

IoT Security

Choose a flexible Zero Trust approach to secure non-traditional devices in the Enterprise of Things

Internet of Things (IoT) devices often remain invisible on enterprise networks. Unlike traditional systems, they can't be easily tracked and rarely support software agents. These devices expand the attack surface and greatly increase organizations' risks, as they can be compromised and used as entry points into vulnerable networks. Enterprises need a security solution that can continuously identify, segment and enforce compliance of every IoT device on heterogeneous networks.

IoT devices: Is the risk worth the reward?

IoT devices are valuable and often critical corporate assets. They boost productivity, enhance product and service quality and improve the bottom line. In fact, 63% of enterprises expect to achieve financial payback in three years for their IoT projects.² Sophisticated, well-funded bad actors are constantly on the lookout for areas in an organization to exploit such as gaps in IoT visibility and security – gaps that lead to downtime, compromised data, loss of intellectual property and reputational damage. Consider this:

- Nearly nine out of 10 respondents in a recent Ponemon Institute survey expect their company to experience a cyberattack or data breach caused by unsecure IoT devices or applications in the next two years.³
- By 2023, the average CIO will be responsible for more than three times the endpoints they managed in 2018.⁴

ZERO TRUST DEFINED

Forrester's Zero Trust model of information security is a conceptual and architectural approach to enterprise security. In its simplest form, Zero Trust is about establishing trust by ensuring you have a trusted user on a trusted device with trusted access. Access is restricted to only the corporate assets that each user needs to do their jobs. According to Forrester,¹ to implement effective Zero Trust policies, you must:

- Redesign networks into secure microperimeters
- Strengthen data security using obfuscation techniques
- Limit the risks associated with excessive user privileges and access
- Dramatically improve security detection and response with analytics and automation

In today's Enterprise of Things (EoT), where countless IT, IoT and OT (operational technology) things connect and intersect, organizations need a security solution that makes IoT and all IP-connected devices visible and controllable, and that conforms to a Zero Trust approach to networking. Otherwise, any device can be compromised and exploited for malicious purposes.

The Forescout Zero Trust approach

Forescout believes that IoT security must be based on a Zero Trust approach that combines complete device visibility, proactive network segmentation and least-privilege access control of all digital assets – devices, users, apps and workloads. The Forescout platform lets you effectively manage cyber, operational and compliance risks across your EoT environment by:

- Providing complete visibility into unmanaged IoT, Internet of Medical Things (IoMT) and OT devices as well as all IP-connected systems
- Assessing and identifying IoT devices with factory-default or weak credentials and automating policy actions to enforce strong passwords
- Providing real-time insight into IoT devices' communication and risky behavior across the extended environment
- Segmenting devices into trusted zones by enforcing least-privilege access by Zero Trust policy
- Automating unified Zero Trust policy orchestration across multivendor environments and multiple network domains
- Knocking down security management silos to accelerate response and maximize the value of your investments in other security solutions
- Helping Health Delivery Organizations (HDOs) proactively detect and reduce vulnerabilities/threats, granularly enforce segmentation and network access rules, and immediately contain medical device threats while facilitating remediation via tight integration with Medigate



Forescout is the vendor for Zero Trust IoT/OT-focused security. IoT/OT device security is one of the hardest problems to solve within the enterprise. This is Forescout's sweet spot, and the vendor's platform capabilities for IoT/OT security shine above those of the competition.

THE FORRESTER WAVE: ZERO TRUST EXTENDED ECOSYSTEM PLATFORM PROVIDERS, FORRESTER RESEARCH, OCTOBER 2019



Figure 1: Forescout actively defends all devices in your Enterprise of Things by identifying, segmenting and enforcing compliance of every connected thing.

Discover and classify 100% of IP-connected devices

It's essential to obtain complete visibility and device context of all IoT, OT and critical infrastructure endpoints across your heterogeneous environment. The Forescout platform:

- Continuously discovers all IP-connected devices, physical and virtual, the instant they enter your network – no software agents required
- Provides in-depth visibility into all devices using 20+ active and passive discovery, profiling and classification techniques
- Leverages the Forescout Device Cloud, the world's largest data lake of crowdsourced device intelligence, providing a cross-industry single source of truth on the fingerprints, behavior and risk profiles of more than 12 million devices

Implement dynamic network segmentation and automate controls

In today's heterogeneous EoT environments, an enterprise that adopts the Zero Trust model must be capable of network segmentation and orchestrated incident response across all EoT domains. With Forescout, you can:

- Correlate access with user identities (who is doing what, where, when and why)
- Provision devices to dynamic network segments based on policies and real-time context
- Map data flows to design segmentation policies and simulate them for non-disruptive deployment
- Automate segmentation to reduce cyber and operational risk

Orchestrate security and enforce compliance

Most organizations are inundated with expensive, single-purpose security solutions that can't share knowledge or coordinate incident response. Forescout offers the cure for this inefficiency. Forescout eyeExtend products share device context between the Forescout platform and other IT and security products to automate workflows and policy enforcement across disparate solutions. These orchestration capabilities can help you:

- Increase IoT security and overall device compliance
- Reduce mean time to detect and respond
- Increase ROI from your existing tools
- Automate your configuration management database (CMDB) updating process, eliminating time-consuming and error-prone manual inventorying

1. Five Steps to a Zero Trust Network, Roadmap Report, Forrester Research, October 2018
2. Internet of Things: Unlocking True Business Potential, Gartner
3. A New Roadmap for Third-Party IoT Risk Management, Benchmark Study, Ponemon Institute, Sabine Zimmer, June 3, 2020
4. Gartner Top Strategic IoT Trends and Technologies Through 2023, September 2018

"Today we know what's on our network—including IoT devices such as printers, VoIP phones and security cameras. Forescout classifies the device and slips it onto the appropriate VLAN segment."

– KEN COMPRES, SENIOR NETWORK SECURITY AND INTEGRATION ENGINEER/CSO, HILLSBOROUGH COMMUNITY COLLEGE

**Don't just see it.
Secure it.**

Contact us today to actively defend your Enterprise of Things.

forescout.com/platform/IoT

salesdev@forescout.com

toll free 1-866-377-8771