Forescout Releases Inaugural Device Cloud Research based on Leading Device Intelligence

May 15, 2019

- *Expanded Forescout Device Cloud now includes more than 8 million IT, IoT and OT devices*
- *New Forescout Device Cloud Report reveals cybersecurity risks associated with today's healthcare IT environments; OT systems represent a growing attack surface*
- *Healthcare riddled with devices running legacy Windows; 70% of Windows devices will no longer be supported by Microsoft in January 2020*

SAN JOSE, Calif., May 15, 2019 (GLOBE NEWSWIRE) -- Forescout Technologies, Inc. (NASDAQ: FSCT), the leader in device visibility and control, today announced insights from 75 real healthcare deployments with more than 10,000 virtual local area networks (VLANs) and 1.5 million devices contained within the Forescout Device Cloud, with a specific focus on 1,500 medical VLANs with more than 430,000 devices. Launched in July 2017, the Forescout Device Cloud is one of the world's largest crowdsourced device repositories and now contains more than eight million devices from more than 1,000 customers who share anonymized device insights.

"The Forescout Device Cloud provides us with game changing data from millions of devices around the world, and what we are releasing today is just the tip of the iceberg," said Elisa Costante, head of OT and Industrial Technology Innovation at Forescout. "Our findings reveal that healthcare organizations have some of the most diverse and complex IT environments, which are compounded due to compliance risks. Every time a patch is applied, there is concern around voiding a warranty or impacting patient safety. These organizations are dealing with lifesaving devices and extremely sensitive environments."

The convergence of IT, IoT and OT makes it more difficult for the healthcare industry to manage a wide array of hard-to-control network security risks. IoT and OT devices are rapidly increasing in numbers, but traditional IT still represents the most vulnerable attack surface. Forescout uses the Device Cloud data to analyze more than 150 attributes per device to bring increased device intelligence and improved auto-classification to its customers. Forescout will leverage the increasing amount of data and intelligence gathered from the Device Cloud to generate future insights on the characterization and risk posture of connected devices across industries.

The Forescout Device Cloud Report key findings include:

Healthcare OT increases attack surface
Forescout researchers found that the most common devices on medical networks are still traditional computing devices (53 percent) followed by IoT devices (39 percent), including VoIP phones, network printers, tablets and smart TVs. OT systems, including medical devices, critical care systems, building automation systems, facilities, utilities and physical security, comprise eight percent of the devices on medical networks.

Within the OT device category, the three most common connected medical devices found were patient tracking and identification systems (38 percent), infusion pumps (32 percent) and patient monitors (12 percent). Considering the growing number of vulnerabilities in OT environments, we can see an increase in the attack surface in healthcare environments.

Healthcare organizations riddled with devices running legacy Windows operating systems
The Forescout Device Cloud Report highlights that 71 percent of Windows devices within these healthcare deployments are running Windows 7, Windows 2008 or Windows Mobile, with Microsoft support planned to expire on January 14, 2020. Running unsupported operating systems poses a risk that may expose vulnerabilities and has the potential to impact regulatory compliance.

Diversity of operating systems and vendor sprawl creates headaches
The diversity of device vendors and operating systems present on medical networks adds to the complexity and increases security challenges. Forescout's research found that 40 percent of healthcare deployments had more than 20 different operating systems. When looking at the different types of operating systems found on medical VLANs, 59 percent were Windows operating systems and 41 percent were a mix of other variants, including mobile, embedded firmware and network infrastructure and many more.

In addition, more than 30 percent of healthcare deployments had 100 or more device vendors on their network. Patching in healthcare environments, especially acute care facilities, can be challenging and require devices to remain online and available. Some healthcare devices cannot be patched, may require vendor approval or need manual implementation by remote maintenance personnel.

Vulnerable protocols are leaving a door open
Eighty-five percent of devices on medical networks running Windows OS had Server Block Messaging (SMB) protocol turned on, allowing uncontrolled access for attackers to get beyond the perimeter and move laterally. Device manufacturers sometimes leave network ports open by default—often unbeknownst to IT and security staff.

About Forescout
Forescout Technologies, Inc. provides security at first sight. Our company delivers device visibility and control to enable enterprises and government agencies to gain complete situational awareness of their environment and orchestrate action. Learn more at www.forescout.com.

Media Relations Contact:

Katie Beck
Forescout Technologies, Inc.
650-314-8705
katie.beck@forescout.com

Investor Relations Contact:
Michelle Spolver
Forescout Technologies, Inc.
408-721-5884
michelle.spolver@forescout.com
FSCT-O

Source: ForeScout Technologies, Inc.