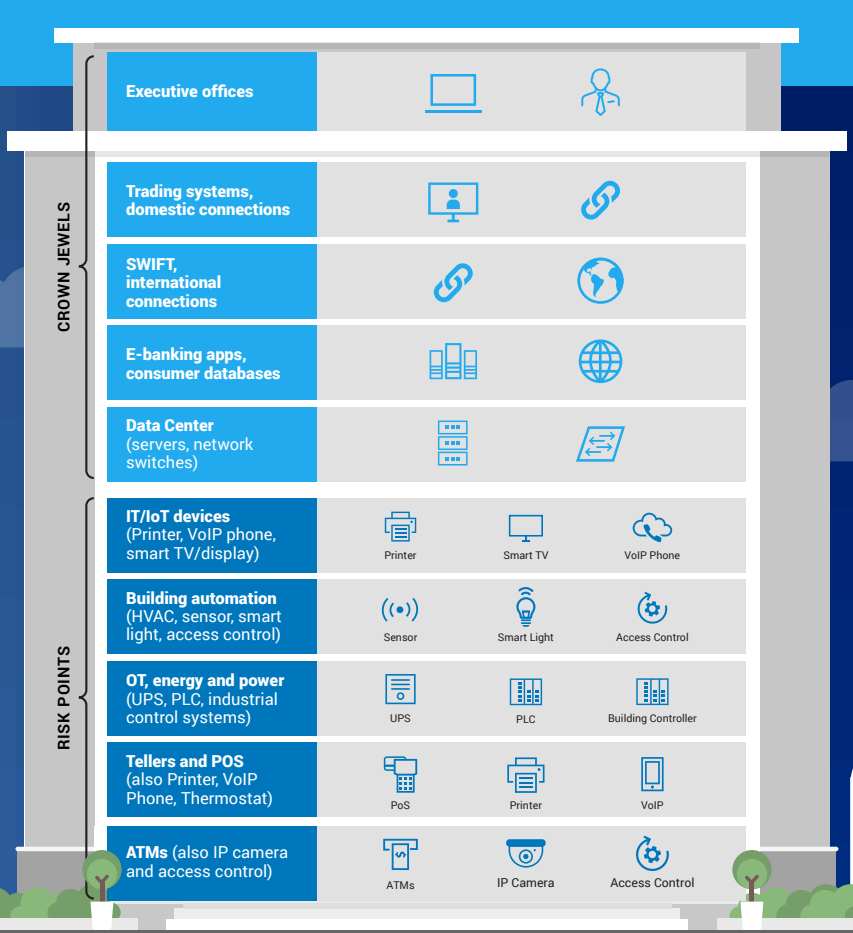
FORESCOUT

Banking on Security: What's Hanging Around Your Building?

Forescout researchers find multiple risky devices sharing network segments with these essential machines

The Forescout Device Cloud contains anonymized details of more than 11 million devices. Forescout Researchers analyzed 8,500 Financial Services network segments that contain either building automation, energy and power devices, ATMs or POS systems. Evaluating the risk profiles of almost 1 million devices identified, they found potentially unsecure devices sharing networks with sensitive and critical systems.



Financial Service devices are increasingly IP-enabled, connected to the Internet, and share network segments with many other IT, OT and IoT devices.

Connected Building – Who Authorized That?

For every 100 computers on the network there are 99 other devices.

Almost half of the IoT devices are printers. The rest are:

26% Energy and power systems

25% IP cameras and surveillance devices

23% Building automation and physical security

WHAT'S THE RISK?

OT, Energy and Power

- Embedded web server and exposed services
- Trigger shutdown or disruption of trading systems
- Overheat server room or other sensitive equipment

Building automation

- Extract Wi-Fi credentials and intercept data
- Escalate privileges or take advantage of admin privilege
- Lateral movement to Data Center, SWIFT workstation and other critical systems

61% ATM and POS systems that are exposed to non-financial IoT devices on their network segments

ATM – Who is Watching?

ATMs are installed in many locations, but many are in a kiosk or separated room. Security guidelines recommend that these areas be equipped with security cameras[1].

68% IP Cameras and surveillance devices

18% Connected building and physical security

14% Other IoT, such as uninterruptible power supplies and digital signage

WHAT'S THE RISK?

IP Cameras

- Drop malware onto camera
- Spy on ATM users
- Lateral movement to access control system

Access control

- Add new user and authorization
- Add new badge
- Enable badge to open door

POS – What is Printing?

POS devices are widely used in many environments. In a consumer bank branch, these devices are often connected alongside printers, VoIP phones, IP cameras, access control and building automation systems.

45% POS systems exposed to printers on the same segment

WHAT'S THE RISK?

Printers[2,3]

- Gain access to private and confidential documents
- Copies of access and authorization credentials
- Botnet, malware, persistent threats

IoT devices

- HVAC – Escalate privilege and gain network access
- Phone – Eavesdrop on conversations
- Building automation – Extract Wi-Fi credentials and access other systems

Recommendations

Gain visibility, control access, and automate response

VISIBILITY

- Discover every physical and virtual IP-connected device
- Automatically classify IT, IoT and OT devices in real time
- Continuously monitor and assess device behavior

SEGMENTATION

- Group devices by type and sensitivity
- Limit network access
- Restrict non-compliant and compromised devices

ENFORCEMENT

- Control access to enterprise resources
- Automate incident response and contain threats
- Integrate with other security systems

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

DOWNLOAD REPORT

1. https://www.pcisecuritystandards.org/pdfs/PCI_ATM_Security_Guidelines_Info_Supplement.pdf
2. https://www.forescout.com/company/resources/iot-enterprise-risk-report/
3. http://andreicostin.com/papers/Conf%20-%20EuSecWest2010_AndreiCostin_HackingPrintersForFunAndProfit_full.pdf

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