FORESCOUT

EBOOK

Putting Healthcare Security Under the Microscope

Executive Summary

Key findings

- **Today's healthcare environments are increasingly diverse:** Rapid growth and diversity of connected medical devices and operating systems make it increasingly difficult to secure networks.
- **Legacy Microsoft Windows operating systems are a major vulnerability:** Many networks still use unsupported Microsoft Windows operating systems. A major Windows milestone is soon approaching that will leave many more devices unsupported.
- **Segmentation strategies are lacking:** Network segmentation, a best practice for limiting malicious lateral movement by focusing on data sensitivity, location and criticality, is inconsistently applied on today's diverse networks.
- **Common services left on leave the network vulnerable:** Common protocols left open provide uncontrolled access to attackers.

For this study, researchers limited Device Cloud analysis to 75 healthcare deployments with over 10,000 virtual local area networks (VLANs) and 1.5 million devices. Since the primary focus of the report is the status of medical devices, many of the results are based on analysis of more than 1,500 medical VLANs with 430,000 devices.

Healthcare challenge

$429

Per capita cost of data breach; highest among all industries

(Ponemon Institute)

74%

Experienced significant security incidents in the past 12 months

(HIMSS Survey)

1 in 5

Breaches are caused by a vendors

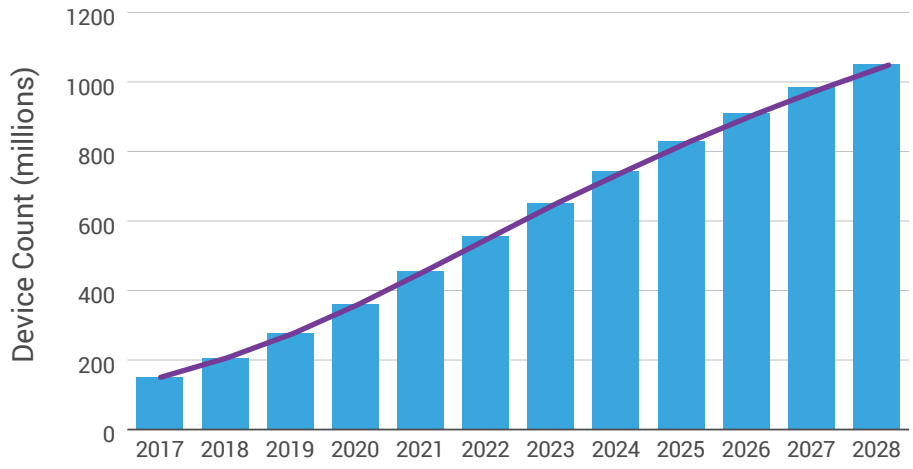
(Health IT Security)

Healthcare Device Growth Makes Security Challenging

Challenge

Connected Device Growth in Healthcare

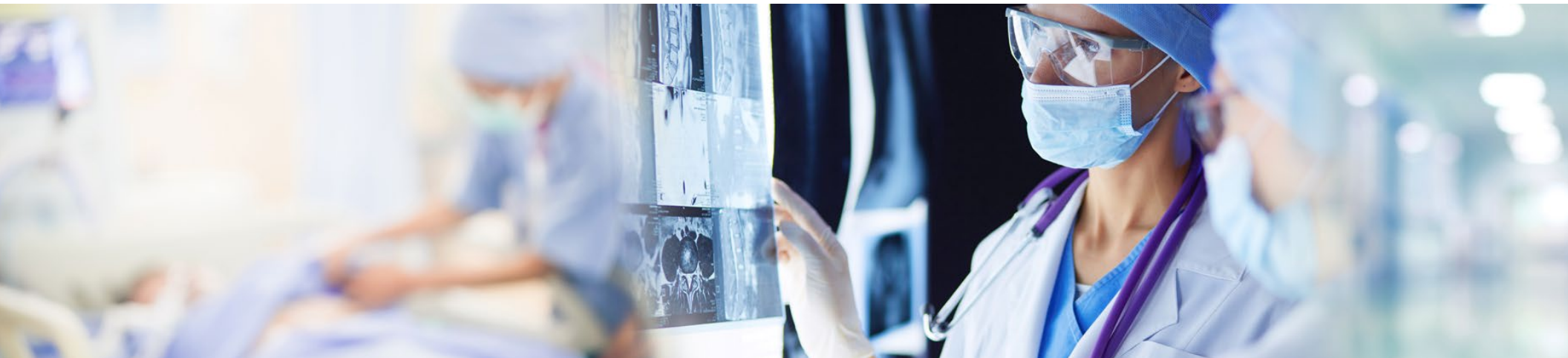
19% Compound Annual Growth Rate



Source: Gartner Machina IoT Database–Dec 2018

The proliferation of connected devices in healthcare makes security an increasing challenge in these environments:

1. The diversity of devices on medical networks adds significant security management complexity.
2. Legacy equipment and operating systems prevent IT from patching and leave networks susceptible to attack.
3. Unnecessary services—often used by vendors—leave healthcare environments exposed.
4. Segmentation, an effective control technique to reduce system attack surfaces, is not sufficiently used.



Diversity of Devices Adds Security Management Complexity

Challenge

Device growth and diversity means more security blind spots and management difficulties.

47% of devices on medical networks are or IoT or OT systems.

40% of deployments had more than 20 different operating systems on their medical VLANs.

Forescout Device Cloud Research, 2019

How Forescout helps

Achieve exceptional, continuous visibility and see devices that other solutions can't:

- Discover information technology (IT), Internet of Things (IoT) and medical devices as they connect to your network without requiring software agents
- Auto-classify devices, users, applications and operating systems without disruption
- Benefit from crowdsourced device insight from a growing community of over 800 enterprise customers across more than 10 industries from Forescout Device Cloud
- Continuously monitor devices to detect any change in device security posture to ensure real-time situational awareness

According to an IDC study, respondents could see 24 percent more devices after deploying the Forescout platform.[1]

1. IDC white paper, *The Business Value of Pervasive Device and Network Visibility with Forescout*, 2017

Legacy Equipment and OSes Leave Networks Susceptible to Attacks

Challenge

Certain devices don't work on more recent versions of Microsoft Windows due to lack of vendor support, compatibility or license issues.

Running unsupported operating systems poses a risk that negatively impacts compliance with many regulations.

Forescout Research Found:

71% of devices that will be running unsupported Windows OSes by January 14, 2020

How Forescout helps

Assess cyber risk with confidence and perform proper security controls:

- Identify devices that need remediation
- Update equipment running soon-to-be unsupported Windows OSes
- Isolate devices that can't be updated to prevent them from becoming an entry point

Forescout can orchestrate updates based on policy with existing security and IT investments.

Limit Vulnerabilities by Controlling Common Protocols

Challenge

Forescout research indicates common protocols left open provide uncontrolled access for attackers.

Forescout Research Found:

BlueKeep and DejaBlue exploits RDP vulnerability → **32%** of Windows devices still had RDP turned on

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

Services Left On in Healthcare Environments:

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

How Forescout helps

Reduce the risk from known vulnerabilities and demonstrate security compliance:

- Inventory devices with services running to assess posture and find all open ports
- Apply appropriate controls based on device context and security policy
- Utilize Security Policy Templates to speed remediation

Forescout can orchestrate updates based on policy with existing security and IT investments.

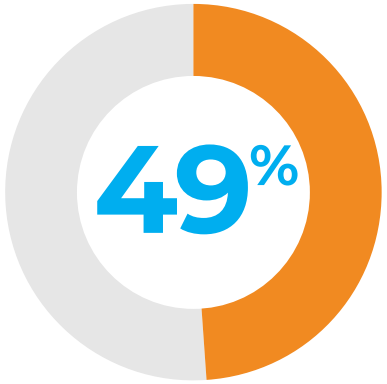
Isolate and Segment Vulnerable Legacy Devices that Are Still Required

Challenge

Forescout research indicates healthcare organizations haven't sufficiently invested in segmentation—a critical control technique to limit security risk, especially with legacy equipment.

Forescout Research Found:

Medical Device VLANS



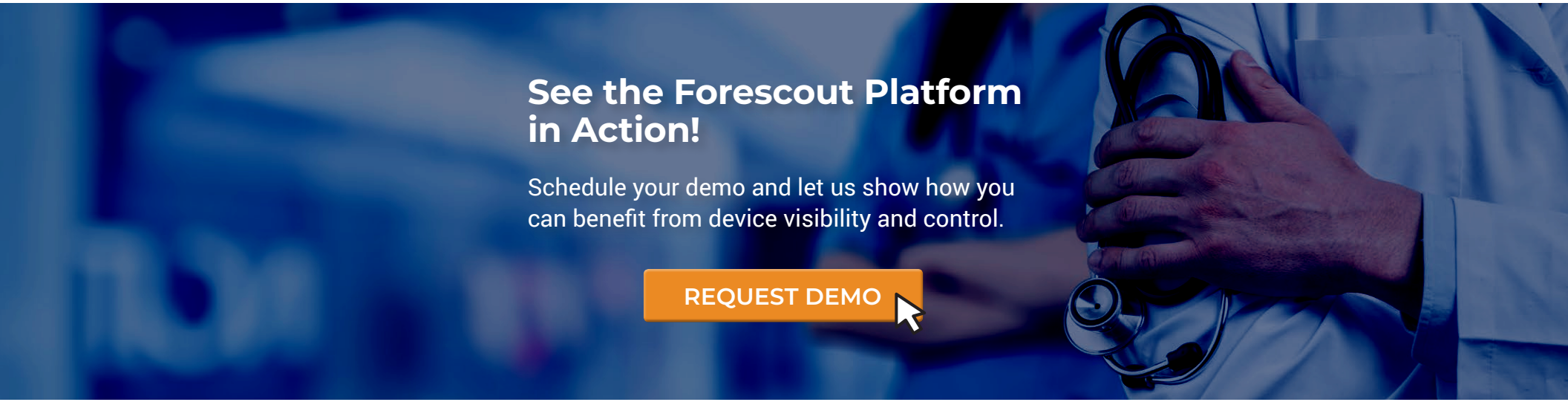
Nearly half had less than 10 VLANS—a key segmentation technique

How Forescout helps

Ease segmentation complexity with actionable device context and policy-based controls:

- Monitor traffic to understand device dependencies
- Apply appropriate controls based on device context and security policy
- Share context with leading virtual infrastructure, cloud and micro-segmentation platforms
- Automate info sharing to next-generation firewalls to enable dynamic segmentation

Forescout can orchestrate updates based on policy with existing security and IT investments.



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