



Interoperability & Security in the IoT Landscape

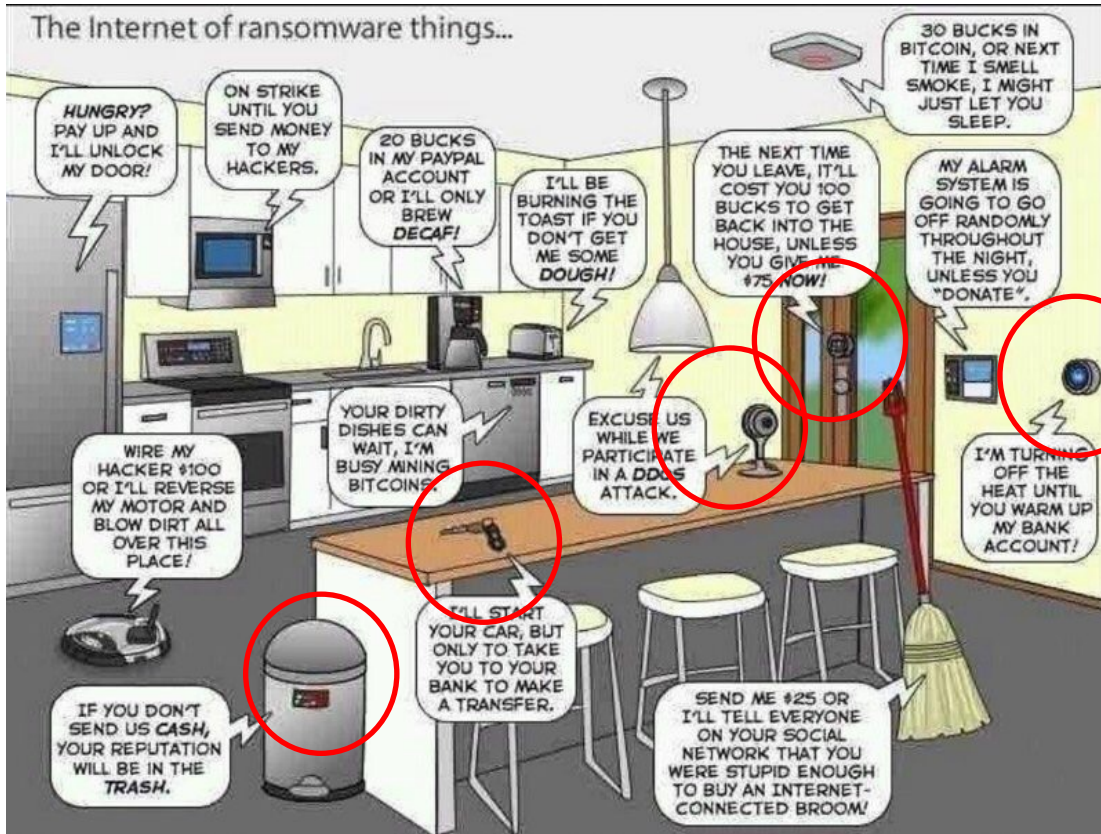
Toni Buhrke

WW Director, Channel Systems Engineering

June, 2017



IoT: Internet of Threats



One by one,
these are
becoming a
reality.

Time to secure
them is now.

IoT Attack Targets



Botnet



Retail



Finance



Various
other banks



Automation



Physical Security



Transportation



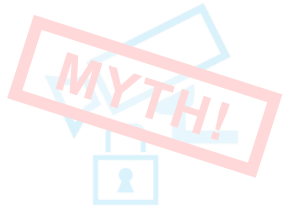
Gaming



PLAYSTATION
Network

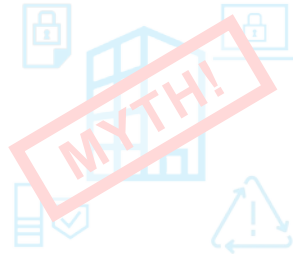


Dispelling the IoT Security Myths



Myth 1

Manufacturers will build IoT devices with embedded security



Myth 2

Current security investments will protect the company



Myth 3

Block employees from connecting IoT devices



Myth 4

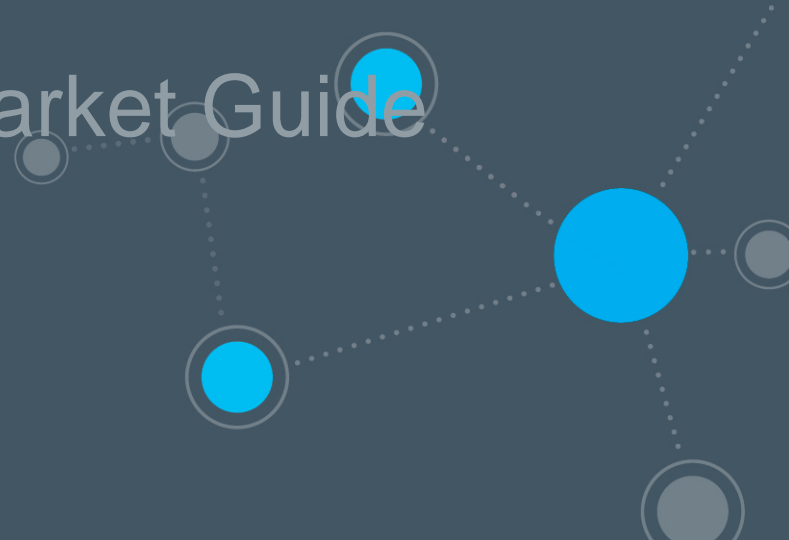
Find, fix hacked IoT devices

1 IoT Landscape

2 Threat Landscape

3 Gartner IoT Security Market Guide

4 ForeScout Solution



Exponential IoT Growth

PC's & Mobile Devices

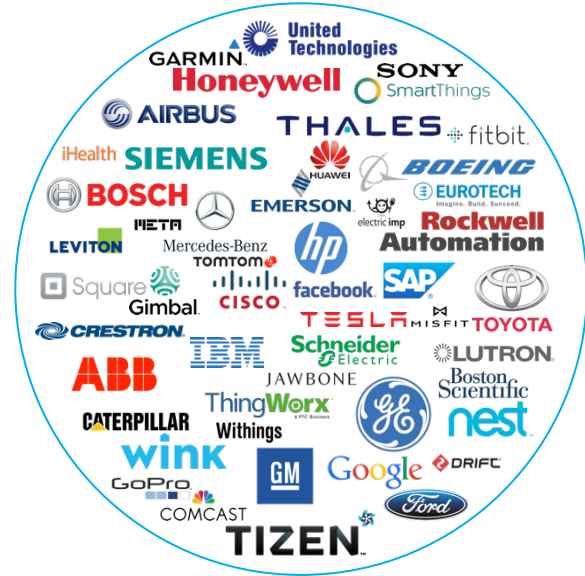


Took **25 years** to get to
10 Billion devices*

Source: Gartner IoT, PC and Mobile device forecast 2015

Reference acronym glossary at the end of presentation

IoT Devices



Will take only **5 years** to get
to **30 Billion devices***

IoT Device Landscape is Fragmented

IoT Device / Solution Vendors by Physical Environments



Device landscape is going from few devices and OS types to innumerable devices and OS types

Source: Harbor Research, 2014; McKinsey Global Institute, 2015

Reference acronym glossary at the end of presentation

IoT Adoption Driven by Business Needs

Challenges and Lessons Learned

BYOD

Resistance was futile – Shadow IT
Users needed it to do their jobs
Non-IT provisioned devices
IT couldn't manage the devices via agents

IoT

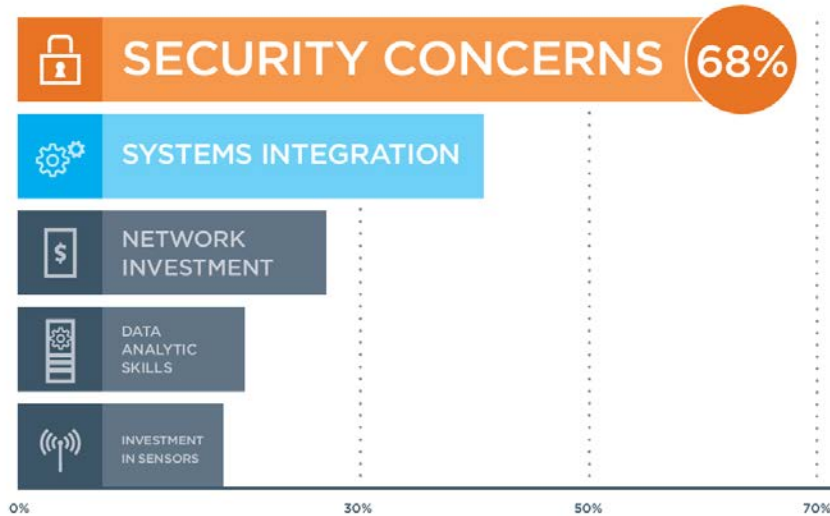
Resistance is futile – Shadow IoT Devices
Businesses need IoT to improve their business
Non-IT provisioned devices
IT can't manage the devices via agents

Nothing is more powerful than an
idea whose time has come –
Victor Hugo

Security is the Top Impediment to IoT Adoption

WE ASKED:

What are the biggest IT challenges with respect to IoT?



Source: 2016 ForeScout IoT Survey

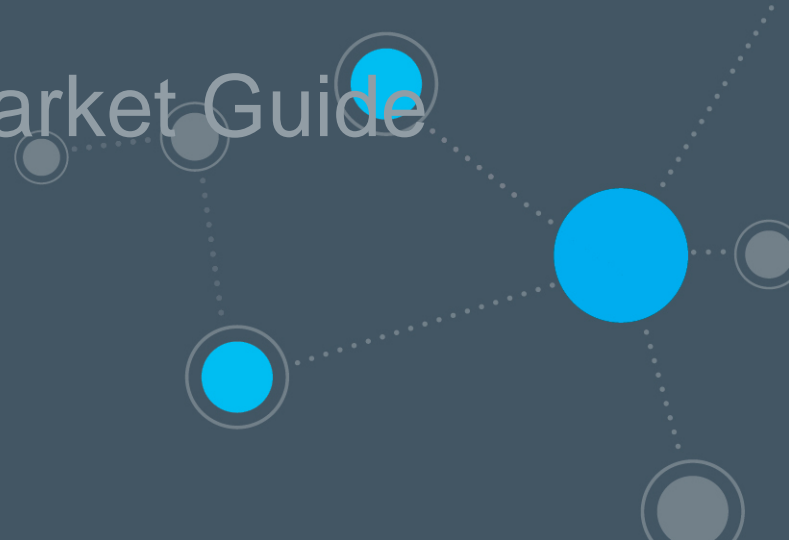
Reference acronym glossary at the end of presentation

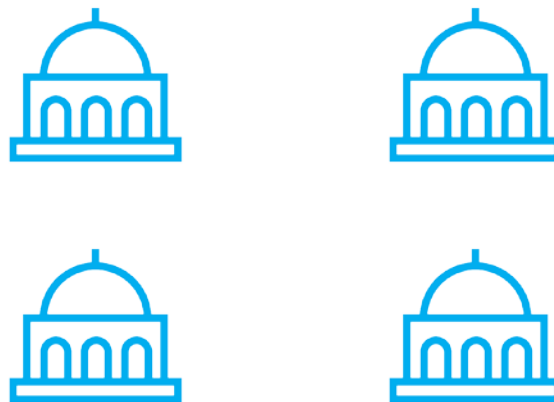
1 IoT Landscape

2 Threat Landscape

3 Gartner IoT Security Market Guide

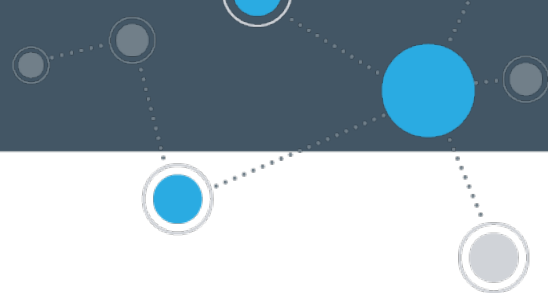
4 ForeScout Solution





Various banks

Various Banks



Overview: The Billion Dollar Bank Job: How hackers stole \$1bn from 100 banks in 30 countries

Devices: Video surveillance camera among others

Industry: Finance

Description: Carbanak gang (named after the malware it uses), with members in Russia, Ukraine, China and other parts of Europe, has been stealing tens of millions of dollars from banks, e-payment systems and other financial institutions since 2013. In addition to other means the gang used the bank's own cameras against them, the gang were able to see and record everything that was happening on the screens of bank employees. By monitoring these screens the hackers were able to gain intimate knowledge of just how each bank's specific internal systems worked, allowing them to tailor each attack.

<http://www.ibtimes.co.uk/billion-dollar-bank-job-how-hackers-stole-1bn-100-banks-30-countries-1488148>

Reference acronym glossary at end of presentation

Sberbank & Alfabank



Overview: Russian banks floored by withering DDoS attacks

Devices: Botnet on CCTV cameras

Industry: Finance

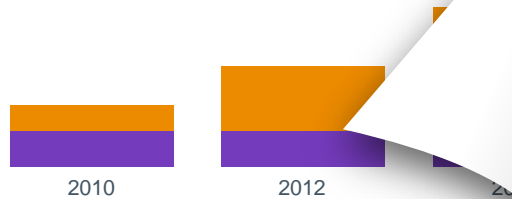
Description: The Central Bank officially confirmed that a DDoS attack was made using the devices related to the Internet of things. This is the first officially recognized case in Russia, where criminal activity could be used to attack smart refrigerator, smart TV, security system, front door or even a light bulb.

http://www.theregister.co.uk/2016/11/11/russian_banks_ddos/

IoT Opens Much Bigger Attack Surface



Less than 10% of new devices connecting to the corporate environment will be manageable through traditional methods



Source: Gartner, BI Intelligence, Verizon, ForeScout

[Reference acronym glossary at the end of presentation](#)

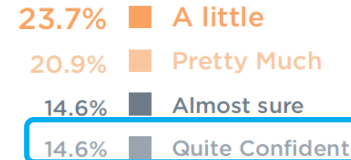
66%
of all networks will have an IoT security breach by 2018



Visibility is a Top Security Concern

WE ASKED:

How confident are you that you are aware of all the IoT devices on your network?



Only 14.6% quite confident about visibility into their IoT devices

A Perfect Storm of Threats Creating New Security Needs

Attacks targeting devices that corporations can't see



Insecurity of Things: Danger Rankings



DISASTROUS
Cause irreversible damage



Security Systems



Energy Meters



DISRUPTIVE
Disrupt corporate and operational processes.



Smart Video Conferencing Systems



Connected Printers



VoIP Phones



DAMAGING
Enable information stealing



Smart Fridges



Smart Lightbulbs

Insecurity of Things: Danger Scenarios



Tampering with temperature controls



Spying via video and microphone



Extracting Wi-Fi credentials to carry out further attacks



Disabling to allow physical break-ins



Snooping on calls



Accessing private company and user information



Obtaining user credentials



IP-Connected Security Systems

Many use proprietary radio frequency technology that lack authentication and encryption.

Attackers can form radio signals to send false triggers and access system controls.

User compute capability to exfiltrate large amounts of data.

Disable camera to allow physical break in.

Hijack camera to spy on employees usage of computers, passwords, applications, designs.

Use as launching point for DDoS attacks.





IP-Connected Infrastructure: Climate Control & Energy Meters

HVAC systems provide an avenue for hackers to gain network access

Attackers can force critical rooms (for example, server rooms) to overheat and cause physical damage.



IP-connected infrastructure uses wireless technology that is often accessible to anyone within range.



Smart Video Conference Systems

These often only require the click of a button for users to share screens – and for hackers to commandeer it.

Attackers have full access to all software, memory and hardware, exposing the microphone, camera and stored credentials.



Smart TVs connect to the local network over IP and also serve as a pivot point for hackers to gain full network access.



Connected Printers

Nearly all printers are networked over IP - a welcome mat to hackers to infiltrate the enterprise.

Without physical access, hackers can compromise printers to siphon private documents printed through them.



Many exploitable issues are not resolvable without updates to firmware or an intrusion detection system.



VoIP Phones

VoIP phones leverage the network for many sophisticated features that makes communication easy, not only for employees – but also malicious hackers.



Hackers can exploit configuration settings to evade authentication and then update the phone, allowing them to listen to phone conversations or make calls.



Smart Lightbulbs

Smart lightbulbs operate on Wi-Fi and proprietary mesh networks which can be hacked.

Mesh network communication channels can be sniffed by attackers.



Hackers can extract password-protected Wi-Fi credentials without being on the network, allowing them to gain access to other systems and devices in the network.

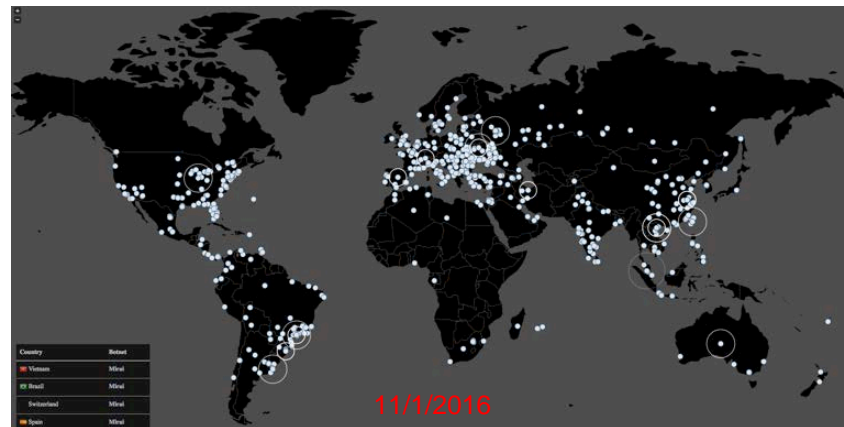
Mirai Botnet


Mirai used in DynDNS attack on ~100K devices involved.



Follow Mirai Attacks on Twitter – [@MiraiAttacks](https://twitter.com/MiraiAttacks).

A tweet is sent each time a Mirai attack is detected, as of Feb 6th 2017, there were over 1,750 tweets with count starting in October 2016.



- 1 IoT Landscape
 - 2 Threat Landscape
 - 3 Gartner IoT Security Market Guide
 - 4 ForeScout Solution
- 

Market Guide for IoT Security

Published: 03 October 2016 **ID:** G00310115

Analyst(s): Saniye Burcu Alaybeyi, Earl Perkins, Ruggero Contu

Summary

IoT security solutions enable organizations to securely manage IoT devices, and ensure IoT endpoint and data security, and asset discovery. IoT security and risk management leaders should use this research to understand how to evaluate and select solutions to meet their IoT security requirements.

Overview

Key Findings

- Three eclectic types of product vendors are emerging for securing IoT: embedded trust; device identity and key/credential management; and real-time visibility and control.
- Clients who are performing proof-of-concept trials are getting better clarity about a product's compatibility with their organization's environment and requirements.
- Low complexity in IoT deployment, flexibility of IoT security controls, ease of integration and competitive product pricing are the main selection criteria for IoT security and risk management leaders.

Key Insights

VIEW FULL DOCUMENT



Real-Time Discovery, Visibility and Control Are Critical for IoT Security

Published: 03 November 2016 ID: G00317261

Analyst(s): *Saniye Burcu Alaybeyi | Lawrence Orans*

Summary

Discovery and visibility are critical prerequisites to Internet of Things security. Security and risk management leaders in charge of IoT implementations will need to select an IoT network and device security strategy that will address specific visibility use-case requirements.

Overview

Key Findings

- Lack of network and device visibility is a top concern of security and risk management leaders, both in consumer and industrial IoT verticals, as they don't know what assets they have and if protection is required. Discovery is a prerequisite to IoT security.
- Unrecognized business benefits of "discovery and

List of Figures

Figure 1. Business Drivers for IoT Security via Discovery, Visibility and Control

Figure 2. Risk Management as Business Driver

Figure 3. Asset Discovery as Business Driver

Figure 4. Authentication as Business Driver

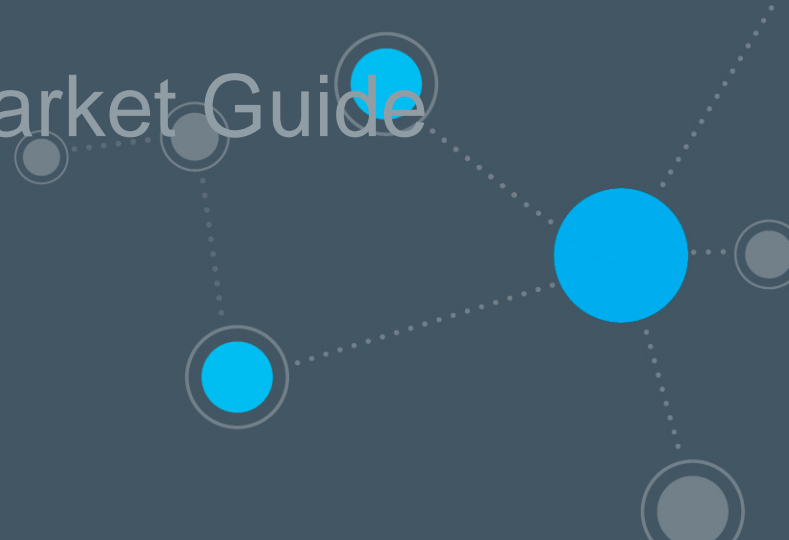
Figure 5. Incident Response as Business Driver

Table of Contents

Figure 1.

Business Drivers for IoT Security via Discovery, Visibility and Control



- 1 IoT Landscape
 - 2 Threat Landscape
 - 3 Gartner IoT Security Market Guide
 - 4 ForeScout Solution
- 

Many IoT Devices Are Invisible

Many IoT devices cannot host an agent

Many IoT devices run on outdated or unsupported software

Many IoT devices cannot be patched

Many IoT devices lack firewall capability



ForeScout's agentless solution helps overcome these limitations

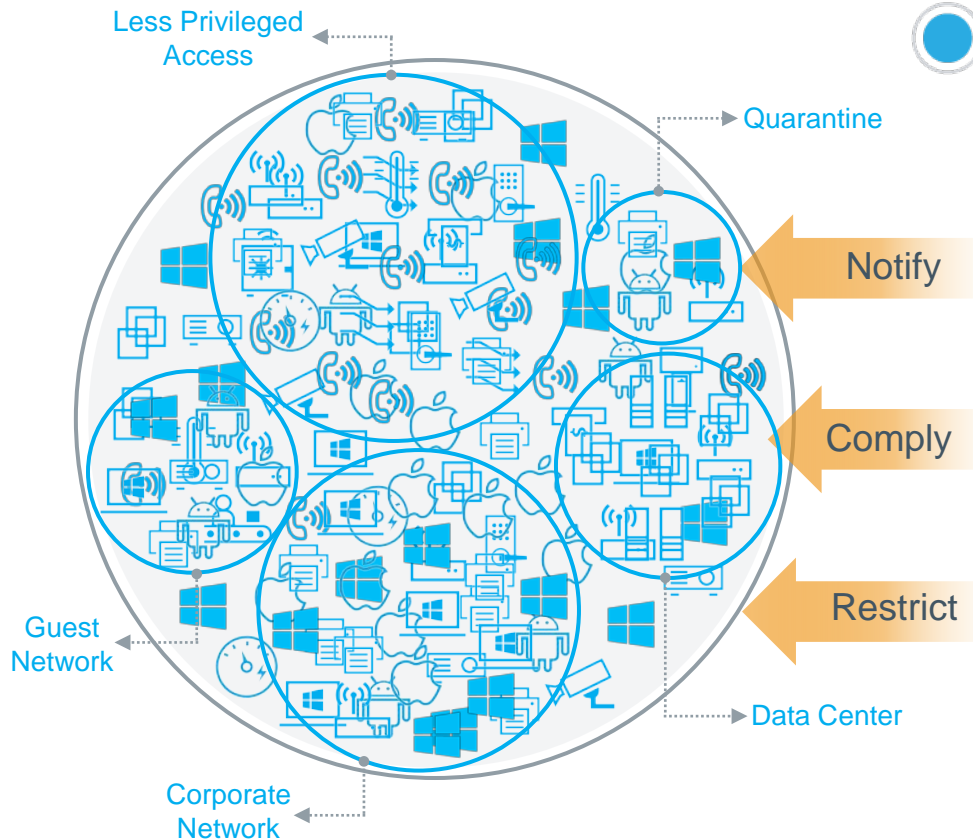
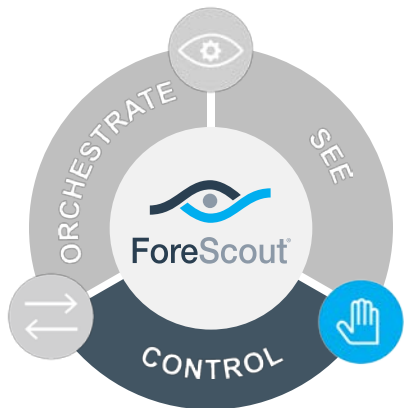
Many IoT devices are invisible to the traditional security systems



	Manageable with an Agent	Non-Traditional/IoT
Computing Devices		
Network Devices		
Applications		
IoT	See with	

- What is the device?
- Who owns the device?
- Where/how is it connecting?
- What is the device hygiene?
- What IP's should the device connect to?
- Which users have access to administrate the device?

Control



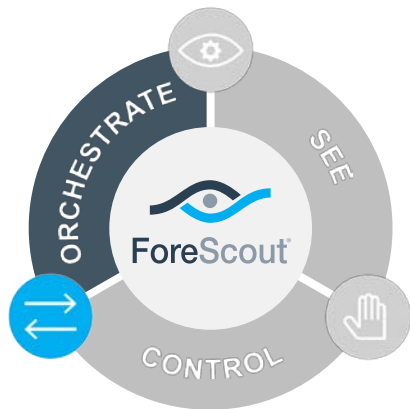
Is the device trying to use a different port to communicate?

Is the device trying to connect to additional IP's on the network?

Is an unauthorized user trying to access the device?

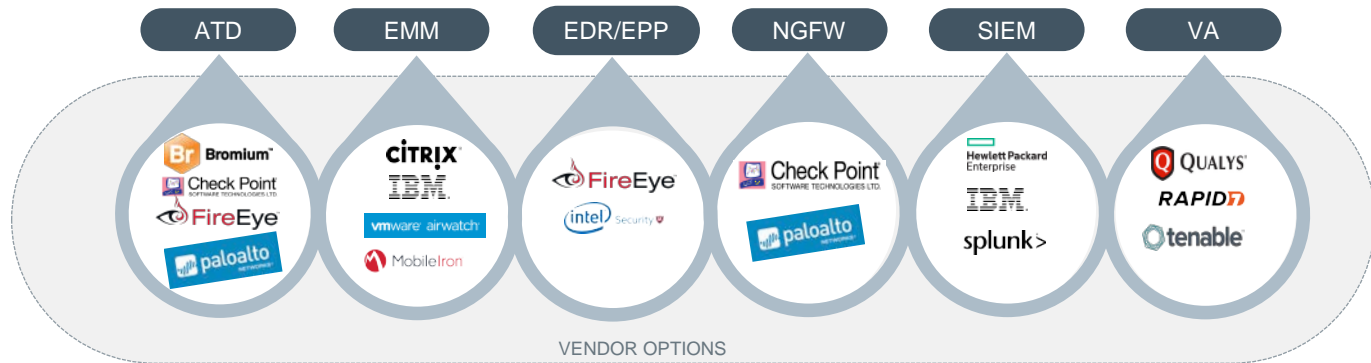
Is the device trying to reach the internet?

Orchestrate

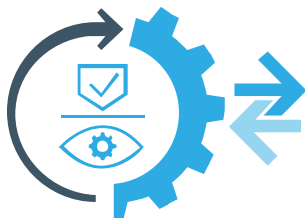


BREAK DOWN SILOS

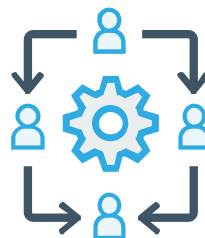
MAXIMIZE EXISTING INVESTMENTS



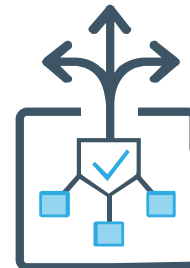
Share Contextual Insights



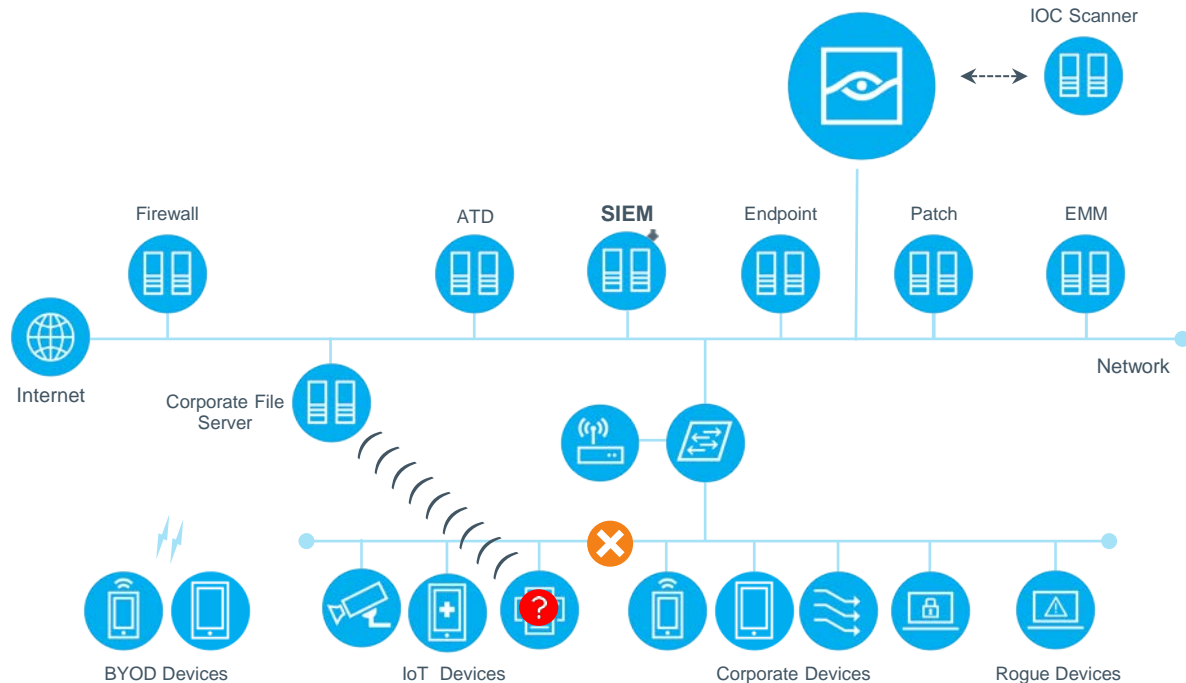
Automate Workflows



Automate Response Actions



IoT Use Case

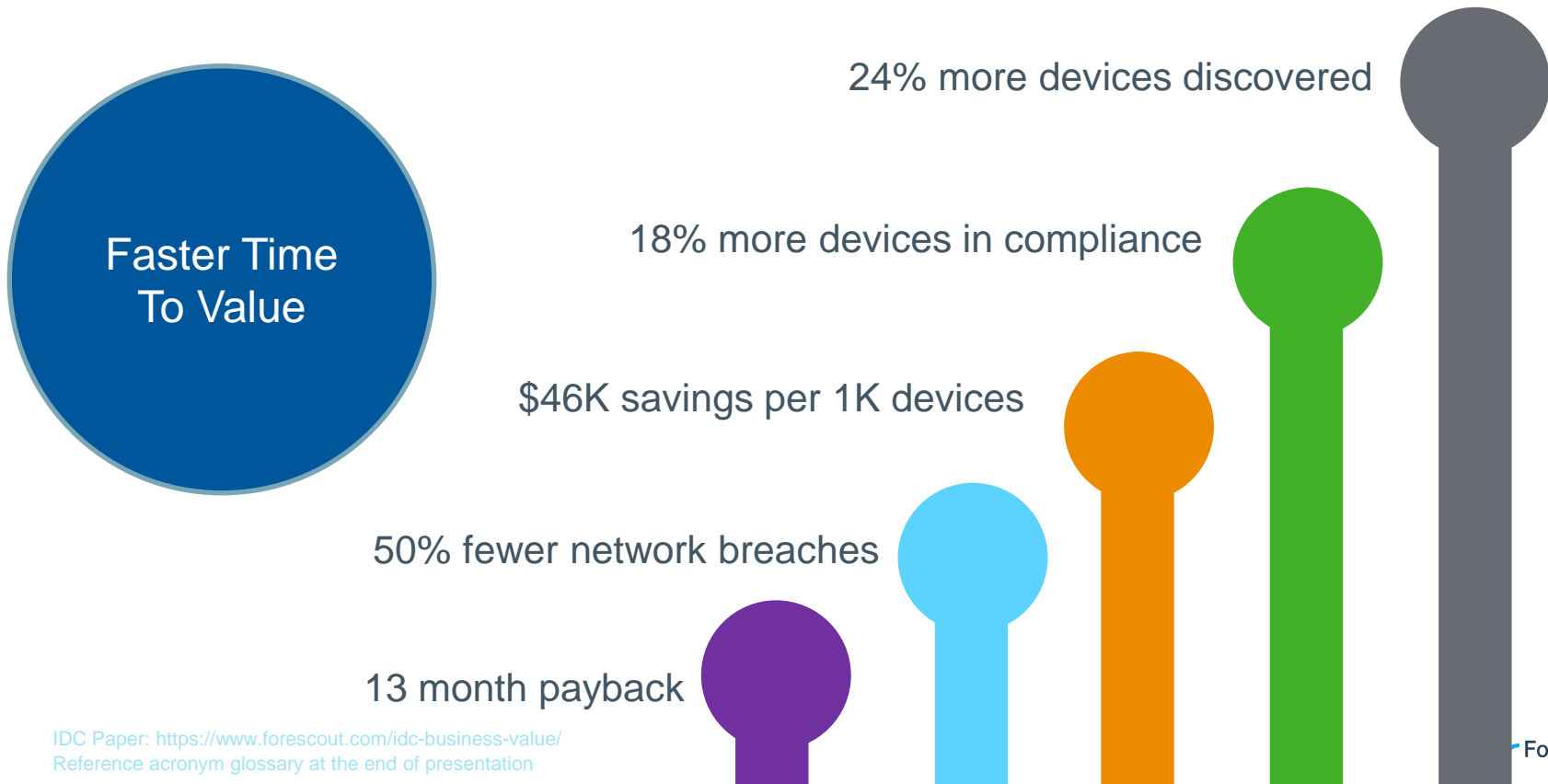


- 1 Device connects to the network
- 2 Device is detected and classified as a printer
- 3 Compromised printer* communicates with the corporate file server
- 4 SIEM detects an anomaly
- 5 Compromised printer is blocked from accessing the network

* This printer could be one of the many other IoT devices as well and ForeScout would secure it

Business Value of a ForeScout Solution

IDC interviewed 7 ForeScout customers, and on an average, benefits were



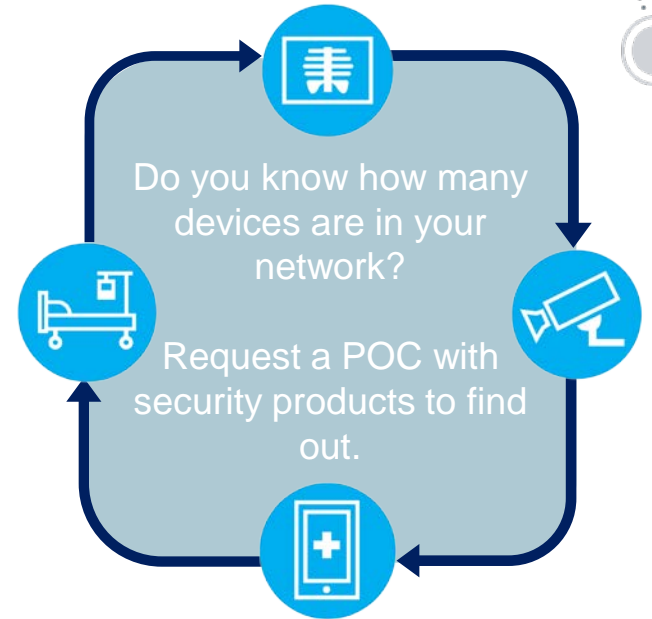
Summary

IoT devices are entering Healthcare industry in a big way.

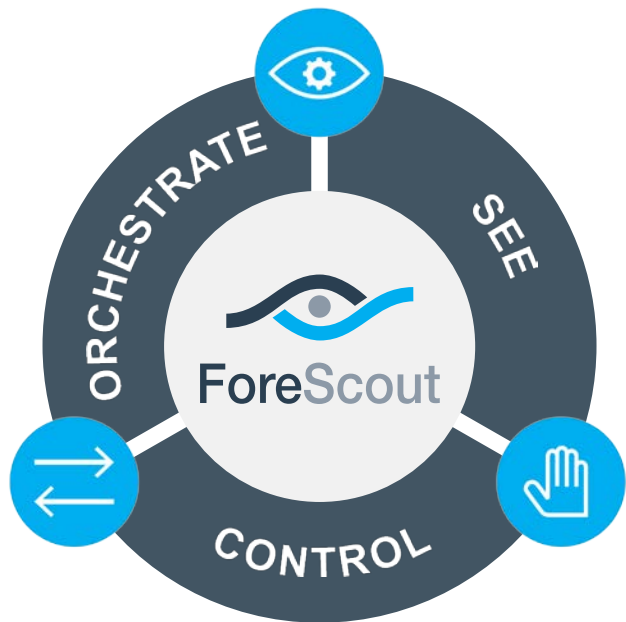
Many IoT devices lack basic security features and are invisible to traditional security systems, posing bigger security risk!

Many organizations underestimate number of IoT devices in their networks thereby opening up vulnerabilities.

ForeScout's agentless approach has helped companies discover on an average 24% more devices on their networks – IDC Report.



ForeScout Benefits



- Real time and continuous visibility
- Agentless approach
- 24% more known devices
- 18% more devices in compliance
- 50% fewer network related security breaches

Source: IDC white paper on Business Value and IT impact of visibility and control <https://www.forescout.com/idc-business-value/>

Reference acronym glossary at the end of presentation



The End

