<)FORESCOUT

6 Essential Steps Healthcare Providers Should Take Across the Digital Terrain

Now more than ever, hospitals have an ever-changing threat landscape. The diverse types, and sheer numbers of devices, events, and users being added to the network are too many to manage and too risky to not secure. It's also virtually impossible to patch every single vulnerability.

Across today's digital terrain of IT, OT, BYOD, IoT, and IoMT, medical assets are critical. So how can you prioritize them and ensure their protection?

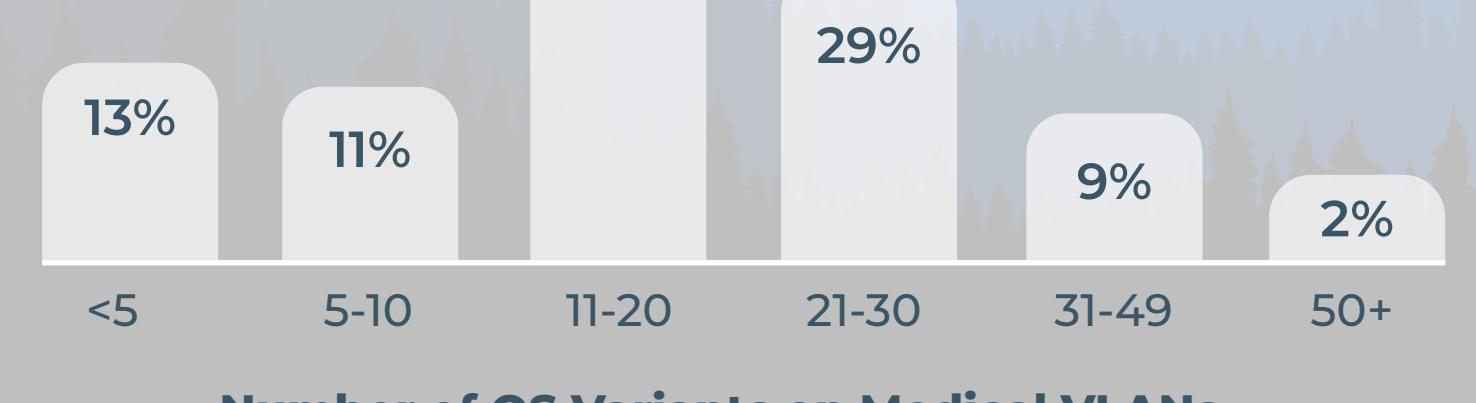
We can mitigate clinical risks by implementing network-based controls and using **automated cybersecurity** to segment those devices. Forescout Continuum (now empowered with CyberMDX software) will help you with the full workflow. Here's how.

Most Common Connected Medical Devices

Step 1

Continuously Discover.

As new devices are added to the network, **they should all be discovered in real-time to protect from variants.**
-- And this needs to be done across all platforms and operating systems (IoT, Medical Devices, OT, IT, etc.).



Number of OS Variants on Medical VLANs

Step 2

Profile Assets.

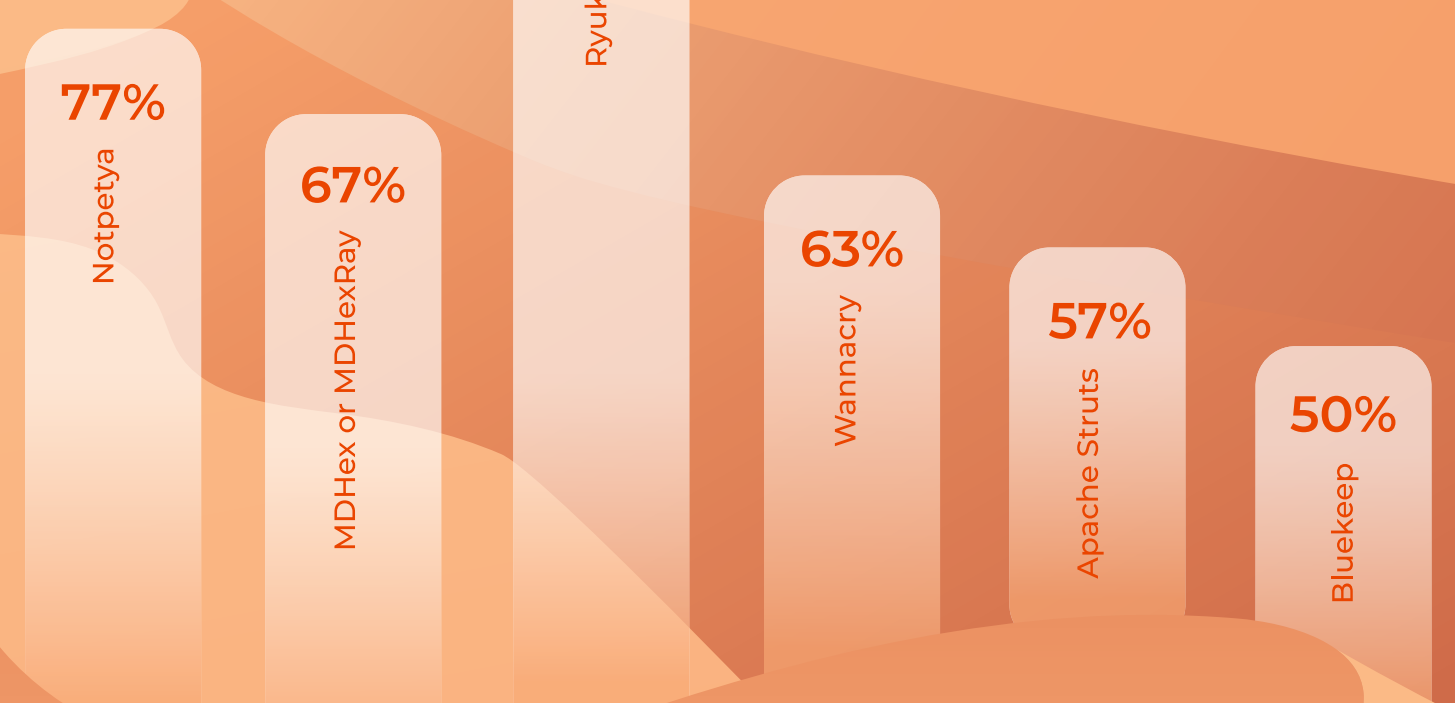
A detailed asset profile must automatically be established. It should include details such as, IP/MAC address, Physical Location, Recalls, Vulnerabilities, MDS2 files, VLAN/Subnet, Serial Numbers, and more.

Only 10% of clinical engineers know the exact number of devices in their network.

Step 3

Risk Assess & Prioritize.

You'll want an **intelligent risk score that incorporates multiple factors about the device** – Beyond just the CVSS number, algorithms need to consider the asset function. Does it carry PHI? Is it critical for patient safety? Is it a revenue generator?



Medical Devices Not Protected for Common Vulnerabilities in US Hospitals

Step 4

Recommend Actions.

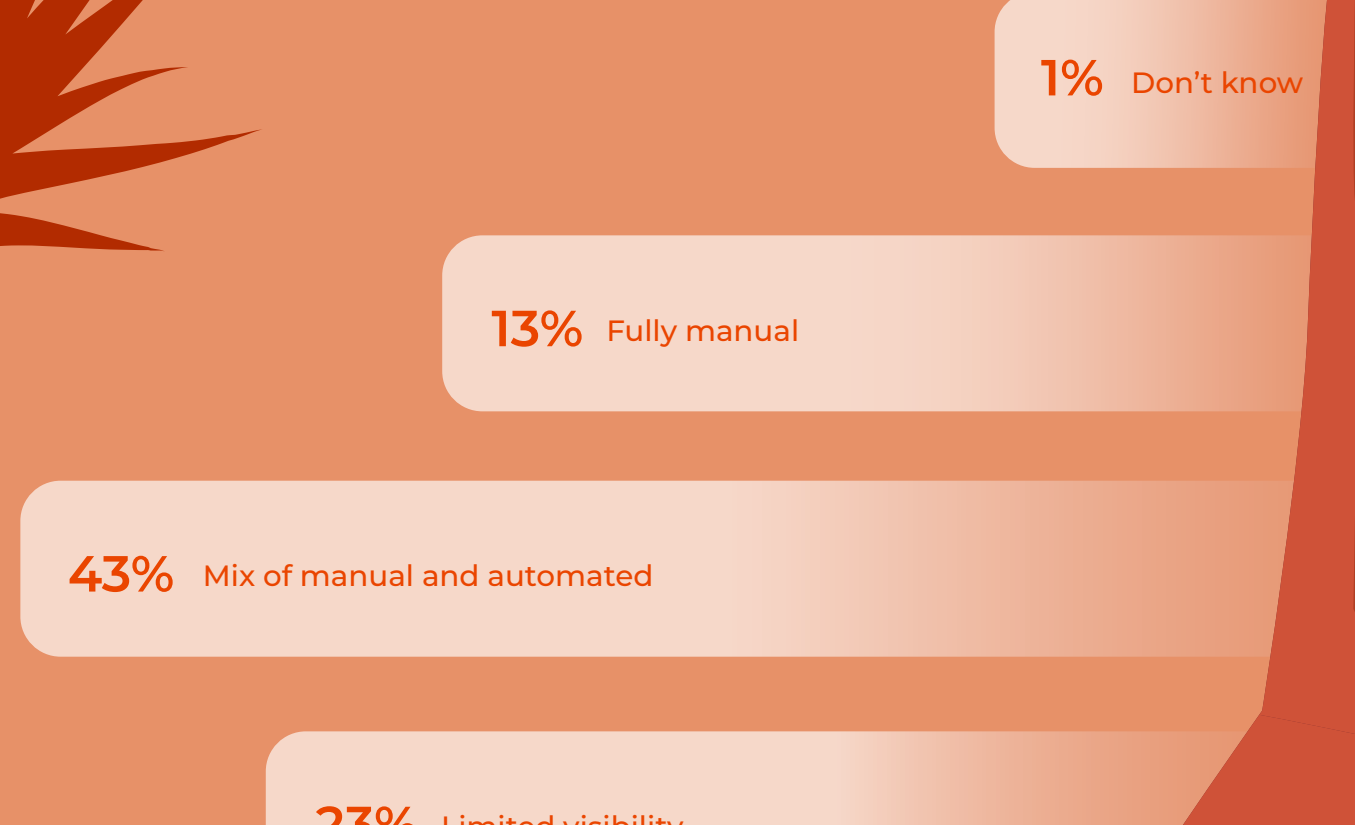
You should **generate Access Control Lists (ACL) to help mitigate risk without impacting the device performance**. These recommended actions are automatically fed into Forescout Continuum (or can be fed into a ticketing system to kick off a workflow).

Step 5

Implement Controls.

After ingesting the ACLs, you need to have an automated way to execute them. Forescout Continuum ensures that **ports/protocols, which can be used maliciously, are shut off without impacting the device's function.**

Are you automating cybersecurity or not?



Status of Device Inventory Mechanics in US Hospitals

Step 6

Segment the Network.

Continuous visibility into how the devices are grouped, ensuring that Medical Devices remain on their own separate VLANs. Proper segmentation is made easy. Risk is reduced without slowing down or impacting patient care.

34% of an HDO's medical VLANs support more than 100 distinct device vendors.

Source: IPSOS study by CyberMDX and Philips "Perspectives in Healthcare Security", August 2021

It's critical for a healthcare organization's clinical, security, and risk management leaders to work together to secure all devices across the extended HDO. Solely focusing on securing medical devices rather than securing all device classes can cause significant gaps in your security posture. A holistic approach to security requires continuous visibility and control over the entire connected-device ecosystem—including understanding the role a device visibility and control platform can play in orchestrating actions among heterogeneous security and IT management tools.

For more information or to understand how Forescout Continuum would secure your healthcare organization, visit Forescout.com.

<)
FORESCOUT

Forescout Technologies, Inc.

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591