CISCO
SECURE

Case Study
Public

NHS experiences a clear advantage with Cisco Secure Endpoint

“Physically looking for malware takes time! When you’ve got 3 or 4 servers, that’s 30 minutes to 40 minutes per server, it all adds up!”

“Instead, with Secure Endpoint, it was much faster, 90 seconds with Orbital searching across all endpoints. So that’s an example of how Talos, Orbital and Secure Endpoint all work together to improve efficiencies.”

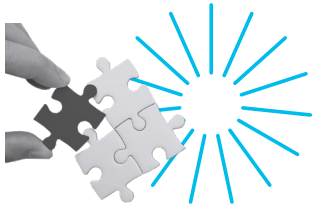
Cole Two Bears, Systems Architect, NHS Management

Customer Name
NHS Management

Industry
Healthcare

Location
Tuscaloosa, AL

Employees
7,000 employees at 60 locations



Objective

NHS Management sought to build a top-notch security capability with an emphasis on simplicity and efficiency to better defend their highly targeted PII data against online criminals and to safeguard information from phishing attacks, ransomware, data exfiltration, and more.

Solutions

Cisco® Security Enterprise License Agreement (ELA)

- Cisco SecureX
- Cisco Secure Email
- Cisco Secure Firewall
- Cisco Secure Network Analytics
- Cisco Talos
- Cisco Secure Malware Analytics
- Cisco Umbrella
- Cisco Secure Endpoint

SecureX platform

- Every Cisco Secure customer is entitled to the SecureX platform, a cloud-native, built-in platform experience that connects our Cisco Secure portfolio and your infrastructure.

And third-party solutions.

Benefits

- Enhanced security with a unified platform based on Cisco SecureX providing daily benefits from overall simplification and eXtended Detection and Response (XDR) capabilities
- Achieved consistent time savings inspecting all endpoints - going from 90 minutes to as short as 90 seconds
- 10X improvement in response times measured in minutes from what used to take hours
- Improved operational efficiencies with proactive threat intelligence from Cisco Talos

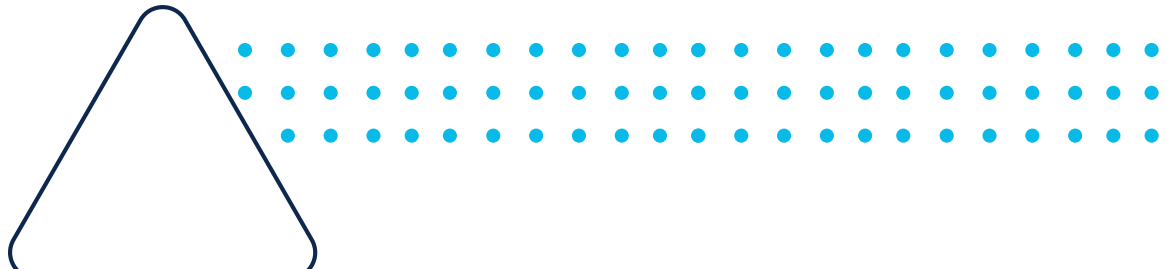
Challenge

For years so many businesses have been challenged with establishing a security posture that they feel confident in, but have been limited by minimal interoperability between security solutions, while simultaneously having to defend against advanced threats.

Speaking on prior security solutions, Cole Two Bears, Systems Architect of NHS, laments; “There had been no interoperability between these solutions and there was no visibility into what’s going on. Yes, you can have a syslog server. You can have an event, but that is just a recording based off of those event logs, and so the major challenge was the lack of visibility and understanding of what was transpiring among the endpoints when an incident occurs, when there was some type of vulnerability.”

“Frankly, it’s like the tools weren’t ready for prime time!”

> “My role is to primarily maintain the security operations of the organization. And that is to protect against the current emerging threat landscape relative to any type of attack, for example; ransomware, exfiltration potentially on modern applications, phishing, and the like.”
>
> Cole Two Bears
> Systems Architect, NHS Management



> “We received an email from Cisco, as we have Secure Endpoint, and it said; “Talos has the indicators of compromise for the SolarWinds malicious activity and has been updated as a retrospective verdict. Please inspect your organization.” So that was a huge reassurance for us that knowing that Cisco was already on top of it due to the Talos threat intelligence backing the solution.”

Cole Two Bears
Systems Architect, NHS Management

Solution

In recent years Cisco has unified the security platform and expanded capabilities beyond Next Generation Antivirus (NGAV) and Endpoint Detection and Response (EDR).

In 2020, Cisco, launched the SecureX platform enabling new capabilities such as eXtended Detection and Response (XDR) to provide much needed visibility and context that accelerates investigations and remediation by enabling control points to work together as a unified platform.

Two Bears sees the benefits that Cisco and the unified platform brings, and goes on to say, “now there’s really two levels of visibility - you’re seeing what’s happening real-time at the endpoints but then you can also see across all your control points.”

“Even using SecureX in the Beta form it was a very polished product. At the end of the beta task, I said, well I’ve gotten so used to using it and I said, well, is it possible for me to keep this?”

“Well, it’s amazing!”

Results

“For the feature set of Orbital (as part of Secure Endpoint) we were able to save a tremendous amount of time because there are SolarWinds products in our organization. So, we know what DLLs are out there because Talos published that for us.”

“We didn’t have to spend time on opening and inspecting Servers or use other methods such as PowerShell which involves writing a special script to go out and search for all these DLLs. Even then you never know if it was renamed to something different! “

“With the information that was published by Talos, we were able to skip all the manual steps and go through that quite easily.”

“We were just able to search knowing these machines have SolarWinds on them, or are Orion products. So because we know what they are we were able to simply search through the hashes using Orbital.”

“It took maybe a minute or two minutes versus much more time either writing a script – and not solely having to depend on if that observation was actually the name of the file in my environment,” Two Bears happily states.

*Note: SecureX dashboard capabilities are noted in demos here.

“Through the SecureX dashboard* you’re spending a quarter of the time that you normally would and it also encourages the positive behavior of proactively looking into things before they’re an actual issue.”

Cole Two Bears
Systems Architect, NHS Management

"Based on my experience with other products, the speed in which I can identify, isolate and remediate is ten-fold, for coherency."

Cole Two Bears
Systems Architect, NHS Management

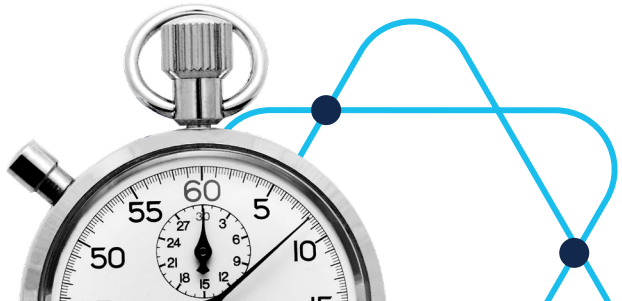
" Based on my experience with other products, even other EDR and XDR products, the speed in which I can identify, isolate and remediate is ten-fold, instead of taking hours. For example, when I have an alert that there's an endpoint with potentially malicious software, I go through a set of steps."

The old way; "Okay, let's do some manual steps: Well, is this a false positive? Are there any other threat intelligence seeing this potential file as potentially malicious? And then, now I've got to manually quarantine it and coordinate. And so, all this process that I described in a traditional sense, using traditional endpoint protection, results in an hour, up to an hour and a half of work."

The new way with Cisco SecureX orchestrating and automating security; "When I do perform an investigation with Secure Endpoint, having SecureX Threat Response, having Talos threat intelligence behind it, and seeing all the other sources available that are out there for a particular malicious code, **I'm able to do that in about 45 seconds – as opposed to an hour and a half**, so we can figure out the ratio for that as far as performance increase!"

Two Bears points out the advantage that visibility enables, "as we know Secure Network Analytics provides confidence intervals based upon the traffic after the initial baseline is established. So, you don't want to always have an alert because then you're not going to look into it. But I can see visually that there's a slightly higher than normal confidence interval that we have, e.g., data hoarding indicates that there is some type of potential exfiltration happening. That pushes me to look and dig into it."

"So instead of getting into a 3-hour process, as in the past, I now spend maybe 15 - 20 minutes!"



"Any Cisco customer is going to have some type of interaction with customer support, but I'm very happy to say that every interaction I've had has been pleasant. And Cisco is the only vendor that I have ever dealt with that proactively calls me."

Cole Two Bears
Systems Architect, NHS Management

Making it a Daily Routine

Using SecureX has become part of my daily operations. I think about it broadly as just using the Cisco Secure platform. So, generally, I'll go to the console and I'll log in there and navigate from the bottom SecureX Ribbon* to the other components of the Cisco secure platform, and from there Secure Network Analytics is just easy for me to log in from there. That's how I view the entire system and all my integrations and see the Talos updates over on the right-hand side providing Intel about what's occurring in the cyber security world. So I just see it as a daily platform for use more and more, rather than a set of individual components."

How's your relationship and your experience been with Cisco Security?

"Yes, so of course any Cisco customer is going to have some type of interaction, but I'm very happy to say that every interaction I've had has been pleasant. And Cisco is the only vendor that I have ever dealt with that proactively calls me."

"As an example, and referring to the CX team specifically, that calls and says, "hey, we know you have this product. We wanted to see how it's working for you. Is there anything we can do to make your experience using this product any better?""

For more information on the Cisco portfolio and platform approach to security, go to: cisco.com/go/secure.

*Note: SecureX Ribbon capabilities are noted in demos here.