

# Mapovanie digitálneho terénu

09.06.2022  
Martin Vívodík  
Clico Security Consultant

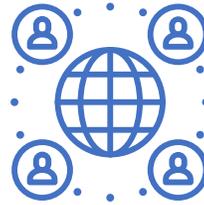


# Trends Impacting Your Digital Terrain

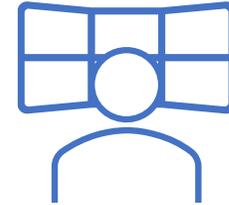
Growth of Assets & Threats



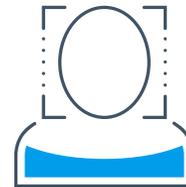
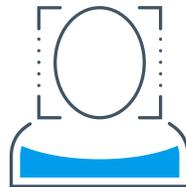
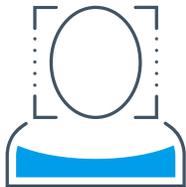
Distributed Enterprise & Anywhere Operations



Fragmented Solutions



Shortage in Cybersecurity Personnel

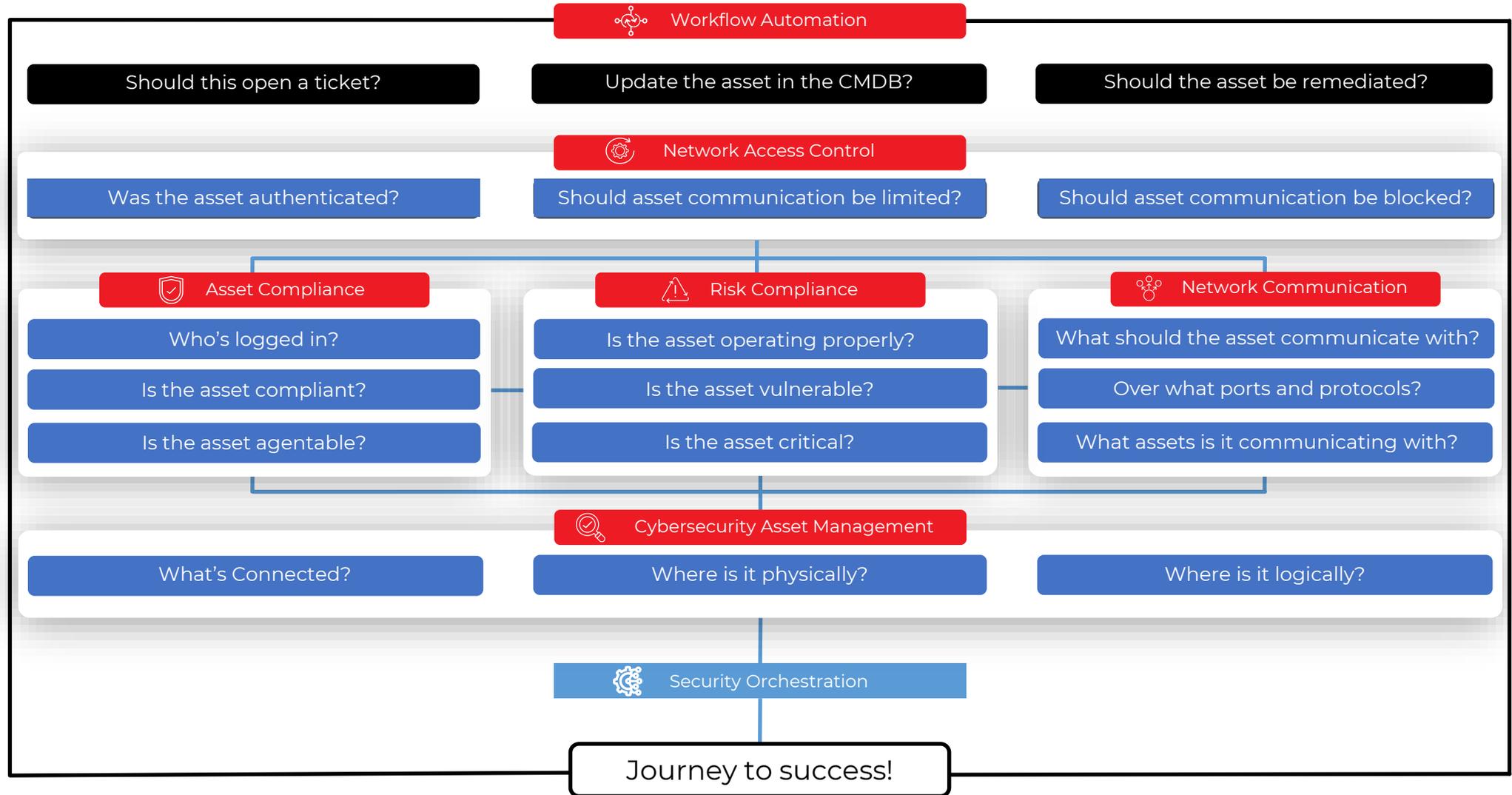


You Need A **Force Multiplier!**



# Much to Consider for Connected Assets

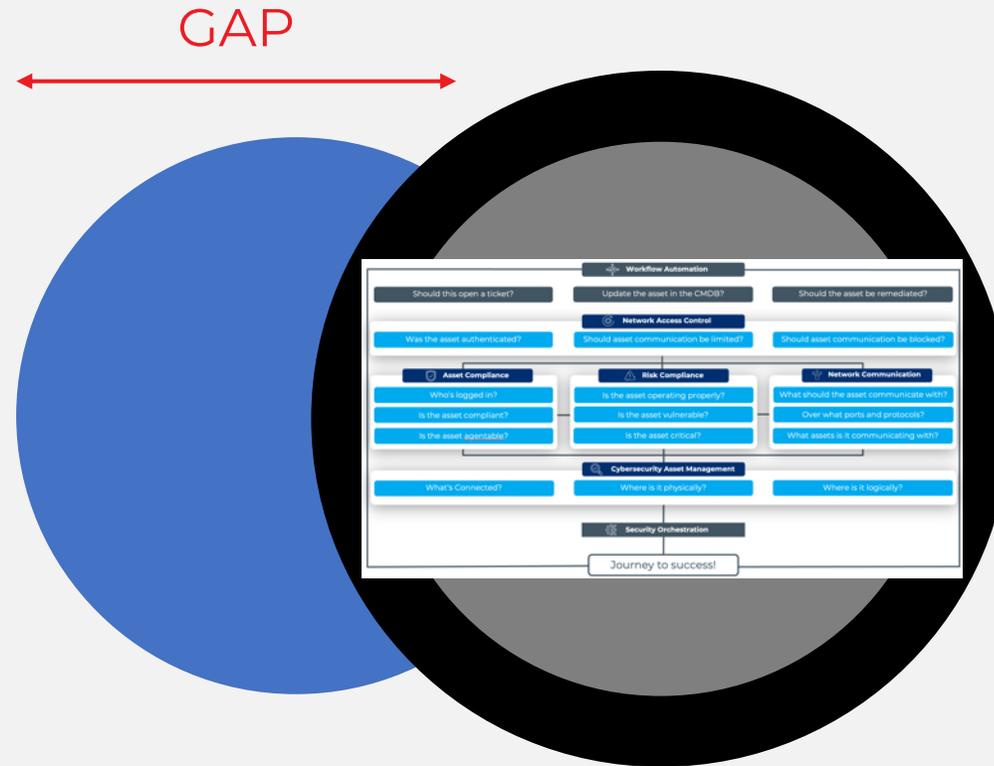
 Zero Trust  
 CIS Critical Controls  
 NIST  
 PCI DSS  
 NERC CIP  
 HIPAA



# Your Never-Ending Security Challenge?

## Constant Changes:

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



## Security Framework:

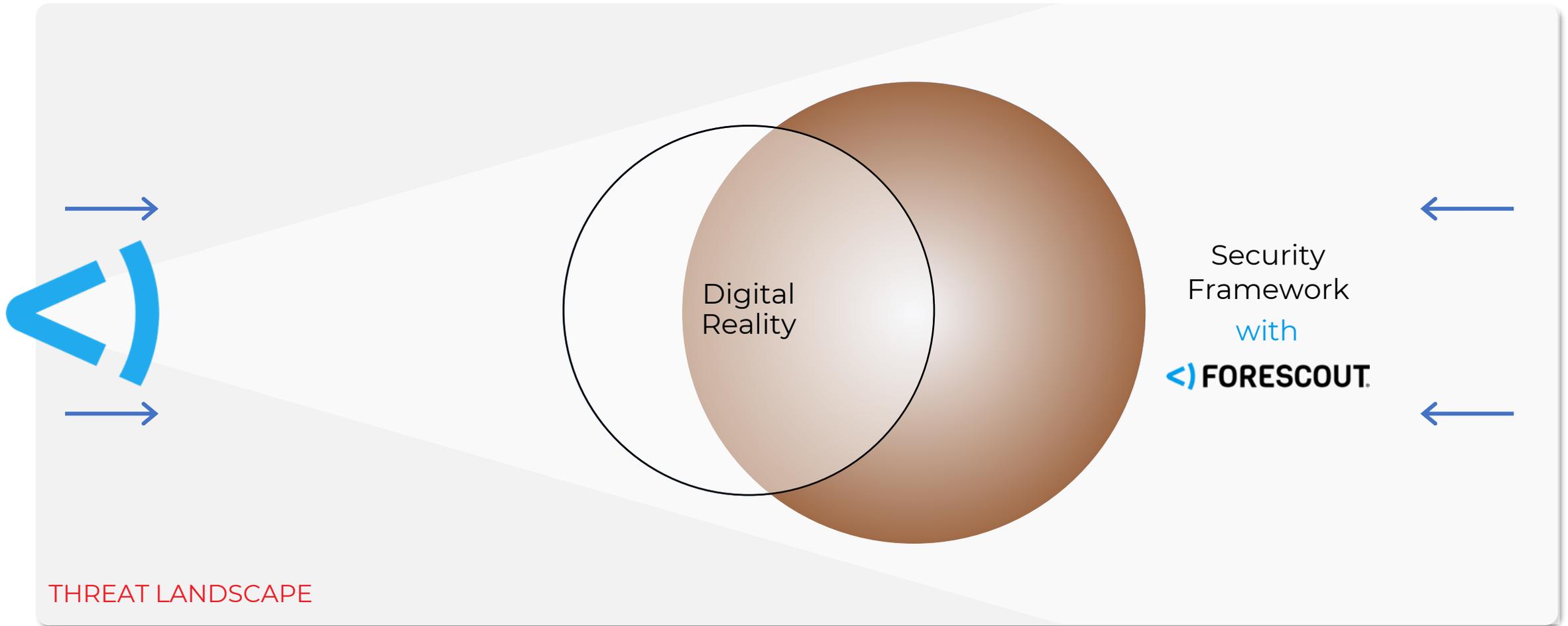
- Regulatory Compliance
- Security Policies
- Risk Management
- Security Tools

THREAT LANDSCAPE

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



# Your Never-Ending Security Challenge?

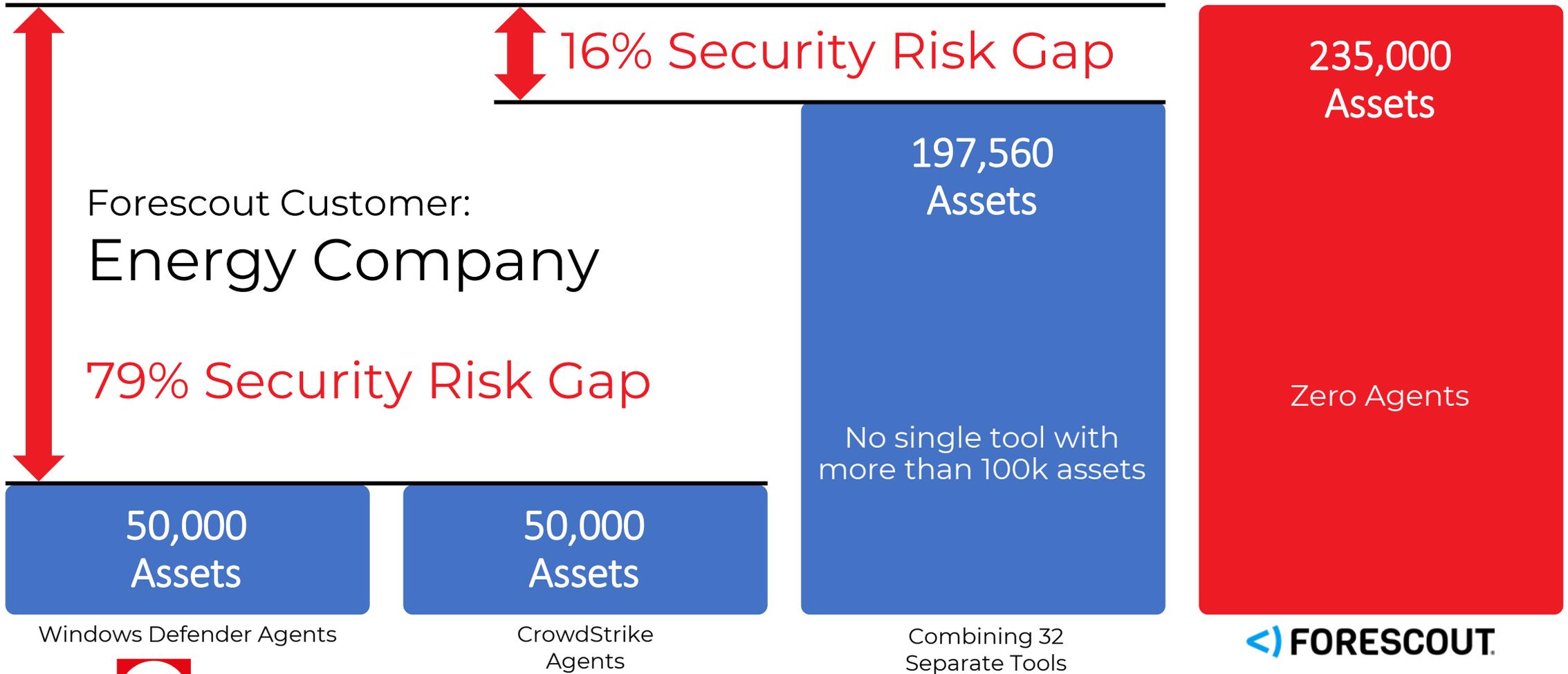


Forescout **Aligns** Your Digital Reality & Your Security Framework  
... and **Operates Continuously** to **Maintain Alignment**



# Real-World Example

Rapid time to value for a holistic view of all devices



**FORESCOUT**

# 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.**



Windows Defender Agents



CrowdStrike Agents



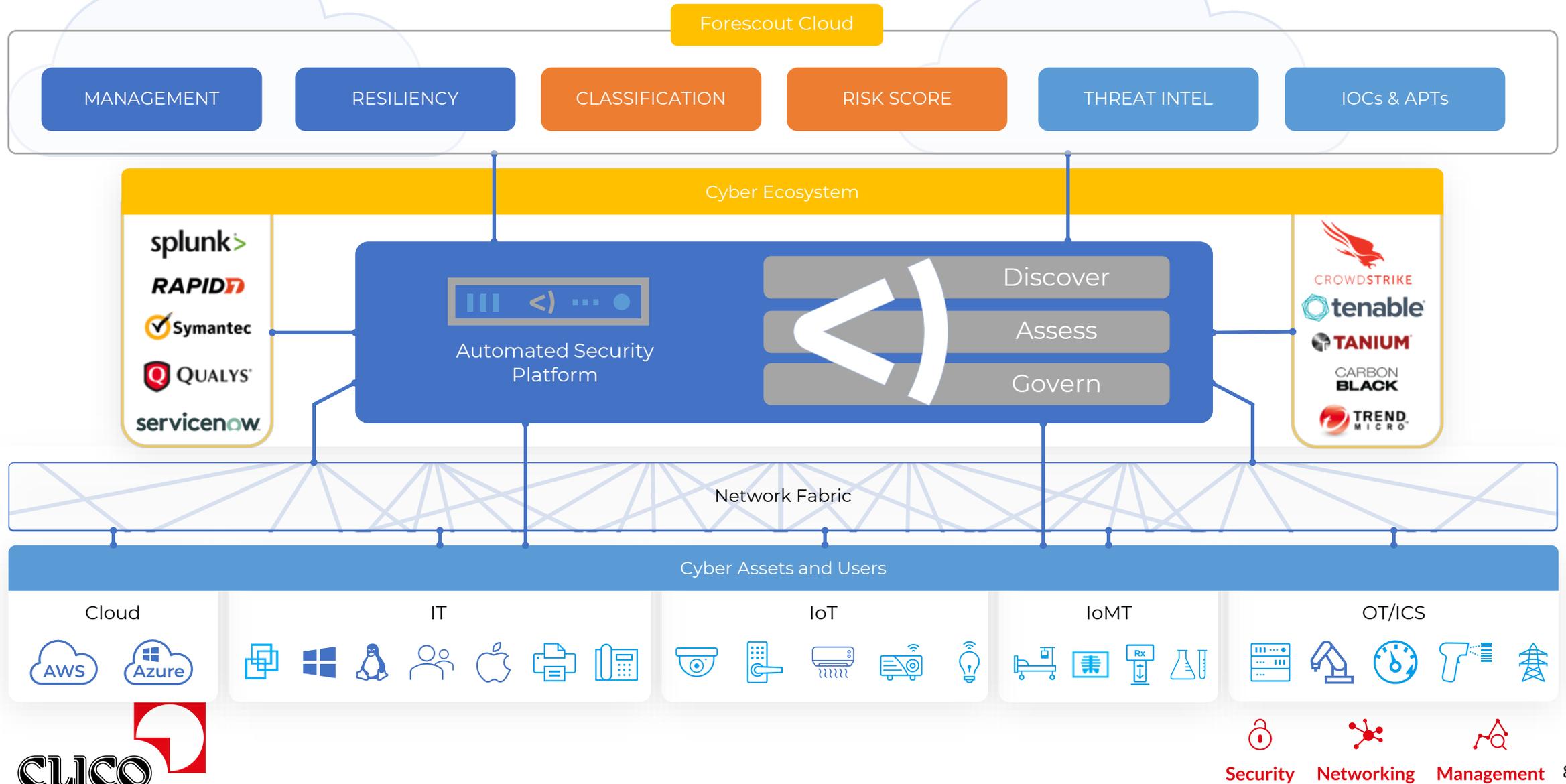
Combining 32 Separate Tools



 **FORESCOUT.**



# Forescout Continuum



# Connected devices under attacks

## MedC 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.

### Foxconn returning to normal

Tech manufacturing giant Foxconn is returning to normal after a ransomware attack crippled it last month.

The LockBit ransomware group claim they threatened to leak sensitive data from the Taiwanese company last month.

A spokesperson from the Taiwanese company said it is now back to normal. [new report.](#)

### Psychiatrická nemocnice v Kosmonosech

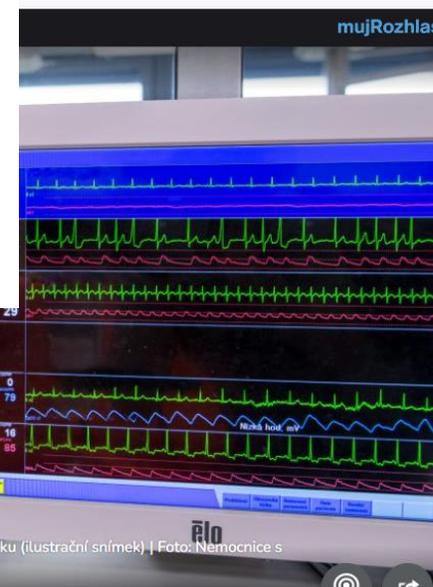
Následoval útok na psychiatrickou nemocnici, který proběhl jen o několik málo dnů později. 27. března došlo k ransomwarovému útoku, který s největší pravděpodobností zneužil slabá, nedostatečně zabezpečená místa na serverech. Útočníci se v takovém případě přihlásí, vypnou v zařízení bezpečnostní řešení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

held for ransom

as reportedly breached by a

nemocnice se potýká s následky

útku



ilustrační snímek | Foto: Nemocnice s

Jonathan Greig  
June 2, 2022

Cybercrime Malware

News Technology



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



## Discover all devices

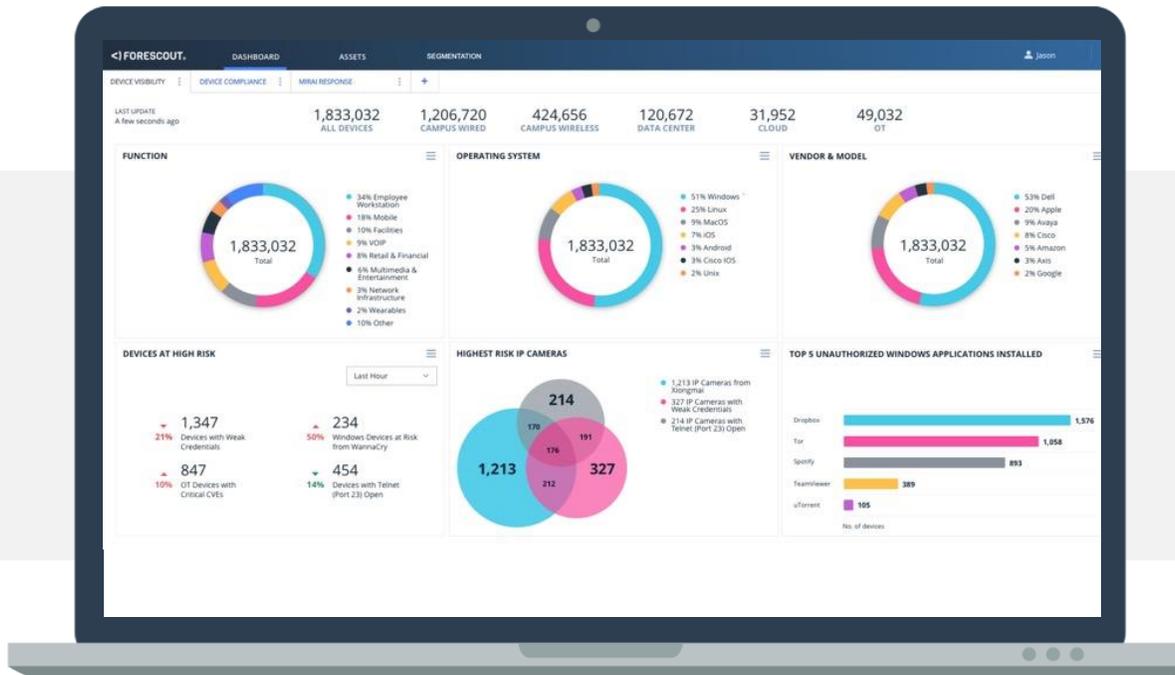
Inventory of all connected cyber assets with the industries most robust choice of 30+ techniques, without agents or disruption

## 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

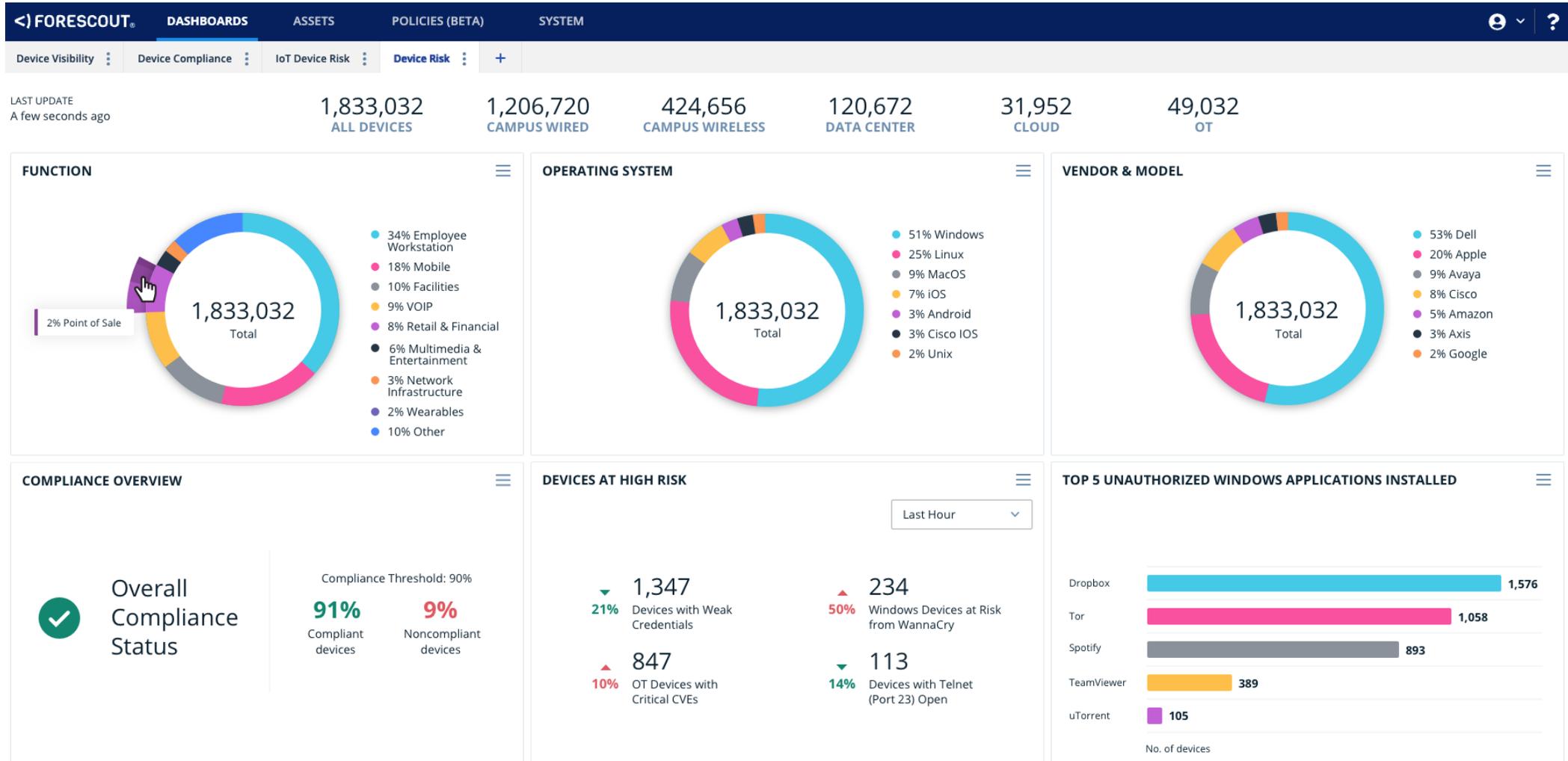


## Forescout Can Help

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



# Dashboards



# Detailed view

← GEVCT
Overview Network Analytics Cyber Risks Recalls

**CT**  
10.104.131.253  
Site Hospital3

[Quarantine](#) [Group](#)

[MDS2](#)

**Asset Attributes**

Category	Medical Device
Type	CT
Vendor	GE
Model	LightSpeed VCT
Equipment Function	6: Diagnostic - Other Physiological Monitoring
Classification Fidelity	High
MAC	18:60:24:88:EF:29
Location	Hospital3 > Building C > Floor 4 > Room 412
Serial Number	22558
Asset Tag	
Criticality	Critical
FDA Classification	Class II
Last Seen	04/19/2022 18:07
First Seen	12/24/2021 14:06
Last Vendor Access	04/19/2022 12:01
Last Scan Time	
Last Queried by	CyberMDX

**Taqs**

**Risk Assessment**

You are screen sharing Stop Share

**93** Critical

CMDX Score

**1** Vulnerabilities

**1** Threats

**1** Compliance Issues

Device	Software	Mitigations	Network
Criticality <b>Critical</b>	Outdated Version <span style="color: red;">❗</span> <a href="#">Yes</a>	Endpoint Protection	VLAN Type <b>MD Only</b>
PHI <b>Yes</b>	Default Credentials	Managed <span style="color: red;">❗</span>	Internet Connection <b>Yes</b>
Recalls <span style="color: red;">❗</span> <a href="#">Yes (10)</a>	Known Vulnerabilities <span style="color: red;">❗</span> <a href="#">Yes</a>		Threats Detected <span style="color: red;">❗</span> <a href="#">Yes</a>

**Take Action**

All Device Level Network Level Perimeter Level

**Blocklist**

Disabled ⚙️

**Risk Reduction**

Reduce Attack Surface

**Allowlist**

Disabled ⚙️

**Risk Reduction**

Reduce Attack Surface

**Update OS - Linux ker...**

To Do ⚙️

**Risk Reduction**

1 x Medium

**Network Context**

IP	10.104.131.253	MAC	18:60:24:88:EF:29
VLAN	20	NIC Vendor	HP
Subnet Name	Hospital3	Binding Expiration Ti...	
Connection Type	Wired LAN	Binding Source	

Security
 Networking
 Management
12

# Assess cyber asset compliance and risk hygiene, continuously.



## Asset compliance

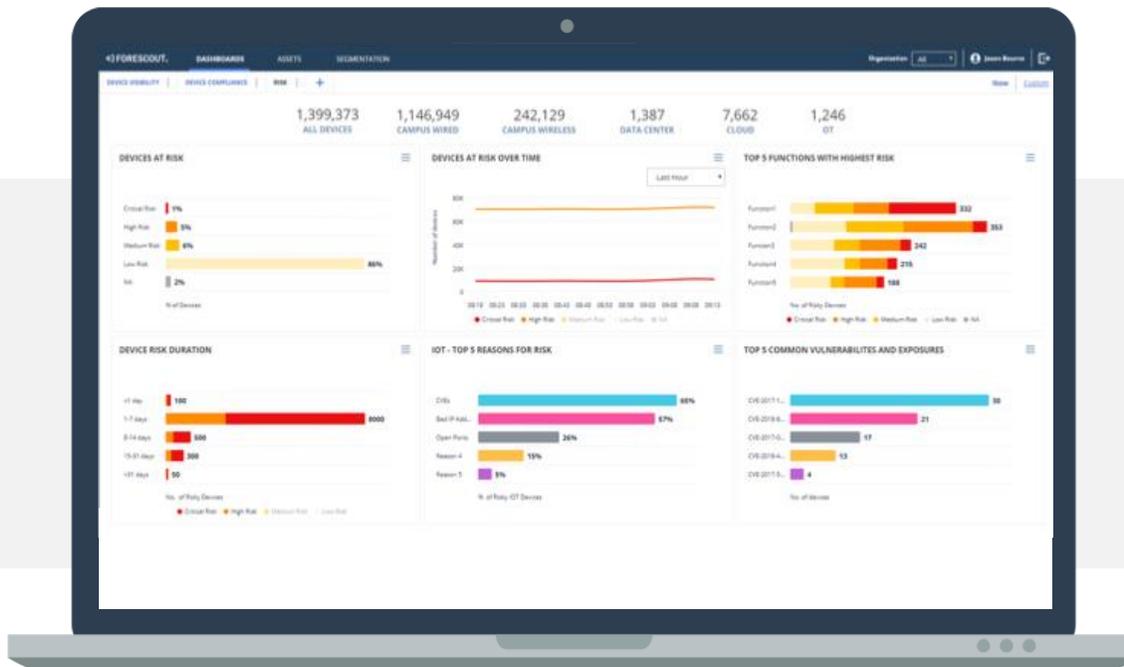
On-connect agentless validation of cyber asset state against security frameworks. Ensure security investments are deployed and running

## 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

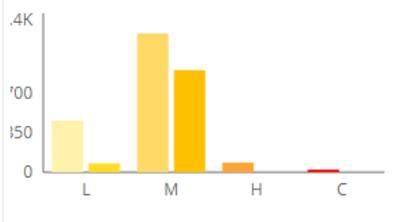


## Forescout Can Help

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

# Risk Scoring

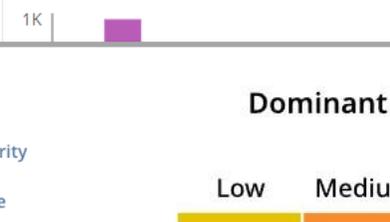
ASSETS PER RISK 2,048



VULNERABILITY INST... 1,464



ASSETS PER PURDUE ... 2,377



TOP PROTOCOLS 84



Filters: Roles IoT Device, IT De... Protocol Select

**Risk**

Risk Severity

Risk Score

Device Critic.

Risk Indicato

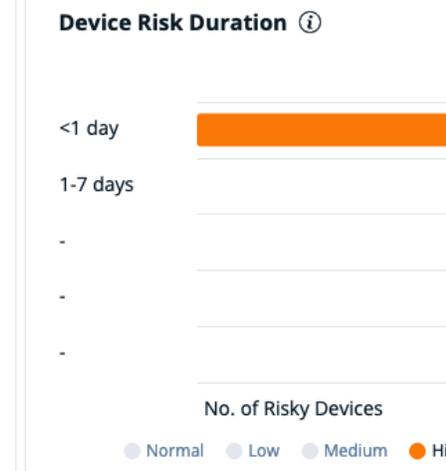
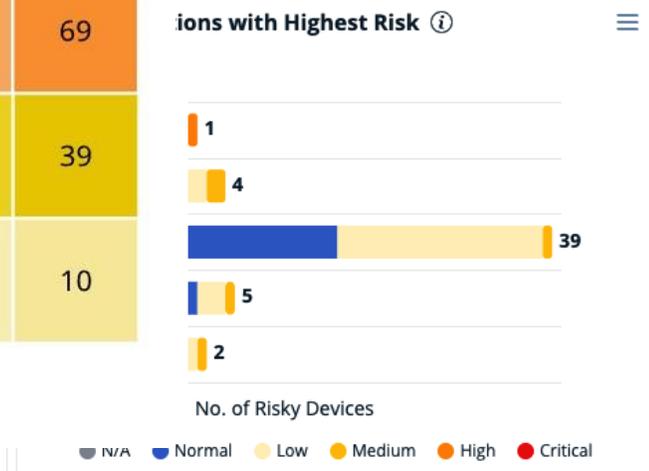
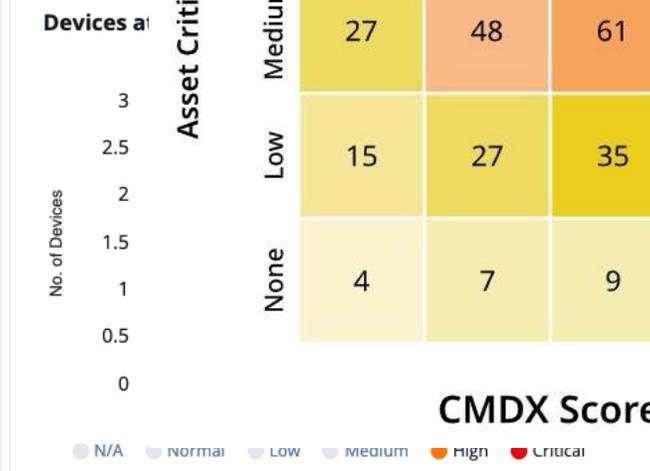
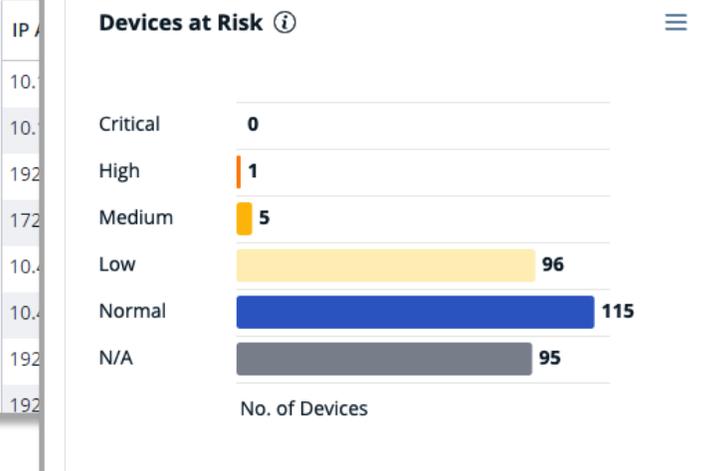
### Dominant & Auxiliary Risk

	Low	Medium	High	Critical
Critical	39	69	89	100
High	35	61	79	89
Medium	27	48	61	69
Low	15	27	35	39
None	4	7	9	10

es (20), Exposed Services (7)

ABILITY TITLE | VULNERABILITY SCORE

Internet Explorer code execution | 10



CMDX Score



# Device-Centric Risk Management

**Customize Risk Prioritization**

**Assign Case**

**Choose Mitigation Method**

**Add Notes for Documentation**

Severity	Score	Case ID	Vulnerability Group	Description
High	88	V-000311	CVE-2018-10...	BusyBox project BusyBox
High	88	V-000351	Microsoft RDP...	A bundle of BlueKeep and
High	88	V-000352	CVE-2019-0736	This device is possibly exp
High	88	V-000390	MDhex-Ray	Affected modalities are de
High	88	V-000605	Microsoft RDP...	A bundle of BlueKeep and
High	88	V-000606	CVE-2019-0736	This device is possibly exp
Medium	79	V-000101	CVE-2021-26...	Microsoft Windows Media
Medium	79	V-000280	CVE-2020-171...	Microsoft Windows Secur
Medium	79	V-000282	CVE-2020-17...	Windows NTFS Remote C
Medium	79	V-000642	CVE-2021-28...	Remote Procedure Call Ri
Medium	79	V-000649	CVE-2021-28...	Remote Procedure Call Ri
Medium	70	V-000085	CVE-2021-26...	Windows Event Tracing El

**Case ID: V-000390**  
MDhex-Ray | Ultrasound | GE Healthcare

**High**  
Score 88  
Status Active  
Category Medical Device  
Dwell Time (Days) 8  
Affected Assets 1  
Confidence High  
First Seen 04/14/2021 01:14  
Assignees Not Assigned

**Recommended Actions**  
For all affected devices, implement a network access policy that restricts the following TCP ports to only be available for GE maintenance servers: 21, 22, 23, 512. Read the full advisory by CISA. Contact GE Healthcare support and request that the credentials will be changed for all affected devices.

**Note**  
[Text Area]  
Cancel Save

**Additional Info**  
<https://us-cert.cisa.gov/ics/advisories/icsma-20-343-01>

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



## Proactive remediation

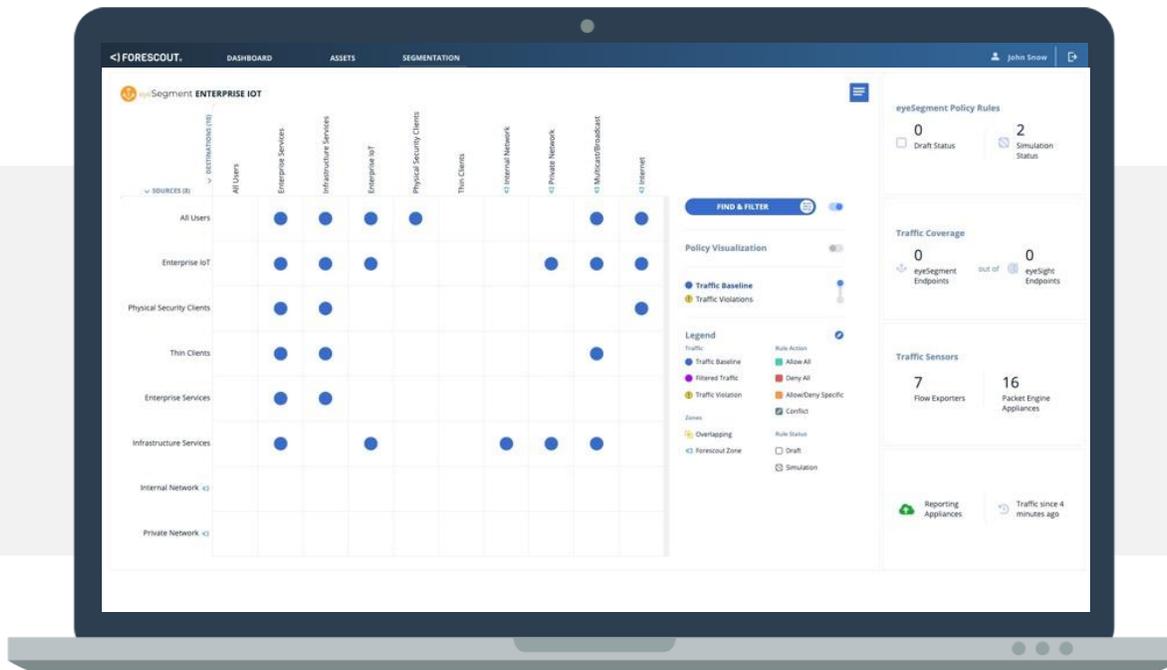
Correct misconfigurations with non-compliant cyber assets before they present challenges that require extensive triaging

## Pin-point controls

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

## Enforce Zero Trust security

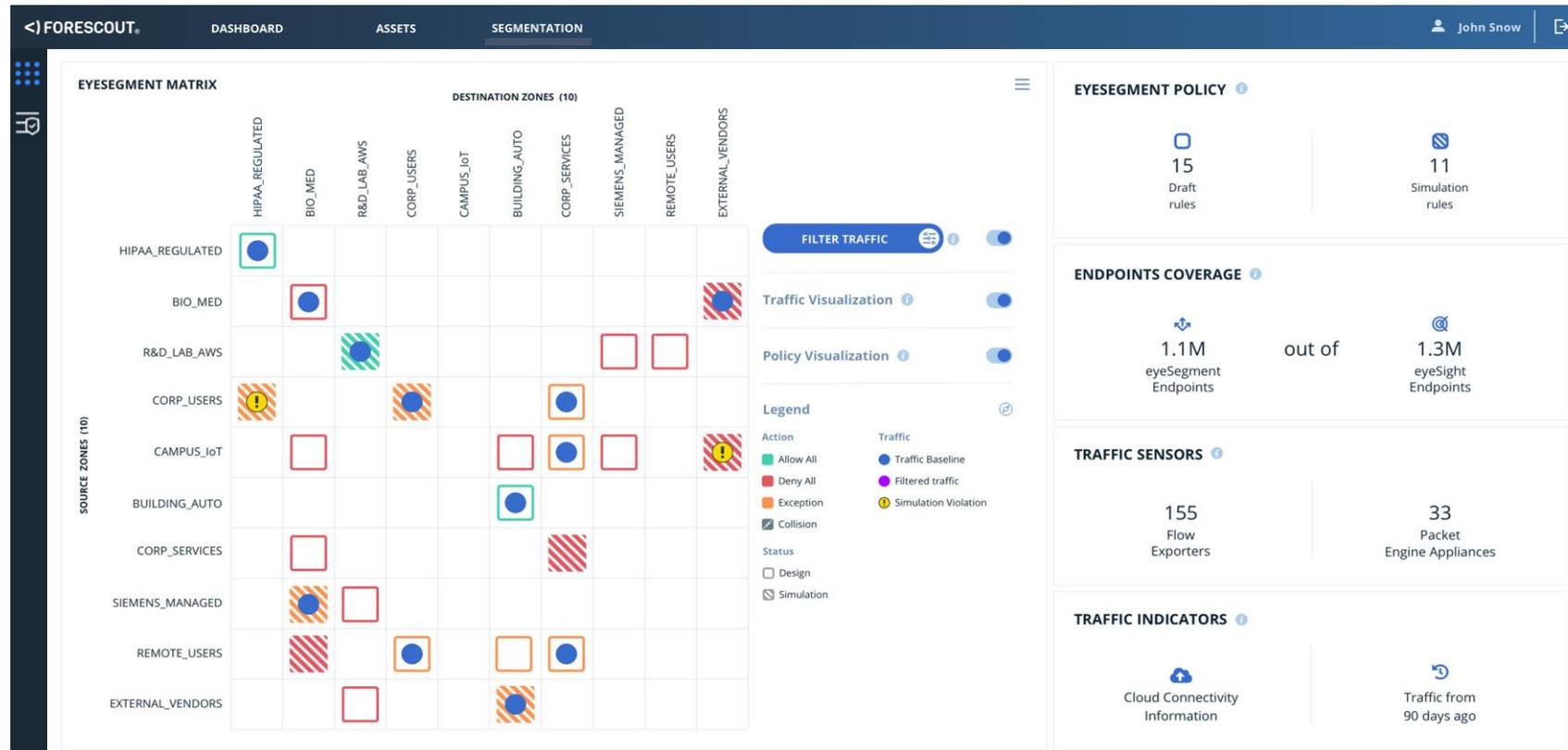
Implement least-privilege Zero Trust policies based on user, device, connection, posture and compliance for all cyber assets



## Forescout Can Help

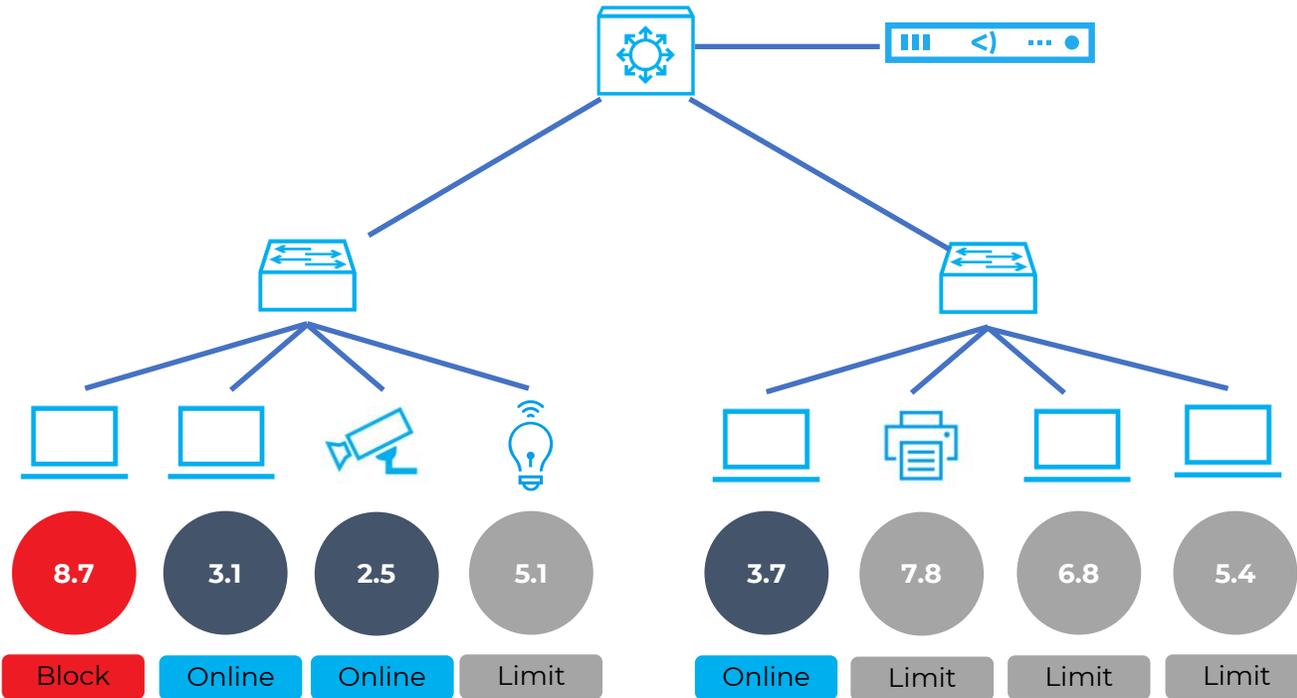
- Can you automatically remediate assets without human intervention?
- Can you limit blast radius... without negative impact?

# 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

CONNECT APPS

## 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

The screenshot displays a network management interface. At the top, a window titled 'Assign Net' shows a policy: 'Policy: 'Assign Network by CMDDB Profile'-->Sub-Rule: 'Corporate Network' -'. Below this, an 'Action' configuration window is open. The window title is 'Action' and it contains a search bar with 'palo' entered. A list of actions is shown on the left, with 'Firewall - Tag Endpoint' selected. The right pane shows the configuration for this action: 'This action adds a tag to the endpoint. The tag is then matched to Firewall Dynamic Address Groups'. Under the 'Parameters' tab, the 'Tag' field is set to 'CT-Restrict'. Below this, there are radio buttons for 'Specify one or more Firewalls': 'Send to all firewalls' (selected) and 'Send to specific firewalls' (with a dropdown arrow). At the bottom of the window are 'Help', 'OK', and 'Cancel' buttons.

# Automated response

The screenshot displays the configuration window for a Palo Alto Networks rule named 'Palo Alto restricted Hosts'. The window is titled 'Policy: 'Palo Alto restricted Hosts' --> Main Rule -'. It is divided into three main sections: Condition, Actions, and Advanced.

**Condition:** A host matches this rule if it meets the following condition:  
All criteria are True (dropdown menu)  
Criteria: IPv4 Address - 10.0.1.3

**Actions:** Actions are applied to hosts matching the above condition.  
A table lists the actions:

Ena...	Action	Details
<input checked="" type="checkbox"/>	Firewall - Tag Endpoint	Firewall - Ta...

**Advanced:**  
Recheck unmatched: Every 8 hours, All admissions  
Recheck matched: Every 8 hours, All admissions

Buttons: Help, OK, Cancel (at the bottom of the window)

# Automated response

Members Count  
dynamic

### Address Groups - CT-Restrict

2 items

Address	Type	Action
10.0.1.3	registered-ip	Unregister Tags
CT-Restrict	dynamic-group	

Close

# 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.

# Research and investments

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

Forescout Technologies Inc. vers



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.

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



IoT  
great  
efficiently.

# Vedere Labs

**39 Billion**

Unique Data Points

**18.7 Million**

Unique Device Profiles

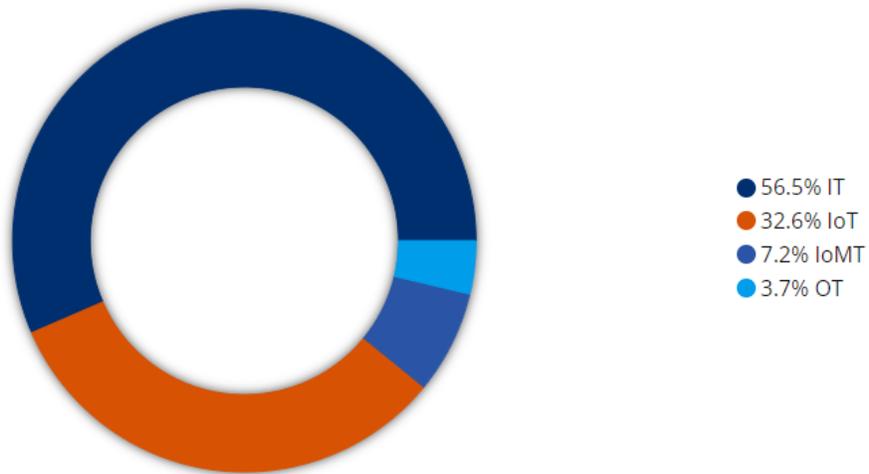
**8132**

Unique Vendors

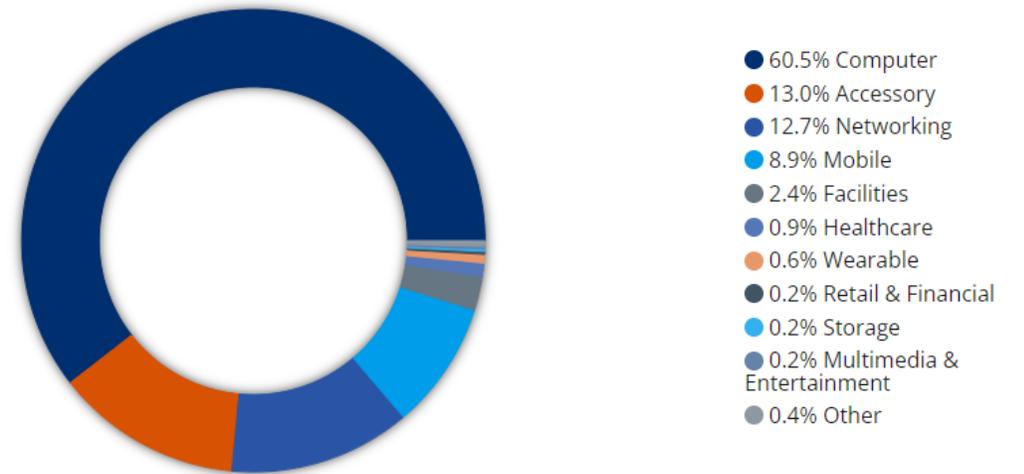
**2014**

Unique OS Versions

Device Ecosystem

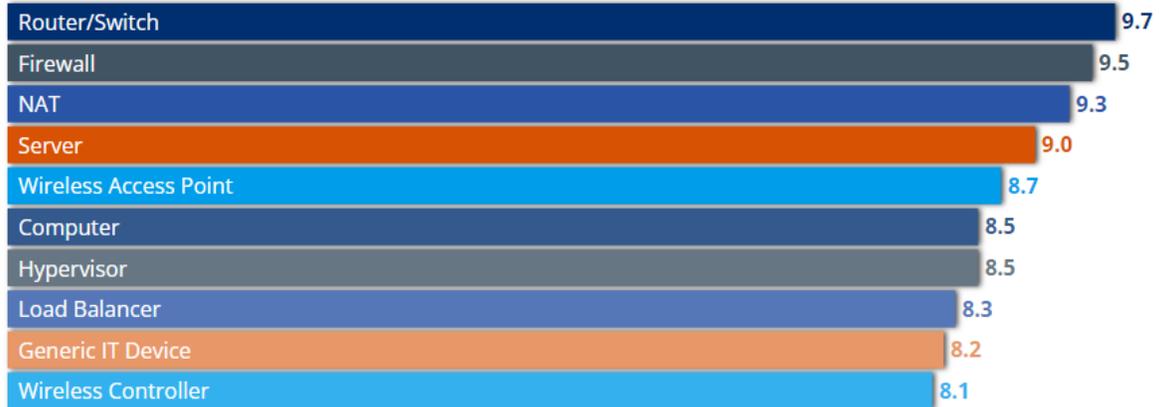


Device Functions

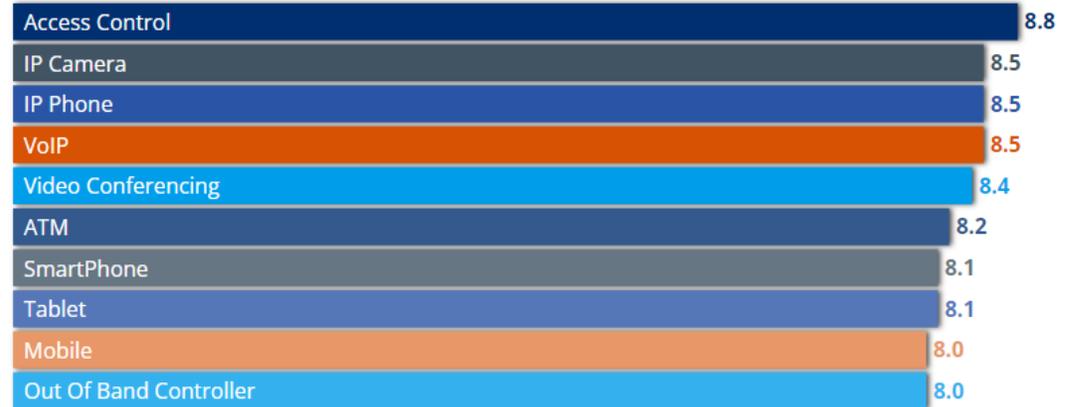


# Vedere Labs

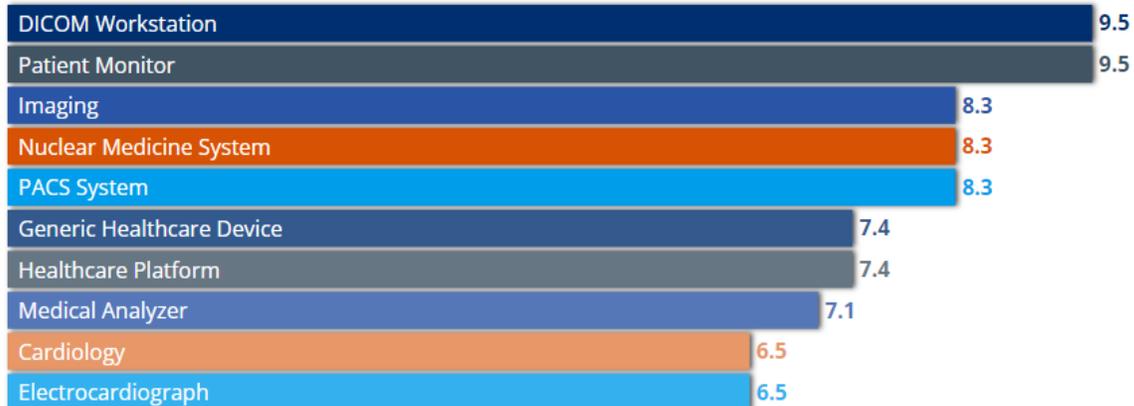
## Riskiest Devices - IT



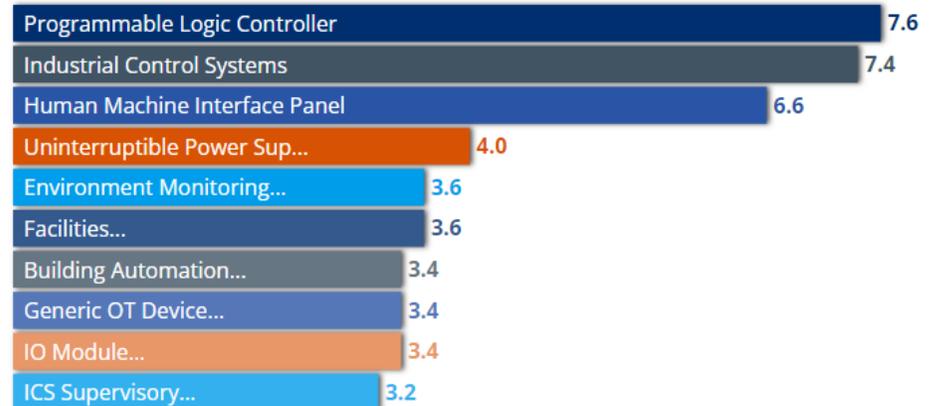
## Riskiest Devices - IoT



## Riskiest Devices - IoMT



## Riskiest Devices - OT



# Thank you



[martin.vivodik@clico.sk](mailto:martin.vivodik@clico.sk)