VECTRA
Security that thinks®

Bolton NHS Foundation Trust

Bolton NHS keeps the focus on quality patient care with AI-powered cyberattack detection and threat hunting

"We are duty bound to protect our patient information," says Brett Walmsley, CTO of Bolton NHS Foundation Trust.

More than 140,000 people in Bolton and the surrounding area northwest of Manchester depend on Bolton NHS for community health centers and clinics. It also provides district nursing and intermediate care as well as services at the Royal Bolton Hospital, which is a hub for women's and children's services in the greater Manchester area.

Transforming patient care

Digital transformation is helping Bolton NHS deliver high-quality care while controlling costs.

"Digital technologies make doctors' and nurses' jobs easier," says Walmsley. "They can spend more time with the patients."

But for the convenience and efficiency of digital healthcare, protecting patient information across a growing number of mobile devices, medical internet-of-things (IoT) devices, data center workloads and cloud services is a growing challenge.

Healthcare providers have a treasure trove of patient, financial and clinical research data, making healthcare a top target for data theft. Criminals also target healthcare providers for extortion with ransomware, knowing that hospital systems must operate around the clock.

And Bolton NHS is just down the road from ground zero of the 2017 WannaCry outbreak in the U.K.

If someone is in your network, how would you know?

Thankfully, Bolton NHS was spared from WannaCry.

Organization

Bolton NHS Foundation Trust

Industry

Healthcare

Challenge

Continuously monitor and detect hidden cyberattackers that could impact clinical care, operations and patient safety

Selection criteria

Automate threat detection to reveal hidden attackers across data center and cloud workloads and user and medical IoT devices

Results

- Detect hidden attacks in a complex IT infrastructure of data center and cloud workloads and user and medical IoT devices
- Gain unprecedented visibility into hidden attacks
- Reduce workload of IT team with AI-powered threat hunting and investigations

"We were not affected in any way," says Walmsley. "Our executives were appreciative that we didn't lose any service."

But the ransomware crisis, which affected organizations around the world, sparked many conversations at Bolton NHS. "We had proven security, but we still reassessed our weaknesses and gaps," says Walmsley.

"After WannaCry, security was on top of people's minds," he says. "If someone is in your network, how would you know?"

Now, Walmsley does.

Bolton NHS uses the Cognito® platform from Vectra® as the cornerstone of security monitoring.

An AI-powered cyberattack-detection and threat-hunting platform, Cognito enables the security operations team to detect and stop hidden attackers in real time – from its data center and cloud workloads to its user and medical IoT devices.

Detect attacks in a complex ecosystem

Bolton NHS relies on a complex, highly integrated IT ecosystem to deliver quality care.

Doctors and other caregivers have seamless access to patients' electronic health records, medical images and medications. The staff needs access to an array of productivity and administrative applications. The use of cloud is rising, and the healthcare system is migrating to Microsoft Office 365.

Connected medical devices is an area of innovation, from Wi-Fi-enabled infusion pumps to smart MRI machines. Medical IoT devices offer new ways to monitor patients and equipment while improving care and lowering costs. But many of these smart devices have unknown security provenance.

The patient experience is important, too. Patients and their families use the guest Wi-Fi to stay connected and entertained while waiting for appointments or during a hospital stay.

Bolton NHS has strong security protections – from using virtual desktops to firewalls, intrusion detection, network access controls, endpoint protection and data loss prevention software. Each layer is critical.

But Cognito gives the IT team visibility into attacks that they simply could not see before.

"Cognito filled a gap," says Walmsley. "We needed to know what we didn't know, and Cognito showed us what was hidden."

Find threats faster

Cognito exposes hidden attackers by collecting, analyzing and storing network metadata, relevant logs and cloud events. Always-learning behavioral models enable Cognito to detect attackers in real time so the security operations team can respond quickly and decisively – and have a logical starting point for investigations.

"When I see something in Cognito, I sit down and triage it immediately," says Walmsley.

Cognito's ease of use delivered immediate value. Cognito automatically triages, scores and correlates threats to compromised hosts, and maps attack behaviors across hosts so the security operations team can see the narrative of developing attacks. Threats are prioritized on an intuitive user interface.

Cognito has proven itself as the go-to tool of the security operations team at Bolton NHS.

"With Cognito, if something looks odd, you know after a couple of clicks," says Walmsley. "You see what it looks like when it's a smash-and-grab or an exfiltration. You know Cognito is working."

Reduce the security workload

Automating threat detection eliminates the time-consuming work of manual threat hunting and investigations, and that makes the security operations team far more efficient and effective.

"There's a massive skills gap," says Walmsley. "We can't get enough good people. Cognito helps us augment our security staff."

A strong consulting partner

Core to Cloud, a UK solution provider specializing in security and infrastructure, introduced Cognito to the team at Bolton NHS as it was seeking to strengthen cybersecurity posture. The relationship has stayed strong.

"Core to Cloud is consultative and can translate our needs into a solution," says Walmsley. "Core to Cloud gives us the support and knowledge that we need when we need it."

Eliminate ambiguity

"We have a strong security infrastructure, but there's always ambiguity," says Walmsley. "With Cognito, we don't have to worry about not knowing an attacker is in our network."

VECTRA®
Email: info@vectra.ai
Tel: 1 408-326-2020
vectra.ai