eBook

FORESCOUT

Reducing Risks from IoT Devices in an Increasingly Connected World

The Connected World

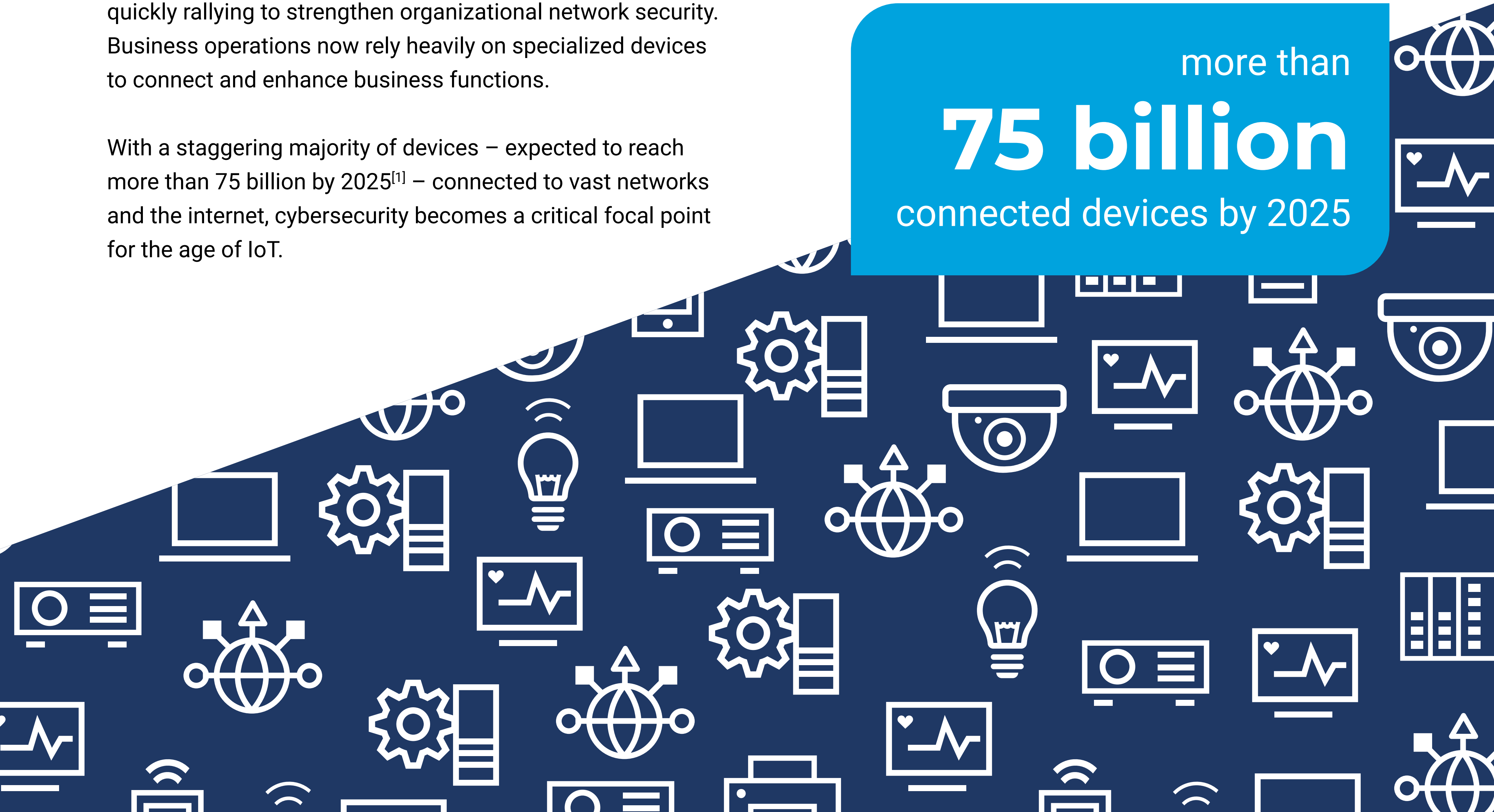
With the rise of automation, remote access, and the ever-expanding Internet of Things (IoT), IT Security teams are struggling with the added responsibility of identifying IoT devices entering the network at an unprecedented rate and quickly rallying to strengthen organizational network security. Business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

With a staggering majority of devices – expected to reach more than 75 billion by 2025[1] – connected to vast networks and the internet, cybersecurity becomes a critical focal point for the age of IoT.

more than

75 billion

connected devices by 2025



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:

1. Are mostly unmanaged.
2. Come from a multitude of vendors.
3. Use non-standard operating systems.
4. Use a diversity of often insecure protocols.
5. 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 recent research report on the plethora of connected "things" on the enterprise network[2] identified IoT devices as 4 out of the top 5 riskiest devices.

IoT System

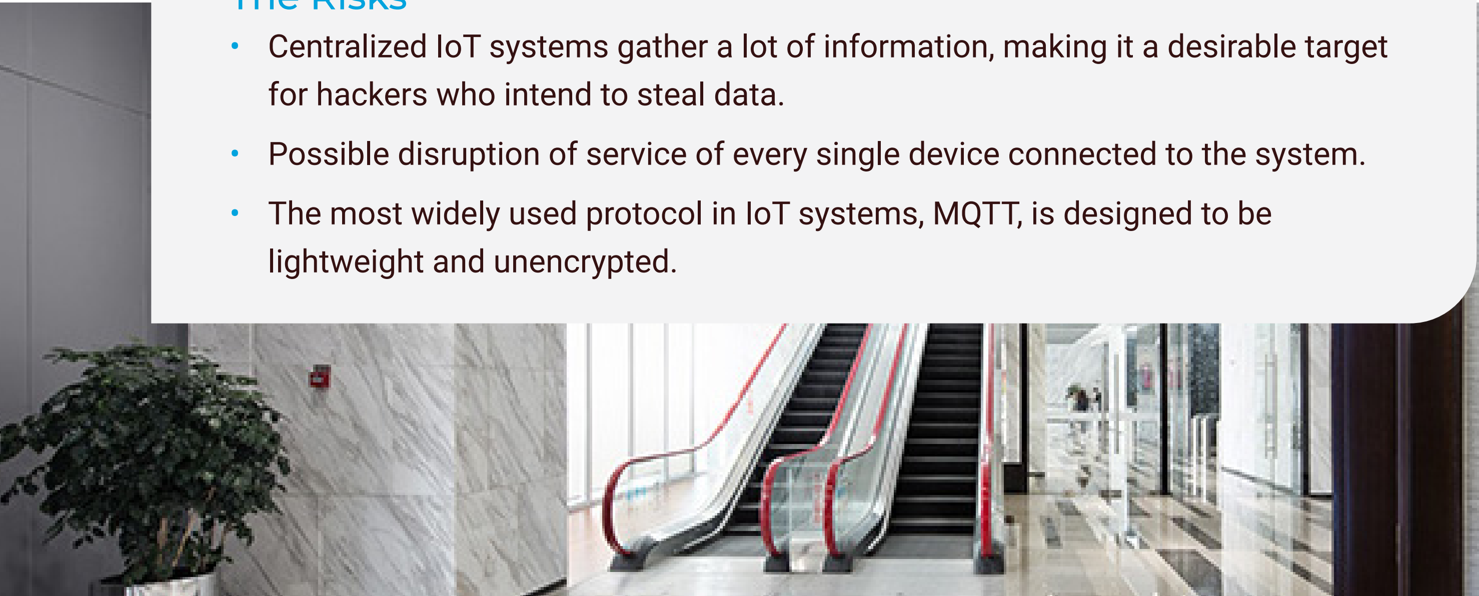
An IoT system, which integrates components in different subsystems to offer services like monitoring energy consumption and space utilization or predicting infrastructure maintenance needs, is typically made up of several components:

1. IoT devices, like smart TVs and smart plugs.
2. IoT gateways that allow the devices to communicate the data and measurements they collect.
3. 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 it a desirable target for hackers who intend to steal data.
- 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 Solution

These devices open or close door locks in the presence of authorized badges literally bridging the gap between the cyber and physical realms. In Forescout's research[2], they were often found configured with open ports (including Telnet port 23), connected to other risky devices and containing serious reported vulnerabilities.

In 2019, hackers penetrated the network of a large hotel brand[3], compromising their door access control systems.

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.

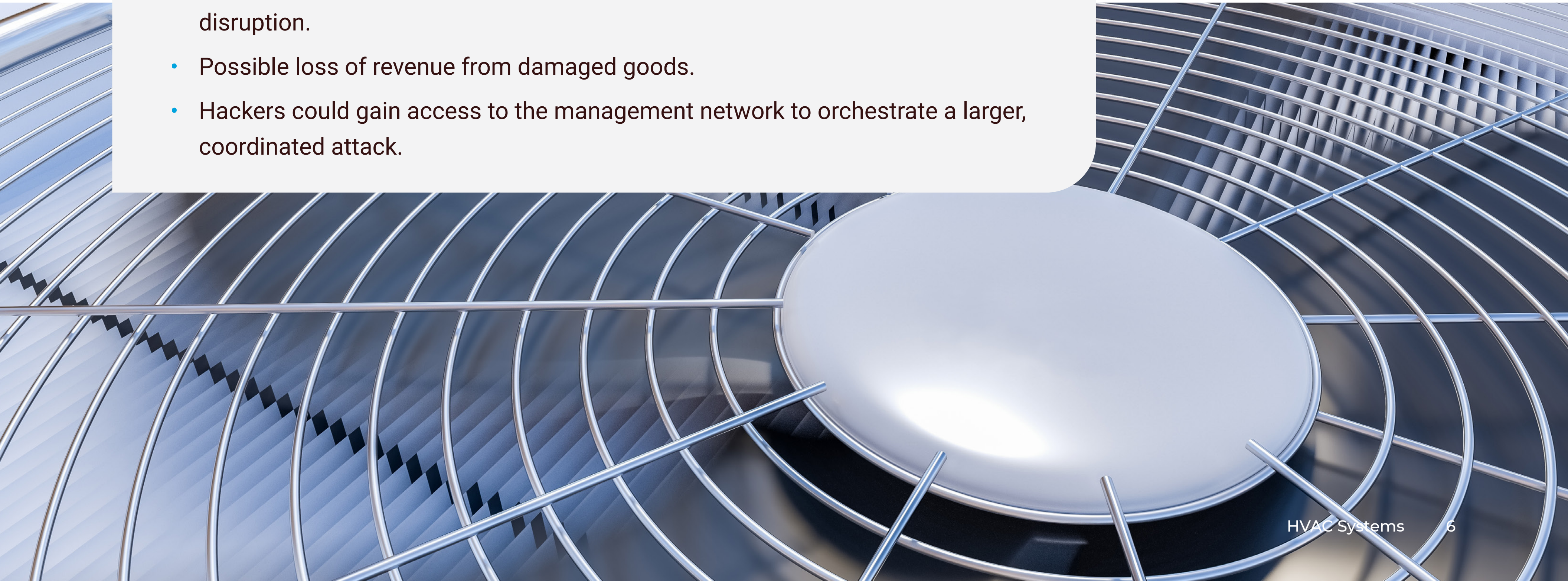
HVAC Systems

In 2018, a hacker in the Netherlands shut down the cooling system used to store pharmaceutical drugs in a supermarket[4].

Our research found these devices 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

- Raised temperature in data centers to cause overheating and business disruption.
- Possible loss of revenue from damaged goods.
- Hackers could gain access to the management network to orchestrate a larger, coordinated attack.



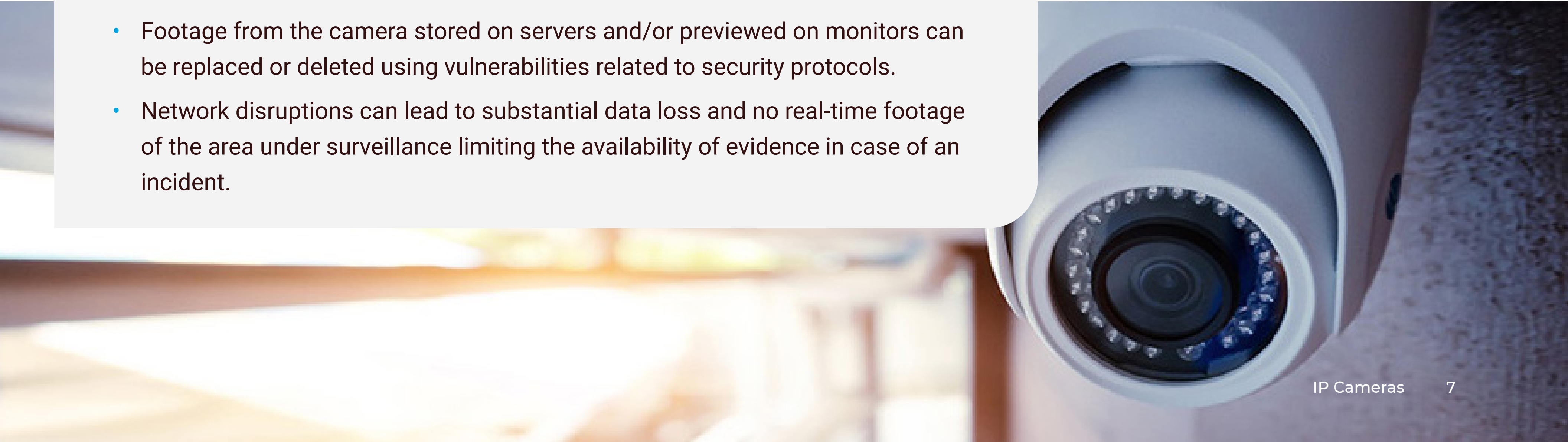
IP Cameras

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. For more about this device risk, read our past research on the topic[5].

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.

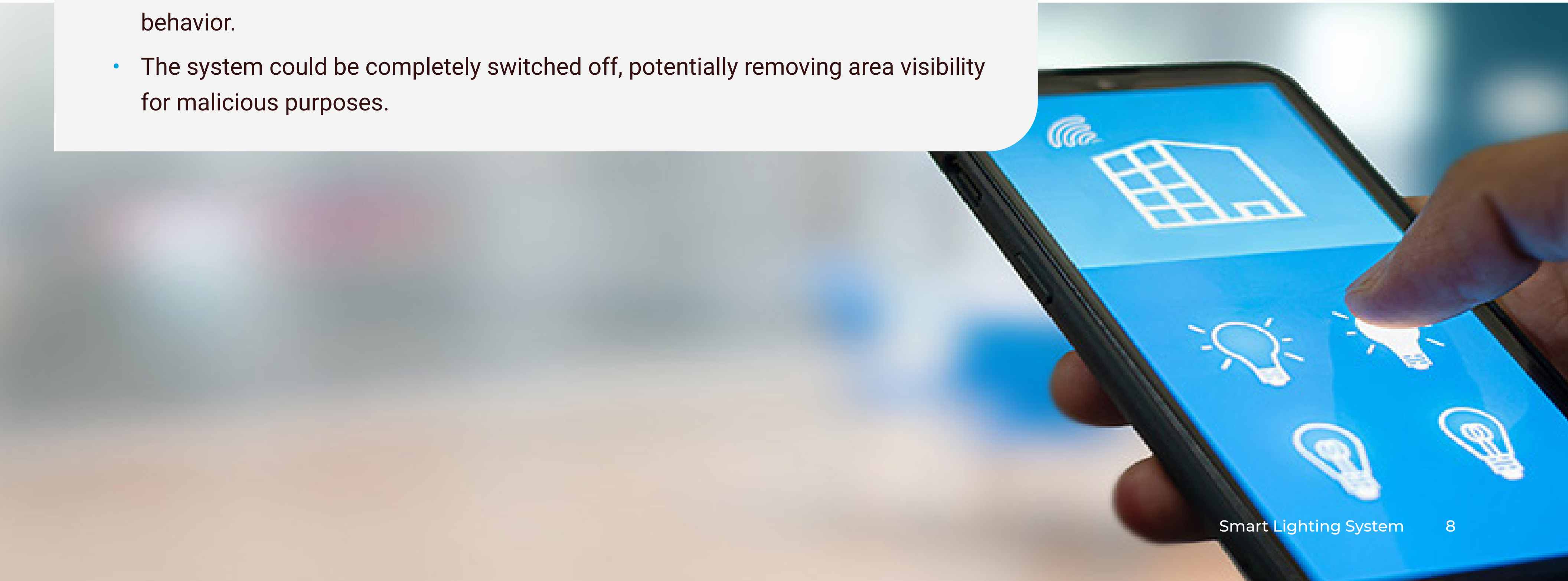


Smart Lighting System

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.



Proactively Reduce Risks from IoT Devices

According to Gartner[6], Infrastructure and Operations (I&O) leaders deploying IoT solutions on the enterprise infrastructure must:

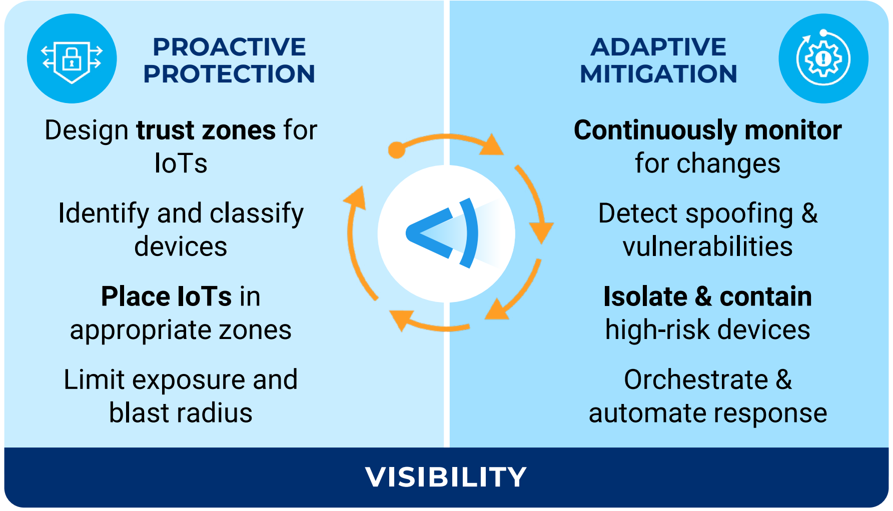
- Discover and classify all devices attached to the network
- Virtually separate all IoT Solutions – from the device to the application – from the rest of the network
- Monitor continuously to identify compromised devices and implement role-based policy enforcement to quarantine them

Forrester views Forescout as a Zero Trust platform vendor. Forrester says about Forescout, "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"[7].

Forescout's Zero Trust approach for IoT Security

Reducing Risk in IoT systems requires **complete network visibility** – a critical component for identifying and classifying IoT and other devices on the campus network, in the data center and in the cloud.

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.



PROACTIVE PROTECTION

Design **trust zones** for IoTs

Identify and classify devices

Place IoTs in appropriate zones

Limit exposure and blast radius

ADAPTIVE MITIGATION

Continuously monitor for changes

Detect spoofing & vulnerabilities

Isolate & contain high-risk devices

Orchestrate & automate response

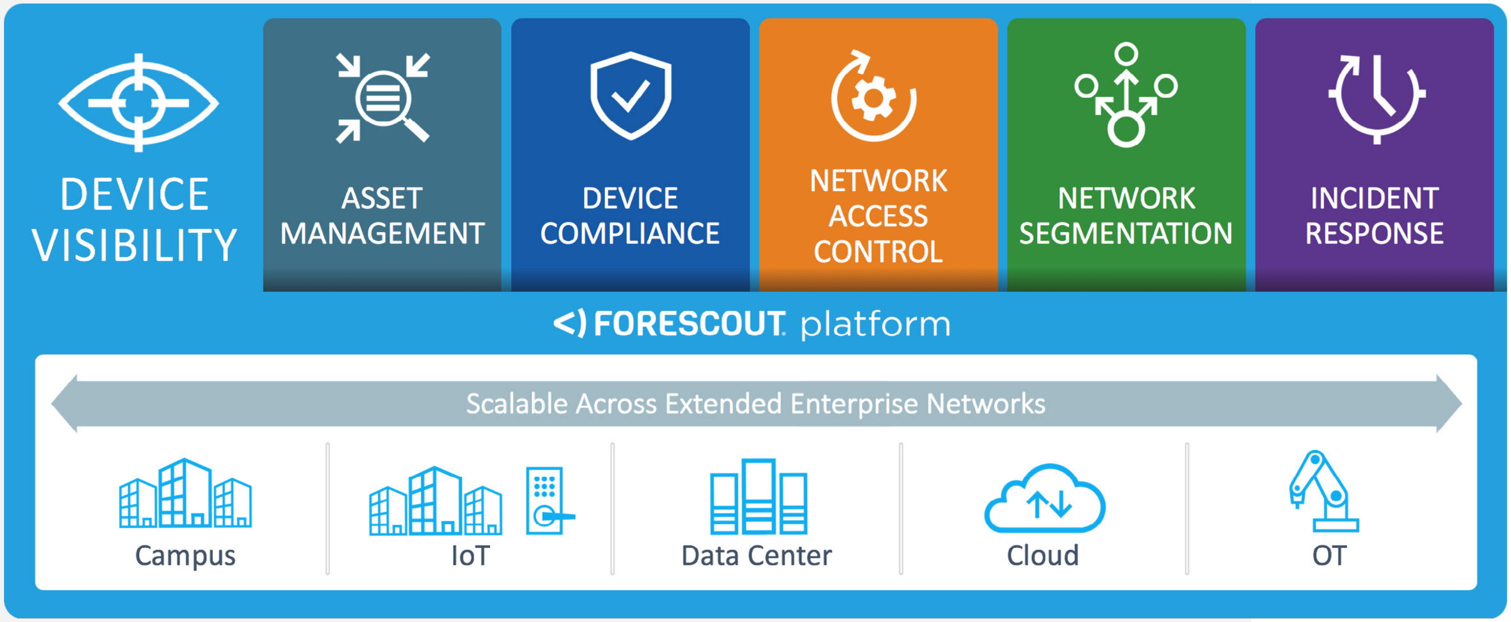
VISIBILITY

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 and end-to-end appropriate response and resolution swiftly **deescalates the incident** and prevents the impact from spreading across the enterprise.

How Forescout Helps

Forescout helps organizations reduce both business and operational risk through complete situational awareness of their extended enterprise by providing continuous, unified visibility and control of all IP-connected devices across campus, data center, cloud, IoT and OT networks.

This includes critical capabilities in support of **asset management**, **device compliance**, **network access control**, **network segmentation**, and **incident response initiatives**.



See the Forescout Platform in Action!

Schedule your demo and let us show you how Forescout can help secure the IoT in your enterprise.

REQUEST A DEMO

[1] Statista, 2016 https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[2] Forescout Research Labs, Annual Connected Enterprise Report: The state of IoT Cybersecurity in 2020

[3] Physical Security at risk as hackers target vulnerable systems

[4] Hacker changes the temperature at Plus Supermarket

[5] Forescout Research Labs; Smart Building Cybersecurity Research

[6] IoT Solutions Can't Be Trusted and Must Be Separated from the Enterprise Network to Reduce Risk, Gartner, October 2019

[7] Forrester Wave TM: Zero Trust eXtended Ecosystem Platform Providers, October 2019

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