UNVEILING THE PERSISTENT RISKS OF CONNECTED MEDICAL DEVICES

Forescout analyzed over 2 million medical devices to uncover the most vulnerable assets in hospital networks today

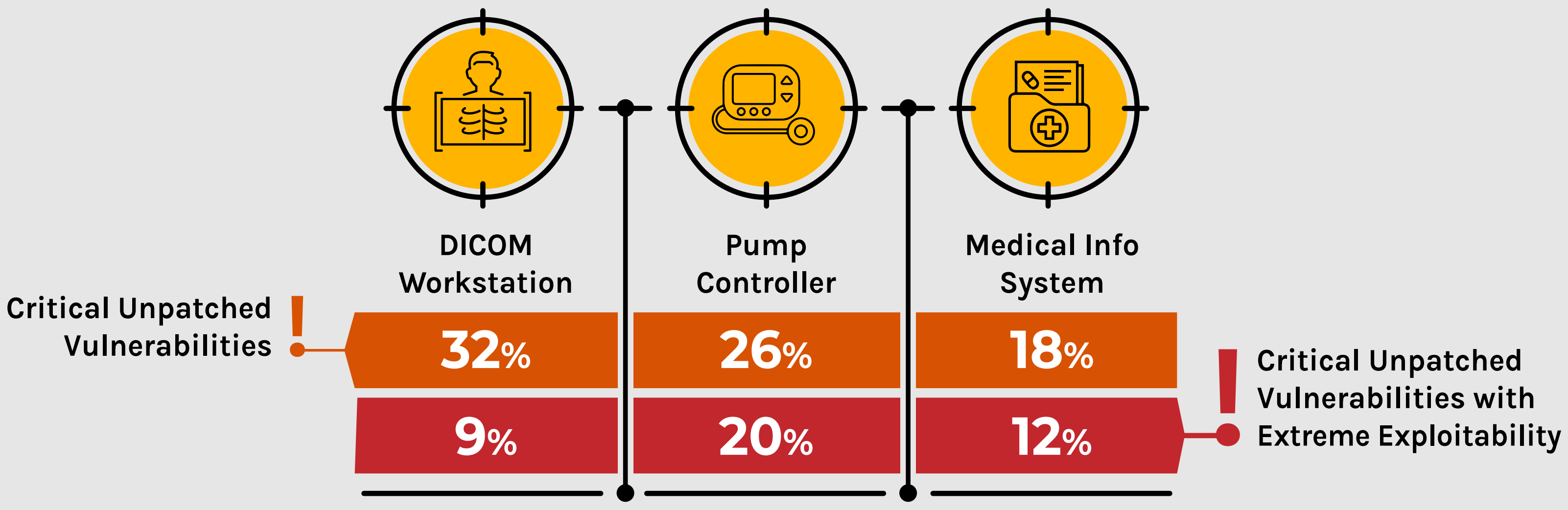
TRENDS IMPACTING HEALTHCARE'S SECURITY POSTURE

Healthcare delivery organizations (HDOs), such as hospitals and clinics, host a broad range of Information Technology (IT), Internet of Medical Things (IoMT), Operational Technology (OT) and Internet of Things (IoT) devices.

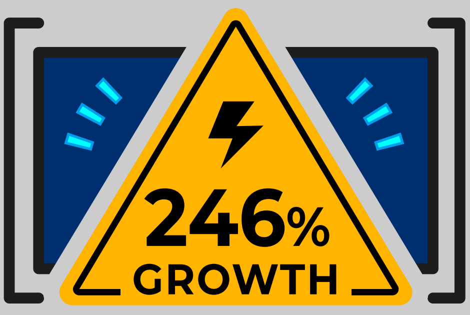
The growing number and diversity of devices in HDOs has introduced new cybersecurity risks. The ability to compromise devices and demand large ransom payments, as well as the possibility of monetizing patient data, has led to an increase in the number and sophistication of cyberattacks targeting HDOs in recent years.

- Surge of Connected Medical Assets
- Fragmented Solutions, Unprotected Vulnerabilities
- Distributed Facilities & Anywhere Operations
- Shortage of Cybersecurity Personnel

TOP 3 RISKIEST CONNECTED MEDICAL DEVICES



	DICOM Workstation	Pump Controller	Medical Info System
Critical Unpatched Vulnerabilities	32%	26%	18%
Critical Unpatched Vulnerabilities with Extreme Exploitability	9%	20%	12%



246% GROWTH

In Internet Exposed DICOM Workstations
(2017 - 2024)

OPEN PORTS & INTERNET EXPOSURE

DICOM workstations and PACS often run legacy vulnerable IT operating systems, have extensive network connectivity to allow for sharing imaging files, and use the DICOM standard for sharing these files.

UNIQUE OPERATING SYSTEMS ARE DIFFICULT TO MANAGE

The variety of special purpose operating systems is a nightmare for security teams to keep track of and is one of the main reasons for more visibility into networked devices. We observe more than 110 unique versions present in HDOs. Embedded firmware is also well known for presenting systematic security issues, such as backdoors, hardcoded credentials and keys and memory corruption vulnerabilities.

110	Unique OS in HDO Networks
300+	Different Device Vendors
10%	Are Running Active Anti-malware

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. 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 can secure your healthcare organization, visit Forescout.com.

FORESCOUT
See it. Secure it. Assure it.

Source: Forescout Device Cloud, a repository of host and network information for more than 8 million devices