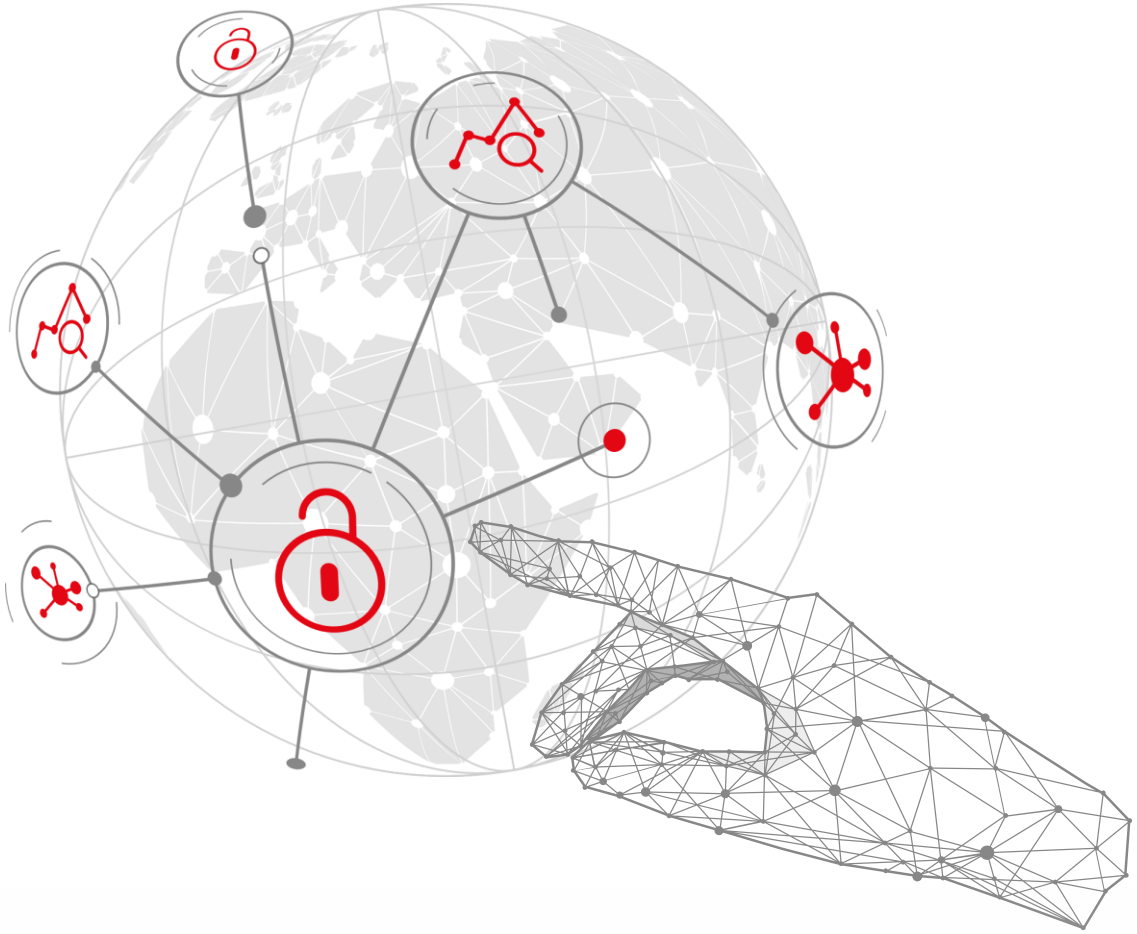


Mapovanie digitálneho terénu

09.06.2022

Martin Vívodik
Clico Security Consultant

CLICO

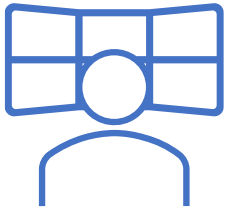
Security Networking Management

Trends Impacting Your Digital Terrain

Growth of Assets & Threats

Distributed Enterprise & Anywhere Operations

Fragmented Solutions



Shortage in Cybersecurity Personnel

You Need A Force Multiplier!

Much to Consider for Connected Assets

Zero Trust

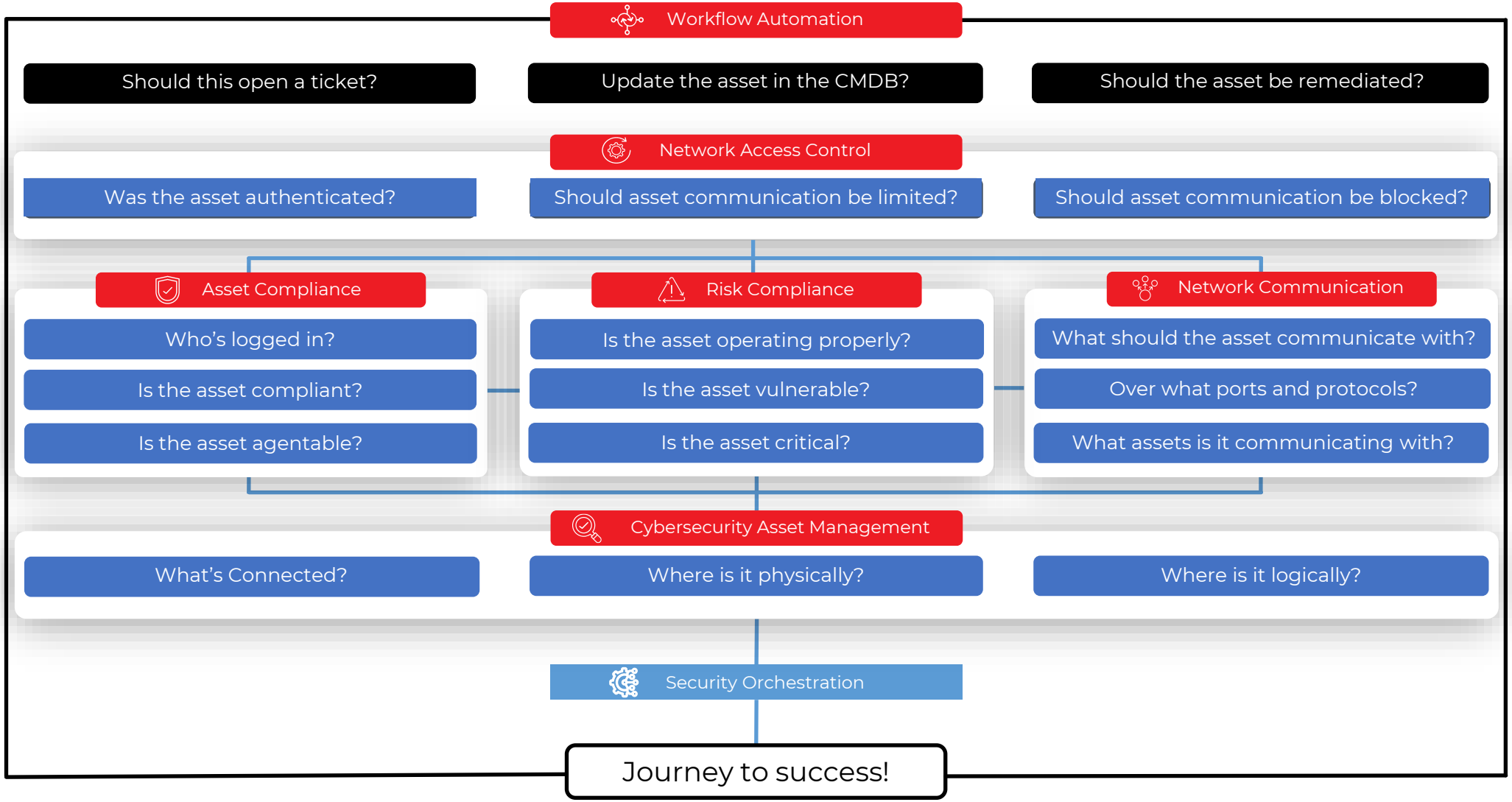
CIS Critical Controls

NIST

PCI DSS

NERC CIP

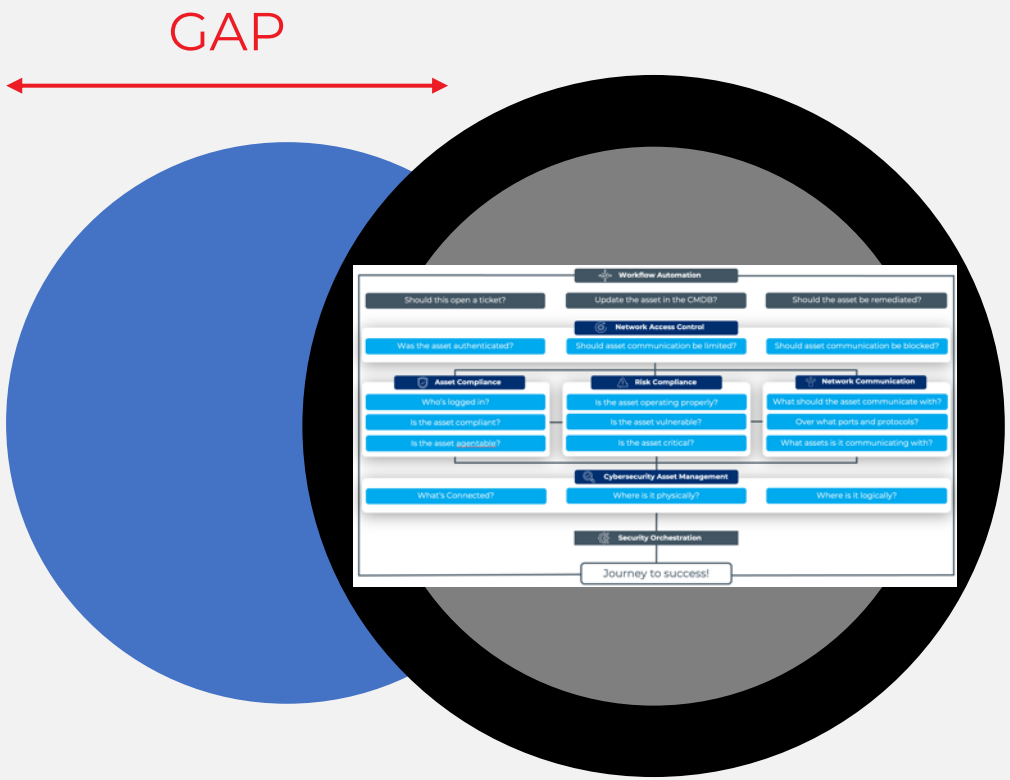
HIPAA



Your Never-Ending Security Challenge?

Constant Changes:

- Device Lifecycle
- Applications
- People
- Device Decay
- Software failures
- Acquisitions



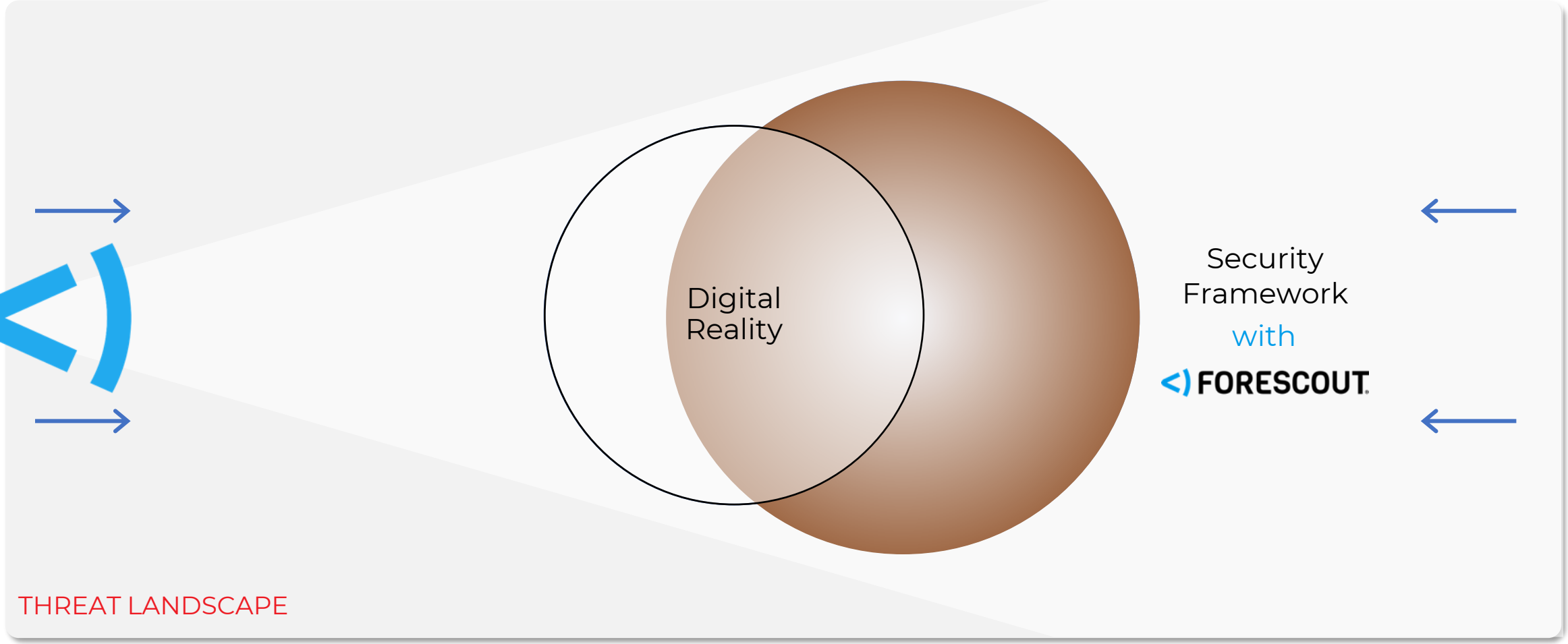
Security Framework:

- Regulatory Compliance
- Security Policies
- Risk Management
- Security Tools

THREAT LANDSCAPE

Constant Change Drives Misalignment
and Widens the Gap in Security Risk Posture

Your Never-Ending Security Challenge?

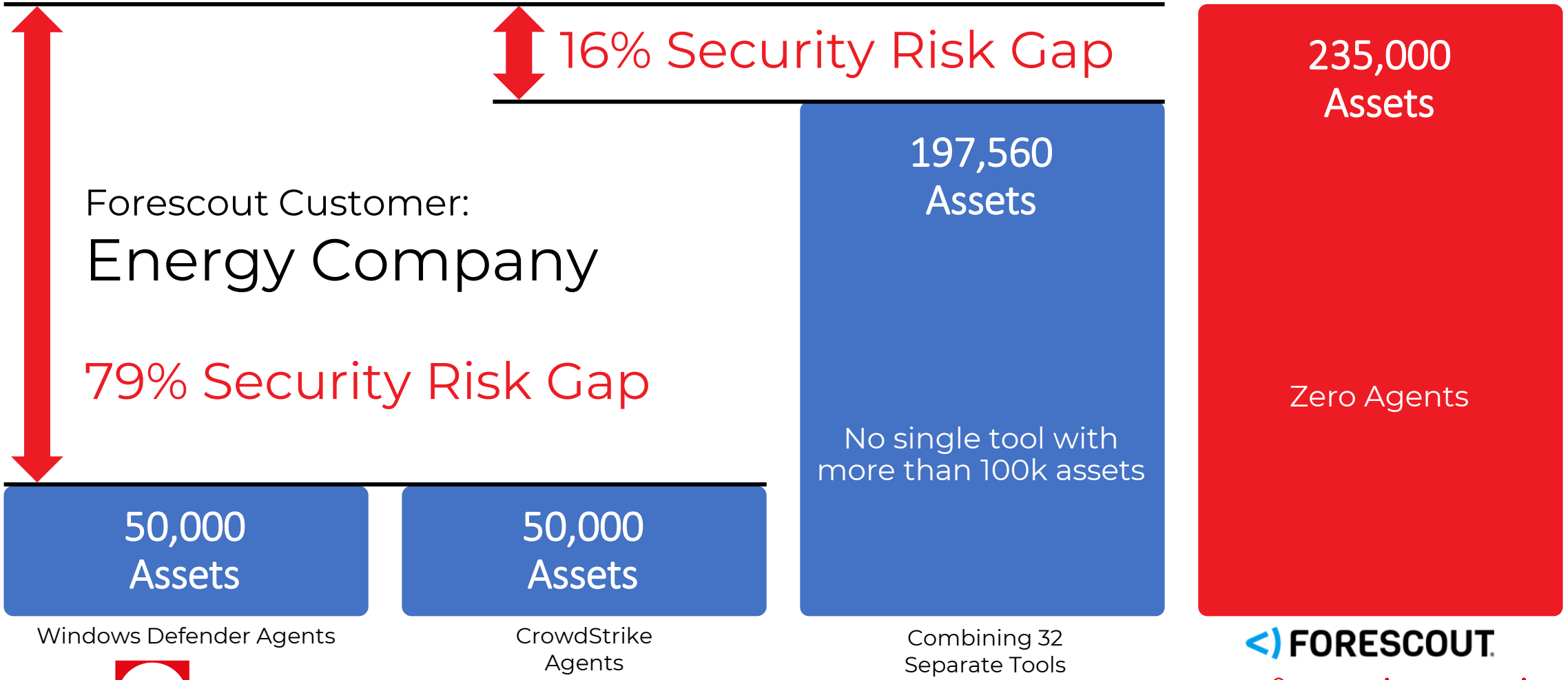


Forescout Aligns Your Digital Reality & Your Security Framework

... and Operates Continuously to Maintain Alignment

Real-World Example

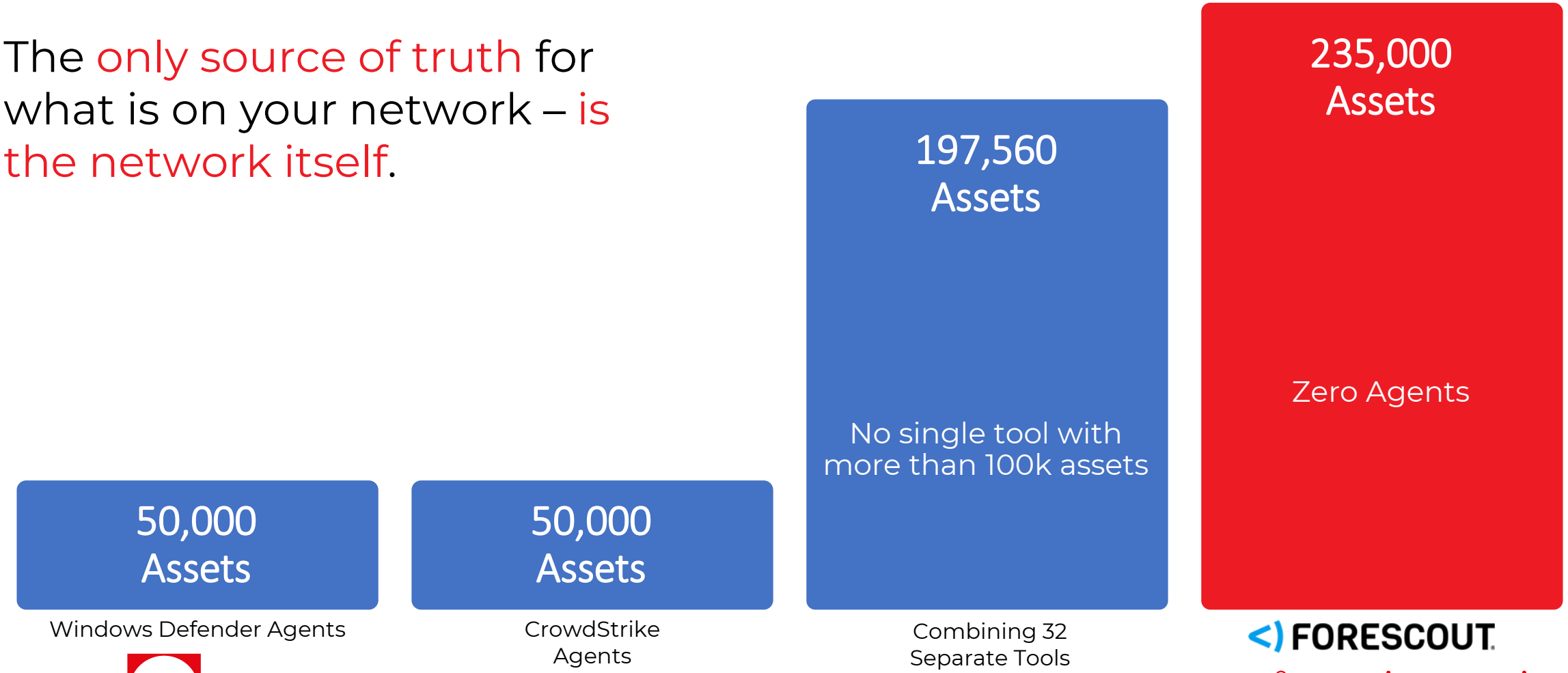
Rapid time to value for a holistic view of all devices



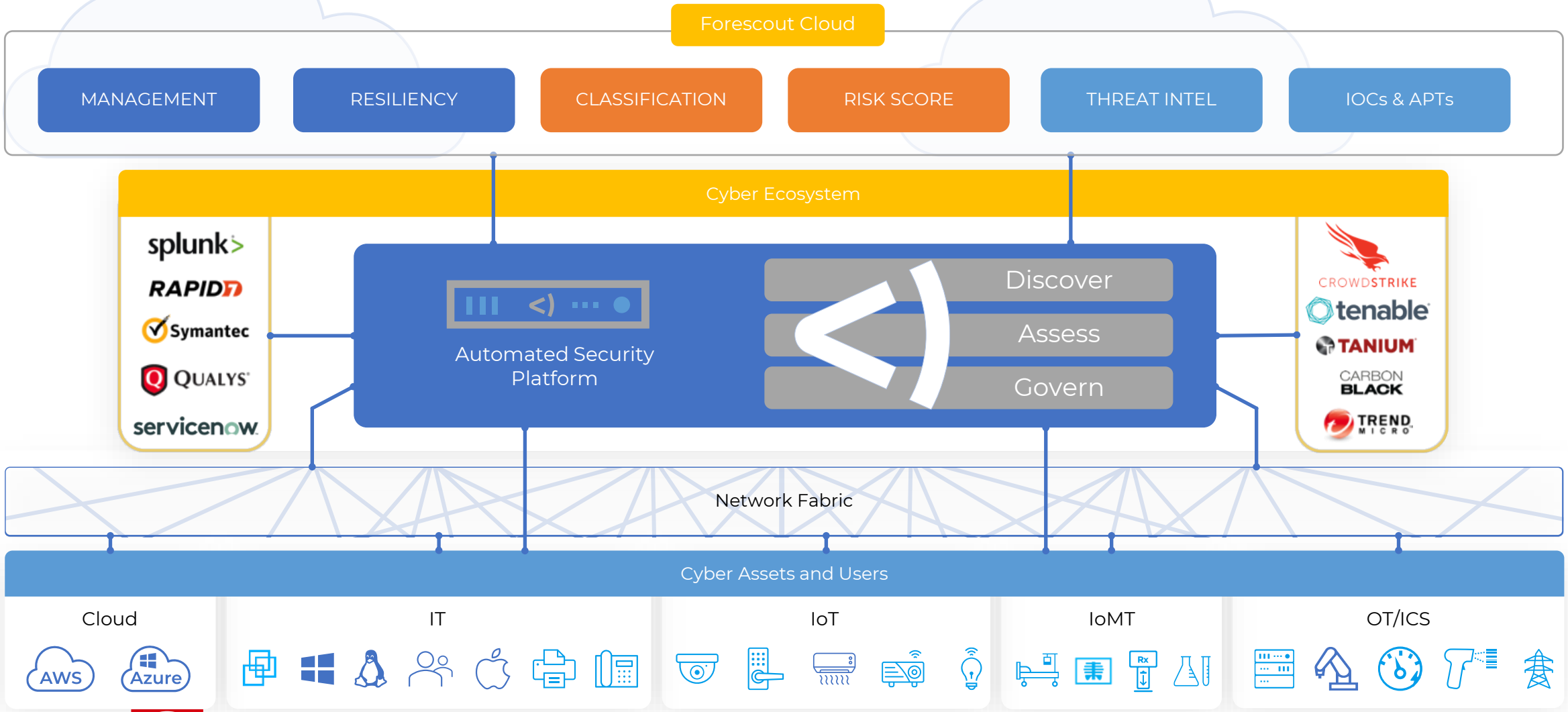
Real-World Example

Rapid time-to-value for a holistic view of all devices

The only source of truth for what is on your network – is the network itself.



Forescout Continuum



Security Networking Management

Connected devices under attacks

Kyberútoky na české nemocnice

HEALTH IT, HOSPITALS

Report: First hal

Ransomware v Nemocnici Rudolfa a Stefanie Benešov

V nemocnici v Benešově došlo k útoku na konci roku 2019. Kvůli omezení lékařských výkonů, zrušení plánovaných vyšetření, operací, výroby a nákladům na obnovu se škody za necelé tři týdny omezení provozu vyšplhaly na 59 milionů korun.

NÚKIB: České nemocnice stále čelí hackerským útokům

10. 11. 2021, 15:53 – Brno
Miloslav Fišer, Novinky, ČTK

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) v říjnu evidoval 14 kybernetických incidentů, letos druhý nejvyšší počet po březnu s 30 útoky. Většina neměla vážné následky a rychle se vyřešily. Zvýšenému tlaku hackerů podle NÚKIB stále čelí zdravotnictví. Ke konci října úřad eviduje 24 kybernetických incidentů, o osm víc než za celý loňský rok. NÚKIB o tom informuje na webu.

Jonathan Greig
June 2, 2022

Cybercrime | Malware | News | Technology

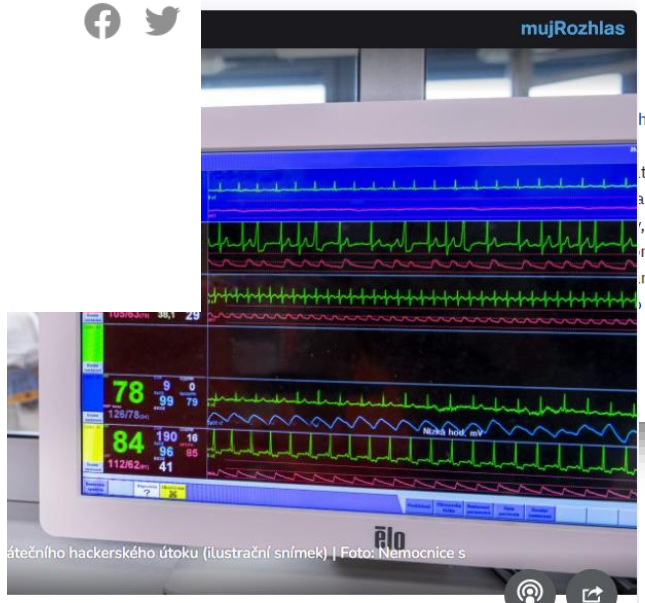
Tech manufacturing giant Foxconn s
after a ransomware attack crippled t

The LockBit ransomware group claim
last month. They threatened to leak

A spokesperson from the Taiwanese
new report.

Psychiatrická nemocnice v Kosmonosech

Následoval útok na psychiatrickou nemocnici, který proběhl jen o několik málo dnů později. 27. března došlo k ransomwarovému útoku, který s největší pravděpodobností zneužil slabá, nedostatečně zabezpečená místa na serverech. Útočníci se v takovém případě přihlásí, vypnou v zařízení bezpečnostní řešení a ručně spustí škodlivý kód, jenž ze zařízení zašifruje všechny dostupné lokální a síťové disky. Takový útok není nijak náročný a jde s největší



átečního hackerského útoku (ilustrační snímek) | Foto: Nemocnice s

Discover and inventory all cyber assets on your network, continuously.

Discover all devices

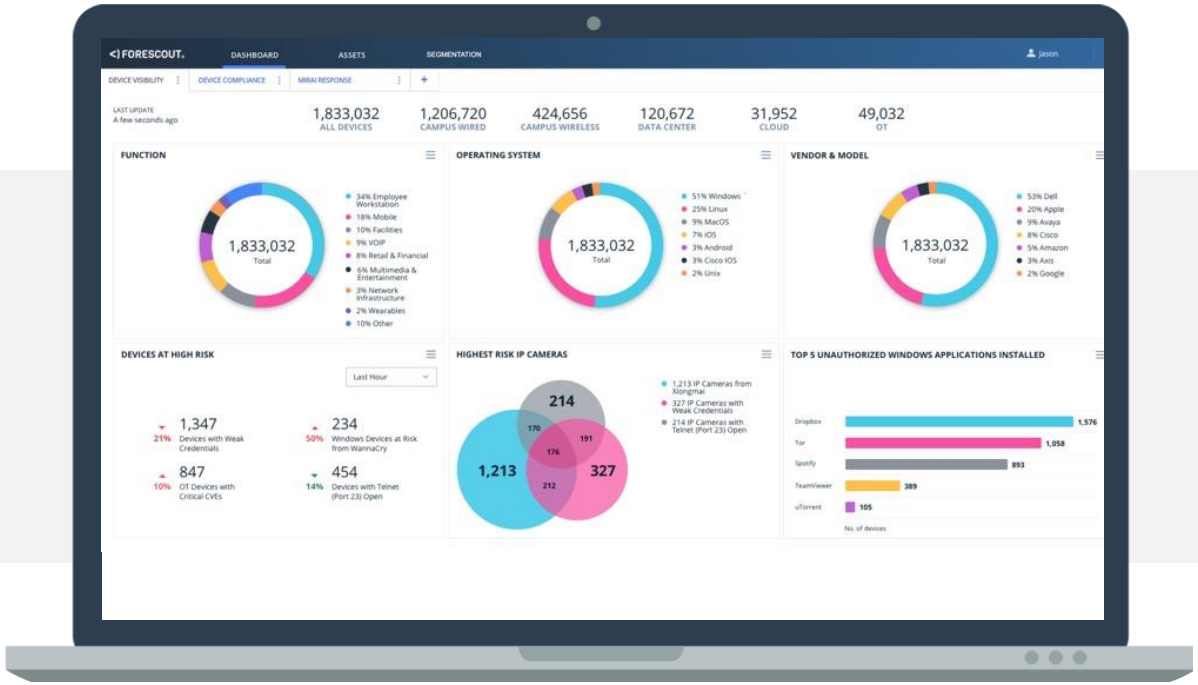
Inventory of all connected cyber assets with the industries most robust choice of 30+ techniques, without agents or disruption

Rich Context with High Fidelity

| Manufacturer | Model | MAC | IP | Serial Number | Firmware, OS | Software | Location | Vulnerabilities | Recalls | Traffic Analysis | Threat Detection | Risk Assessment |

Leverage insights

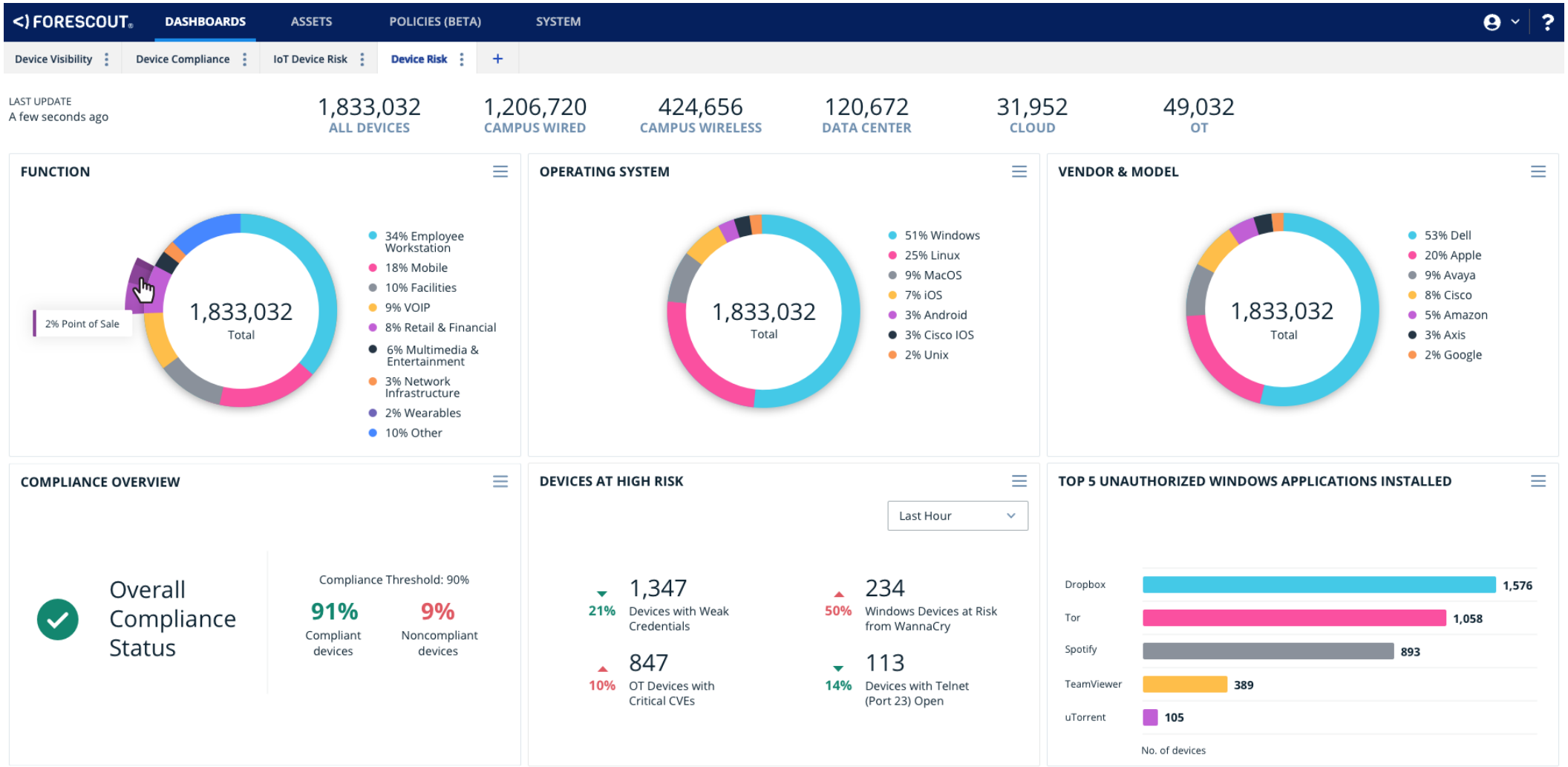
Derived from tens of millions of assets across many of the world's largest companies heavily targeted by threat actors



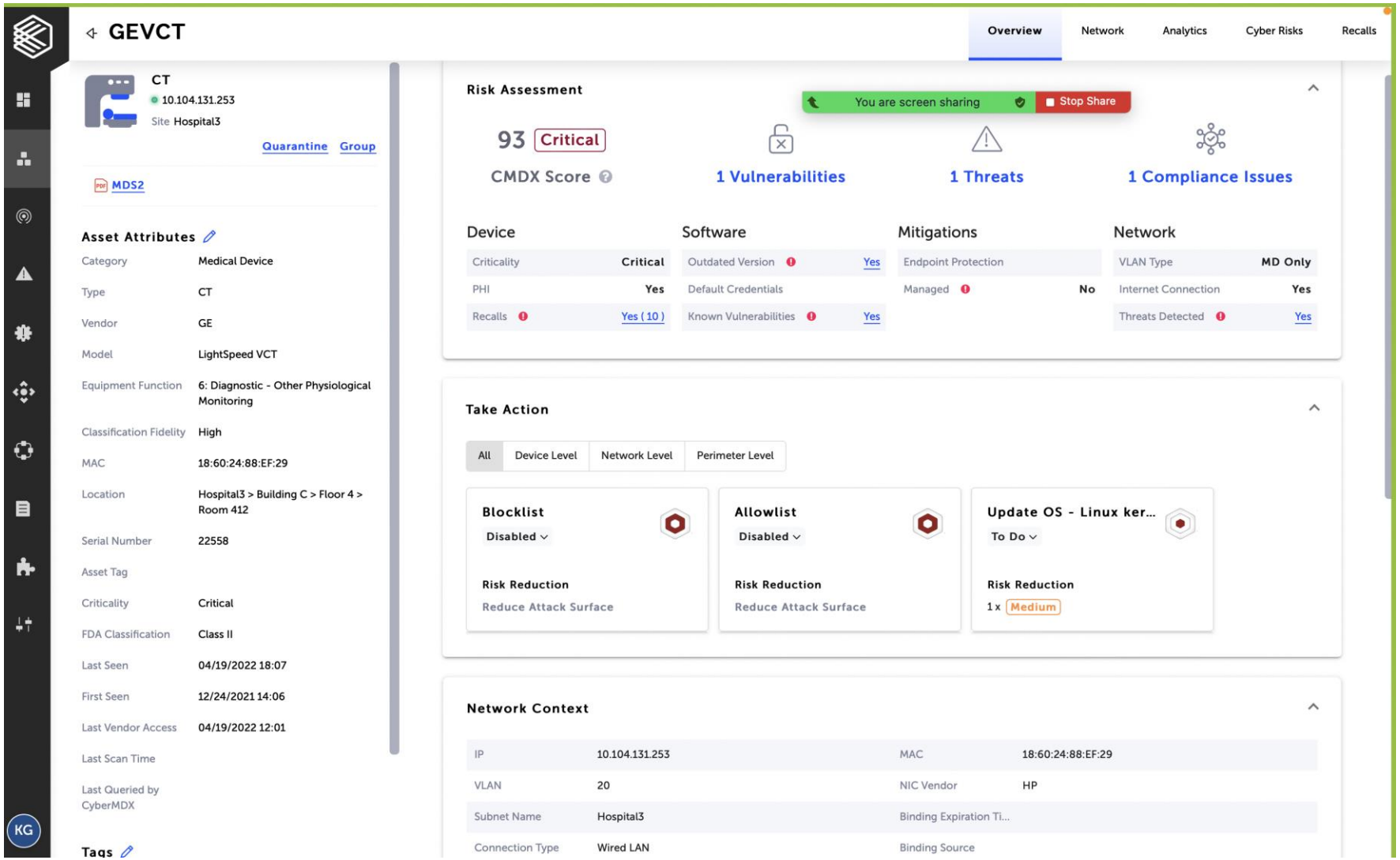
Forescout Can Help

- Are you aware of every connected device? Globally?
- Do you have full context in one platform?
- Is this information updated, continuously?

Dashboards


FORESCOUT
DASHBOARDS
ASSETS
POLICIES (BETA)
SYSTEM
Device Visibility
Device Compliance
IoT Device Risk
Device Risk
LAST UPDATE
A few seconds ago
1,833,032
ALL DEVICES
1,206,720
CAMPUS WIRED
424,656
CAMPUS WIRELESS
120,672
DATA CENTER
31,952
CLOUD
49,032
OT
FUNCTION
2% Point of Sale
1,833,032
Total
34% Employee Workstation
18% Mobile
10% Facilities
9% VOIP
8% Retail & Financial
6% Multimedia & Entertainment
3% Network Infrastructure
2% Wearables
10% Other
OPERATING SYSTEM
1,833,032
Total
51% Windows
25% Linux
9% MacOS
7% iOS
3% Android
3% Cisco IOS
2% Unix
VENDOR & MODEL
1,833,032
Total
53% Dell
20% Apple
9% Avaya
8% Cisco
5% Amazon
3% Axis
2% Google
COMPLIANCE OVERVIEW
Overall Compliance Status
Compliance Threshold: 90%
91%
Compliant devices
9%
Noncompliant devices
DEVICES AT HIGH RISK
Last Hour
1,347
21%
Devices with Weak Credentials
234
50%
Windows Devices at Risk from WannaCry
847
10%
OT Devices with Critical CVEs
113
14%
Devices with Telnet (Port 23) Open
TOP 5 UNAUTHORIZED WINDOWS APPLICATIONS INSTALLED
Dropbox
1,576
Tor
1,058
Spotify
893
TeamViewer
389
uTorrent
105
No. of devices

Detailed view



Assess cyber asset compliance and risk hygiene, continuously.

Asset compliance

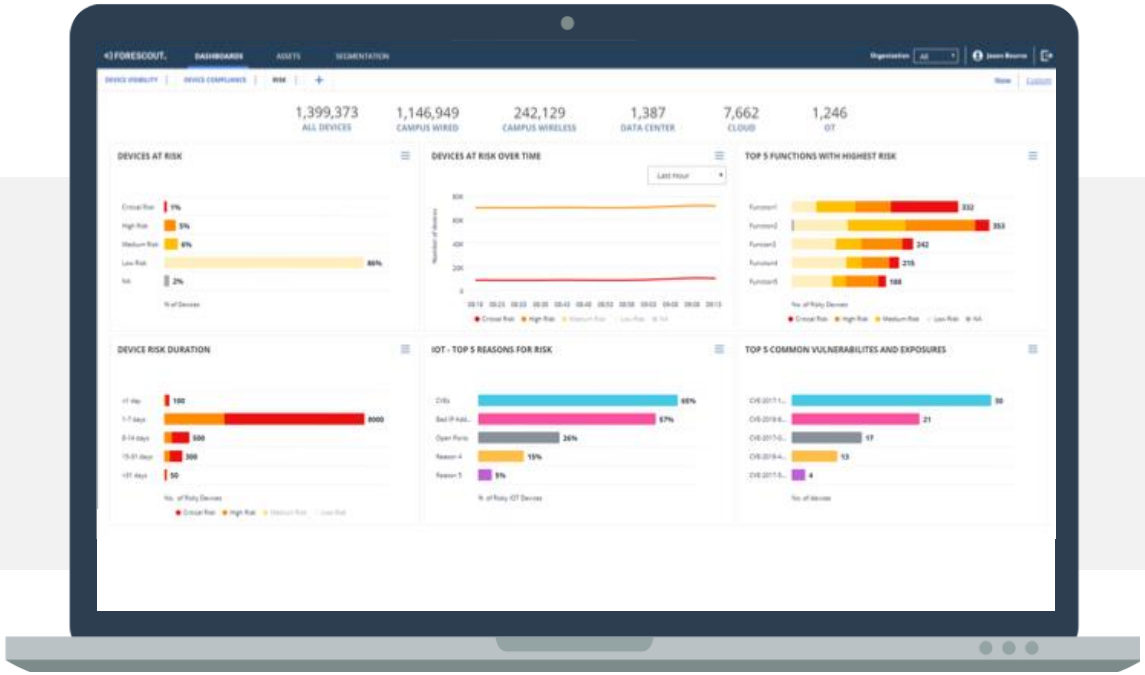
On-connect agentless validation of cyber asset state against security frameworks. Ensure security investments are deployed and running

Identify and prioritize risk

Real-time, multi-faceted risk analysis and mitigation for all connected cyber assets based on asset trends and threat feeds

Group and baseline flows

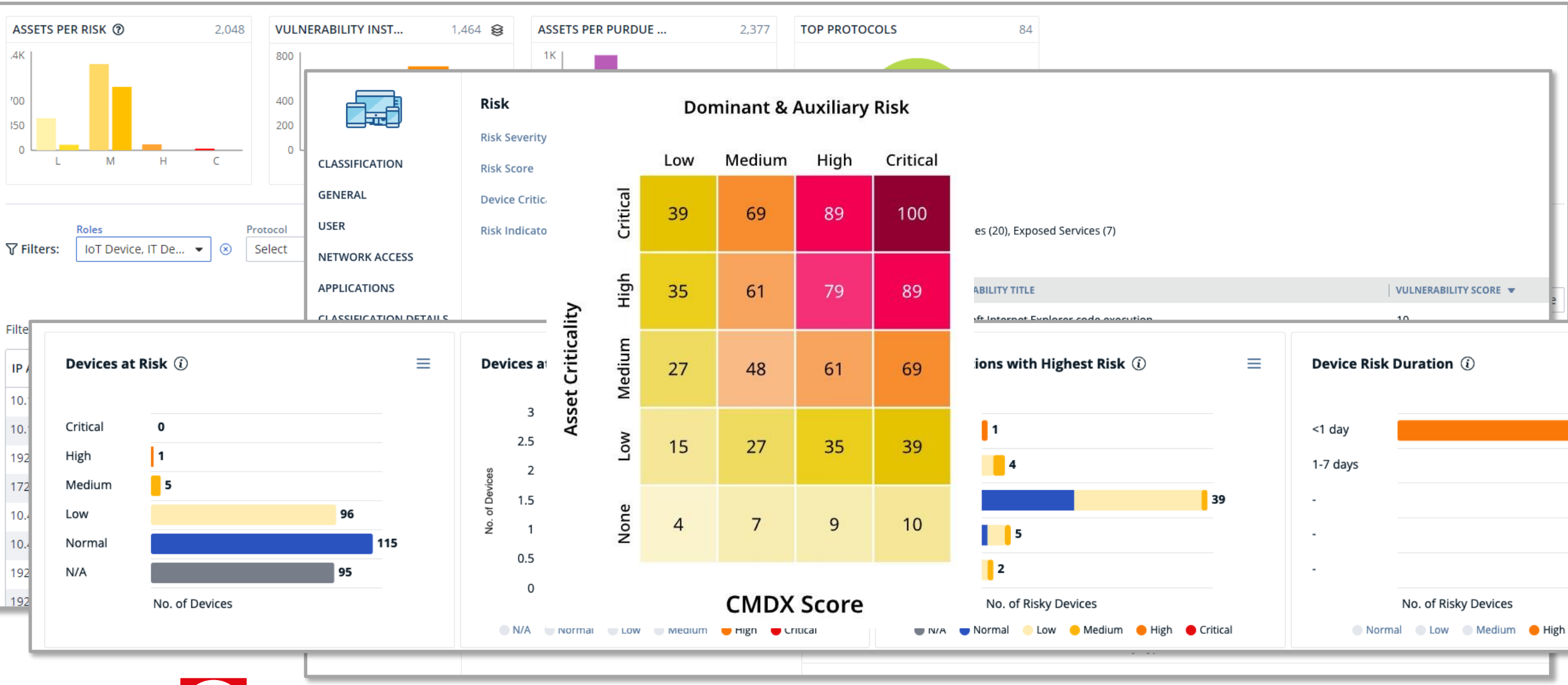
Dynamically group cyber assets by type and role to map traffic flows and cross-talk between groups



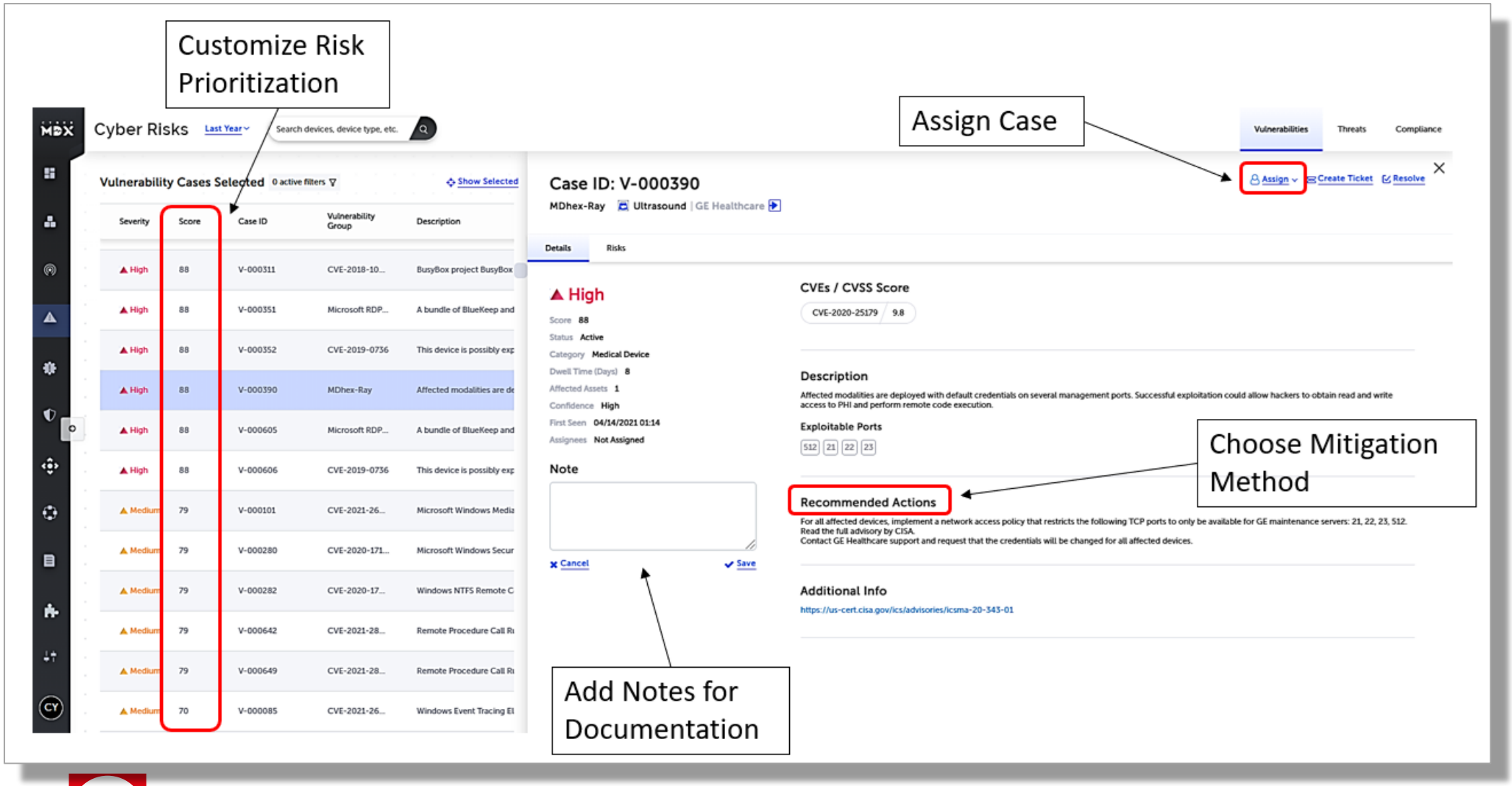
Forescout Can Help

- What validates installation/configuration of agents?
- How do you prioritize remediation of assets today?

Risk Scoring



Device-Centric Risk Management



Govern cyber assets proactively to minimize attack surface and breach impact, continuously.

Proactive remediation

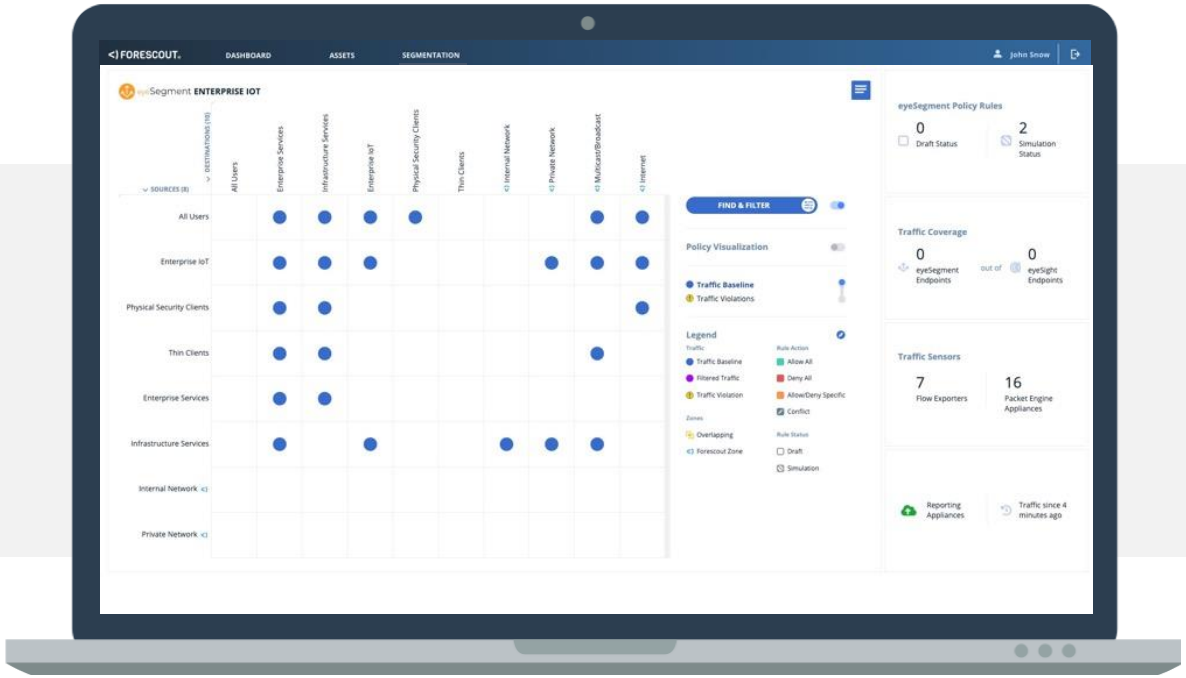
Correct misconfigurations with non-compliant cyber assets before they present challenges that require extensive triaging

Pin-point controls

Simulate targeted policy decisions before enforcement to reduce blast radius without widespread operational impact

Enforce Zero Trust security

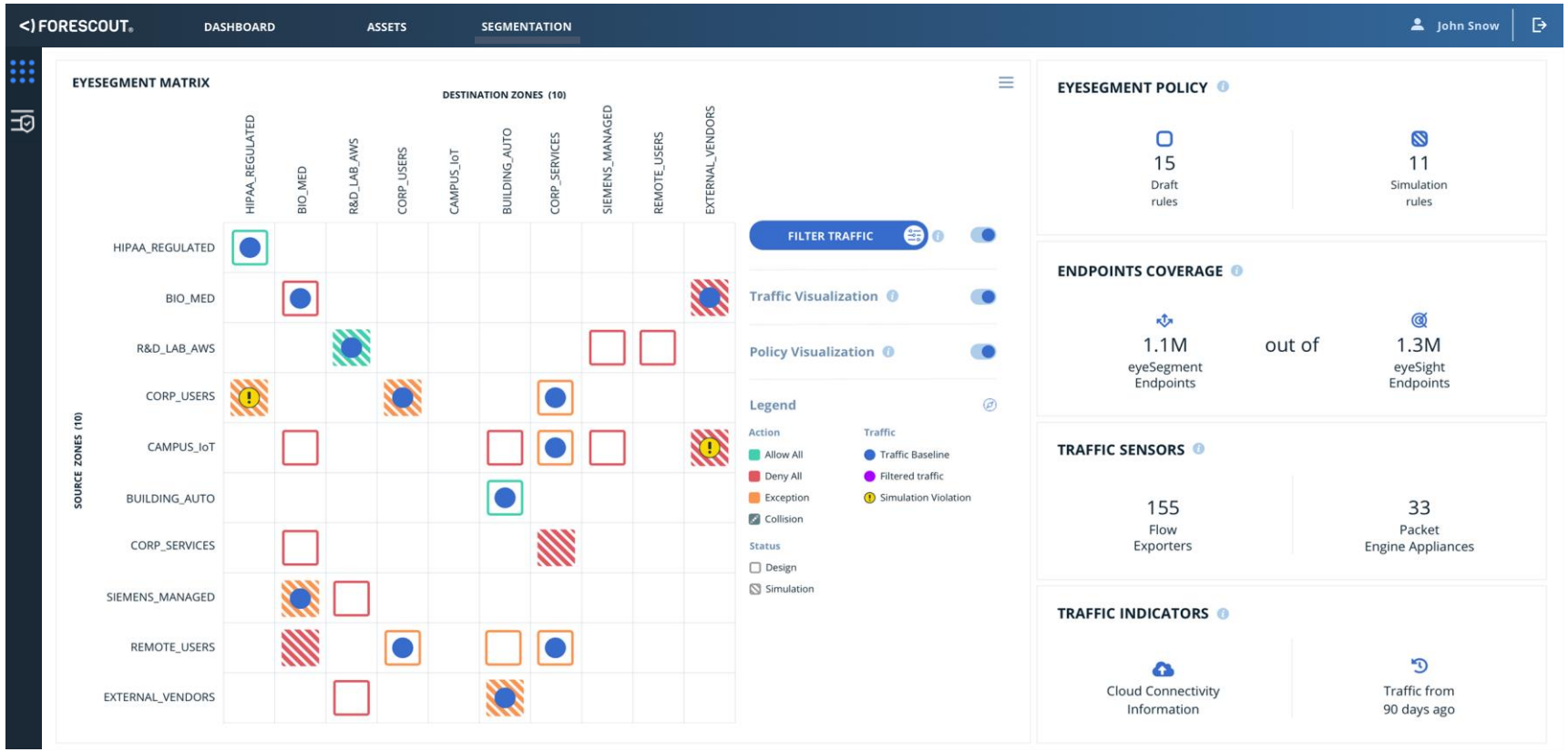
Implement least-privilege Zero Trust policies based on user, device, connection, posture and compliance for all cyber assets



Forescout Can Help

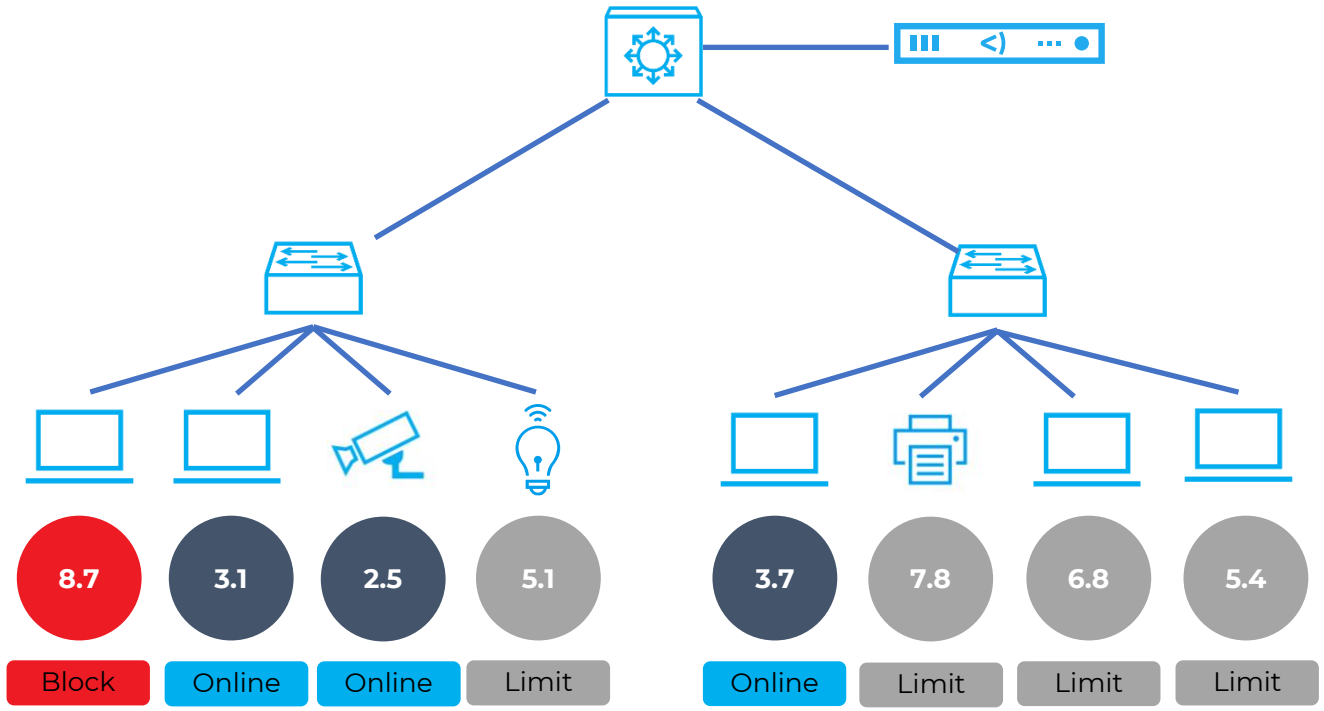
- Can you automatically remediate assets without human intervention?
- Can you limit blast radius… without negative impact?

Segmentation & Zero Trust



Quickly identify higher risk assets
and segment them automatically

Multifactor Network Access Control



01 Discover – every connected device within depth accuracy.

02 Assess – your cyber asset hygiene and risk compliance.

03 Govern – assets proactively depending on your security framework and risk tolerance. Remediate assets automatically or limit network access

Automate security and response workflows.

Share Contextual Insights

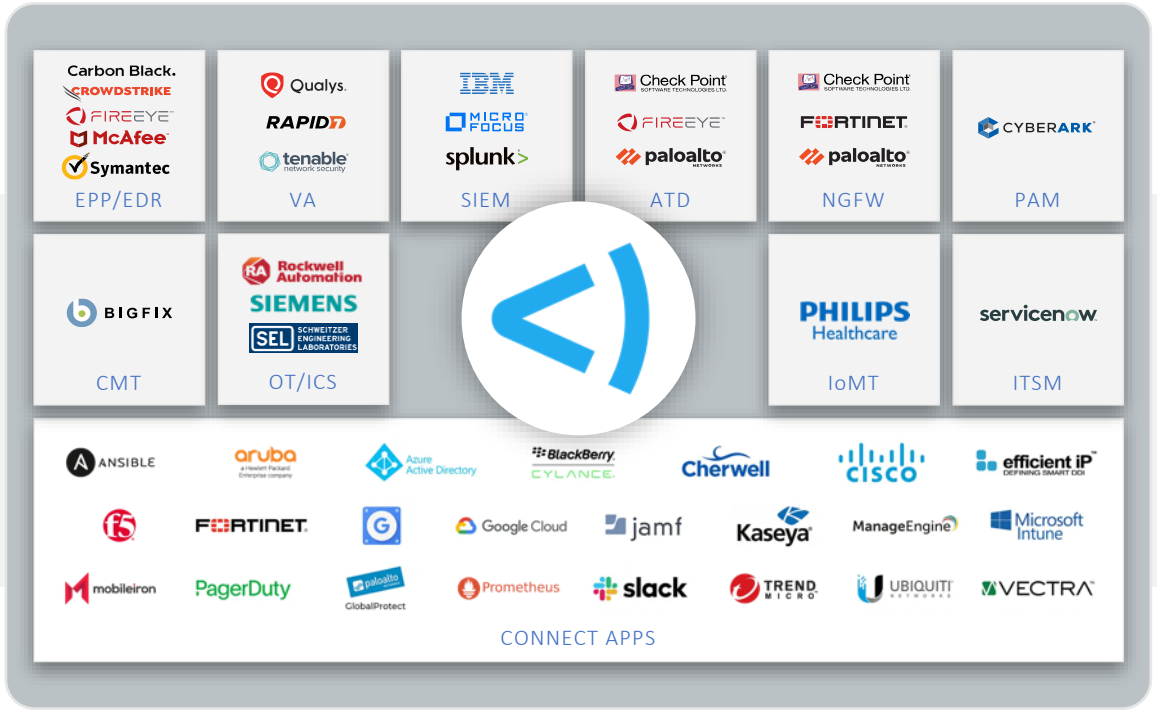
Share in-depth device, user and network context for all cyber assets — managed and unmanaged

Automate Workflows

Automate cross-product processes and bridge gaps between tools with pre-built integration modules, community apps and open APIs

Accelerate Response

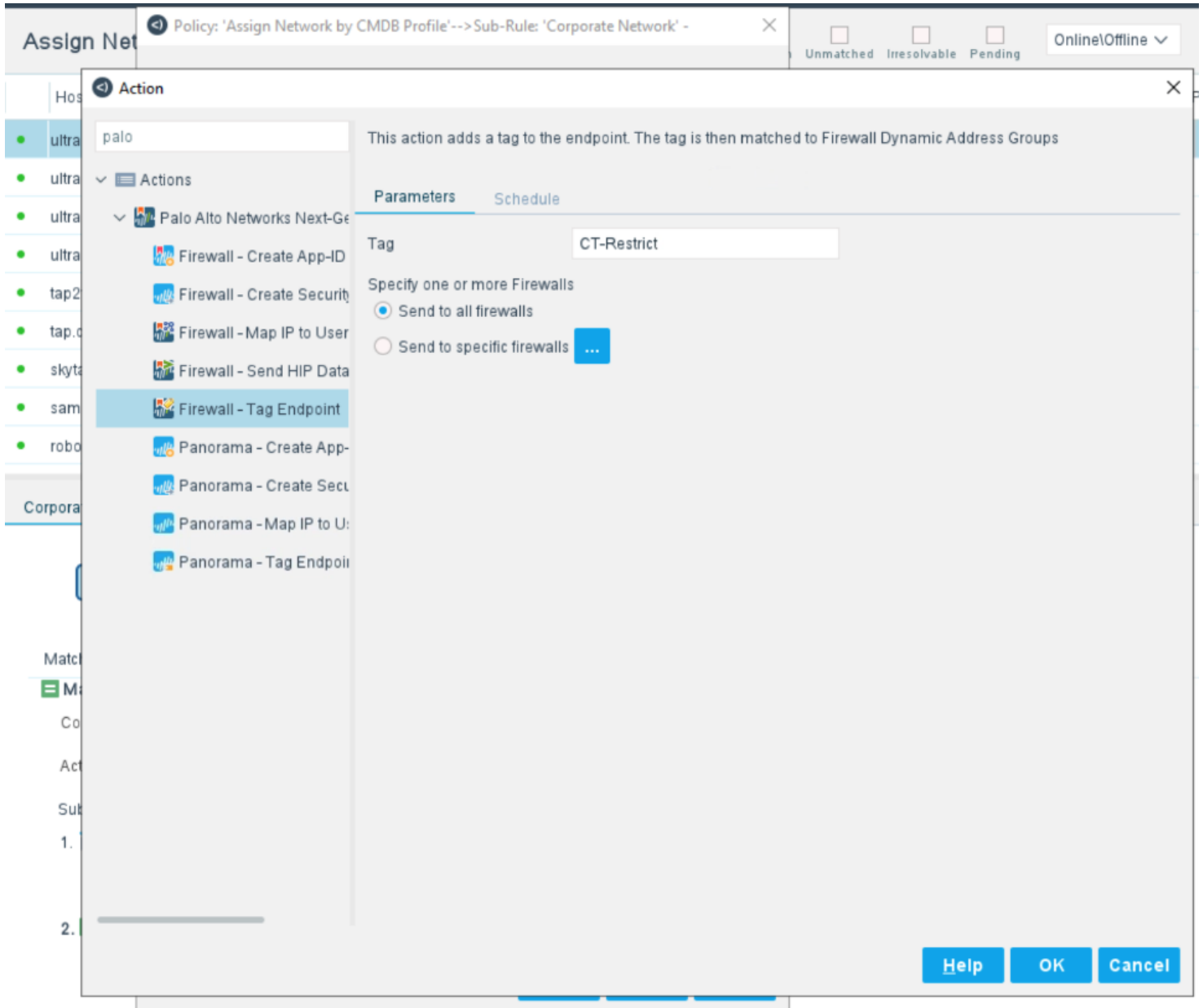
System-wide policy enforcement and incident response actions at machine-speed to contain threats, minimize propagation and mitigate risks



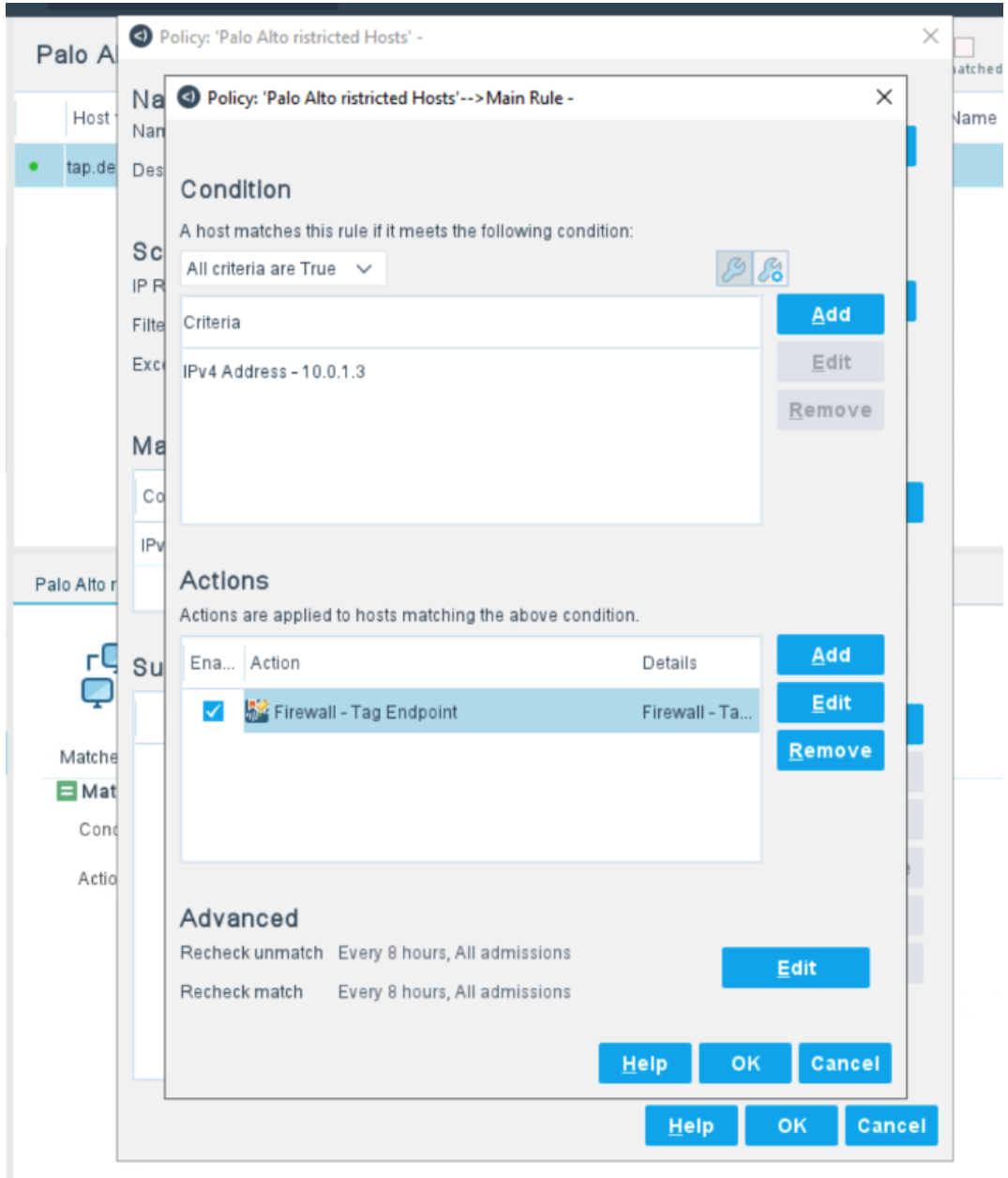
Forescout Can Help

- How do your security products enrich one another?
- How have you automated workflows between products and people?
- How do the number of people & systems impact response times?

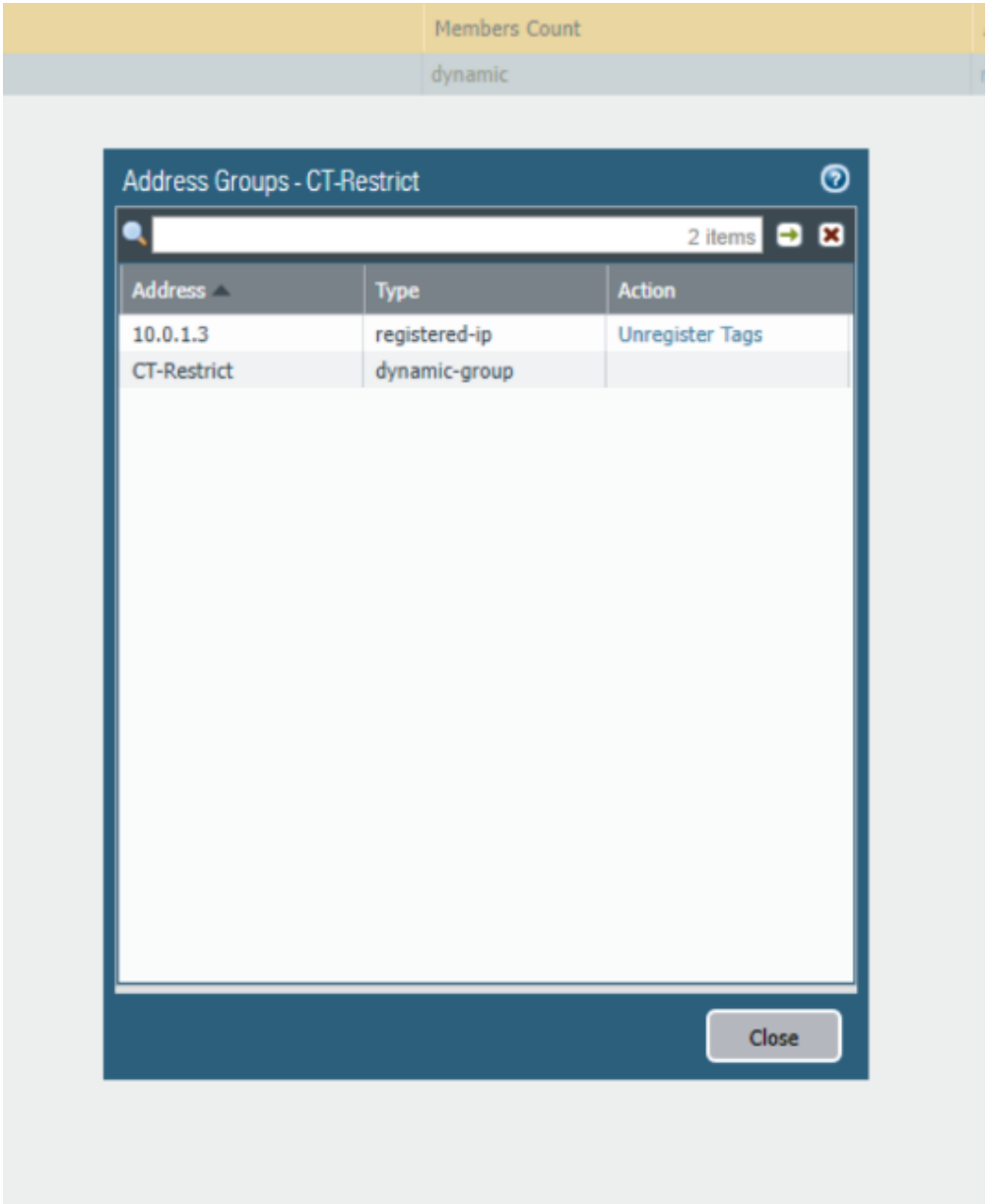
Automated response



Automated response



Automated response



Who is Forescout?

Over 20 years of cybersecurity expertise...

- Headquartered in Dallas, Texas
- Employees in over 30 countries
- Leader in threat research and intelligence

Over 3000 customers globally...

- 30% of Fortune 100, 20% of Global 2K
- Expertise across Financial, Insurance, Healthcare, Government, and Utilities industries

Trusted and Proven...

- Millions of end points deployed in US DoD Comply-to-Connect Program
- Completed Project Memoria, the most extensive study of TCP/IP stacks that uncovered 97 new vulnerabilities impacting over 400 vendors
- Diverse customer case studies and recognized by numerous industry awards

Managing cyber risk through automation and data-powered insights.

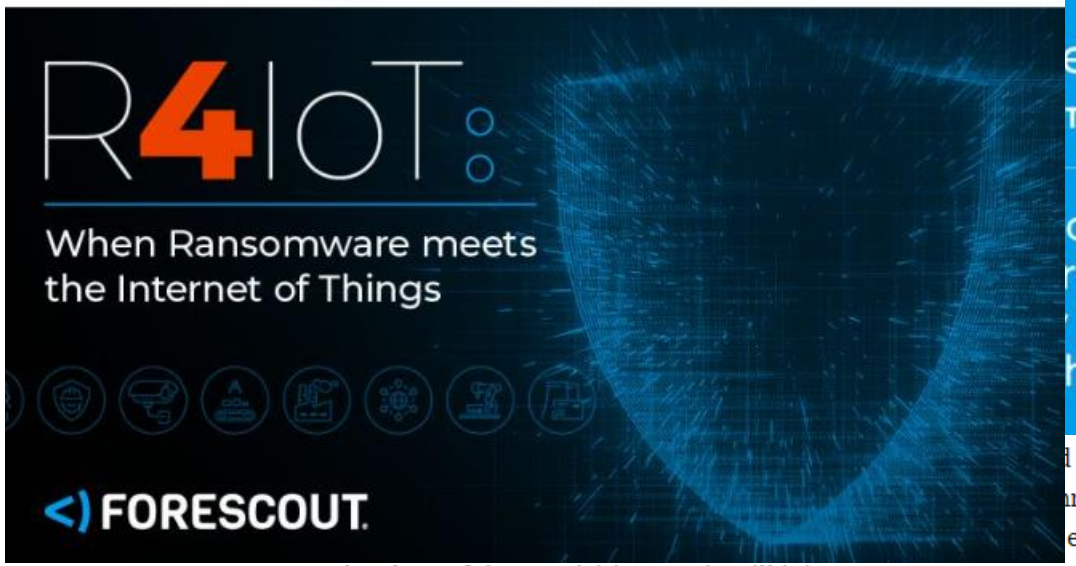
Security Networking Management

Research and investments

Forescout Announces Intent to Acquire Cysiv to Deliver Data-Powered Threat De

Forescout Technologies Inc.
38.1K followers
6d •

Today, Forescout's **Vedere Labs** released a new report that includes a detailed playbook describing how organizations can protect themselves against a new type of ransomware that exploits IoT devices, such as video cameras, to deploy...



Upon the close of the acquisition, Cysiv will join Forescout.

Forescout Technologies Inc.
vers

scout Company has won the 2022 Fortress Cyber Security
s in Leadership! The industry awards program sought to
the world's leading companies and products that a ...see more

l IoMT
reat
efficiently.

Vedere Labs

39 Billion
Unique Data Points

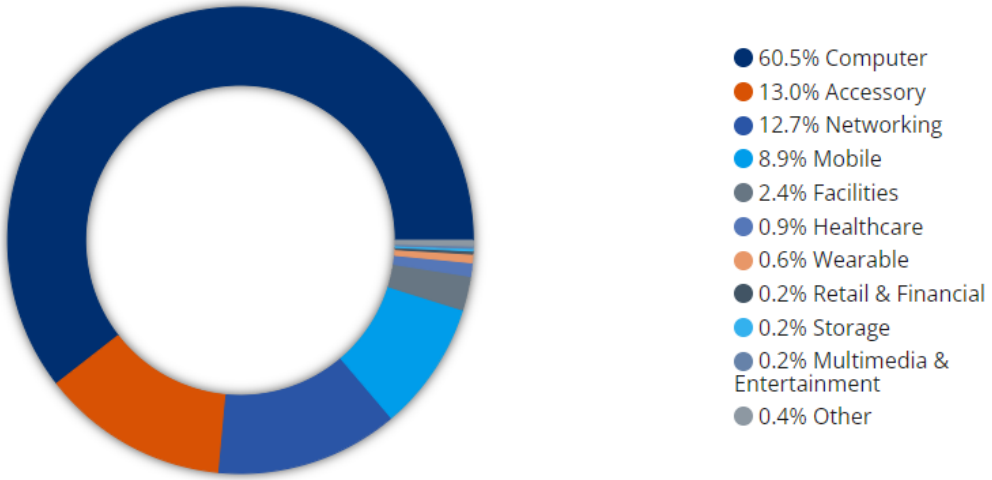
18.7 Million
Unique Device Profiles

8132
Unique Vendors

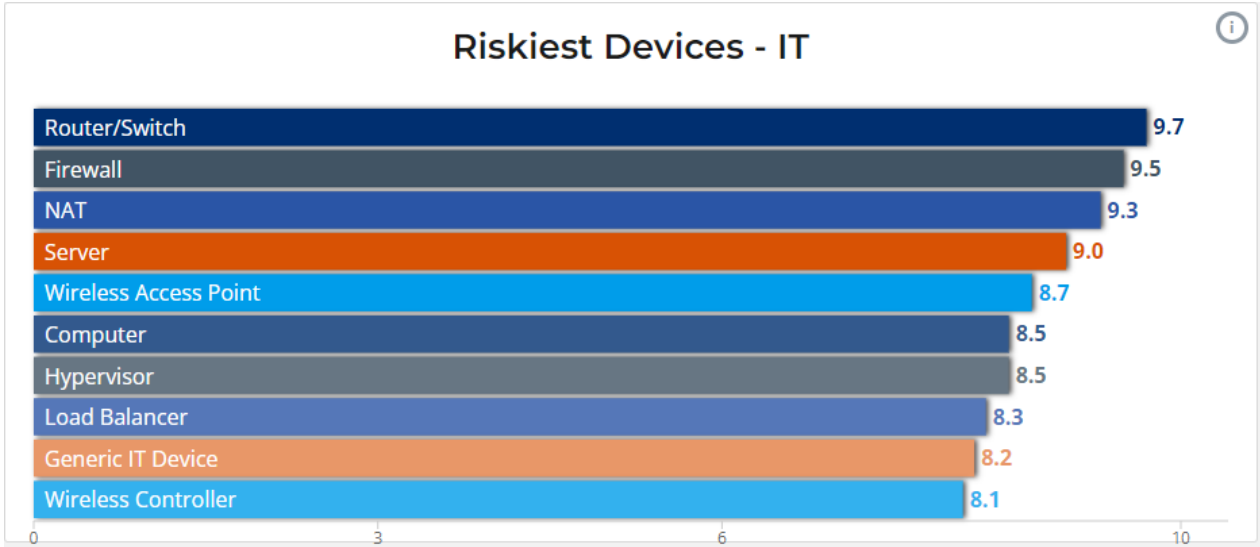
2014
Unique OS Versions

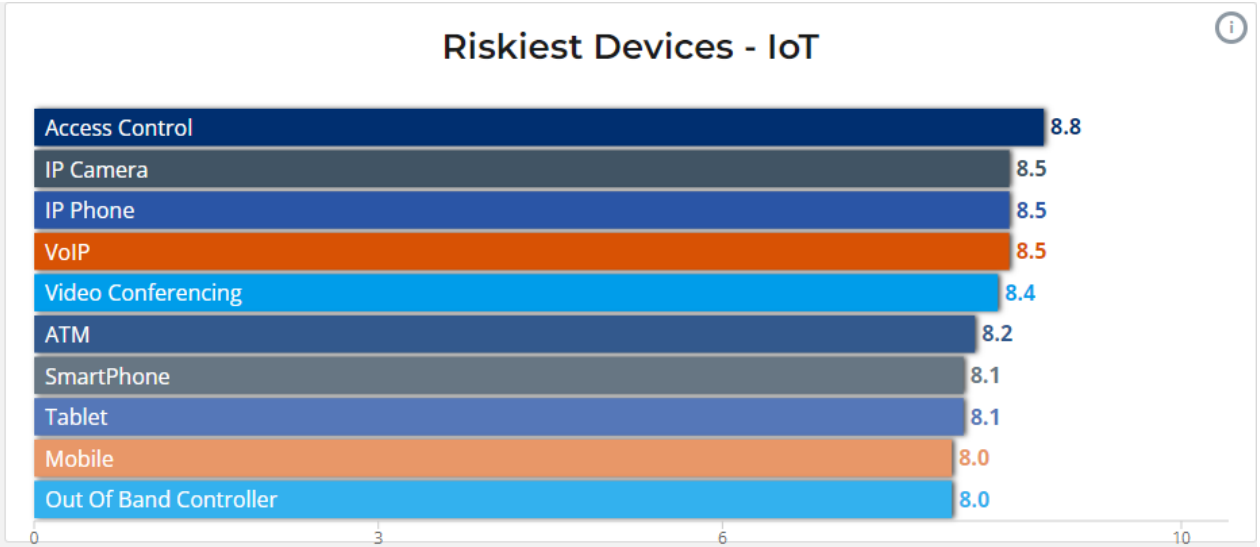
Device Ecosystem

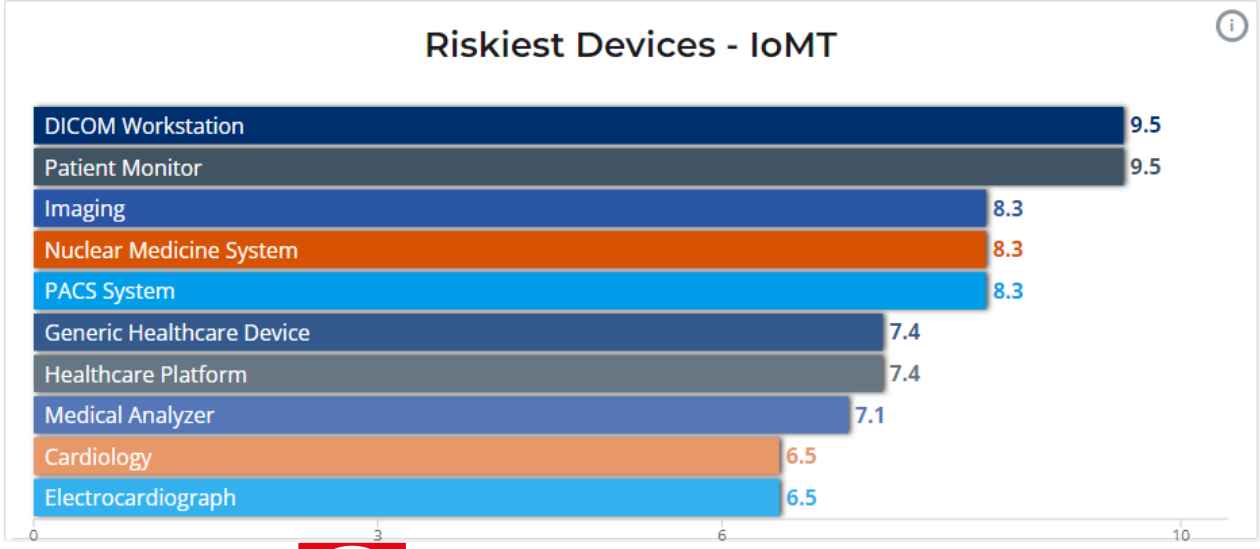
Device Functions

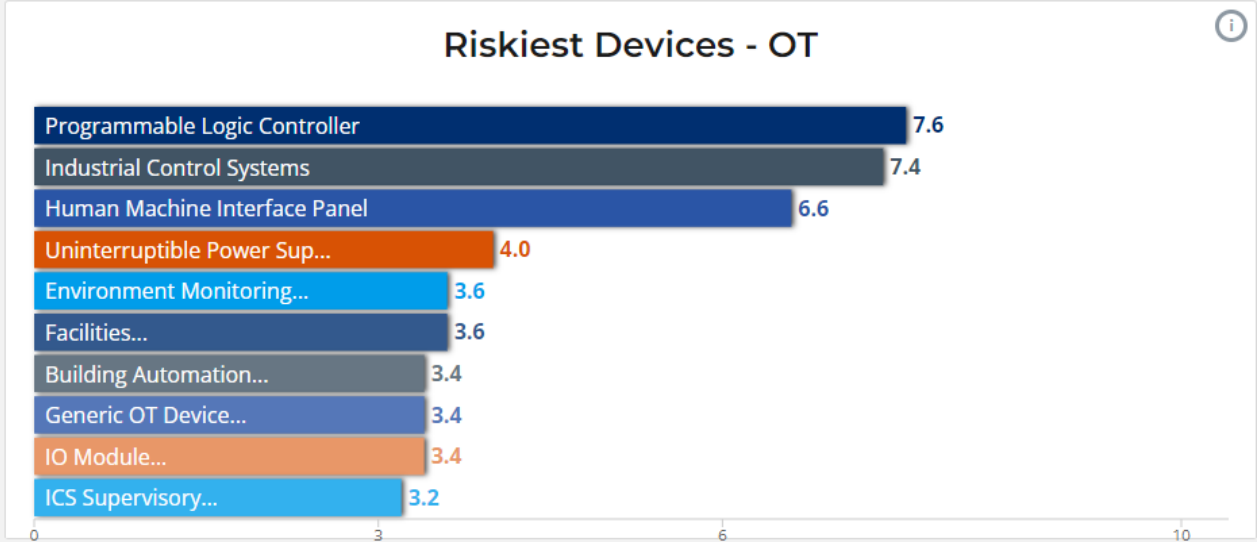


Vedere Labs


Riskiest Devices - IT
Router/Switch 9.7
Firewall 9.5
NAT 9.3
Server 9.0
Wireless Access Point 8.7
Computer 8.5
Hypervisor 8.5
Load Balancer 8.3
Generic IT Device 8.2
Wireless Controller 8.1
0
3
6
10


Riskiest Devices - IoT
Access Control 8.8
IP Camera 8.5
IP Phone 8.5
VoIP 8.5
Video Conferencing 8.4
ATM 8.2
SmartPhone 8.1
Tablet 8.1
Mobile 8.0
Out Of Band Controller 8.0
0
3
6
10


Riskiest Devices - IoMT
DICOM Workstation 9.5
Patient Monitor 9.5
Imaging 8.3
Nuclear Medicine System 8.3
PACS System 8.3
Generic Healthcare Device 7.4
Healthcare Platform 7.4
Medical Analyzer 7.1
Cardiology 6.5
Electrocardiograph 6.5
0
3
6
10


Riskiest Devices - OT
Programmable Logic Controller 7.6
Industrial Control Systems 7.4
Human Machine Interface Panel 6.6
Uninterruptible Power Sup... 4.0
Environment Monitoring... 3.6
Facilities... 3.6
Building Automation... 3.4
Generic OT Device... 3.4
IO Module... 3.4
ICS Supervisory... 3.2
0
3
6
10

Thank you

martin.vivodik@clico.sk