. The Cisco security team relies on this solution alongside other technologies including Cisco Stealthwatch, Umbrella, and AMP.

What NVM provides on the endpoint in terms of visibility, Stealthwatch provides on the network. Correlating telemetry from the network and endpoints allows the Cisco infosec team to effectively piece together all the pertinent details surrounding network activity, including any potential attacks.

Once identified, malicious software and files can be blocked with Cisco AMP, and connections to bad domains can be remediated with Cisco Umbrella. AMP and Umbrella also work as visibility engines within the enterprise environment, for bad files and malicious domains, respectively, to help detect any risks.

Cisco Endpoint Security Analytics Built on Splunk is also used in conjunction with the Cisco Identity Services Engine (ISE) to conduct forensics after an incident – unveiling details such as what type of attack occurred, on which machines, who owns them, which technology the attack originated from, and so on. This integrated toolset enables Cisco and its customers to more quickly and comprehensively see and respond to incidents and strengthen overall security.

> “There is no other product on the market that can profile an endpoint like NVM.”

Imran Islam
Cisco CSIRT

For more information

For more information on Cisco Endpoint Security Analytics Built on Splunk, go to: cisco.com/go/cesa.