FORESCOUT CLOUD

Proof of Value Risk Report

Executive Summary

29th January 2024

Continuously identify, protect and ensure the compliance of your cyber assets

Committed to your Success

Introduction from Barry Mainz, CEO, Forescout

In today's interconnected world, our cybersecurity industry goes beyond just creating products. It's about building trust, ensuring the effectiveness of our solutions, and ultimately empowering the seamless continuity of business operations.

Here at Forescout, we understand the significant responsibility your organization carries. You're tasked with securing an ever-evolving landscape from threat actors and ensuring compliance with regulations. We recognize the delicate balance needed for continuity while facing these challenges.

This is where our mission aligns with your goals. Forescout is committed to continuously identifying, protecting, and ensuring compliance for all digital assets within your organization.

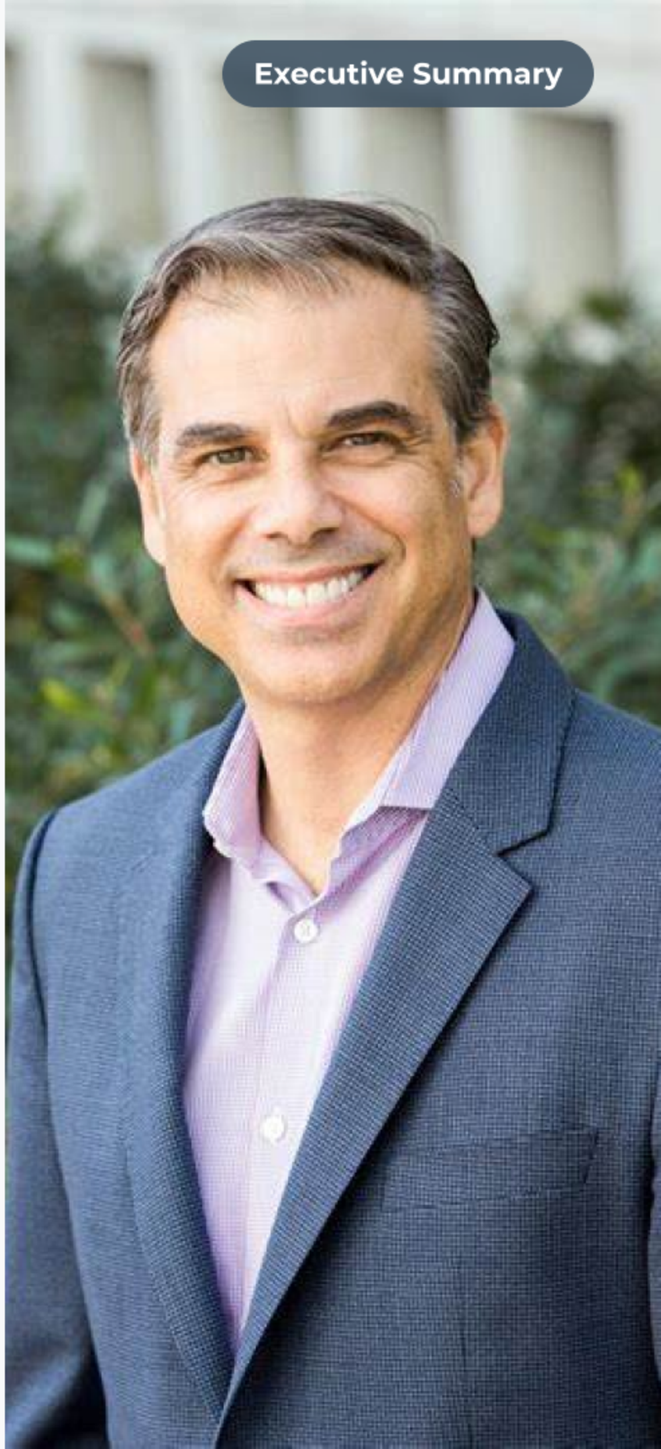
Our approach is not just reactive but proactive, aiming to secure your network preemptively, providing a comprehensive shield that adapts to emerging risks.

With Forescout as your partner, I'm confident that we can strengthen your organization's defenses and successfully navigate the challenges ahead.

I am sincerely thankful for the opportunity you've given us to showcase our capabilities through this proof of value.

Thank you for entrusting us with this crucial task.

> "Forescout is committed to Identifying, protecting, and ensuring the compliance of every cyber asset, continuously: IT, OT, IoT, IoMT."



Risk and Exposure **Management**

Identify, Quantify and Prioritize Risk and Compliance

The attack surface is expanding, driven by the growth of shadow IT, hybrid work environments and cloud adoption.

The rate of expansion continues to outpace network and security teams' ability to safeguard organizations and their high-value digital assets. Obsolete technology, unpatched vulnerabilities and other "low-value" IT assets are often forgotten but make for easy targets.

Malicious actors leverage these weak points to compromise the network and spread laterally to higher value assets.

This is where our mission aligns with your goals.

Forescout is dedicated to continually identifying, protecting, and ensuring the compliance of all digital assets within your organization.

Our approach is designed to preemptively secure your network, offering a comprehensive shield that evolves in tandem with emerging risks.

Forescout tracks the effectiveness of response actions across your security ecosystem to reduce your risk posture and exposure state, using an automated risk-based approach to remediate vulnerabilities.

Visit **www.forescout.com** to learn more about Forescout's approach to risk and exposure management and request a demo.

Risk and Exposure Management

Your Attack Surface

What's the attack surface that I'm securing?

Maintaining comprehensive visibility over all connected devices is the first step towards understanding the internal attack surface

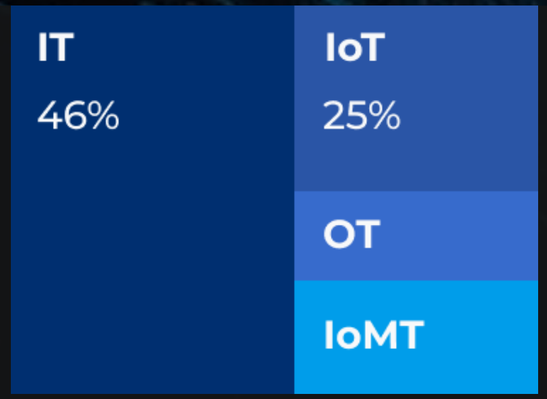
From new devices within the environment that require securing or segmentation, to understanding the devices within the shadow IT organization, recognition of their function and purpose allows the mitigation of emerging threats within the environment.

This fundamental practice allows the creation of an effective security strategy.

57,289

Total Devices

Utmo has a total device count of 57,289, which is higher than the expected device count for an organization of its size.



Device Composition

Utmo's device composition is dominated by IT devices, with 26,353 devices. IoT devices are the second most common, with 14,322 devices. IoMT devices are the third most common, with 9,652 devices. OT devices are the least common, with 6,875 devices.

87

Unknown Devices

Less than 1% of devices on the network are unknown. This is good. Unknown devices can pose a security risk as they may not be properly configured or patched, making them more vulnerable to attack. It is important to identify and classify all devices on the network to ensure that they are properly secured.

752

New Devices (Last Week)

The total number of devices increased by 1.3% from 56,537 to 57,289. The most significant change was in the OT category, which increased by 8% from 6,366 to 6,875 devices.

782

Missing Devices (Over a Week Offline)

There are 782 missing devices that have not been seen in the environment in the last week. Missing devices can pose serious security risks, such as data breaches and vulnerability to cyber-attacks. It is important to investigate these devices to ensure the security of the environment.

9,821

Guest Devices

There are 9,821 devices connected to the guest network. It is recommended that the guest network be separate from the corporate network, if it is not already. This will help to improve security by preventing unauthorized access to the corporate network.

348

Rogue Devices

There are 348 rogue devices on the network. These devices are not registered and cannot be managed, which poses a significant security risk. Rogue devices can be used to launch attacks on the network, steal data, or disrupt operations.

> Last week saw an 8% rise in new endpoints that are primarily OT devices. These devices are primarily seen in Chicago, IL and in the network segment "Chicago Factory"

Securing the Enterprise

What Risks are inherent within my network?

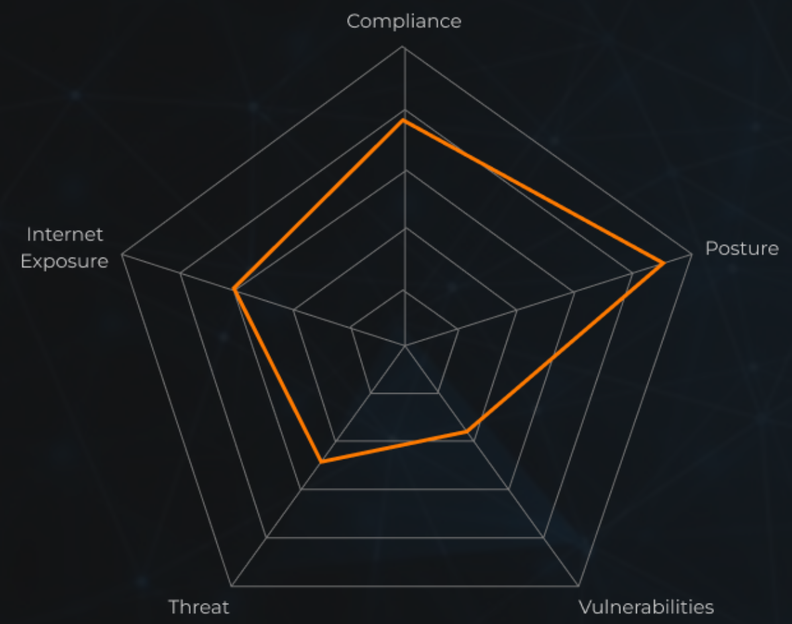
Understanding the risks of devices connected to the Utmo network is an essential part of proactively preventing security hygiene and posture.

Forescout assesses internal risks as non-compliant devices, posture, vulnerabilities, threat activity and internet exposure. The criticality of these devices are also factors of consideration in understanding the risks as they represent a larger business impact.

This is vital in maintaining a robust and secure environment

65 B

Organizational Risk



The overall risk score is impacted positively by the high scores in compliance for IT and posture of IoT. However, the low scores in vulnerabilities and internet exposure pose significant security risks. The low vulnerability score indicates that the company is susceptible to attacks, while the low internet exposure score indicates that the company's systems are not well-protected from external threats.

78 Compliance — B

Utmo's compliance for IT score is above average. The company has implemented several security measures that are working well. However, there is still room for improvement. The company should focus on improving its patching schedule and ensuring that all endpoints are registered within management systems.

92 Posture — A

Utmo's IoT posture is strong, with only 4% of endpoints having open Telnet ports and 3% of endpoints having expired or self-signed certificates. This indicates that Utmo is taking appropriate steps to secure its IoT devices. However, there is still room for improvement, as even a small number of open ports or expired certificates can create security risks. Utmo should continue to monitor its IoT devices and take steps to close any open ports and update any expired certificates.

39 Vulnerabilities — D

Utmo's vulnerabilities score is low, indicating that the company is at risk of being exploited by attackers. The critical CVEs that were discovered are related to remote code execution and denial of service attacks. Utmo should prioritize patching these vulnerabilities and implementing additional security measures to protect its systems.

50 Threats — C

Utmo's threat score indicates that there are some security risks that need to be addressed. To improve the score, Utmo should consider implementing additional security measures, such as network monitoring and intrusion detection systems. If Utmo has these systems in place, telemetry from them can be integrated into Forescout to improve the threat score.

66 Internet Exposure — B

Utmo's Internet exposure score is below average. There are unnecessary communications with the internet, especially endpoints that are accessible from the internet. This can lead to security risks. To improve the score, Utmo should reduce unnecessary communications with the internet and make sure that endpoints are not accessible from the internet.

> Utmo should focus on mitigating the vulnerabilities as a result of Cisco Unity Connected flaw (CVE-2024-20272). Additionally, there are indicators of potential threat activity surrounding these devices.

Forescout Research Sierra:21

Supply Chain Vulnerabilities in IoT/OT routers

"SIERRA:21 - Living on the Edge" features research into Sierra Wireless AirLink cellular routers and some of its open-source components, such as TinyXML and OpenNDS.

This research details specific attack scenarios as well as potential mitigation techniques.

Forescout Vedere Labs studies where attackers are working towards by observing actual attacks in our sandboxes, on the Darknet and in our Adversary Engagement Enviornment.

21

new vulnerabilities that affect OT/IoT routers

These will increase the risk exposure to critical infrastructure. The affected products are prevalent in multiple industries, particularly healthcare and manufacturing, but also technology, financial services, governement, and power generation.

66%

vulnerabilities are in third party components

Highlighting the increasing threat posed by supply change vulnerabilities

245,000

networks worldwide running Sierra Wireless Routers

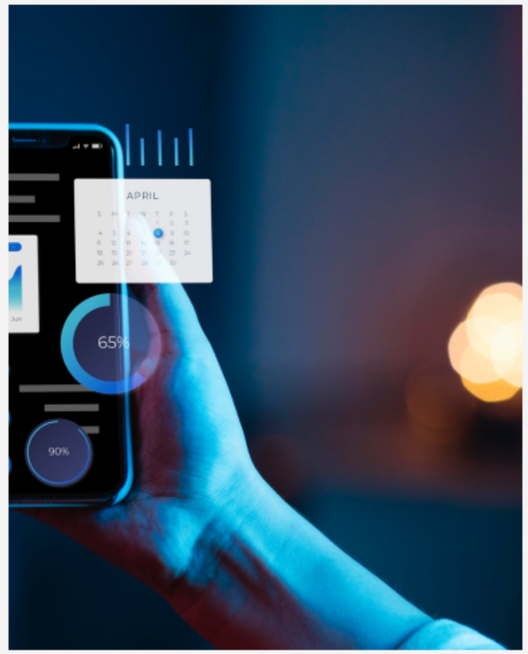
For example, Sierra Wireless routers are used for police vehicles connecting to a central network management system or to stream surveillance video, in healthcare facilities providing temporary connectivity.

86,000

vulnerable routers still exposed online

Less than 10% of these routers are confirmed to be patched against known vulnerabilities found since 2019.

These vulnerabilities allow attackers to steal credentials, take control of a router by injecting malicious code, persist on the device and use it as an initial access point into critical networks.



90%

of devices have reached end of life

Patching can't fix everything. 90% of devices exposing a specific management interface have reached end of life, meaning they cannot be further patched

It's an uphill battle to secure supply chain components. Open-source software elements continue to go unchecked and increase the attack surface of critical devices, leading to vulnerabilities that may be hard for organizations to track and mitigate.

Forescout Research Vedere Labs

> Vulnerabilities impacting critical infrastructures are like a open window for bad actors in every community. State sponsored actors are developing custom malware to use routers for persistence and espionage.

Threat and Research Intelligence

"Vedere" is the Italian word meaning "to see," which epitomizes the mission of Forescout Vedere Labs, the cybersecurity research arm of Forescout.

What We Do

Our team of global experts focuses on increasing visibility of cybersecurity threats and vulnerabilities for all connected asset types and providing mitigation steps organizations can use to protect themselves.

Our research is fed into the Forescout Platform and shared with the cybersecurity community including CISA and other cybersecurity agencies, CERTs, ISACs, open-source projects, device manufacturers, universities and other researchers.

How We Do It

Forescout Vedere Labs studies what attackers are working towards by observing actual attacks in our sandboxes, on the Darknet and in our Adversary Engagement Environment.

We analyze significant attacks and generate vulnerability and threat intelligence that is consumed by the **Forescout Platform**.

We also create corresponding detection rules that are added to **Forescout XDR** to help ensure customers can protect their IT, OT, IoT and IoMT environments.

Data Lots of Data

The threat intelligence data we analyze comes from millions of connected devices that we monitor that give us billions of data points about device configuration and network behaviour.

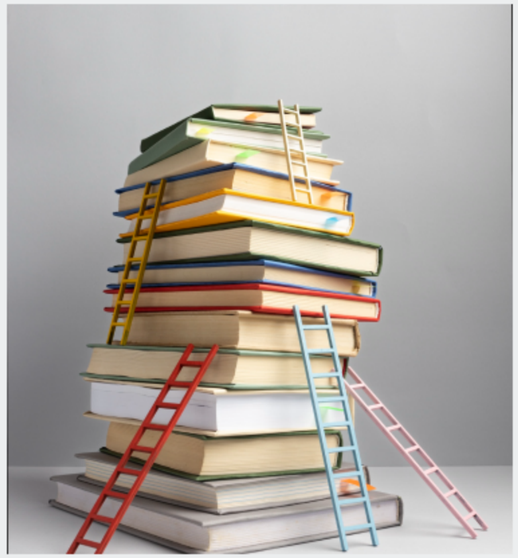
It also comes from attacks we observe and dissect and other sources we monitor

60%

are CVEs not included in CISA Known Exploited Vulnerabilities

Forescout Vedere Labs maintains a list of known exploited vulnerabilities

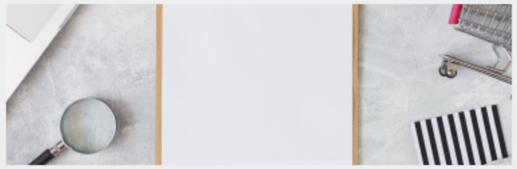
> Cybercriminals are also leveraging routers and related infrastructure for residential proxies and to recruit into botnets. Our discoveries reaffirm the need for heightened awareness of the OT/IoT edge devices that are so often neglected



Vulnerability Research

Focus on vulnerabilities against managed and unmanaged devices (IT/IoT/IoMT/OT)

- 200+ vulnerabilities discovered in last 5 years
- 89 unique known exploited vulnerabilities on unmanaged devices



Threats Report

Manual and automatic analysis of malware samples collected via customer telemetry and other sources

Threat Intelligence and Detection

Daily context-rich, machine-consumable threat feeds
Detection rules to keep our XDR solution on top pf emerging threats

About Vedere Labs

Located in Eindhoven, Netherlands, our research laboratory is where we observe firsthand the vulnerabilities being exploited and attacks in progress.
The information we collect is analyzed to generate threat intelligence, calculate **multifactor risk scores** and create **detection rules.**

Learn more about Vedere Labs