FORESCOUT

How to Secure Your Digital Terrain

Five Security Challenges

FORESCOUT

TABLE OF CONTENTS

Introduction

Cyber assets in today's hyperconnected environments are out of control. Both in terms of numbers (billions) and types (IT, OT, IoT, IoMT), they are exploding. Some are managed and known while others slip through unknown and undetected. As for device users, they are all over the map – literally. Employees, contractors, partners and customers all connecting to the data center or the cloud from anywhere, securely or otherwise.

All of this makes your digital terrain complicated : an ever-expanding attack surface that requires thoughtful planning and decisive action when it comes to securing connected assets.

What follows are the five key security challenges for today's CISOs and other security and operations leaders to consider, as well as pragmatic recommendations for putting these challenges in the rear-view mirror.

Challenge 1

How can you inventory and manage the explosion of unmanaged devices?

62% of survey respondents say their organizations do not have a complete inventory of their IoT/OT devices.

Ponemon Institute

Managed devices with security agents on board, such as corporate-owned PCs, laptops and smartphones, are becoming scarce compared to the billions of agentless IoT and operational technology (OT) devices joining networks. IT-OT network convergence is taking place at the same time. increasing productivity and streamlining network management but adding risk. Getting a handle on the attack surfaces of today's heterogeneous networks is harder than ever before.

Recommendations:

- Determine which tools can give you 100% connected asset visibility – no blind spots
- Narrow your selection process to only include solutions that can assess device poster agentlessly and in real time
- Empower security operations and IT staff with real-time asset inventorying capabilities

Challenge 2

In today's enterprise environment, where does risk reside?

"IP cameras, VoIP phone, video conferencing systems and medical imaging equipment represent the riskiest IoT device groups."

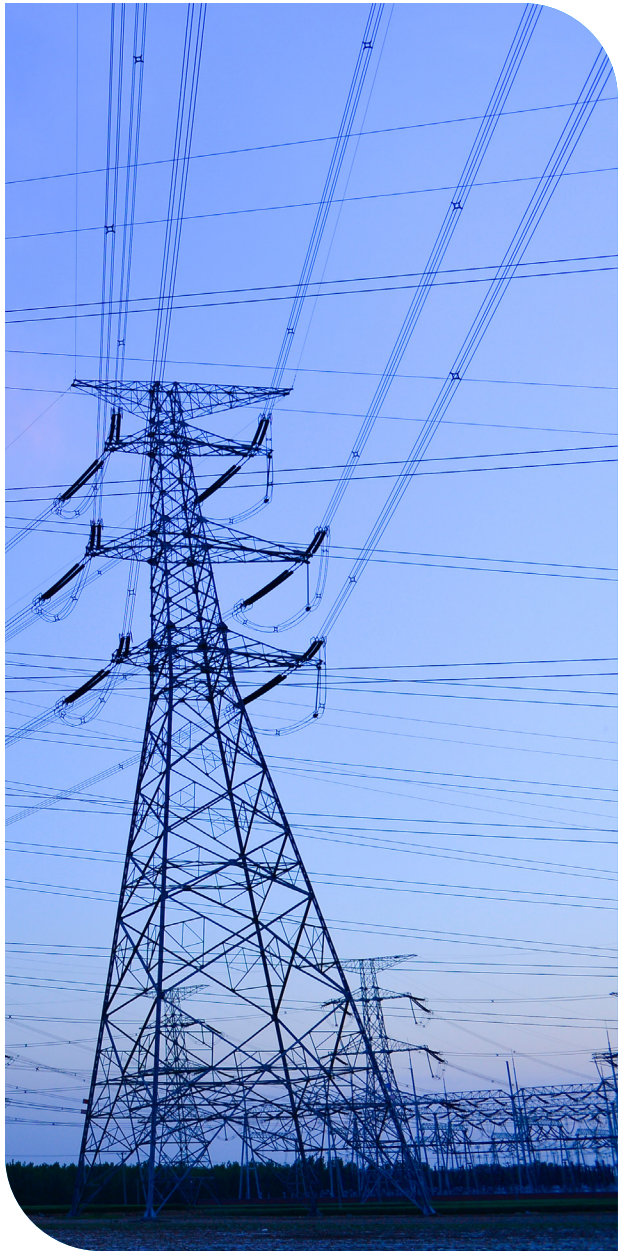
Vedere Labs

The concept of risk analysis is changing and expanding along with your attack surface. A recent Vedere Labs analysis determined that risk is spread across all device types. IT devices are still the main target of malware, including ransomware, and the main initial access points for malicious actors. But a growing number of IoT devices on enterprise networks are being actively exploited because they are harder to patch and manage than IT devices.

Programmable logic controllers (PLCs) and human machine interfaces (HMIs) are the riskiest OT devices because they are critical, allow for full control of industrial processes and are known to be" insecure by design." Connected medical devices are obviously risky because of their potential impact on healthcare delivery and patient safety.

Recommendations:

- Employ multifactor risk analysis to understand your attack surface
- Move to an active defense strategy that incorporates zero trust
- Accelerate threat response by prioritizing alerts according to the risk level
- And again, 100% device visibility is key



Challenge 3

The network perimeter has vanished. Now what?

"In a nutshell, zero trust assumes that the system will be breached and designs security as if there is no perimeter."

National Cybersecurity Center Of Excellence, Nist

Open yet secure? How is that possible on networks that span campus, data center, cloud and OT environments? Now that enterprise networks extend to wherever in the world workloads and workers happen to be, there is no such thing as a defensible perimeter around an organization. We have reached the point where perimeters must surround each connected device and every workload. Security begins at the asset's edge.

Recommendations:

- Limit access to corporate assets using a least-privilege model such as zero trust
- Perform continuous discovery and posture assessment of all devices accessing the network regardless of location
- Enforce strict, policy-based compliance on all on-premises, BYOD and remote assets

Challenge 4

Segmentation is a must, but why do so many projects fail?

"The failure rate for network segmentation projects is high, and most projects last longer than the average tenure of a CISO."

Gartner, "The 6 Principles Of Successful Network Segmentation Strategies," November 2022

Network segmentation is a core tenet of zero trust and least-privilege initiatives and a top priority across industries. Unfortunately, network segmentation projects experience a high failure rate because they start with policy enforcement point solutions that don't touch all connected assets. A simplified approach facilitates policy design with 100% visibility of all devices on the network, visualized mappings of communications and traffic flows and policy simulation to minimize business disruption.

Recommendations:

- Visualize segmentation and simulate policies prior to deployment to prevent unnecessary disruption
- Make sure your primary solution can simplify segmentation of any device, anywhere
- Accelerate zero trust implementation across the enterprise environment
- Pick a modern NAC platform that is built to facilitate network segmentation

Challenge 5

How do you deal with the "do more with less" paradox?

"Between 2013 and 2021 the global number of unfilled cybersecurity jobs grew from one million to 3.5 million."

Cybersecurity Ventures

In addition to the cyber skills shortage, the exponential growth of connected devices, IT/OT convergence, unactionable alerts and rapidly evolving threat landscape have accelerated organizational timelines to automate whatever can safely be automated.

The Forescout Continuum Platform takes serially performed tasks and automates them to occur continuously. By continuously sharing device context, automating workflows and accelerating response actions among existing tools, in frees up SOC teams to focus on what requires human intervention.

Recommendations:

Choose a single platform that continuously automates every step in the cybersecurity continuum, including:

- Discovery and inventory of all cyber assets on your network – IT, IoT, OT and IoMT
- Assessment of cyber asset compliance and risk hygiene, with proactive remediation
- Multifactor risk identification and prioritization
- Accelerated incident response to minimize breach impact

The bigger challenge behind these five challenges

Each of the five challenges covered here can be daunting. If left unresolved, however, each one can lead to the ultimate challenge: a cyberattack that results in operational problems, stolen data, brand reputation damage, massive fines, public safety issues – the list goes on and on.

Prevention is the key, which means an effective solution must be capable of 100% agentless device visibility, continuous monitoring and automated threat detection and response.

Forescout delivers automated cybersecurity across the digital terrain, maintaining continuous alignment of customers' security frameworks with their digital realities, including all asset types. The Forescout Continuum Platform provides 100% asset visibility, continuous compliance, network segmentation and a strong foundation for Zero Trust. For more than 20 years, Fortune 100 organizations and government agencies have trusted Forescout to provide automated cybersecurity at scale. Forescout customers gain data-powered intelligence to accurately detect risks and quickly remediate cyberthreats without disruption of critical business assets.

FORESCOUT

Forescout Technologies, Inc.
Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
Learn more at Forescout.com