IoT Security

Choose a flexible zero trust approach to secure nontraditional devices in your digital terrain

ZERO TRUST DEFINED

Zero Trust Architecture (ZTA) is a data-centric security model based on least-privileged access, not a fixed solution or technology that can be purchased from a single vendor. It assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity.

Forescout is participating in the NIST National Cybersecurity Center of Excellence's ZTA Project based on SP 800-207, which will provide practical, interoperable approaches to designing and building ZTAs.

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 platform 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. 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:

- IoT products surpassed traditional internet-connected devices in 2019 and the ratio is projected to be around 3:1 by 2025.
- 70% of survey respondents have low or average confidence in the security of their organizations' IoT devices.

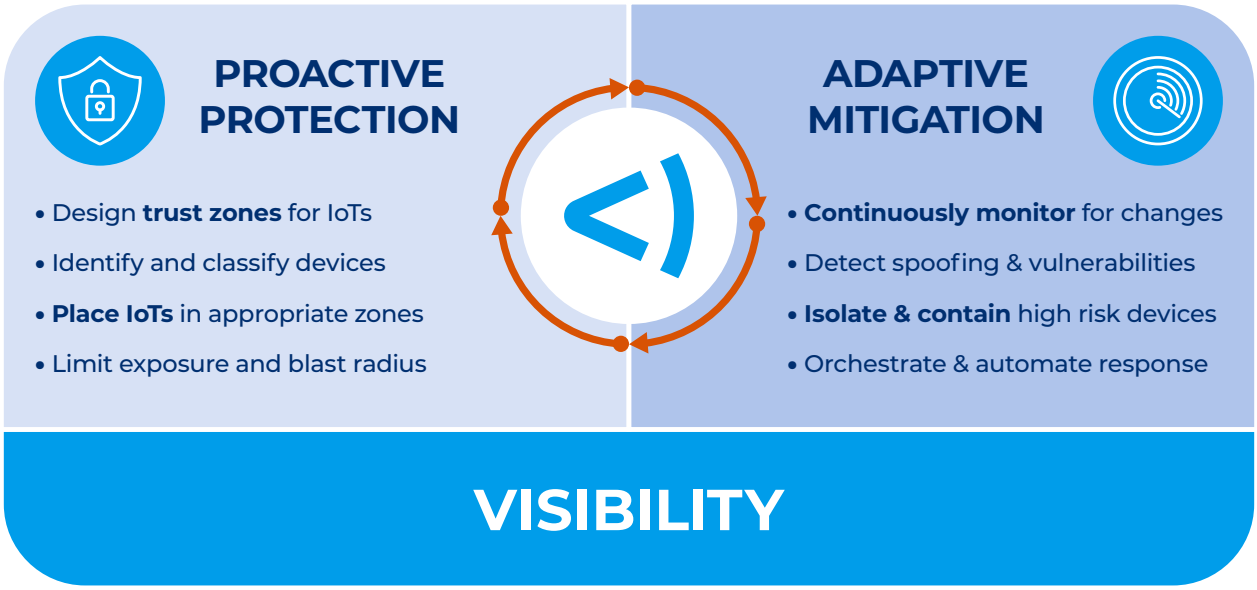
In today's digital terrain where countless IT, IoT and OT (operational technology) things connect and intersect, organizations need a security solution that makes IoT and all IP-connected devices visible and controllable, and that conforms to a ZTA. Otherwise, any device can be compromised and exploited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

> "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*

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 Continuum Platform lets you effectively manage cyber, operational and compliance risks across your 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 proactively detect and reduce vulnerabilities and granularly enforce segmentation and network access rules, and immediately contain medical device threats while facilitating remediation



"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*

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 Continuum 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 18 million devices

Implement dynamic network segmentation and automate controls

In today's heterogeneous environments, an organization that adopts the zero trust model must be capable of network segmentation and orchestrated incident response across all domains. With Forescout Continuum, 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

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