How to Secure the Enterprise of Things
Five Security Challenges
CONTENTS

3 Introduction
4 Challenge 1: How can you inventory and manage the explosion of unmanaged devices?
5 Challenge 2: In today’s enterprise environment, where does risk reside?
6 Challenge 3: The network perimeter has vanished. Now what?
7 Challenge 4: Segmentation is a must, but how do you do it right—without disrupting business operations?
8 Challenge 5: How do you deal with the “do more with less” paradox?
9 Conclusion
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, 2020¹

“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 2019²

Recommendations:

• Determine which tools can give you 100% device visibility—no blind spots
• Narrow your selection process to only include solutions that can provide agentless, real-time device posture assessment
• Empower security operations and IT staff with real-time asset inventorying capabilities

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.
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

“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

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

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

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 Trust segmentation of any device anywhere (including IT, IoT and OT 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

“Interest in security and risk management at the board level is at an all-time high.”

GARTNER RESEARCH, JULY 2019

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
5. *Securing the Enterprise’s New Perimeters*, Gartner, March 27, 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.

forescout.com/platform/eyeSight salesdev@forescout.com

© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at https://www.forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products, or service names may be trademarks or service marks of their respective owners. Version 08, 20