2020 E-BOOK

FORESCOUT
Active Defense for the Enterprise of Things™

How to Secure the Enterprise of Things
Five Security Challenges

CONTENTS

INTRODUCTION

Devices on today's enterprise networks are out of control. Both in terms of numbers (billions) and types (IT, OT, IoT, BYOD), 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 each network environment *complicated*: a veritable **Enterprise of Things** (EoT) that requires thoughtful planning and decisive action when it comes to securing devices and the enterprise itself.

What follows are the five key EoT 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?

> **During 2020 alone, experts estimate the installation of 31 billion IoT devices worldwide.**
>
> ***SECURITY TODAY*, JANUARY 13, 2020[1]**
>
> **"According to 62% of respondents, their companies' ability to achieve a more mature security posture will increasingly depend on the convergence of IT and OT control systems."**
>
> **PONEMON INSTITUTE, FEBRUARY 2019[2]**

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% device visibility—no blind spots
- Narrow your selection process to only include solutions that canprovide agentless, real-time deviceposture assessment
- Empower security operations and IT staff with real-time asset inventorying capabilities

CHALLENGE 2

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

> **"Smart buildings, medical devices, networking equipment and VoIP phones represent the riskiest IoT device groups."**
>
> **FORESCOUT RESEARCH, MAY 2020**[3]
>
> **"IoT and network-enabled device technologies have introduced potential compromise of networks and enterprises…Security teams must isolate, secure, and control every device on the network, continuously."**
>
> **FORRESTER RESEARCH, JUNE 2020**[4]

The concept of risk analysis is changing and expanding along with your attack surface. A recent Forescout Enterprise of Things analysis determined that IoT devices pose your greatest risk. "Not only are they challenging to monitor and control, but they also create vulnerabilities by bridging the gap that used to exist between the cyber and physical realms. IoT devices can be clandestine gateways into networks or primary targets of specialized malware."[3]

Recommendations:

- Employ multi-factor 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?

> **“New best practices must be put in place to secure enterprise network edges.“**
>
> **GARTNER, MAY 2020[5]**

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 how do you do it right without disrupting business operations?

> **"We estimate that 90 percent of the companies that we have talked to have segmentation projects in their plans this year. It is something everyone wants to do, but it is not always clear where to start, what the risks are, or if it's worth the money and effort."**
>
> **FORESCOUT RESEARCH, JANUARY 2019**[6]

Network segmentation has had a bad rap for years. Until recently, the available segmentation tools were a bear to deploy and couldn't cross network domains, resulting in business disruptions and a fragmented environment. The problems only got worse when organizations added new devices and further extended their networks. Today, however, solid segmentation solutions exist. It no longer makes sense to stick with vulnerable flat networks.

Recommendations:

- Visualize segmentation and simulate policies prior to deployment to prevent unnecessary disruption
- Make sure your primary solution can simplify Zero Trustsegmentation of any device anywhere (including IT, IoT andOT devices)
- 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?

> **“Enterprises are making progress in reducing fragmented network management toolsets. However, 64% of enterprises still use 4 to 10 tools to monitor and troubleshoot their networks.”**
>
> NETWORK MANAGEMENT MEGATRENDS 2020, APRIL 2020[7]
>
> **“Interest in security and risk management at the board level is at an all-time high.”**
>
> GARTNER RESEARCH, JULY 2019[8]

It’s difficult to make the case that your SecOps department is an efficient bulwark and provider of cost savings when your company’s security and network management uses a hodgepodge of fragmented, job-specific legacy tools. That said, even best-laid transformation plans can lead to trouble: namely, sluggish deployments, slow ROI, steep learning curves and limited satisfaction with chosen solutions. Fortunately, by selecting the right platform, you can satisfy all concerned parties, including the CFO.

Recommendations:

Choose a platform that can orchestrate existing tools and meets these criteria:

- Fast, flexible, non-disruptive deployment
- Rapid time to value and rapid ROI
- Vendor-agnostic – use your existing infrastructure
- Avoid forced software or hardware upgrades
- Offer integrations with leading IT and security products
- Agentless device discovery, posture and risk assessment
- Avoid 802.1X complexity, deployment delays and costs
- Accommodate growth with enterprise scalability
- Increase security operations productivity
- Provide agentless visibility, control, segmentation and Zero Trust

The bigger challenge behind these five challenges

Each one of the five challenges we have covered here can be daunting. But each one, if unresolved, 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 response.

*Notes

1. *The IoT Rundown for 2020: Stats, Risks, and Solutions*, Security Today, January 13, 2020
2. *Safety, Security & Privacy in the Interconnected World of IT, OT & IIoT*, Ponemon Institute Research Report, February 2019.
3. *The Enterprise of Things Security Report, The State of IoT Security* in 2020, Forescout Research Labs, May 2020
4. *Mitigating Ransomware With Zero Trust: Bolster Your Defenses With Zero Trust Principles and Techniques, June 8, 2020,* Forrester Research
5. *Securing the Enterprise's New Perimeters*, Gartner, March 27, 2020
6. *Network Segmentation*, Forescout blog, January 2019
7. *Network Management Megatrends 2020*, Enterprise Management Associates Research Report, April 2020
8. *Five Board Questions That Security and Risk Leaders Must Be Prepared to Answer*, Gartner Research, July 2019

Don't just see it.
Secure it.™

Contact us today to actively
defend your Enterprise of Things.

ABOUT FORESCOUT

Forescout is the leader in Enterprise of Things security, offering a holistic platform that continuously identifies, segments and enforces compliance of every connected thing across any heterogeneous network. The Forescout platform is the most widely deployed, scalable, enterprise-class solution for agentless device visibility and control. It deploys quickly on your existing infrastructure—without requiring agents, upgrades or 802.1X authentication. Fortune 1000 companies and government organizations trust Forescout to reduce the risk of business disruption from security incidents or breaches, ensure and demonstrate security compliance and increase security operations productivity.

forescout.com/platform/eyeSight

salesdev@forescout.com

toll free 1-866-377-8771

FORESCOUT
Active Defense for the Enterprise of Things™

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com