FORESCOUT

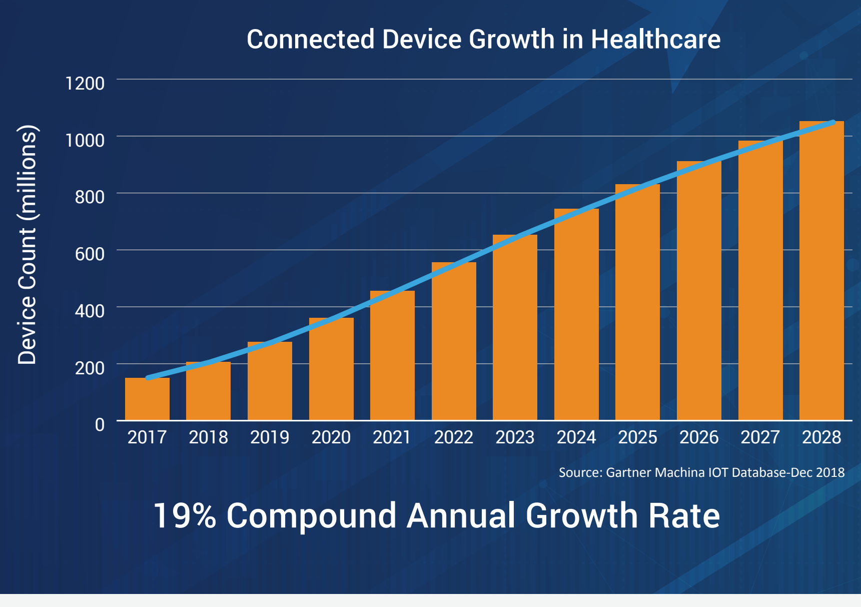
Putting Healthcare Security Under the Microscope

Analyzing deployment data to better understand the cybersecurity risks facing healthcare organizations today

Forescout researchers studied the devices and behavior of healthcare networks to evaluate risk profiles and identify critical security issues. They leveraged the Forescout Device Cloud, which contains the anonymized fingerprints for more than 8 million devices connected to the networks of more than 1,000 Forescout customers. Fingerprints include device function, vendor, model, operating system and version. The study found some surprising risk areas.

DOWNLOAD REPORT

Device Growth Makes Security Challenging



Source: Gartner Machina IOT Database-Dec 2018

19% Compound Annual Growth Rate

The proliferation of connected medical devices makes security an increasing challenge

Internet of Medical Things is Very Diverse

What classes of devices did we find on healthcare networks?

IoT Devices: Printers, tablets, smartphones, controllers, smart TVs, entertainment consoles

OT Devices: Medical devices, critical care systems, building automation, security controls

47% of connected systems were IoT or OT devices

40% of healthcare deployments had more than 20 operating systems on their VLANs

Diversity of device operating systems makes managing security challenging.

Legacy Windows Versions a Major Vulnerability

Many networks still use unsupported Microsoft Windows OSes and another major support milestone is rapidly approaching.

How many unsupported devices did we find? → **71%** of devices ran a Windows OS that will be unsupported as of January 14, 2020

What Windows versions did we identify? → Windows 7, Windows 2008, and Windows Mobile will be unsupported as of January 14, 2020

Too Many Vulnerable and Unnecessary Services

Malware attacks often target vulnerable services and protocols that have been left on but are unnecessary for daily operations on every device.

What commonly exploited services did we find still enabled on healthcare networks?

These include:

- Server Message Block Protocol (SMB)
- Remote Desktop Protocol (RDP)
- File Transfer Protocol (FTP)
- Secure Shell (SSH)
- Telnet
- Digital Imaging and Communications in Medicine (DICOM)

BlueKeep and DejaBlue exploit RDP vulnerability → **32%** of Windows devices still had RDP enabled

WannaCry and NotPetya target SMB → **85%** of Windows devices still had SMB turned on

How Do We Solve This?

49% of healthcare deployments had immature segmentation of 10 VLANs or less

Discover + Classify + Monitor + Segment

Discover: Agentless discovery of every physical and virtual IP-connected device throughout the extended network

Classify: Auto-classification of IT, IoT and OT devices in real time to determine purpose, owner and security posture

Monitor: Continuously monitor and assess devices to detect changes in compliance, posture and behavior

Segment: Group devices by type, usage and sensitivity to limit network access and restrict noncompliant or compromised devices

To learn more about healthcare networks, security concerns, agentless visibility and device control, download the full report:

DOWNLOAD REPORT

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

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

Learn more at Forescout.com