8 SECURITY STRATEGIES FOR UNMANAGED DEVICES IN THE ENTERPRISE WEBINAR

Towerwall
Protecting Data Integrity

armis

Featuring Jack Marsal, Sr. Director of Product Marketing, Armis and Michelle Drolet, Founder & CEO, Towerwall

Your Partner in Data Protection

For **over 25 years**, we have helped scores of companies **safeguard their data** and **leverage their investment in IT** with advanced information security solutions and services.

Towerwall At-a-Glance

Team led by

Michelle Drolet

110+

Years of Experience

Our team has more than 110 years of combined experience protecting data integrity.

100+

Companies Safeguarded

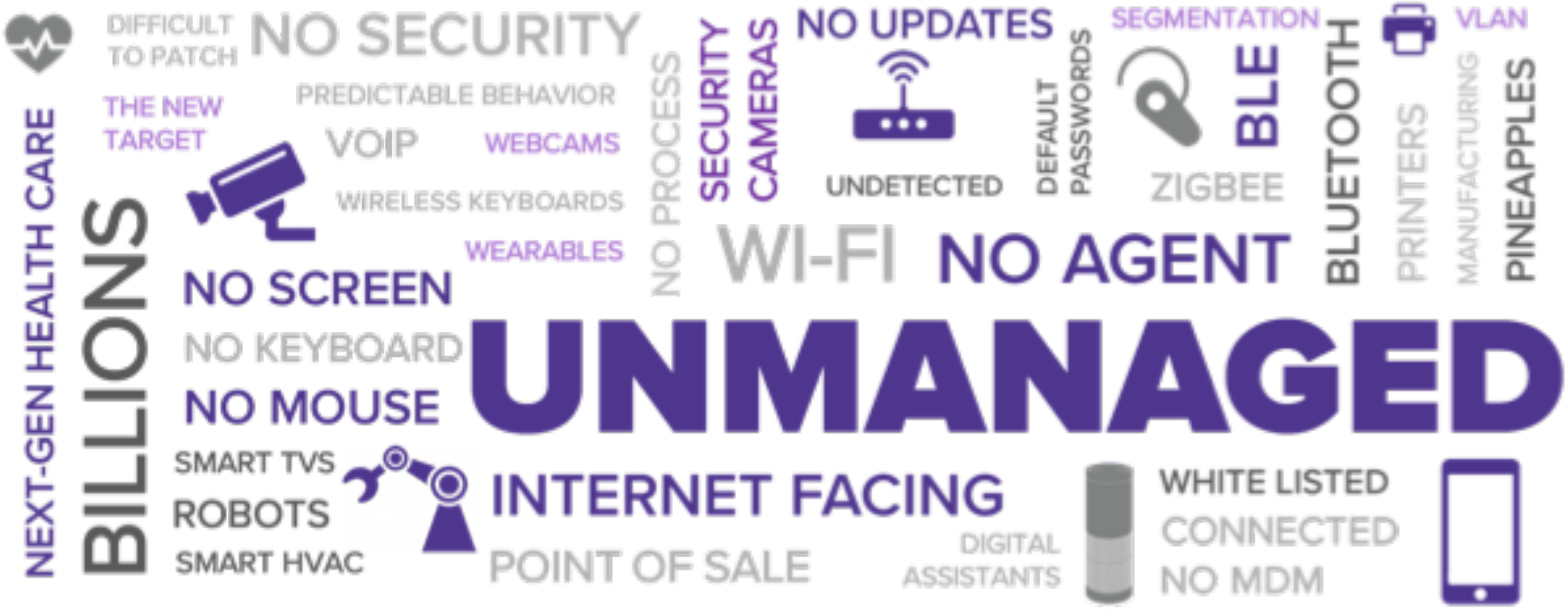
We have helped hundreds of companies safeguard their data and leverage their investment in IT .

8 SECURITY STRATEGIES FOR UNMANAGED DEVICES IN THE ENTERPRISE

Jack Marsal

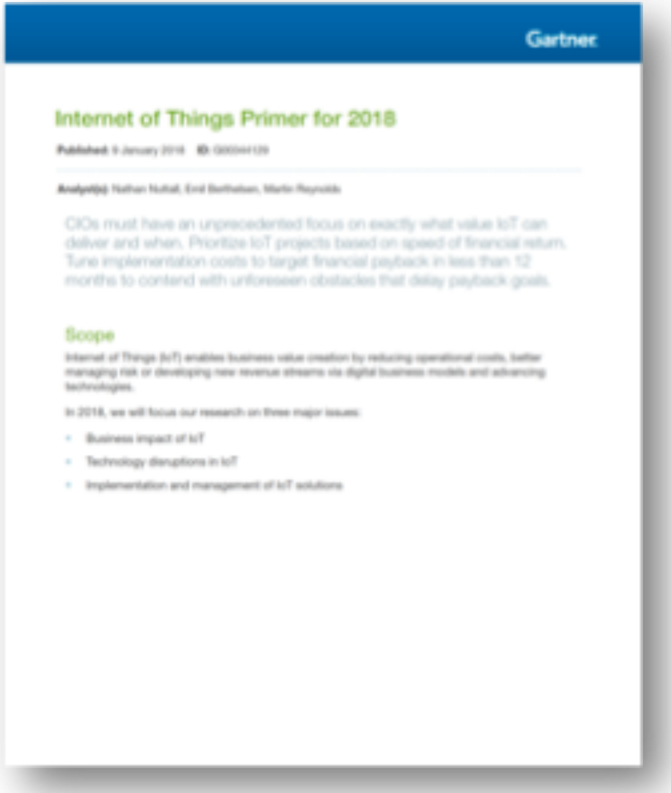
Sr. Director of Product Marketing

Unmanaged Devices = IoT



> “IoT has become the leading technology for digital transformation and is the number one priority for 92 per cent of organizations.”

Inmarsat, “The Future of IoT in Enterprise -- 2017”



Gartner

Internet of Things Primer for 2018

Published: 9 January 2018 **ID:** G00344129

Analyst(s): Nathan Nuttall, Emil Berthelsen, Martin Reynolds

CIOs must have an unprecedented focus on exactly what value IoT can deliver and when. Prioritize IoT projects based on speed of financial return. Tune implementation costs to target financial payback in less than 12 months to contend with unforeseen obstacles that delay payback goals.

Scope

Internet of Things (IoT) enables business value creation by reducing operational costs, better managing risk or developing new revenue streams via digital business models and advancing technologies.

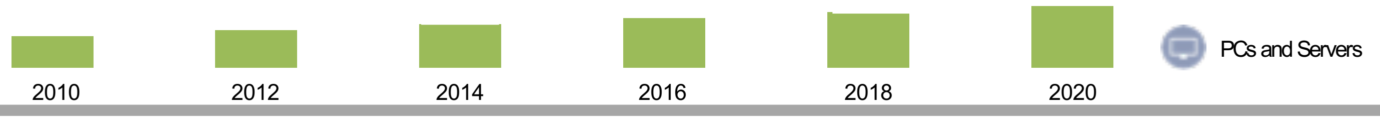
In 2018, we will focus our research on three major issues:

- Business impact of IoT
- Technology disruptions in IoT
- Implementation and management of IoT solutions

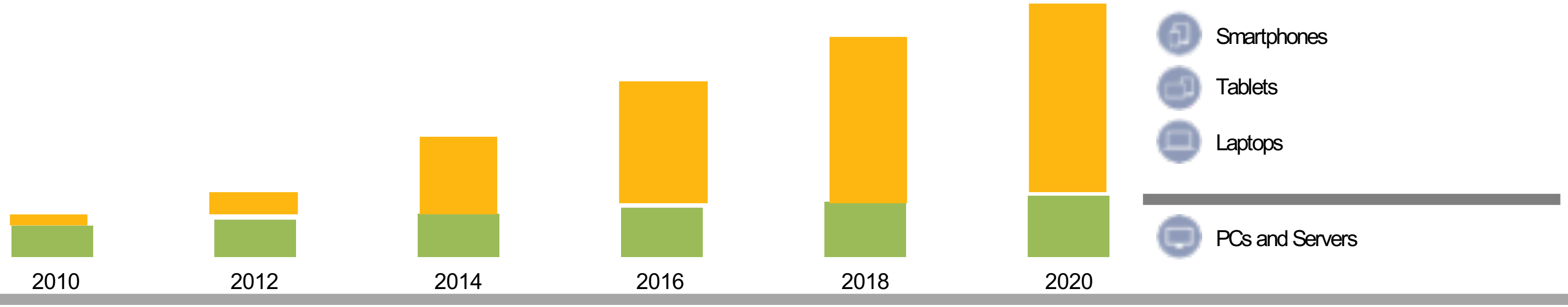
“IoT architectures and solutions are critical enablers to achieving innovative and planned business outcomes.”

Gartner, “Internet of Things Primer for 2018”, 9 January 2018, Nathan Nuttall, Emil Berthelsen, Martin Reynolds

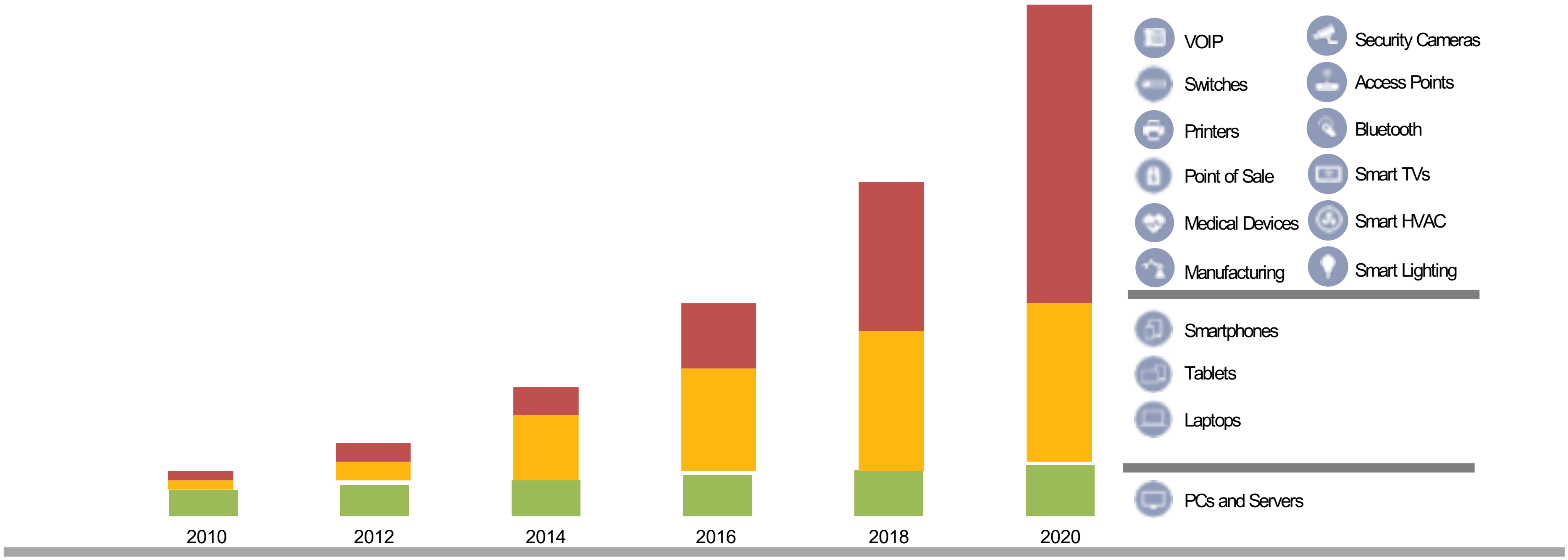
Explosion of IoT on Enterprise Networks



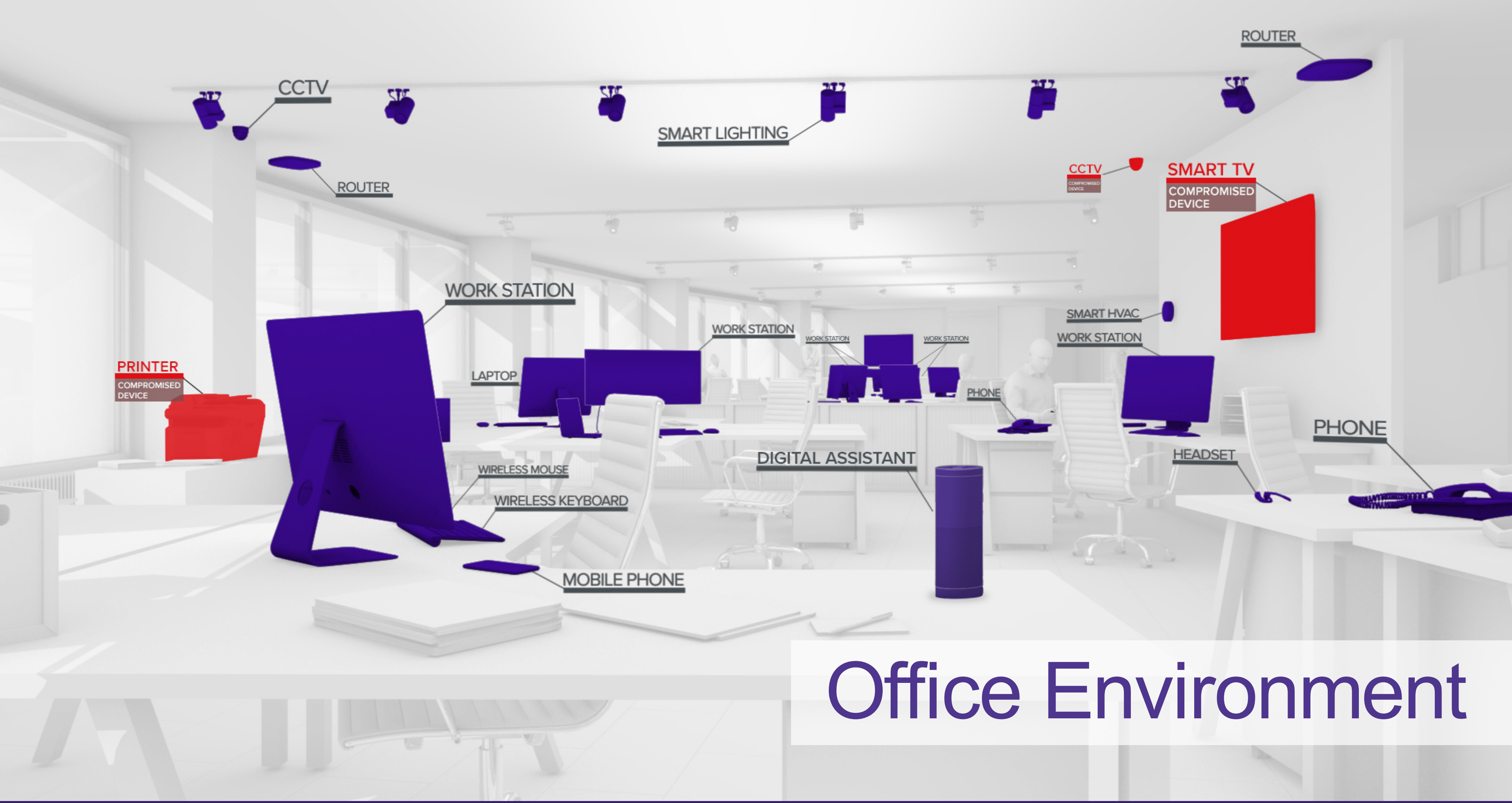
Explosion of IoT on Enterprise Networks



Explosion of IoT on Enterprise Networks

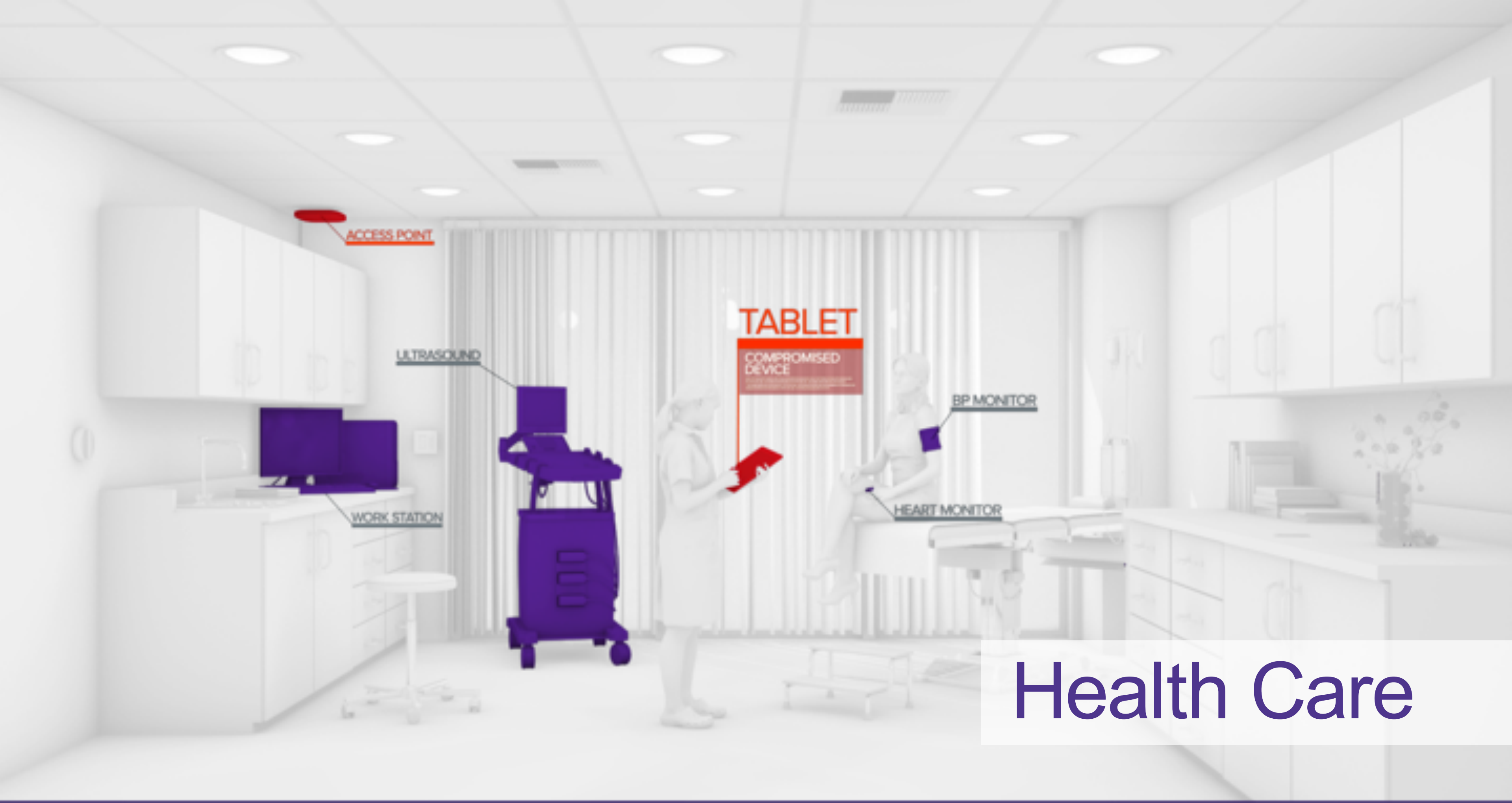


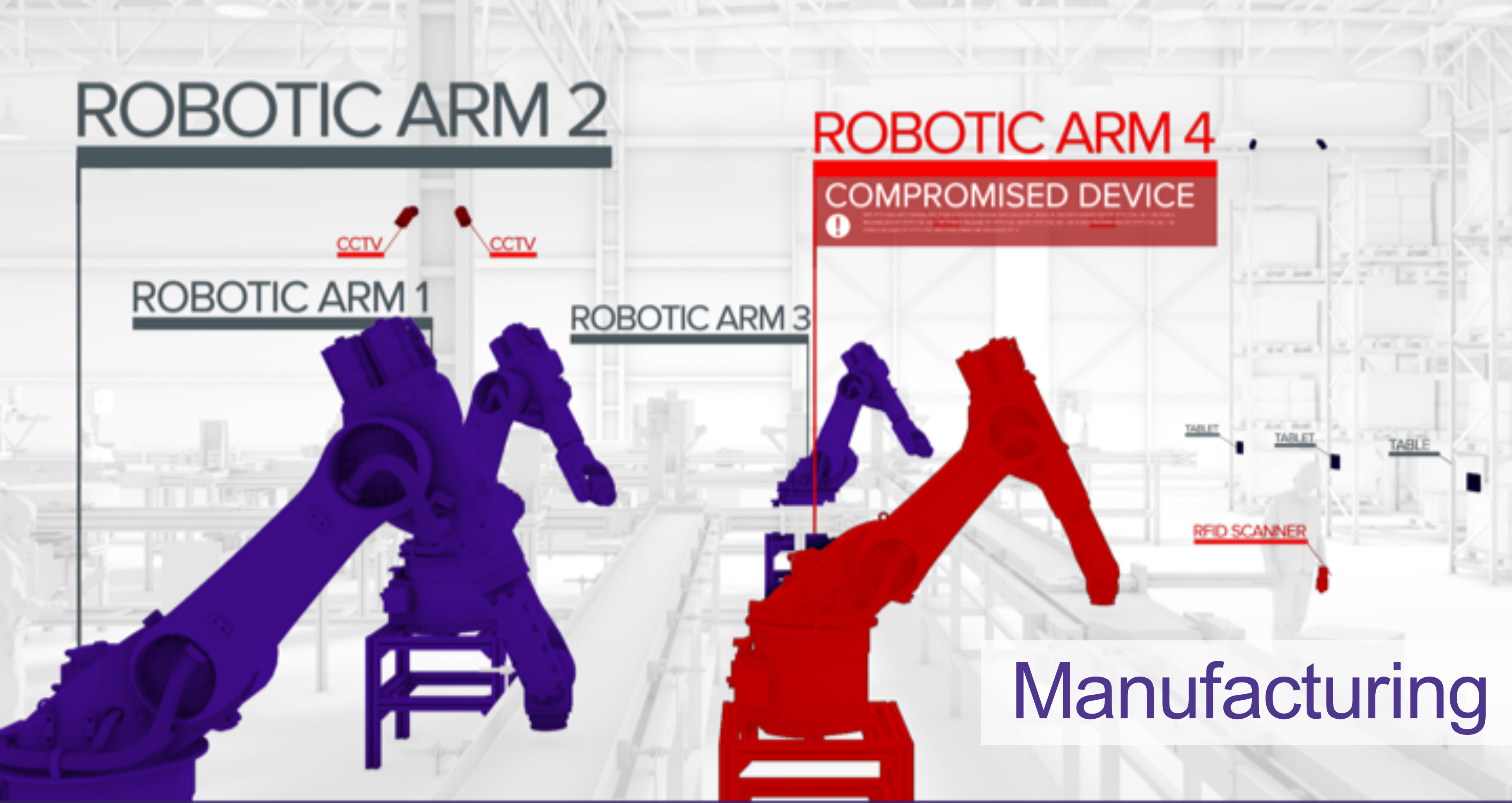
Office Environment



armis

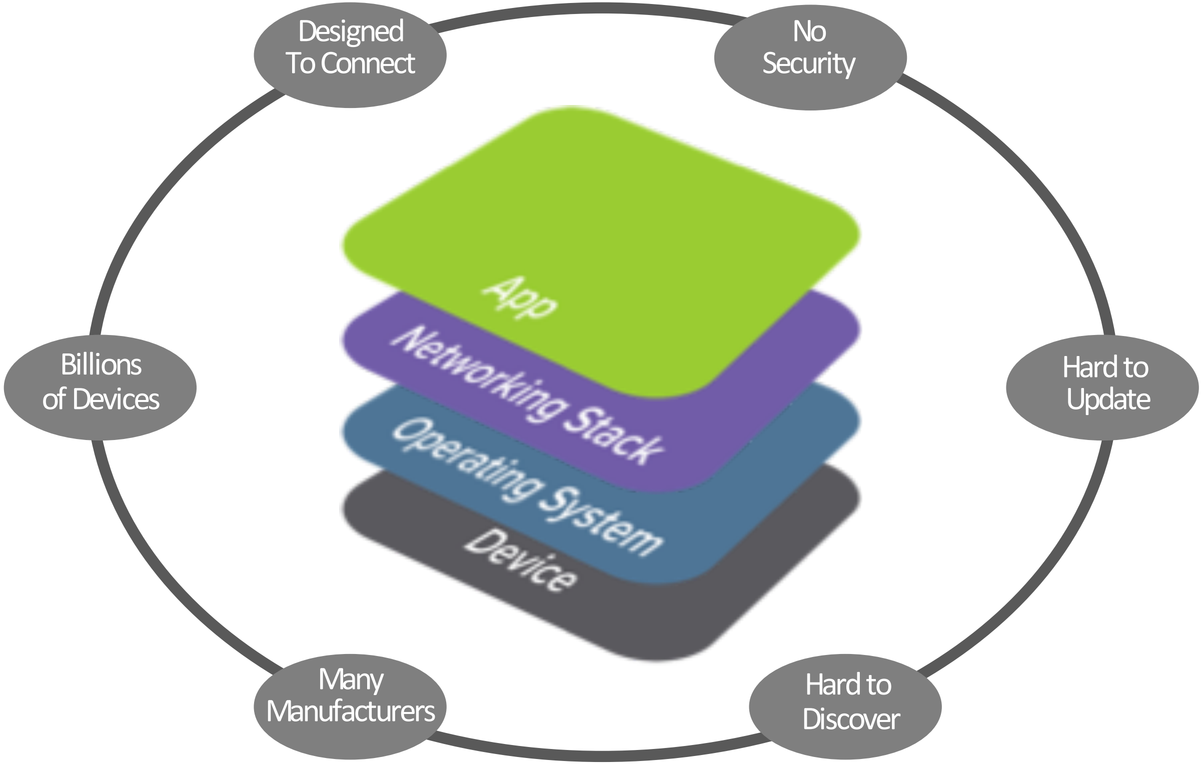
Health Care

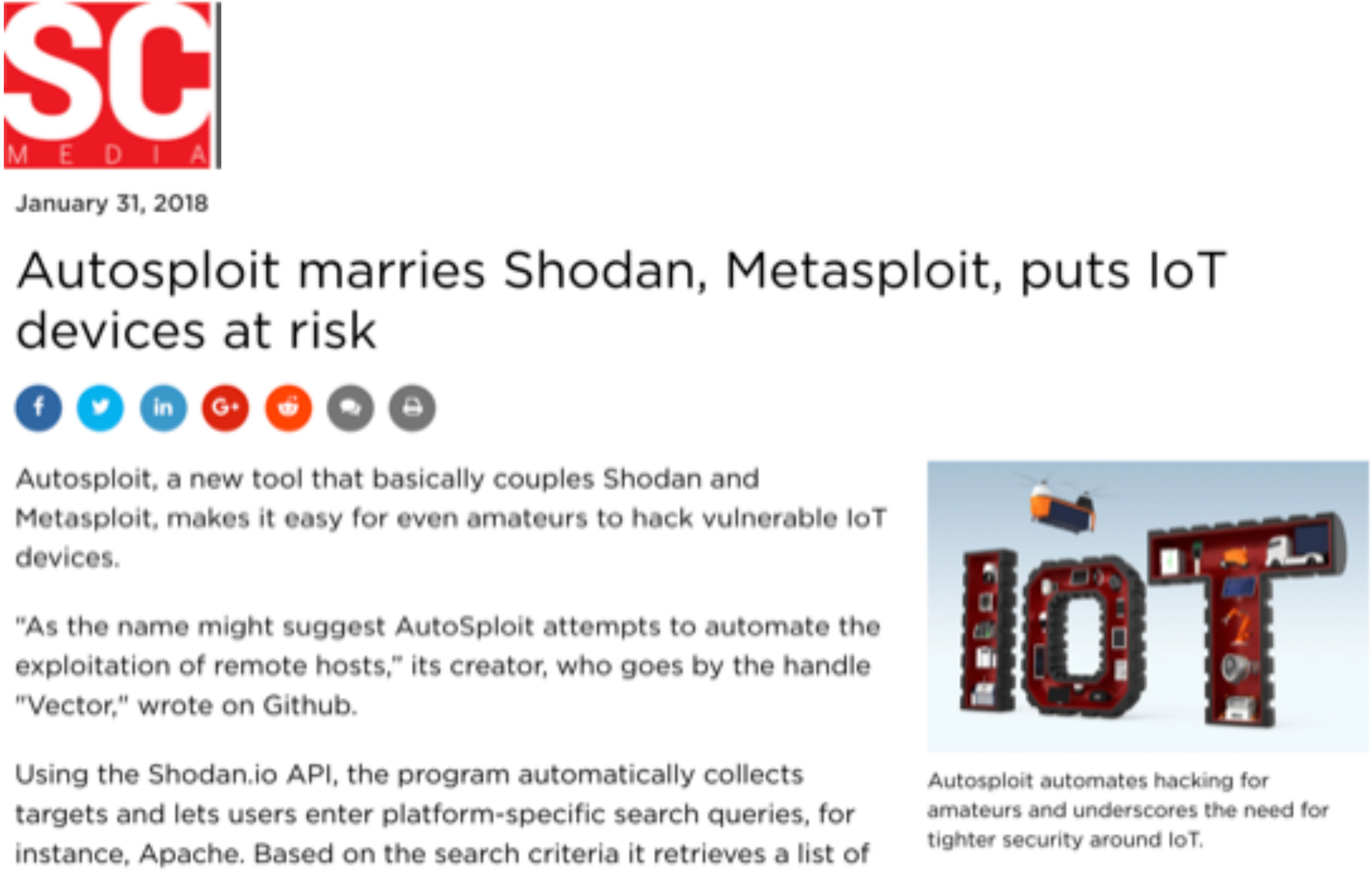

ACCESS POINT
ULTRASOUND
WORK STATION
TABLET
COMPROMISED DEVICE
BP MONITOR
HEART MONITOR



Manufacturing

Meet The New (Insecure) Endpoint





January 31, 2018

Autosploit marries Shodan, Metasploit, puts IoT devices at risk

Autosploit, a new tool that basically couples Shodan and Metasploit, makes it easy for even amateurs to hack vulnerable IoT devices.

"As the name might suggest AutoSploit attempts to automate the exploitation of remote hosts," its creator, who goes by the handle "Vector," wrote on Github.

Using the Shodan.io API, the program automatically collects targets and lets users enter platform-specific search queries, for instance, Apache. Based on the search criteria it retrieves a list of

Autosploit automates hacking for amateurs and underscores the need for tighter security around IoT.

Attacks on Unmanageable Devices are Increasing

600% Increase in attacks from 2016 to 2017

Symantec ISTR 2018

46% had a breach or security incident associated with IoT security.

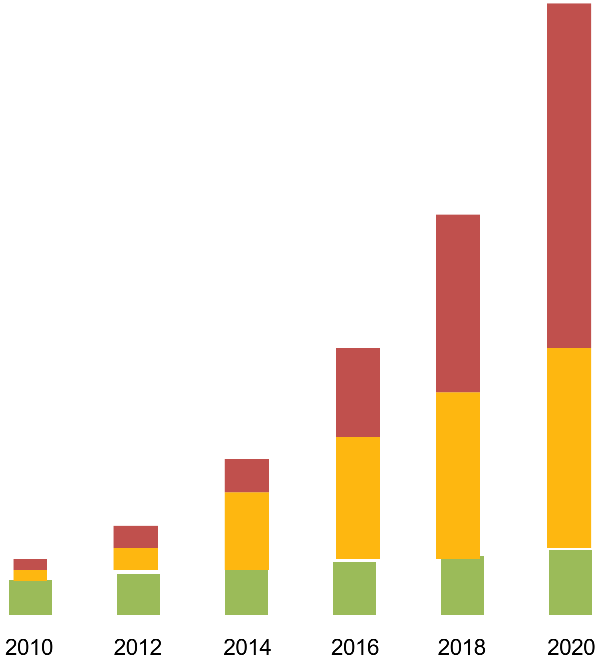
IDC, 2017

25% of all identified attacks in enterprises will involve unmanageable devices by 2020.

Gartner, 2017

Can Spread From Device To Device

What is Your Security Strategy for IoT?



Types of Endpoints

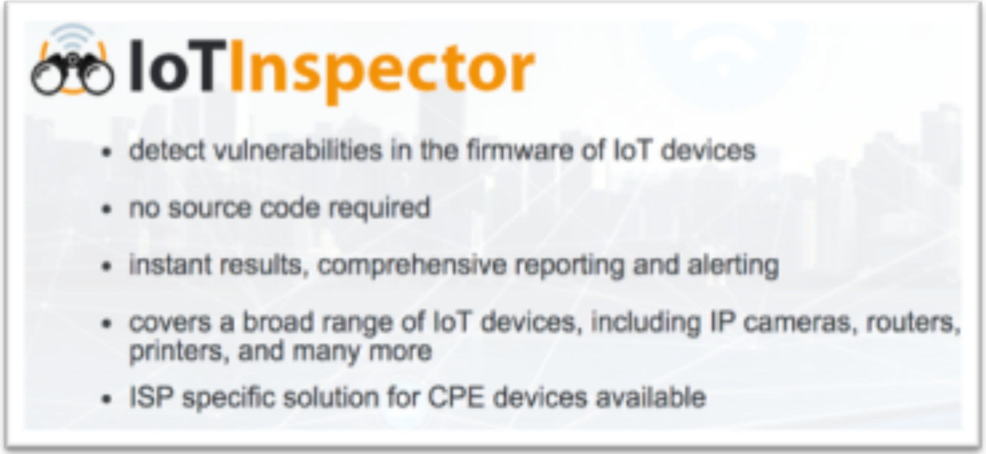
- VOIP
- Switches
- Printers
- Point of Sale
- Medical Devices
- Manufacturing
- Security Cameras
- Access Points
- Bluetooth
- Smart TVs
- Smart HVAC
- Smart Lighting

- Smartphones
- Tablets
- Laptops

- PCs and Servers

Eight Security Strategies for Unmanaged Devices in the Enterprise

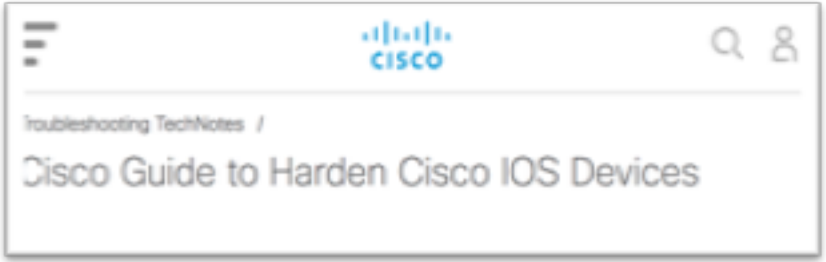
1. Buy devices carefully – look for built-in security


IoTInspector

- detect vulnerabilities in the firmware of IoT devices
- no source code required
- instant results, comprehensive reporting and alerting
- covers a broad range of IoT devices, including IP cameras, routers, printers, and many more
- ISP specific solution for CPE devices available

Eight Security Strategies for Unmanaged Devices in the Enterprise

1. Buy devices carefully – look for built-in security
2. Deploy devices carefully – change default settings



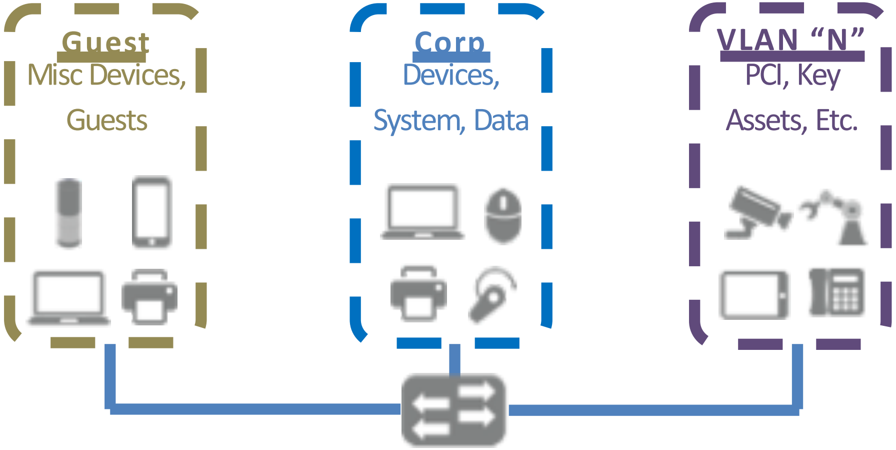
roubleshooting TechNotes /

isco Guide to Harden Cisco IOS Devices

UPnP™

Eight Security Strategies for Unmanaged Devices in the Enterprise

1. Buy devices carefully – look for built-in security
2. Deploy devices carefully – change default settings
3. Use network segmentation – but be aware of its limits



Eight Security Strategies for Unmanaged Devices in the Enterprise

1. Buy devices carefully – look for built-in security
2. Deploy devices carefully – change default settings
3. Use network segmentation – but be aware of its limits
4. Use encryption wherever possible

Eight Security Strategies for Unmanaged Devices in the Enterprise

1. Buy devices carefully – look for built-in security
2. Deploy devices carefully – change default settings
3. Use network segmentation – but be aware of its limits
4. Use encryption wherever possible
5. Maintain a real-time inventory of everything

BYOD Devices
Managed Devices
IoT Devices
Off-Network Devices

Eight Security Strategies for Unmanaged Devices in the Enterprise

1. Buy devices carefully – look for built-in security
2. Deploy devices carefully – change default settings
3. Use network segmentation – but be aware of its limits
4. Use encryption wherever possible
5. Maintain a real-time inventory of everything
6. Proactively assess risk of every device

Eight Security Strategies for Unmanaged Devices in the Enterprise

1. Buy devices carefully – look for built-in security
2. Deploy devices carefully – change default settings
3. Use network segmentation – but be aware of its limits
4. Use encryption wherever possible
5. Maintain a real-time inventory of everything
6. Proactively assess risk of every device
7. Continuously monitor to detect threats

Eight Security Strategies for Unmanaged Devices in the Enterprise

1. Buy devices carefully – look for built-in security
2. Deploy devices carefully – change default settings
3. Use network segmentation – but be aware of its limits
4. Use encryption wherever possible
5. Maintain a real-time inventory of everything
6. Proactively assess risk of every device
7. Continuously monitor to detect threats
8. Have an (automated) plan to contain threats

Eight Security Strategies for Unmanaged Devices in the Enterprise

1. Buy devices carefully – look for built-in security
2. Deploy devices carefully – change default settings
3. Use network segmentation – but be aware of its limits
4. Use encryption wherever possible
5. Maintain a real-time inventory of everything
6. Proactively assess risk of every device
7. Continuously monitor to detect threats
8. Have an (automated) plan to contain threats

Armis helps here

THE ARMIS SOLUTION

Agentless IoT Security Platform

armis

Agentless IoT Security Platform

Discover

- Managed and unmanaged
- Wired and wireless
- On and off the network

Analyze

- Risk and threat quantification
- Behavioral analysis
- Anomaly detection

Protect

- Remove suspicious devices
- Manually or per policy
- Inform firewall, SIEM, etc.

Gartner
Cool Vendor 2017

NO AGENT / HARDWARE

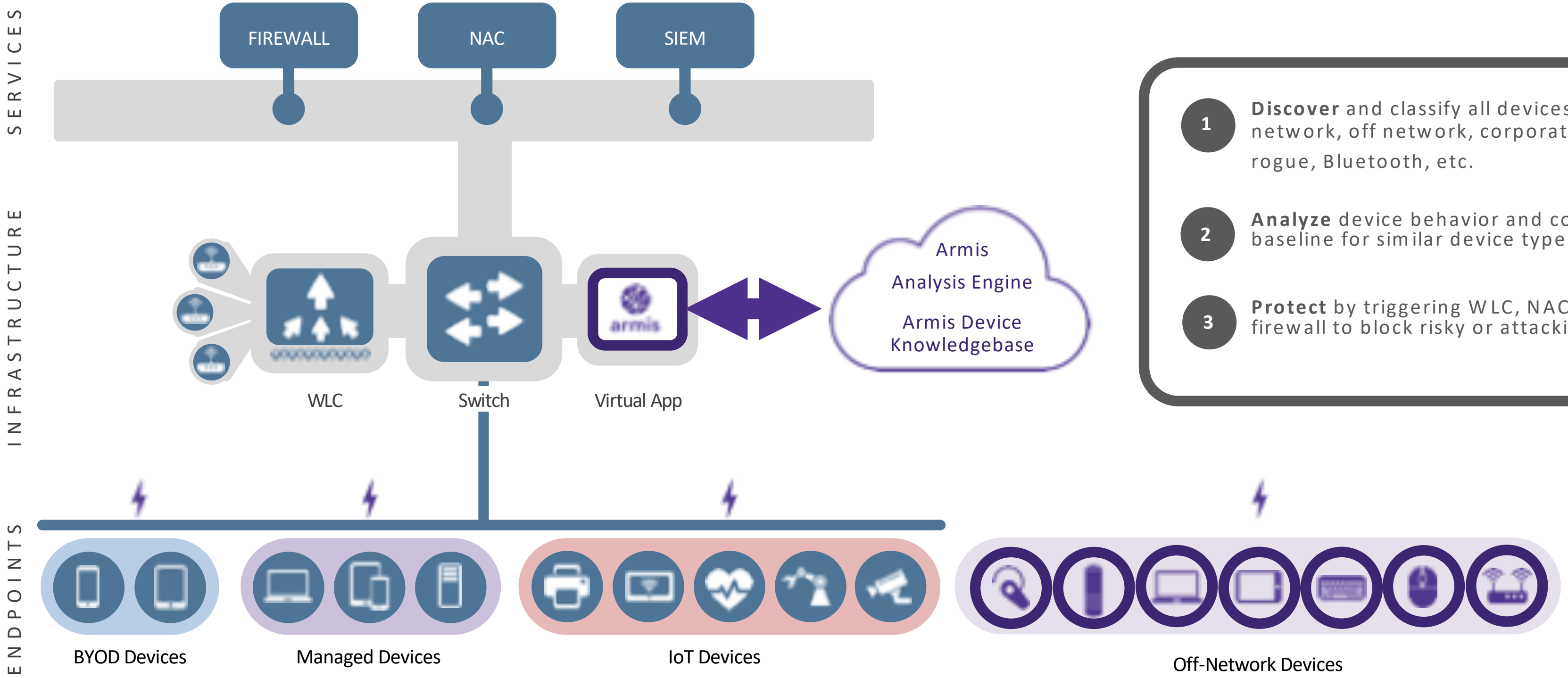
No agent is required on devices for tracking and control. No hardware or sensors required.

FRICTIONLESS

Deploys in minutes. Integrates with existing infrastructure, firewall, and SIEM.

THE CHANNEL CO.
CRN
IoT
SECURITY TOP 10
2018

How Armis Works



1 **Discover** and classify all devices – on network, off network, corporate, BYOD, IoT, rogue, Bluetooth, etc.

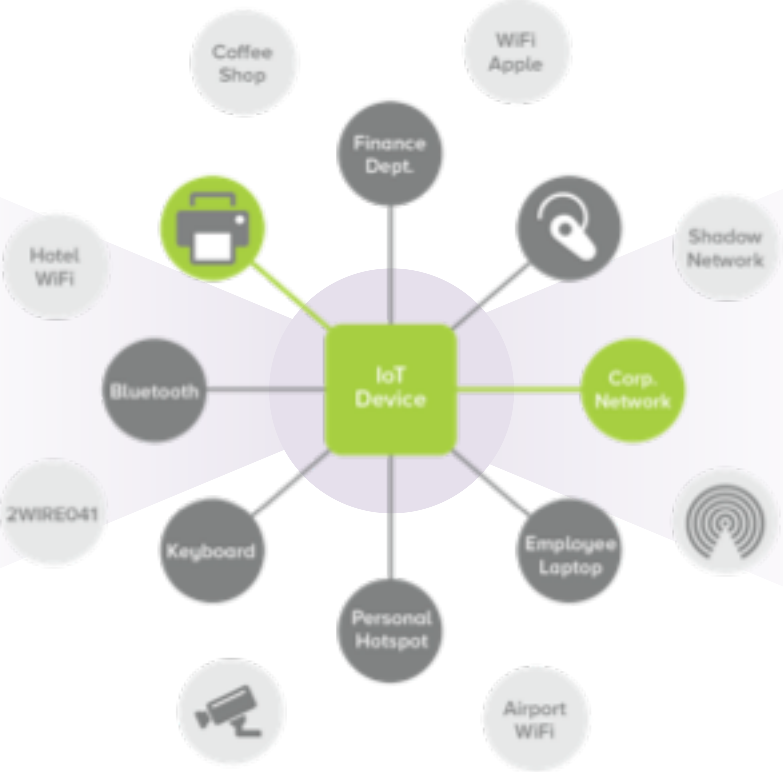
2 **Analyze** device behavior and compare to baseline for similar device types. Assess risk.

3 **Protect** by triggering WLC, NAC, switch, or firewall to block risky or attacking devices

Device Knowledgebase

5M

Unique Device Profiles



Device Tracking

- Device Type
- Behavior
- Connections
- Reputation
- Version
- Data-at-Rest
- History

6 EXPLOITS

Real Stories Behind the Headlines

Compromised Tablet

ISSUE – UNAUTHORIZED VIDEO STREAMING

- Every conference room had an tablet to control the video system on the guest network.
- The tablet in one conference room was streaming video and audio
- This represented a leakage of sensitive conversations.

Armis	NAC	Firewall	IPS/UEBA
✓	✗	✗	✗
• Gleaned WiFi traffic • Discovered and classified all devices and associated traffic volumes • Risk analysis engine identified anomalous traffic with the device	• Inventories devices and controls entry to the network. • Does not monitor traffic volumes • Not designed to detect anomalous devices. Video traffic seemed “normal”	• Designed to protect the perimeter. • Not designed to detect anomalous devices. • Data streaming from tablet seemed “normal” to firewall.	• IPS looks for attacks, not for “normal” traffic such as video. • UEBA is not designed to detect anomalous devices. Video streaming from tablet seemed “normal” to UEBA.

Compromised Smart TV

ISSUE – SMART DEVICE ATTEMPTING TO INFECT OTHER DEVICES

- Boardroom was equipped with a Smart TV that had malware on it.
- Malware on the Smart TV was trying to infect nearby devices via Bluetooth.

Armis	NAC	Firewall	IPS/UEBA
✓	✗	✗	✗
• Monitors Bluetooth & network traffic • Correlated traffic and activity to devices and locations. • Large amounts of WiFi & Bluetooth traffic detected. • TVs were beaconing to infect nearby devices.	• The Smart TV was whitelisted on the NAC, so it let the TV onto the network. • Post-admission, NAC does not monitor behavior or external wireless connections.	• The Smart TV was not sending out anything through the gateway. • The FW cannot see external wireless connections from devices.	• The Smart TV was not sending out anything over the network. • The IPS cannot see external wireless connections from devices

Compromised Security Camera (& Routers)

ISSUE – BOTNET ATTACK

Security cameras on the network were compromised, part of a botnet, trying to propagate.

Armis	NAC	Firewall	IPS/UEBA
✓	✗	✗	?
• Discovered and classified all devices. • Monitored traffic. • Risk Analysis Engine saw cameras trying to connect to other cameras & routers via ports 23 and 80. • Triggered switches to quarantine the devices.	• Inventories devices and controls entry to the network. • Does not monitor traffic over time. • Not designed to detect anomalous behavior.	• Not designed to monitor internal network traffic. • Firewalls have difficult time detecting botnet propagation or C&C because it is disguised as peer-to-peer.	• IPS could have discovered cameras if IPS was in the right location and had a behavior signature. • UEBA might have discovered the behavior anomaly, if it had the right data.

Infected Healthcare Device

ISSUE – SMART DEVICE ATTEMPTING TO INFECT OTHER DEVICES

- MRI machine had an external internet connection for vendor remote support.
- Running Windows XP, unpatched since it would void the warranty.
- Infected with WannaCry and trying to infect other Windows systems via SMB.

Armis	NAC	Firewall	IPS/UEBA
✓	✗	✗	?
• Discovered devices • Correlated traffic with each device • Risk analysis engine saw anomalous SMBv1 traffic. • Trigger sent to NAC to quarantine MRI machine	• Inventories devices and controls entry to the network. • Does not detect attacks.	• Designed to protect the perimeter. • Not designed to monitor internal network traffic.	• UEBA could potentially detect the WannaCry if it was installed in a way that allowed it to see this low level traffic.

Unauthorized Network Bridge

ISSUE – PRINTER ALLOWED ANYONE TO CONNECT

A printer that is connected to the wired network has an open hotspot on it, providing access to unauthorized parties.

Armis	NAC	Firewall	IPS/UEBA
✓	✗	✗	✗
• Monitored the airspace. • Discovered printer with open hot spot, provided an alert. • If there were any actual connections to the printers, Armis would discover those too	• Inventories devices and controls entry to the network. • Does not monitor open hotspots or external connections to printers.	• Designed to protect the perimeter. • Does not monitor open hotspots or connections to those hotspots.	• IPS looks for attack behavior, not for dormant open hotspots. • UEBA would not see the hotspot or the external connections.

Rogue Network Stealing Credential

ISSUE – THEFT OF NETWORK CREDENTIALS

- A corporate device is connecting to a pineapple that is collecting its Active Directory credentials or hashes

Armis	NAC	Firewall	IPS/UEBA
✓	✗	✗	✗
• Detects when a corporate device connects to an external network. • Detects when credentials or hashes move over unencrypted wireless traffic.	• Detects and controls entry to the corp network only. • Would not “see” the external network, nor the connections to it.	• Designed to protect the perimeter. • Would not “see” the external network, nor the connections to it.	• Neither IPS nor UEBA would “see” the external network and the connections to it

THANK YOU

armis