Protecting Medical Devices with Cisco Medical NAC

Mitigating risk in an increasingly connected world

The past few years have witnessed an explosion in both the quantity and diversity of devices connected to the network in all areas of life and industry. The health and care industry is no exception.

Connecting medical devices presents a number of benefits including remote monitoring and the acquisition of telemetry-style information.

However, connecting anything also introduces risk as these devices become accessible and potentially open to compromise. In many cases, devices are purchased by clinical functions and are connected without any direct involvement from the NHS IT teams. This can lead to a lack of visibility and control, as demonstrated by Orangeworm[1], a threat directly related to connected medical devices, which was widely reported in April 2018.

Connected Devices in the Clinical Setting

The clinical setting is no stranger to having non-IT devices connected to the network. However, in the past these were generally large, static devices such as MRI and CT scanners, with connection points that were well known and unchanging. This allowed for security policies to be applied once only, with little concern that this would need to change on a regular basis.

More recently, we have seen an increase in in mobile connected devices such as infusion pumps and blood pressure monitors, but without proper controls, these can increase the risk of disruption in the clinical domain. This is because they expand the overall attack surface where they are not included in IT-managed patching and maintenance processes.

In addition, these devices can be essential to the delivery of patient care and as such, any impact to their availability, or the integrity of the data they produce, could introduce significant clinical risk.

Network Device Profiling

To begin addressing the risks posed by network-connected clinical devices, the first task is to be able to identify each one as it connects to the network. Identification of clinical devices can be undertaken through a variety of means but by far the most effective is through the use of profiling.

Profiling is an automated process of device discovery and classification. It uses various sources of information that combined, form a fingerprint for a particular device type. The sources of information that come together to profile the device can be obtained either passively or actively:

- Passive – by observing specific protocol behaviour such as DHCP, manufacturer information may be revealed through the device MAC address or dhcp-class-identifier fields.
- Active – through scanning or probing of the clinical device. For example, TCP and UDP port scanning and operating system fingerprinting could reveal details about the device type that has been connected.

In some cases, device information might be revealed through only a single technique, but combining multiple techniques improves profiling accuracy.

Access Control

Once a device has been successfully profiled, a suitable security policy that controls how the device can communicate may be enforced. In traditional networks, it is not uncommon for a device that has been connected to have full access to the network and perhaps more importantly, the rest of the network has full access to the device.

One of the most common methods of enforcing a security policy is through the use of network segmentation.

Traditionally, network segmentation is performed logically using virtual LAN (VLAN) technology. VLANs are used primarily to aid structured network design, for example through static assignment of all of the devices on a specific floor in a building to a common VLAN.

To meet the demands of a modern clinical setting, network segmentation must become far more responsive, adapting to security needs of the devices as they connect both wired and wirelessly. This dynamic segmentation can be used to ensure that only the traffic flows necessary are permitted, commonly referred to as the principle of least privilege.

Dynamic VLAN allocation is one method of achieving this. However, a far better approach is to rely on more abstract, software defined segmentation techniques. These techniques remove the complexity of the underlying network topology (IP address, VLAN etc.) and simply enforce policy based on abstract device groupings. Such groupings could be based on device function i.e. infusion pumps, ultrasound machines etc, or more general clinical function groupings such as radiology, maternity or pathology. Once defined, policy can then be enforced between these device groupings without having to be concerned with the VLANs or IP address configuration.

What is critical is that any segmentation policy must not impact the successful operation of the connected clinical device since, by their very nature, these devices are essential to the delivery of patient care.

Careful and gradual policy definition and enforcement is essential and can be aided through the use of 'monitor-mode' deployments – a technique that allows a policy to be applied but not enforced. In this mode, administrators can observe the impact that their chosen policy will have on the network traffic flows and be assured that full deployment will not impact correct operation.

Introducing 'Cisco Medical NAC'

Cisco Medical NAC[2] is an industry leading solution for profiling of medical devices as they are connected and automated, policy-based access control. The solution provides four key benefits to health and care organisations:

Identifies Medical Devices

Delivers instant fingerprinting of more than 250 leading medical devices as well as thousands of nonclinical devices.

Protects Medical Devices

Uses traditional or software-defined network segmentation to protect medical devices and records from non-clinical devices and the lateral spread of malware.

Automates Onboarding

Provides easy onboarding services for guests, patients and staff so that they can gain access to authorised resources over the converged wired and wireless network.

Monitors and Removes Threats

Keeps a constant watch to detect suspicious threats and behaviours across the network.

Security Assured

The solution is based upon the Cisco Identity Services Engine[3] and our library[4] of profiles or fingerprints, preconfigured and updated regularly. It is also possible to modify profiles and create custom profiles.

Network-wide segmentation is delivered through Cisco TrustSec[5] and behavioural analysis using Cisco Stealthwatch[6]. Finally, our rapid threat containment solution[7] enables organisations to contain and control incidents when they occur.

Hence, while Cisco Medical NAC is a unique solution aimed at protection of medical devices, it is important to consider it as part of an overall systematic approach to organisational IT security throughout your healthcare organisation.

Talk to the experts

For more information on medical device security, Cisco Medical NAC, or any of our health and care security solutions, contact us:

Mike Badham
Senior Solutions Architect – UK Health and Care and Local Government 020 8824 4138

Mark Jackson
Principal Information Assurance Architect – UK Public Sector 020 8824 8535

https://cisco.co.uk/healthcare

[1] 'Orangeworm' Targets Healthcare – https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia
[2] Cisco Medical NAC – https://www.cisco.com/c/en/us/solutions/security/medical-nac/index.html
[3] Cisco Identity Services Engine – https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html
[4] Cisco Medical NAC Device Library – https://www.cisco.com/c/dam/en/us/products/collateral/security/medical-nac-white-paper.pdf
[5] Cisco TrustSec – https://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html
[6] Cisco Stealthwatch – https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html
[7] Rapid Threat Containment – https://www.cisco.com/c/en/us/solutions/enterprise-networks/rapid-threat-containment/index.html