Customer Case Study

One of U.K. Largest Public Healthcare Organizations Opts in for Cisco's Integrated Security Approach

Challenges

- Used traditional endpoint solutions that were ineffective against sophisticated threats
- Lacked ability to proactively hunt for threats
- Concerned about patient data privacy and loss of customer trust
- Existing solutions negatively impacted the end-user experience

Solutions

- Cisco Advanced Malware Protection (AMP) for Endpoints
- Cisco Email Security
- Cisco Next-Generation Firewall
- Cisco Threat Response

Results

- Adopted an integrated security approach enabling more robust protection against advanced threats
- Greatly strengthened overall defenses and reduced the "human factor" risk
- Gained granular visibility, reporting capabilities and new functionalities that enabled an improved cybersecurity posture
- Seamlessly integrated security solution into the environment while improving end-user efficiency

Customer Summary

Customer name:
National Health Service (NHS) Greater Glasgow and Clyde

Industry:
Healthcare

Number of employees:
40,000

Location:
Greater Glasgow, Scotland, U.K.

Website:
www.nhsggc.org.uk

Scotland's largest public healthcare organization serves more than 1 million patients

The National Health Service (NHS) is United Kingdom's publicly funded healthcare system, providing comprehensive services to its constituents, largely free of charge. Serving 1.2 million patients, NHS Greater Glasgow and Clyde is the largest of 14 regional NHS Boards in Scotland, and one of the largest in the U.K.

With a staff of about 40,000, NHS Greater Glasgow and Clyde (NHSGGC) provides a broad range of acute and routine health services for six of Scotland's 32 council areas, including Glasgow (the country's most-populous city). NHSGGC's infrastructure includes:

- 35 hospitals
- 50 general practices
- 300 pharmacies
- 270 dental services locations
- 180 optician practices

Security is mission-critical for IT operations and patient care

Like many healthcare organizations, NHSGGC must prioritize patient care in its budget. This leaves limited resources for IT operations. Yet with such an extensive IT environment, maintaining strong security was a struggle.

With a volume of 2 million external monthly emails alone, NHSGGC was bombarded with an average of 170,000 emails containing malicious links or attachments every month. Not surprisingly, the organization had at least two or three computers infected with ransomware every week. And financial loss wasn't the only concern.

"There's potential to lose massive amounts of patient data and fundamentally, that would impact patient care," explains Calum Morrison, head of E-Health Operations at NHSGGC. "The human impact could be significant."

Keeping sensitive data secure was also a matter of maintaining the patients' trust, which is very important for NHSGGC.

"When treating patients, they want to know that their data is not going to be distributed into the wrong hands," says Technical Services Manager Alex Rough.

After the global outbreak of WannaCry, NHSGGC became increasingly concerned about its ability to detect and prevent threats. Following a rigid diagnostic testing cycle, it became clear to the IT team that the existing endpoint security solution was not effective – it did not keep up with the evolving and increasingly sophisticated threat landscape.

"We have incredibly clinically critical IT functions that we have to maintain on a 24/7/365 basis," Morrison says. "The tools we had in place to mitigate the threats just weren't working."

Finding the right partner to improve cybersecurity posture

In looking for a new partner, NHSGGC had several key criteria:

- A more robust platform that could proactively hunt for threats and investigate attacks, including better reporting functionality
- An integrated solution that could replace both its endpoint security and email security products, which had separate vendors and required too much time and resources to manage
- A more lightweight endpoint product that improved the end-user experience

"We struggled in the past with security solutions to make sure they integrated into our environment in a way that complemented our experience for users," Rough says.

NHSGGC needed a product that would integrate seamlessly into the environment "in a way that actually allowed people to do their job more efficiently but at the same time made it more secure," he adds.

A 'huge gain' in ability to keep systems secure

Cisco delivered an integrated security architecture that featured Cisco AMP for Endpoints, AMP for Networks, Threat Grid, Cisco Email Security, and Cisco Threat Response.

Cisco Threat Response automates integrations across the portfolio with Cisco AMP for Endpoints, AMP for Networks, Threat Grid, and Cisco Email Security. The team at NHSGGC wanted a comprehensive view of their environment that would be powered by technology integrations. If the email security appliance detects a malicious attachment, the SOC analyst at NHSGGC should be confident that the endpoint was actually compromised before committing limited resources to investigate or remediate. Cisco's integrated backend for NHSGGC's incident response tool enables these types of scenarios in a scalable manner.

With these multiple attack prevention engines at work, on top of traditional signature-based antivirus capabilities, Cisco AMP for Endpoints provides NHSGGC the necessary endpoint front-line defenses against malware.

Additionally, the Cisco solution:

- Includes Malicious Activity Protection, which provides run-time detection and blocks abnormal behavior of running programs on the endpoint.
- Integrates threat intelligence from Talos, which analyzes approximately 18 trillion emails and blocks 600 billion file threats.
- Continually monitors files and retrospectively protects the environment at the first sign of malicious behavior – thus providing advanced threat detection and response.

"Cisco has a holistic, well-developed and robust security approach," Morrison says. "Reporting functionality is astonishing – it's given us abilities that we've never had before. It has had an immense benefit."

The integrated Cisco architecture has "reduced the human factor that introduced the majority of the risk to the organization," according to Morrison. This has enabled the IT team to focus on other priorities instead of worrying about cybersecurity.

The solution not only "has almost entirely removed some of the previous pain points," but has enabled the IT team to address new questions, Morrison adds.

"Since we've deployed ESA, AMP for Endpoints and Firepower – with the threat intelligence background from Talos – we haven't had a single adverse event," he says.

Rough has been so impressed, he has been recommending Cisco to other NHS Boards – and to any colleagues looking for improved security.

"With the movement toward AMP for Endpoints and other Cisco security products, it gives us more of that protection suite and gives us much more confidence. … For us, using Cisco products is the closest thing to taking the worry out of cybersecurity, and we can go on with other stuff," he says. "And that for us is a huge, huge gain."