FORESCOUT®

RISKIEST CONNECTED DEVICES IN 2025

<) FORESCOUT RESEARCH | VEDERE LABS

Threat Intelligence Sharing Partners

OT-ISAC
OPERATIONAL TECHNOLOGY INFORMATION SHARING AND ANALYSIS CENTER

ACSC Australian Cyber Security Centre

EE-ISAC

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA

Devices

- 19+ million monitored devices
- 39+ billion unique data points
- 6,500+ unique vendors
- 2,300+ unique OS versions

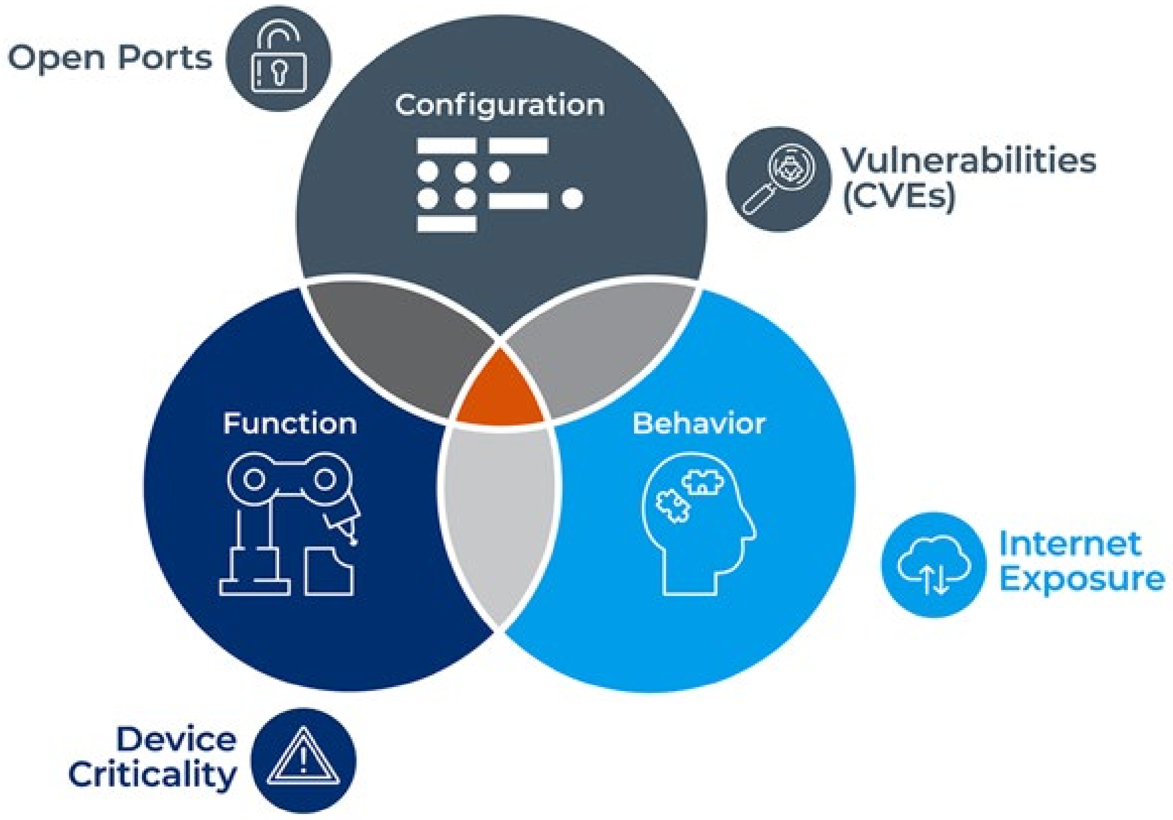
Threats

- 900+ million attacks
- 100,000+ malware samples
- 100+ ransomware group leak sites
- 20+ C2 types monitored on the Internet

Live data

forescout.vederelabs.com

Defining Risk



https://www.forescout.com/solutions/multifactor-risk-scoring/

The Riskiest Devices in 2025

	IT	IoT	OT	IoMT
1	Application Delivery Controller (ADC)	Network Video Recorder (NVR)	Universal Gateway	Imaging Devices
2	Intelligent Platform Management Interface (IPMI)	Network Attached Storage (NAS)	Historian	Lab Equipment
3	Firewall	VoIP Systems	Building Management System (BMS)	Healthcare Workstations
4	Domain Controller	IP Camera	Physical access control systems	Infusion Pump Controller
5	Router	Point of Sale (PoS) Systems	Uninterruptible Power Supply (UPS)	Picture Archiving and Communication System (PACS)

Riskiest IT Devices

#	Device
1	Application Delivery Controller (ADC)
2	Intelligent Platform Management Interface (IPMI)
3	Firewall
4	Domain Controller
5	Router

- **ADC, firewall and router: network infrastructure**
  - Network infrastructure risk surpassed endpoint risk in 2024 and continued that way in 2025
  - Devices that sit at the perimeter (“edge”) of the network
  - **No security agents**
  - **Limited telemetry / visibility**
  - **Lots of vulnerabilities being found and exploited very quickly**
- **IPMI, domain controller**
  - Server technologies
  - That’s where the data lives, part of the “crown jewels”

Riskiest IoT Devices

#	Device
1	Network Video Recorder (NVR)
2	Network Attached Storage (NAS)
3	VoIP Systems
4	IP Camera
5	Point of Sale (PoS) Systems

- **NVR, VoIP and IP camera**
  - Often exposed online
  - Lots of vulnerabilities, open ports, weak credentials, bad segmentation, …
  - Long history of being exploited by threat actors – cybercriminals and APTs
- **NAS**
  - Same as above, but also targeted by specific ransomware
- **PoS**
  - Historically a prime target for cybercriminals with dedicated malware to steal financial data

Riskiest OT Devices

#	Device
1	Universal Gateway
2	Historian
3	Building Management System (BMS)
4	Physical access control systems
5	Uninterruptible Power Supply (UPS)

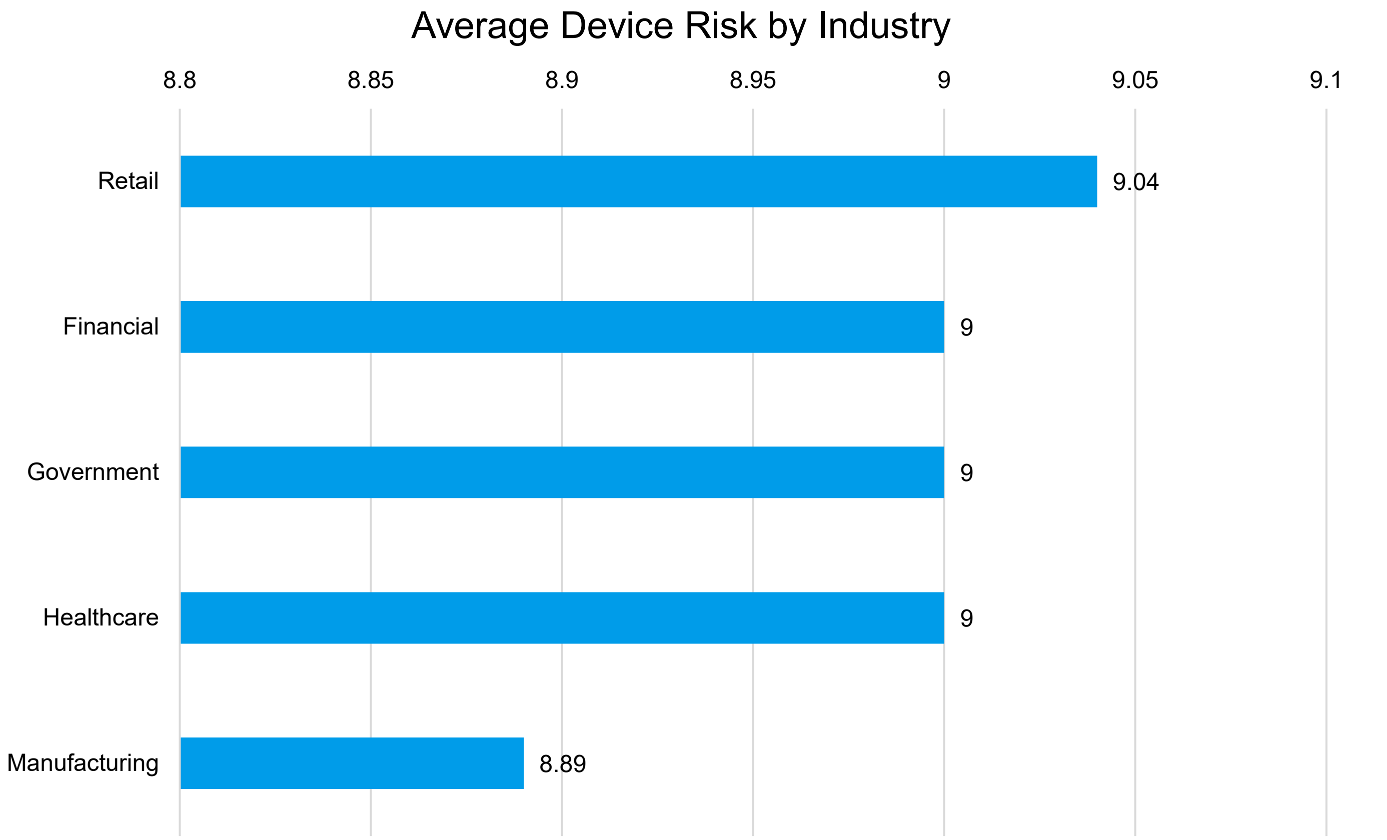
- **Universal Gateways**
  - Interconnect disparate systems, sometimes Ethernet and serial
  - Potential for lateral movement in OT networks
- **Historians**
  - Store operational process data
  - Involved in 10% of OT incidents in 2024 (SANS ICS survey)
  - IT/OT, just like engineering workstations
- **BMS and Access Control**
  - Deployed in facilities throughout the world, often exposed
- **UPSs present in many data centers and other facilities with default credentials**

Riskiest IoMT Devices

#	Device
1	Imaging Devices
2	Lab Equipment
3	Healthcare Workstations
4	Infusion Pump Controller
5	Picture Archiving and Communication System (PACS)

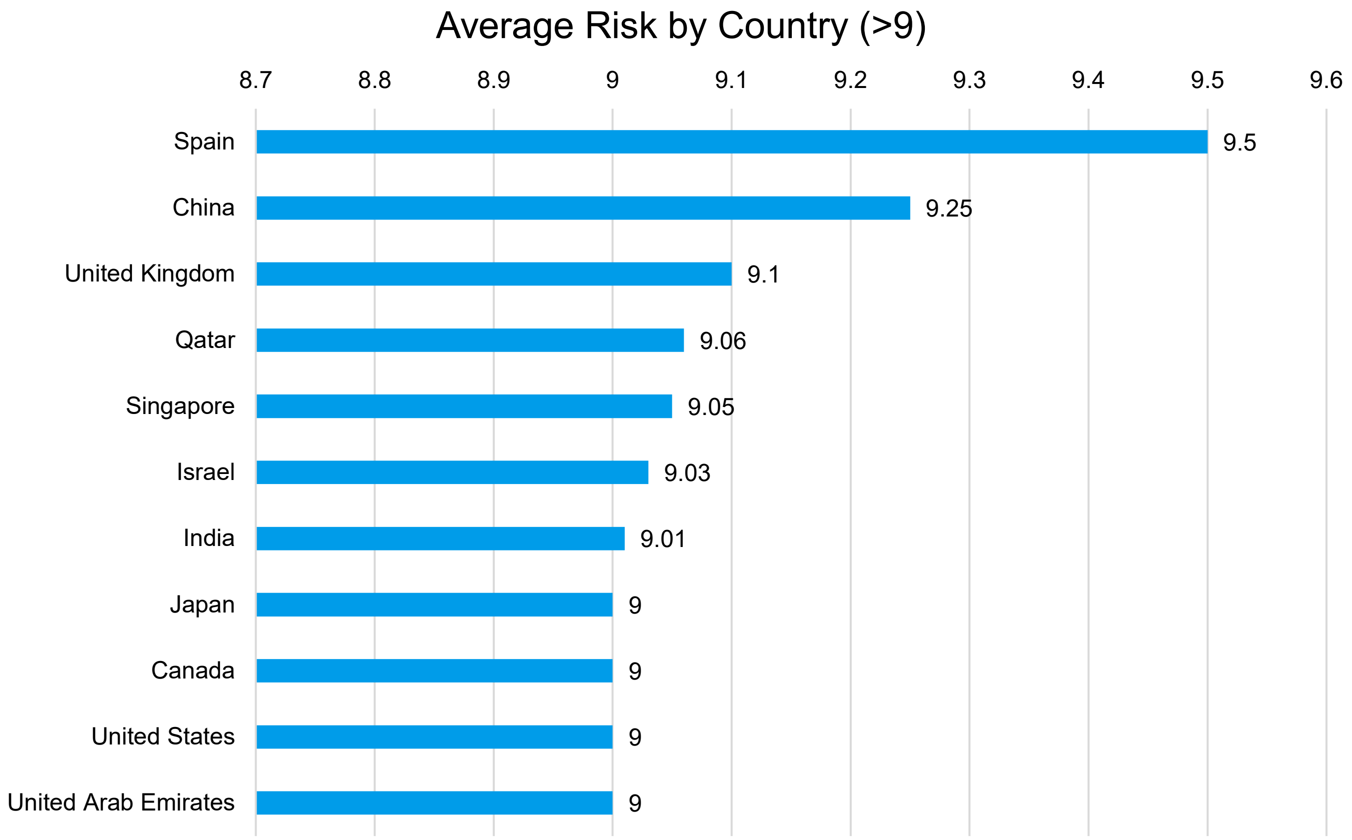
- **Imaging devices often connected to PACS and using the DICOM standard for file storage and communication**
  - Lots of interconnections, often older operating systems
  - DICOM is very popular but also very risky
- **Lab equipment used in diagnostics**
  - Usually runs specialized operating systems
  - Possibility for data exfiltration and tampering
- **Healthcare workstations**
  - Handle clinical data and are perfect targets for ransomware
- **Infusion Pump controllers**
  - Directly connected to patients, so attacks can be critical

Risk by Industry



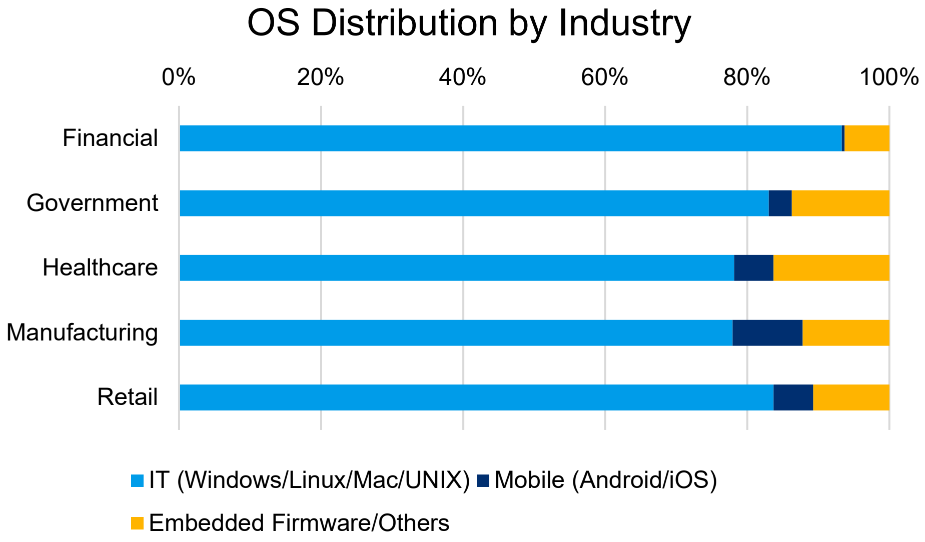
- **Retail** at the top
- Industry-wide **risk increased** by 15%
- The **gap** in risk scores between industry sectors is now **minimal**

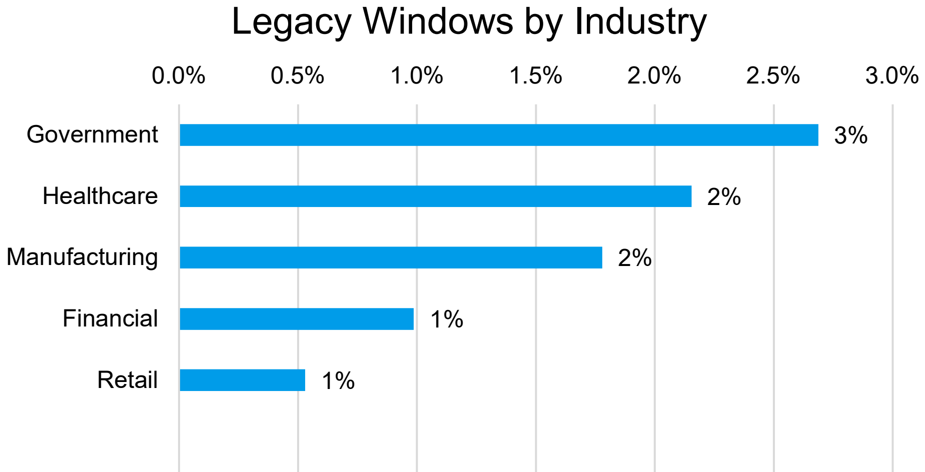
Risk by Country



- **Spain, China and UK at the top**
- Average **risk per country increased** by 33%
- **Differences** between countries also **small**

Operating Systems

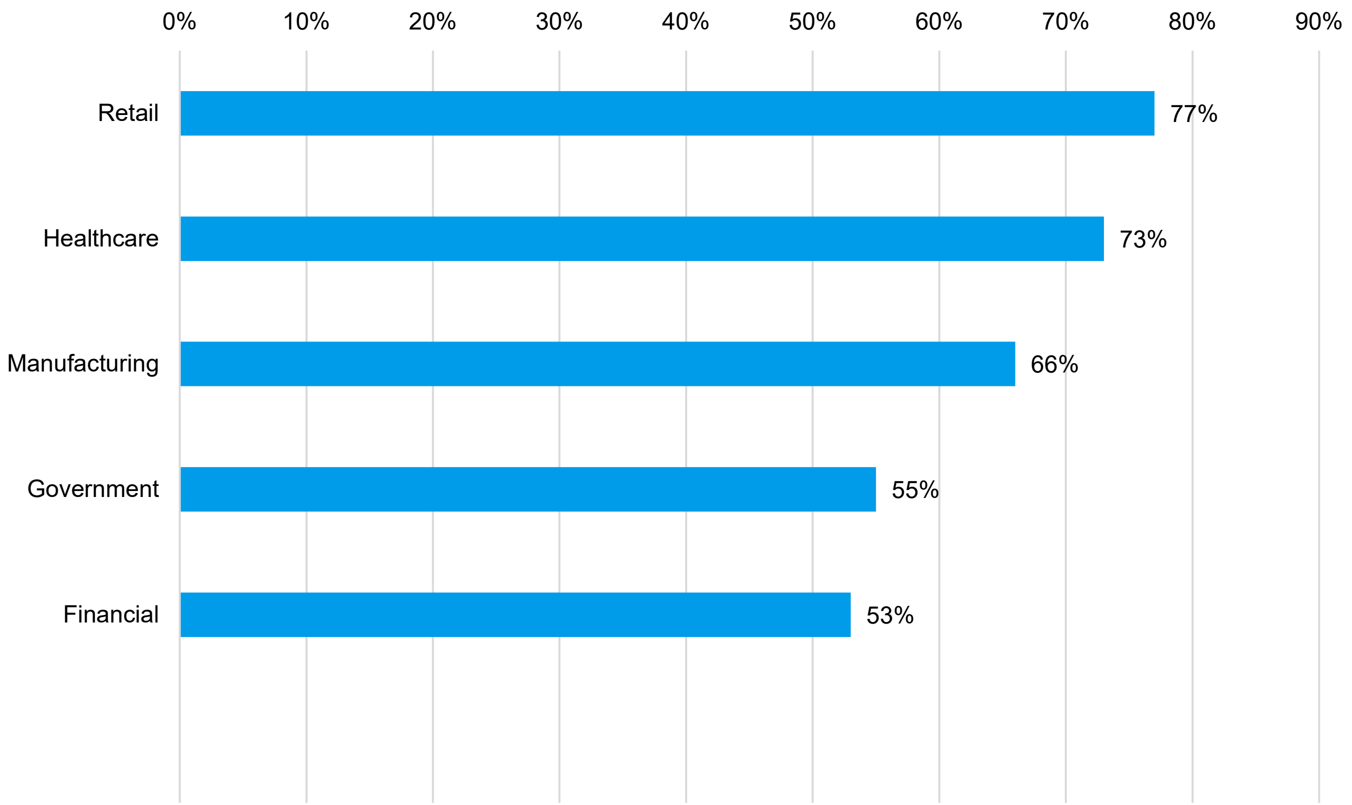

OS Distribution by Industry


Legacy Windows by Industry

- **Special-purpose OSes more prevalent** than mobile across all industries
  - Highest in healthcare, government and manufacturing
- These OSes grew significantly YoY
  - **Highest increase in government** (from 8.6% to 14%)
- Legacy Windows remained most common in government, healthcare and manufacturing
  - Every industry decreased legacy Windows, except government

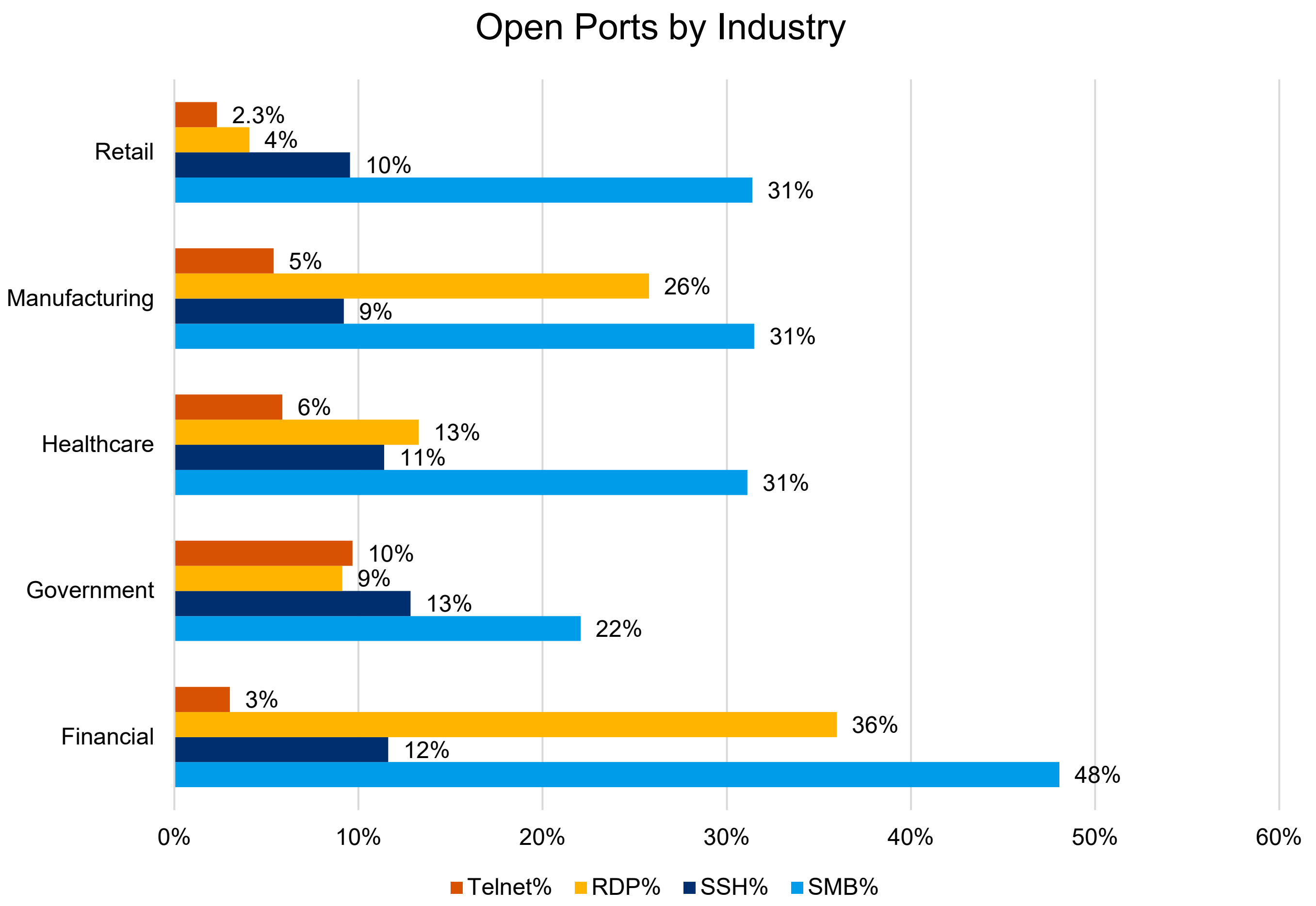
Windows 10

Windows 10 as Percentage of Non-legacy Windows by Industry



- Across all industries, more than 50% of non-legacy Windows devices still run Windows 10
  - Regular support ends in October 2025
- Retail and healthcare around three quarters of devices
- Significant costs to extend security support for the next three years
  - Potential for increase in legacy OSes next year

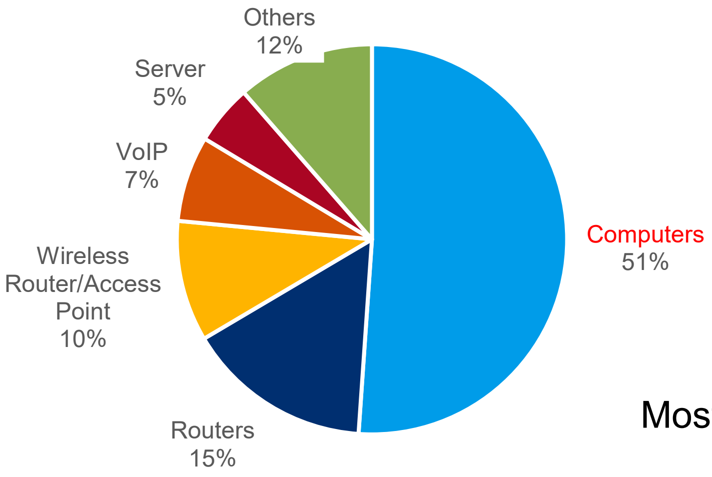
Open Ports



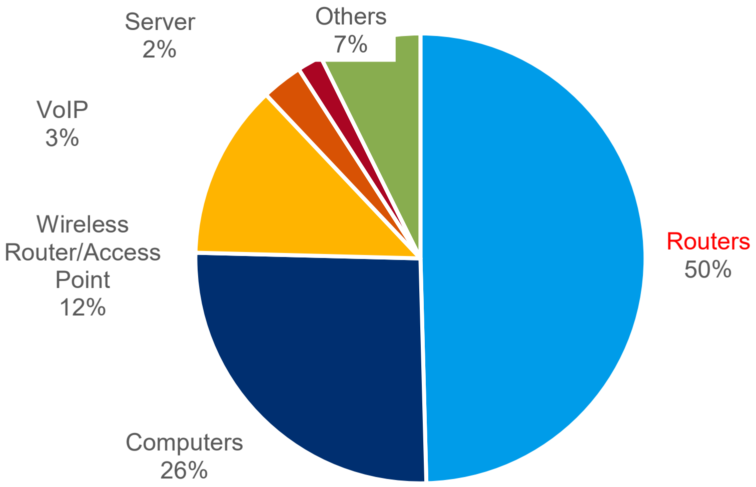
- Encrypted SSH declined, while unencrypted Telnet increased in every industry
  - Government saw the largest growth (2% to 10%)
- SMB increased in financial services and government
  - Declined elsewhere
- RDP grew in financial services, healthcare and manufacturing
  - Decreased in government and retail

Vulnerabilities

Most Vulnerable Devices



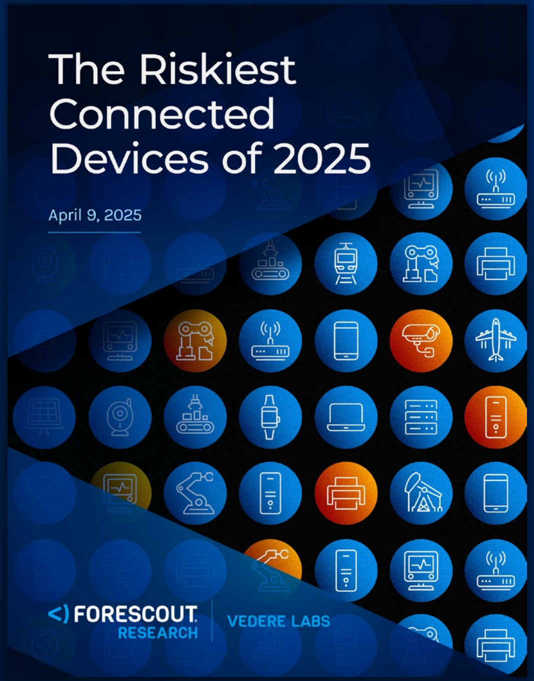
Most Vulnerable Devices (critical, exploitable)



- Most frequently vulnerable devices are computers, routers and wireless routers/access points
- Over 50% of devices with the most critical vulnerabilities are routers

Call to Action

- Get the full report:
  forescout.com/threat-briefings
- Follow the research:
  forescout.com/research
- Subscribe to the threat feed:
  feeds.vederelabs.com
- Subscribe to the newsletter:
  forescout.com/research-labs/#newsletterslignup



The Riskiest Connected Devices of 2025

April 9, 2025

<) FORESCOUT RESEARCH

VEDERE LABS

<) FORESCOUT®