SOCURA

Connected Everything

Protecting health and care from the security challenges of connected devices

Find out how a managed detection and response approach can tackle the cyber security risks of connected technology and the Internet of Things (IoT).

“By the end of 2021, the world will be filled with as many as 25 billion[1] connected ‘things’. In the health and care sector a new era of smart devices is beginning to offer everything from automated insulin delivery to connected inhalers.”

The IoT means connectivity is everywhere. But where there is connectivity, there is also risk.”

JAMIE BRUMMELL – CTO & FOUNDER

[1]Gartner Identifies Top 10 Strategic IoT Technologies and Trends, November 2018

OPERATIONAL TECHNOLOGY:

The Legacy Challenge

It's not only emerging smart medical devices that form the IoT. Legacy operational technology (OT) can also be connected, from MRI machines to electrocardiographs and ultrasound devices. However, the automation of day-to-day medical processes can put such devices within the reach of remote attackers.

82%

of health and care organisations have experienced a cyber-attack against one of their IoT devices[2].

Patching Challenges

Vendors can be slow to fix known issues – leaving large windows of opportunities for attacks. Hospitals can also find it difficult to apply the patches, as it would require taking critical systems offline to test.

Legacy Systems

The operating system used on an OT or IoT device can also play a factor. If the device is relatively old, it may only be compatible with a legacy Windows OS for which there are no longer any patches.

Passwords

Some devices are not designed with security in mind. They may have been shipped with a factory default password, or simply one that is easy-to-guess. Both can easily be targeted by remote attackers.

Protocols

With legacy OT devices often manufactured in an age when cyber crime was not the concern that it is today, they can have little in the way of built-in protection, often using insecure communications protocols.

[2]HIPAA Journal, September 2019

The Emerging Threat

These factors can present big challenges to health and care leaders and their IT teams. Though no co-ordinated attack on connected devices has occurred in the sector, there's a growing opportunity emerging.

Hijacked devices give cyber criminals the means to access patient data stores, conscript the device into a botnet to attack others, or sabotage it to extort a ransom payment.

There’s no silver bullet

The best practice security steps outlined in Cyber Essentials Plus and the Data Security Protection Toolkit (DSPT) will go a long way in mitigating the worst issues, including software vulnerabilities and weak passwords.

Devices can often be too underpowered to install endpoint security. This highlights the importance of layering up protection in the cloud and on networks – through device profiling and segmentation, for example.

The National Cyber Security Centre (NCSC) has been involved in the development of a new international standard for connected devices. ETSI EN 303 645 covers 13 areas, proposing a ban on default passwords and greater transparency on the timeframes for when a product receives security updates.

There’s also the NHS Secure Boundary service, an important initiative to help protect the internet traffic flowing to and from connected devices from digital and cloud-based threats.

But even the best threat prevention technology is not enough to stop determined threat actors.

The MDR Difference

Managed detection and response (MDR) can be a perfect addition for NHS IT organisations, providing:

- 24/7 security operations centre (SOC) offering threat detection and response across remote, endpoint, network, cloud, and OT environments.
- A completely managed service, helping save on the up-front costs of building and staffing the SOC.
- Allows you to take advantage of the economies of scale a specialist provider offers, with the enhanced visibility of multiple customer environments.

Socura's Approach

Our MDR service acts as a trusted extension of your in-house capability and is operated by a team of highly experienced security experts. Our analysts work in partnership with you to detect and defend against cyber threats.

Contact the team at
hello@socura.co.uk

Orchestration & Automation

Our MDR service benefits from simplified security operations by unifying case management, real-time collaboration, threat intelligence management, and automation of containment actions.

Security Analytics

We can ingest all of the security data that your systems generate, resulting in complete visibility across all relevant data sources. Security telemetry data remains hot and instantly searchable for a year, for maximum visibility.

True Partnership

Our service acts as a trusted extension of your in-house capability and is operated by a team of highly experienced security experts. Our analysts work in partnership with you to detect and defend against cyber threats.