FORESCOUT

Banking on Security: Leveraging Device Data to Manage Risk in Financial Services

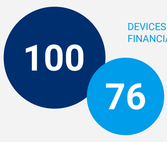
Forescout researchers analyze financial device deployments to identify and illustrate the cybersecurity risks facing financial firms today.

Forescout researchers studied the devices and behavior of financial services networks to evaluate risk profiles and identify critical security issues. They leveraged the Forescout Device Cloud, which contains the anonymized fingerprints of more than 11 million devices connected to the networks of Forescout customers. The study, limited to 100 large Financial Services deployments, identified segmentation best practices and some surprising risk areas.

Download Report

Beyond The Data Center

More IoT and OT Devices for Financial Services IT to Control and Secure



DEVICES IN FINANCIAL SERVICES

- Traditional Computing
- VoIP, Networking Gear, Mobile, Printers, IoT, OT

Forescout Device Cloud Research 2020

IOT DEVICE DIVERSITY

For every 100 PCs, there are

99

other Devices on Financial Services Networks (Includes VoIP, Networking Gear, Mobile, Printers, IoT, OT).

Cybersecurity leaders in financial services have more data center OT and energy-related devices to manage than leaders in other industry verticals.

Financial Services IoT Device Breakdown (Excludes Printers)

Financial Services IoT devices include extensive surveillance, physical security and access control, building automation systems, ATMs and point-of-sale systems.

- OT: UPS, PLC, SCADA/HMI, other Energy & Power devices, 25.65%
- IP Cameras & Surveillance, 25.22%
- Connected Buildings: Physical Security, Building Automation, 23.07%
- Banking & Retail: ATMs, Point-of-Sale, Loss Prevention, 12.33%
- Other IoT, 9.07%
- Multimedia: Digital Signage, Smart TVs, Projectors, Entertainment, 4.66%

Many of these systems run on a mix of new and legacy equipment.

These systems have also been shown to have multiple potential attack entry points. *

* https://www.forescout.com/company/resources/bas-research-report-the-current-state-of-smart-building-cybersecurity-2/

Increased Need for Segmentation

Data Shows Extra Precaution Needed for Critical Business Applications and Devices

Forescout Device Cloud Research 2020

BlueKeep and Windows Operating Systems

BlueKeep Patch Needed

29%

Devices that run older versions of Windows OS that required patching to fix BlueKeep.

BlueKeep is a "wormable" Remote Code Execution vulnerability that leverages RDP in legacy Windows OS versions.

Remote Desktop Protocol Open

16%

Devices running RDP where the Remote Code Execution vulnerability potentially originates.

Combined factors of legacy Windows OS and RDP services open increase BlueKeep susceptibility.

Windows 7

28%

Devices running unsupported Windows 7 OS as of January 14, 2020.

Windows 7 is no longer a supported OS as of January 14, 2020.

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

Propensity for BlueKeep in Financial Services

Recommendations

Safeguarding financial data stores and critical business applications requires end-to-end visibility across the campus, data center and cloud.

Cloud | Data Center | Campus | IoT | OT

Use Device Visibility & Control to Gain Situational Insight and Minimize Risk

Discover + Classify + Assess + Segment + Control + Automate + Orchestrate

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.

Assess: 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 non-compliant or compromised devices.

Control: Control access to enterprise resources based on user, device type & security posture, with or without 802.1X.

Automate: Automate response to security incidents and contain threats to minimize propagation and disruption.

Orchestrate: Streamline operations to bridge gaps between data and security with out-of-the box integrations.

To learn more about financial services 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