FORESCOUT

Reducing Risks from IoT Devices in an Increasingly Connected World

FORESCOUT

TABLE OF CONTENTS

The Connected World

With the rise of automation, remote access, and the ever-expanding Internet of Things (IoT), IT security teams are struggling with the added responsibility of identifying IoT devices entering the network at an unprecedented rate and rallying to strengthen organizational network security. Business operations now rely heavily on specialized devices to connect and enhance business functions.

With the number of IoT devices worldwide forecast to almost triple—from 9.7 billion in 2020 to more than 29 billion in 2030—cybersecurity becomes a critical focal point for the age of IoT.

New Risks from IoT Devices

While these devices enhance our lives and business operations, they also introduce new threats. Most IoT devices are consumer-grade technologies that:

- Are mostly unmanaged
- Come from a multitude of vendors
- Use non-standard operating systems
- Use a diversity of often insecure protocols
- May dynamically connect to other devices inside or outside the organization's network

Additionally, bad security practices like default or simple credentials, unencrypted traffic and lack of network segmentation remain common.

Our research report on the plethora of connected "things" on the enterprise network identified IoT devices as four out of the top five riskiest devices.

IoT Systems

An IoT system integrates components in different subsystems to offer services like monitoring energy consumption and space utilization or predicting infrastructure maintenance needs. Typically it is made up of several components:

- IoT devices, like smart TVs and smart plugs
- IoT gateways that allow the devices to communicate the data and measurements they collect
- An IoT platform, generally running on the cloud, that aggregates collected data and enables the provisioning of different services

Video surveillance and smart lighting are traditionally considered IoT systems, but this specific category includes other generic IoT devices, such as smart sensors and detectors. These devices act as links between other subsystems or as standalone devices that do not fit into a pre-existing subsystem.

The Risks

- Centralized IoT systems gather a lot of information, making them desirable targets for hackers who intend to steal data
- An attack could cause possible disruption of service of every single device connected to the system
- The most widely used protocol in IoT systems, MQTT, is designed to be lightweight and unencrypted

Physical Access Control Solutions

These devices open or close door locks in the presence of authorized badges, literally bridging the gap between the cyberband physical realms. In Forescout's research, they were often found configured with open ports (including Telnet port 23), connected to other risky devices and containing serious reported vulnerabilities.

The Risks

- Endanger the physical security of employees and all physically present
- Possible exfiltration of confidential data including admin credentials
- Could extend to network-wide disruptions of many systems and services

HVAC Systems

In 2018, a hacker in the Netherlands shut down the cooling system used to store pharmaceutical drugs in a supermarket.

Our research found HVAC systems configured with critical open ports (including Telnet), connected to other risky devices and containing a couple of critical vulnerabilities that could allow the complete takeover of a device (CVE-2015-2867 and CVE-2015-2868). Malicious actors can use HVAC systems to bypass "air gaps" via a covert thermal channel and move laterally to exfiltrate sensitive data.

The Risks

- Raising the temperature in a data center could cause overheating and business disruption
- Temperature changes could cause possible loss of revenue from damaged goods
- Hackers could gain access to the management network to orchestrate a larger, coordinated attack

IP Cameras

Many IP cameras are highly exposed to external actors. This exposure is both physical, since many cameras exist in external locations that make it easier for an attacker to tamper with them, and logical, since modern cameras and recording equipment support remote access for improved management and access to cloud services.

The last few years have shown a surge of interest in IP cameras and network video recorders from both the security research community and malicious actors. Our research shows that IP cameras are associated with several vulnerabilities (e.g., CVE-2018-10660). Many are configured with critical ports such as SSH port 22 and FTP port 21 enabled. They are also often connected to risky devices.

The Risks

- Cameras on attacked networks could be forced to deviate from their standard operation, with footage no longer being recorded
- Footage from the camera stored on servers and/or previewed on monitors can be replaced or deleted using vulnerabilities related to security protocols
- Network disruptions can lead to substantial data loss and no real-time footage of the area under surveillance limiting the availability of evidence in case of an incident

Smart Lighting Systems

A smart lighting system can automatically control the lights in a building based on factors like room occupancy and available daylight. As lights are integrated into building automation systems, they become the sources and targets of attacks. Although smart lights are not as widely deployed as surveillance cameras, and most attacks on them are either academic or proof-of-concept examples, companies are rapidly adopting them. We believe that smart lighting in building automation is a trend that could soon be exploited by malicious actors.

The Risks

- Smart lighting systems can be reconfigured to change their patterns and behavior
- The system could be completely switched off, potentially removing area visibility for malicious purposes

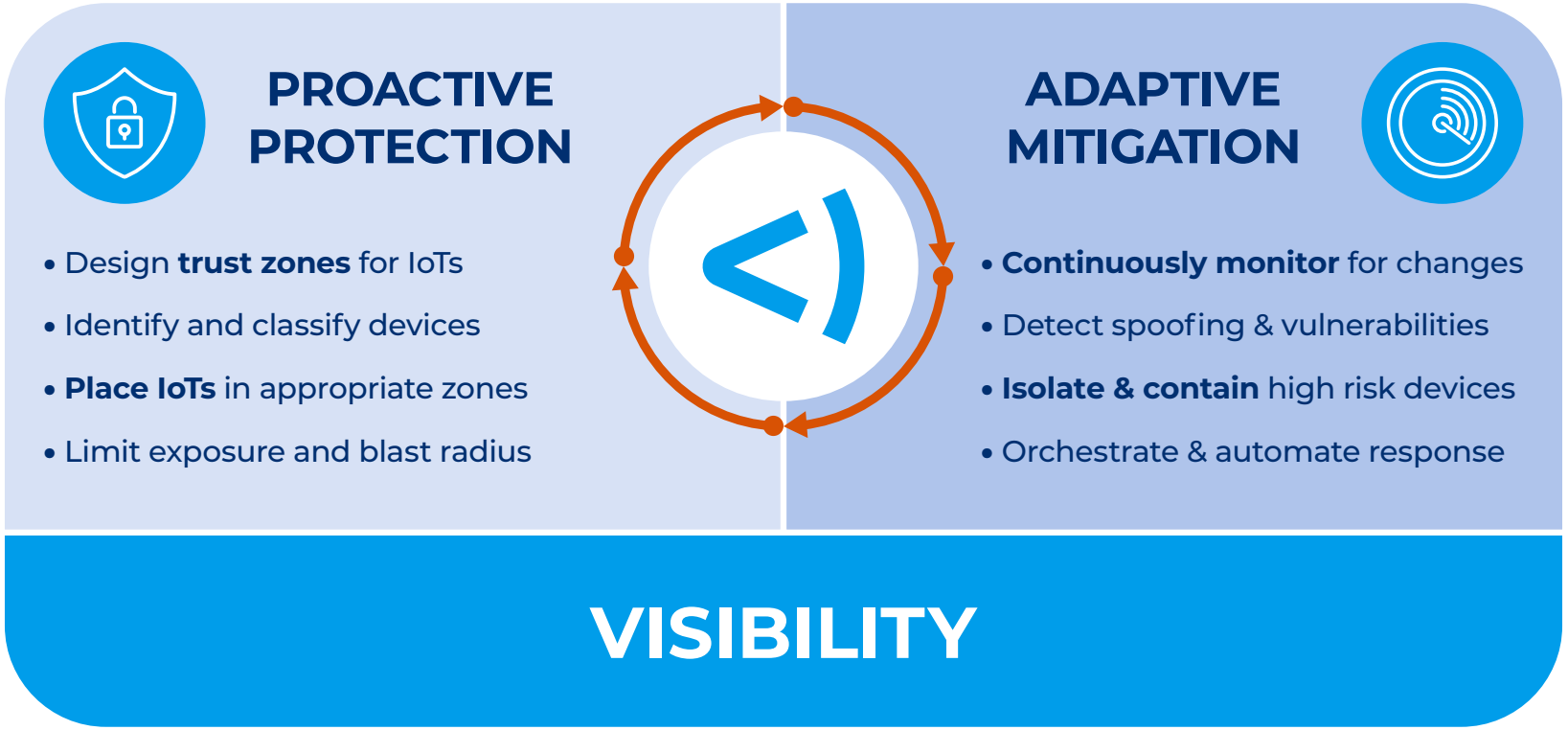
Forescout's Zero Trust Approach to IoT Security

Increasing reliance on IoT devices comes with additional risks of an ever-expanding attack surface. 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.

Forrester has this to say about Forescout's capabilities:

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 and capabilities for IoT/OT security shine above those of the competition. Maximum visibility, leading to maximum operational control and, ultimately, security, is the crux of Forescout's approach to Zero Trust.

Reducing risk in IoT systems requires **complete network visibility** – a critical component for identifying and classifying IoT and other devices across your digital terrain.



Actionable visibility provides the weapons that security teams need to proactively protect devices. By designing **trust zones** for IoT devices before putting them on the network, you can define appropriate communication policies for those devices and detect any anomalous activity, thus limiting the risk exposure and reducing the blast radius.

Continuous monitoring is vital for detecting any configuration changes. With **passive detection** capabilities, IoT devices can be watched carefully, reducing potential business disruptions. Should an incident occur, automated, end-to-end response and resolution swiftly **deescalates the incident** and prevents the impact from spreading across the enterprise.

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