eBook

FORESCOUT

Reducing Risks from IoT Devices in an Increasingly Connected World

The Connected World

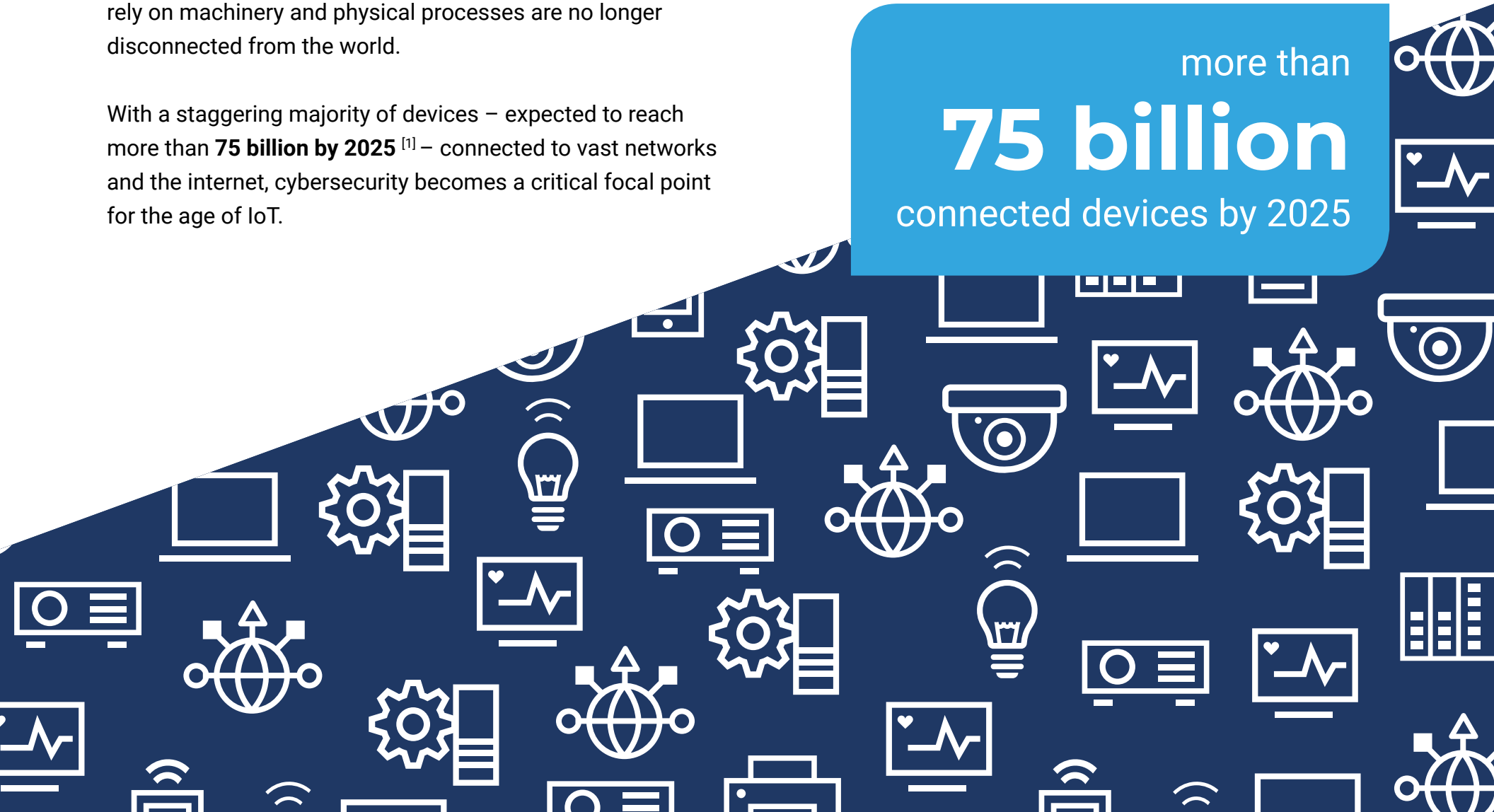
With the rise of automation, remote access, and the ever-expanding Internet of Things (IoT), IT and OT teams are collaborating at an unprecedented rate to strengthen organizational network security. Business operations that rely on machinery and physical processes are no longer disconnected from the world.

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 offer a number of enhancements to our lives, they also introduce new threats. These IoT devices are consumer-grade technologies that are:

1. Mostly unmanaged.
2. Come from a multitude of vendors.
3. Use non-standard operating systems.
4. Support 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 evolving IoT threat landscape [2] is divided into a few distinct areas, focusing on commonly targeted devices and specific points of entry that could be exploited by attackers. In this eBook, we will discuss these potential exploits and how Forescout can help mitigate them.

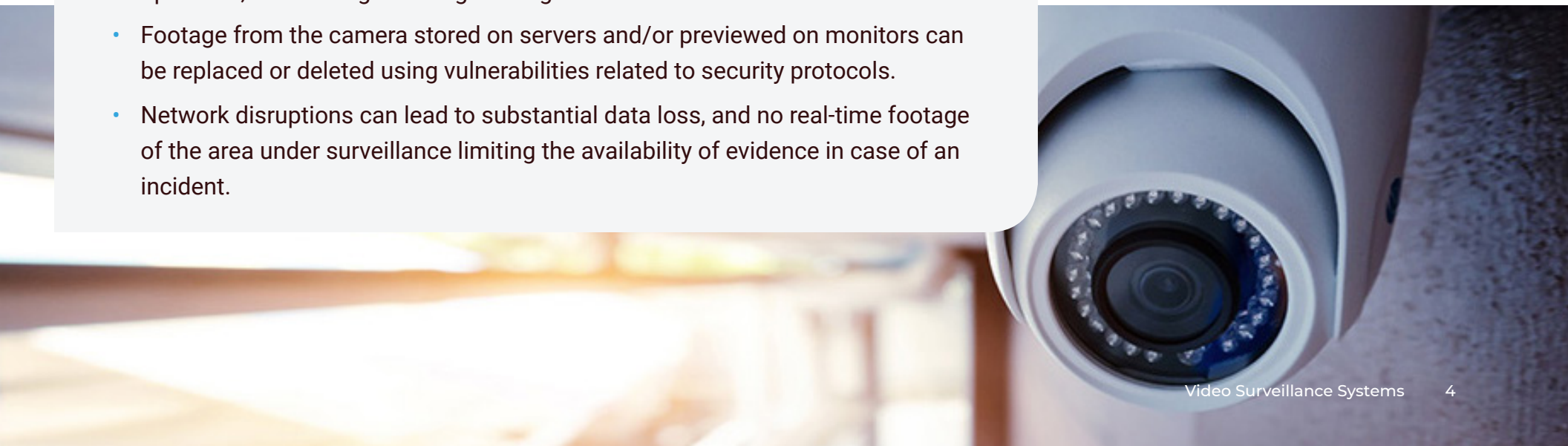
Video Surveillance Systems

A video surveillance system (VSS) helps ensure the security of occupants by allowing a building manager to continuously monitor locations inside or near their facility. VSS's are highly exposed to external actors. This exposure is both physical, since many cameras are placed 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.

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.

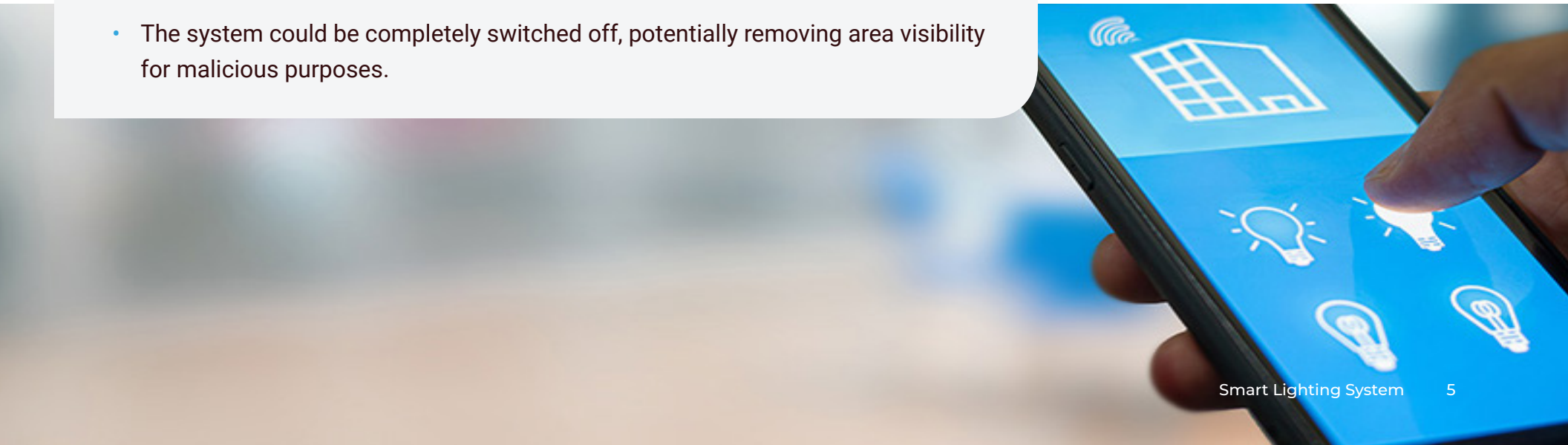


Smart Lighting System

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 too become the sources and targets of attacks. Although smart lights are still not as widely deployed as surveillance cameras, and most attacks on them are either academic or proof-of-concept examples, smart lighting is being rapidly adopted, with Gartner forecasting the technology to reach the "plateau of productivity" in its hype cycle in less than 2 years [3]. 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.



IoT System

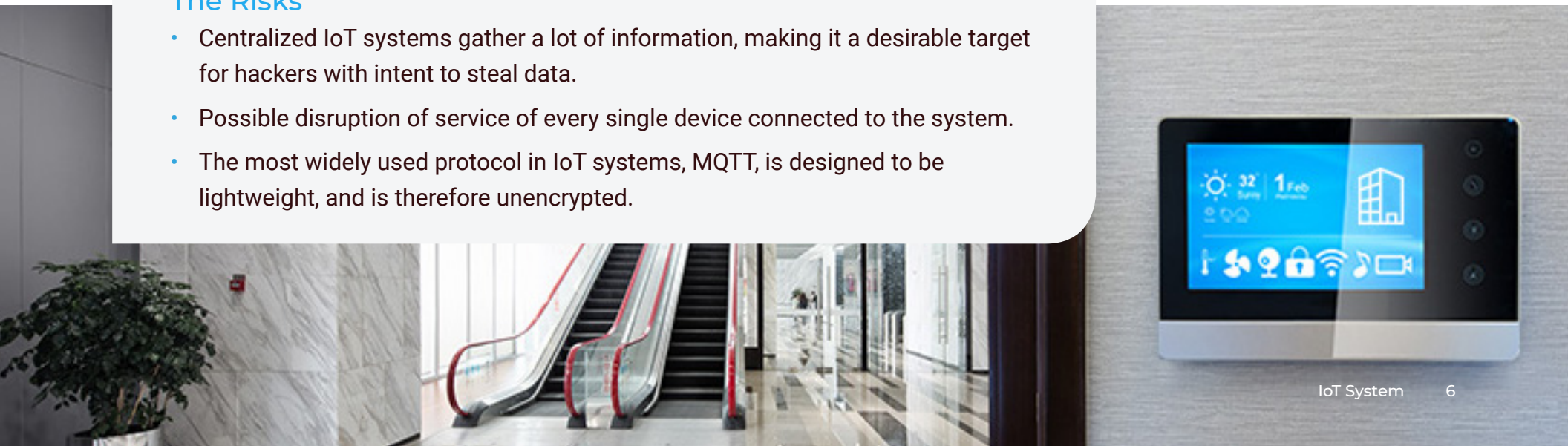
An IoT system, which integrates components in different subsystems to offer services like monitoring energy consumption and space utilization or predicting infrastructure maintenance needs, is typically made up of several components:

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 too, but this specific category includes other generic IoT devices, such as smart sensors and actuators. These devices act as links between other subsystems or as standalone devices which do not fit into a pre-existing subsystem.

The Risks

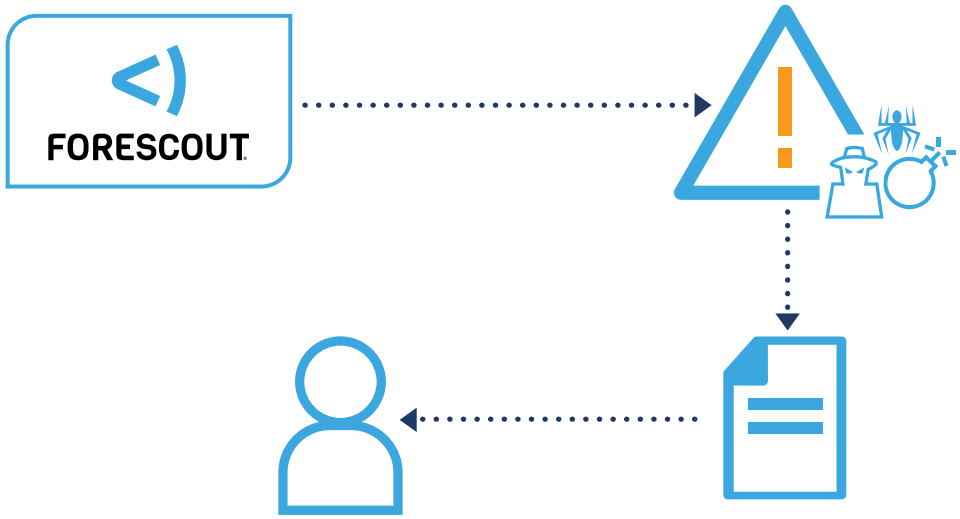
- Centralized IoT systems gather a lot of information, making it a desirable target for hackers with intent to steal data.
- Possible disruption of service of every single device connected to the system.
- The most widely used protocol in IoT systems, MQTT, is designed to be lightweight, and is therefore unencrypted.



Identifying and Mitigating Risks from IoT Devices

Network monitoring is an effective solution to identify and mitigate vulnerabilities in IoT devices and the consequences of potential attacks. Continuously monitoring and analyzing network communications and comparing them with a baseline of legitimate/desired operations and with the “known bad” defined in a collection of checks, and can **help spot cyberthreat and operational problems** in the network in real time.

Forescout’s SilentDefense is an advanced network monitoring and intelligence platform used by critical infrastructure and building automation operators worldwide to help preserve the stability of their networks.



If something bad or unexpected occurs in the network, SilentDefense immediately notifies the operator and provides them with all the intelligence required to respond to the event.

This includes information about the:

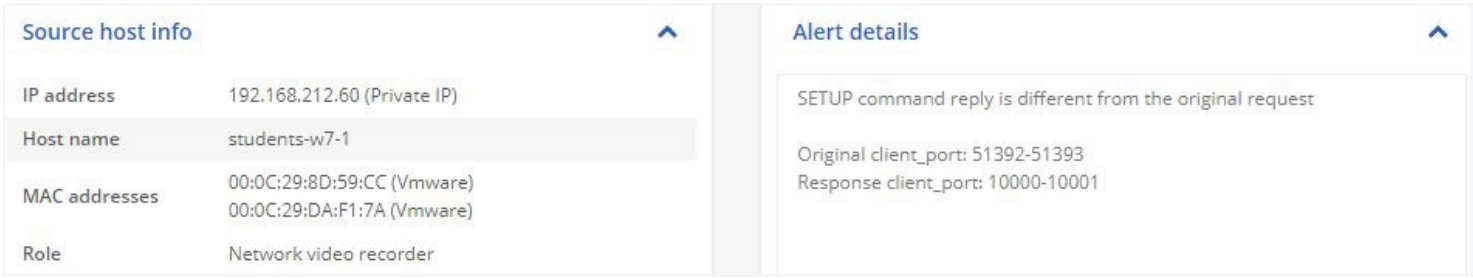
- Source of the problem
- Targeted device(s)
- Nature of the problem
- Packet capture (PCAP) of the traffic related to the event

This traffic capture can become critical information to have if advanced threats, such as a zero-day attack, occur. This key data can then be forwarded to specialized security vendors and organizations for further analysis.

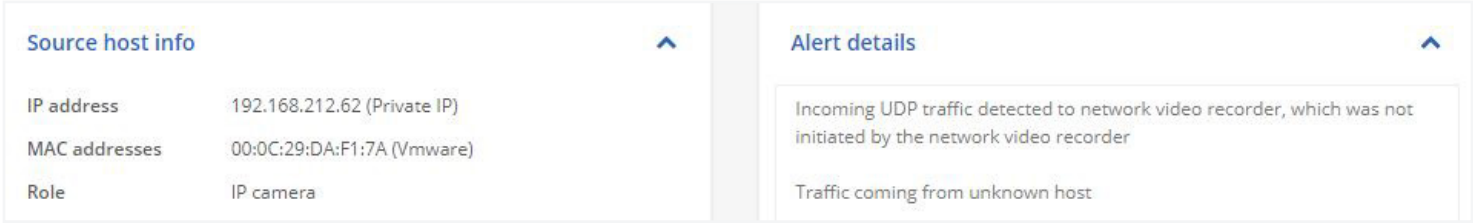
Detecting Attacks on IoT

To detect the attacks on IoT presented in the previous section, SilentDefense uses the combined action of a powerful man-in-the-middle detection module and custom security checks. These custom checks can detect attack signatures even without learning the normal behavior of the network, allowing for an immediate response upon deployment.

The figures below show examples of alerts raised by SilentDefense when an attempted exploitation of the footage replay attack on a VSS is detected.



Alert raised when RTSP change of ports is detected

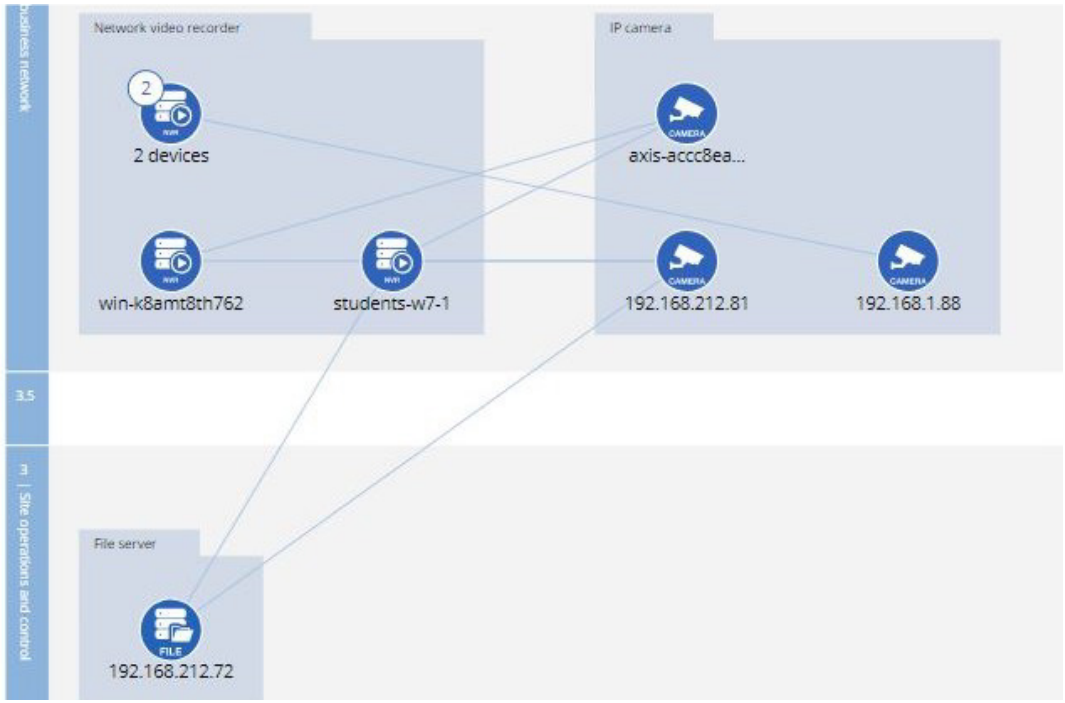


Alert raised when an unknown host streams to an NVR

Passive Detection and Classification of Hosts

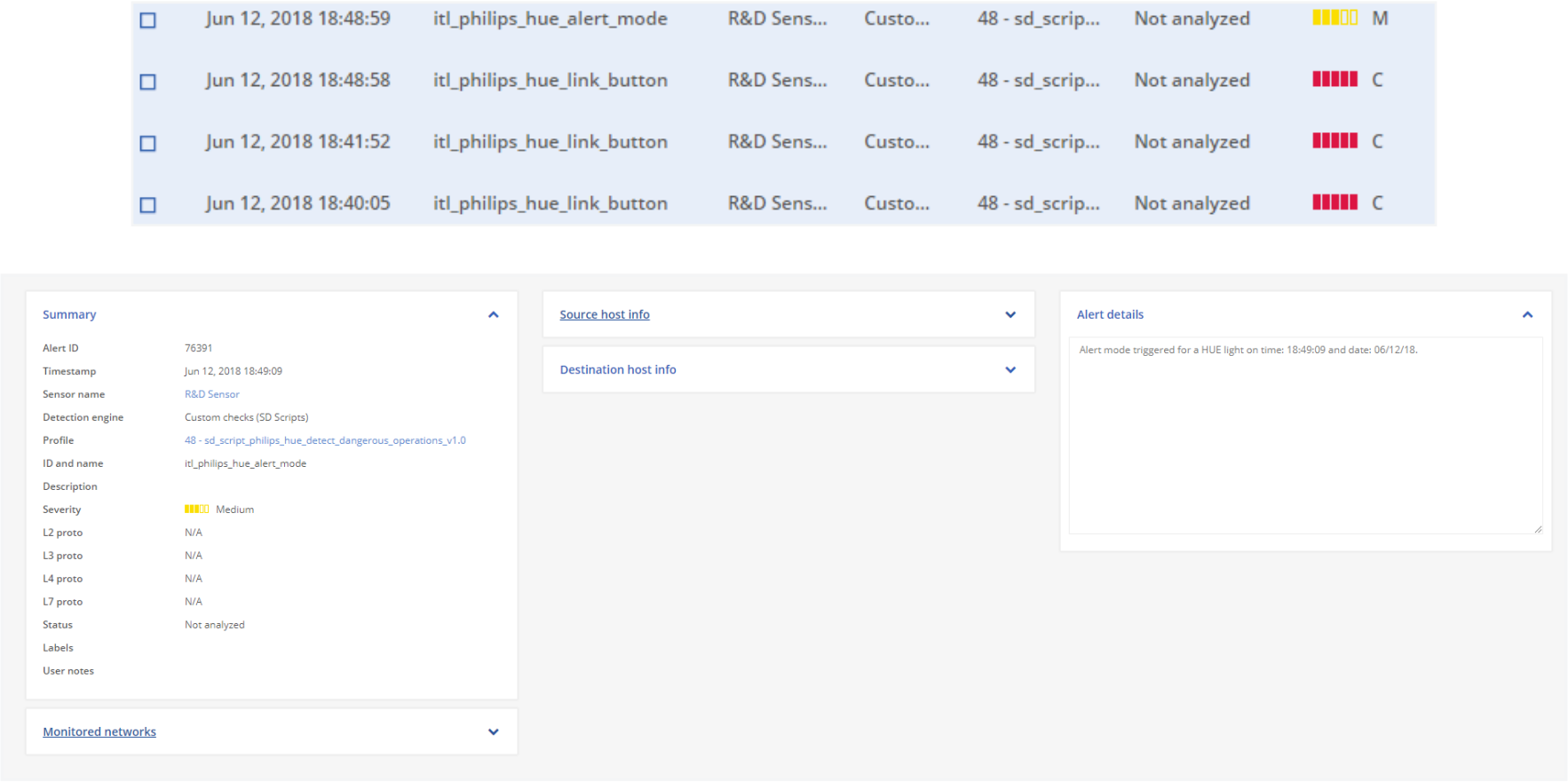
Another important feature of SilentDefense's monitoring capabilities is the **passive detection and classification of hosts seen on the network**.

The figure below shows an example of some hosts used in our lab setup as they are detected and classified, along with their network links by SilentDefense.



Alert raised when an unknown host streams to an NVR

Detecting Alert Mode Activation on the Philips Hue



Alerts for "Alert Mode" Being Remotely Activated on a Philips Hue

Detecting Plaintext Credentials Over MQTT

☐	May 29, 2018 17:12:10	mqtt_pdop_conn_requests	R&D Sensor	Custo...	34 - mqtt_p...	Not analyzed	H	192.168.212.61	192.168.212.69 (dan...	1883 (TCP)	MQTT
☐	May 29, 2018 17:12:10	MQTT Disclosed Credentials	R&D Sens...	Custo...	34 - mqtt_p...	Not analyzed	C	192.168.212.61	192.168.212.69 (dan...	1883 (TCP)	MQTT
☐	May 29, 2018 17:12:10	MQTT Disclosed Credentials	R&D Sens...	Custo...	34 - mqtt_p...	Not analyzed	C	192.168.212.61	192.168.212.69 (dan...	1883 (TCP)	MQTT
☐	May 29, 2018 16:55:11	MQTT Disclosed Credentials	R&D Sensor	Custo...	34 - mqtt_p...	Not analyzed	C	192.168.212.61	192.168.212.69 (dan...	1883 (TCP)	MQTT
☐	May 29, 2018 16:55:11	MQTT Disclosed Credentials	R&D Sens...	Custo...	34 - mqtt_p...	Not analyzed	C	192.168.212.61	192.168.212.69 (dan...	1883 (TCP)	MQTT
☐	May 29, 2018 16:55:06	(FEA Exit) MQTT QoS 2 Exce...	R&D Sens...	Custo...	34 - mqtt_p...	Not analyzed	N/A	192.168.212.61	192.168.212.69 (dan...	1883 (TCP)	MQTT
☐	May 29, 2018 16:53:34	(FEA Enter) MQTT QoS 2 Exc...	R&D Sensor	Custo...	34 - mqtt_p...	Not analyzed	N/A	192.168.212.61	192.168.212.69 (dan...	1883 (TCP)	MQTT
☐	May 29, 2018 16:53:34	MQTT QoS 2 Excessive Usage	R&D Sens...	Custo...	34 - mqtt_p...	Not analyzed	H	192.168.212.61	192.168.212.69 (dan...	1883 (TCP)	MQTT

Summary

Alert ID	71836
Timestamp	May 29, 2018 17:12:11
Sensor name	R&D Sensor
Detection engine	Custom checks (SD Scripts)
Profile	34 - mqtt_pdop
ID and name	mqtt_pdop_disclosed_credentials - MQTT Disclosed Credentials
Description	Attempted sharing of MQTT credentials in plain text.
Severity	Critical
Source MAC	00:0C:29:E6:7D:BE (Vmware)
Destination MAC	B8:27:EB:B3:57:CE (Raspberr)
Source IP	192.168.212.61
Destination IP	192.168.212.69 (daniel-develop.local)
Source port	41172
Destination port	1883
L2 proto	Ethernet
L3 proto	IP
L4 proto	TCP
L7 proto	MQTT
TCP stream opened in hot start mode	false
Status	Not analyzed
Labels	
User notes	

Monitored networks

Source host info

Destination host info

IP address	192.168.212.69 (Private IP)
Host name	daniel-develop.local
Other host names	pi.local
MAC addresses	B8:27:EB:B3:57:CE (Raspberr) 00:0C:29:8C:E3:08 (Vmware)
Role	Unknown
Client protocol(s)	DHCP (UDP 67) DNS (UDP 5353) FailedConnection (TCP 443) HTTP (TCP 80) NetBIOS (UDP 137) NoData (TCP 443, 40386, 40930, 51448) NotAKnownOne (UDP 8610, 8612)
Server protocol(s)	FailedConnection (TCP 80, 33908, 38942, 38948, 54824) MQTT (TCP 1883) NoData (TCP 52102, 52106) NotAKnownOne (TCP 22, 1883) SSH (TCP 22)
Labels	mqtt_role=Broker
Purdue level	4 - Site business network
Criticality	L
Known vulnerabilities	0
Related alerts	454 (Show)
First seen	May 9, 2018 18:56:57
Last seen	Jun 18, 2018 16:49:19

Alert details

Potential sharing of MQTT credentials in plain text.

Alerts for Detection of Plaintext Credentials over MQTT

Conclusion

Network visibility and asset inventory are crucial to identify vulnerable network segments, ensure business continuity and improve incident response strategies for both industrial and building automation networks. This holds especially true for smart buildings serving large corporations, since the network can contain several thousand assets distributed across multiple sites all over the world.

Cybersecurity strategy must be transformed to cope with the rise of the IoT. There are many activities that should be considered in a cybersecurity strategy, such as threat modeling, threat intelligence, vulnerability management, risk management, security reviews, and supply chain risks.

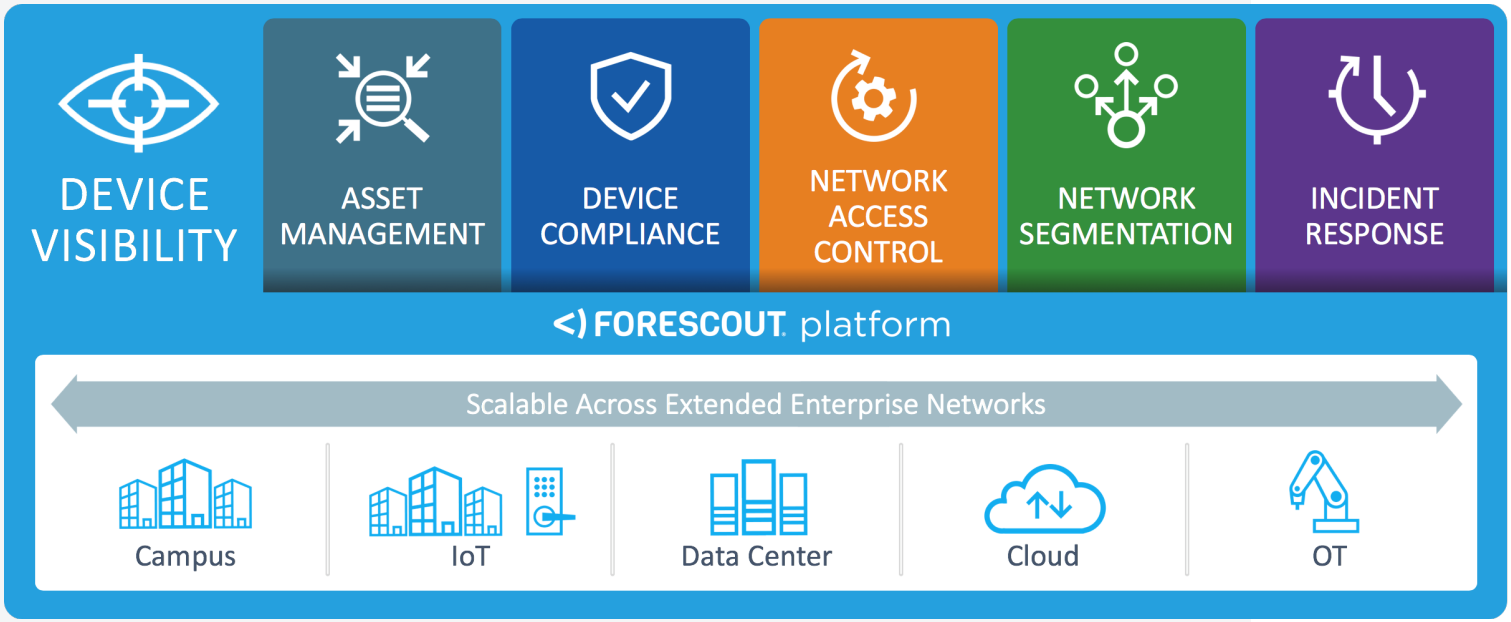
The cornerstones of a robust cybersecurity strategy for the age of IoT are device visibility and control, since they are crucial enablers for other cybersecurity-related activities.

> "Device visibility and control are the cornerstones of a robust cybersecurity strategy."

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, and operational technology (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 SilentDefense 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, 2019 https://www.forescout.com/places-in-network/building-automation-system-bas/transforming-cybersecurity-strategy-for-the-iot/

[3] B. Tratz-Ryan and B. Finnerty, "Hype Cycle for Smart City Technologies and Solutions," Gartner, 2018

FORESCOUT

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