



# Quantum IoT Embedded The Nano Agent offering



Why connected assets require a Prevention-First Strategy!

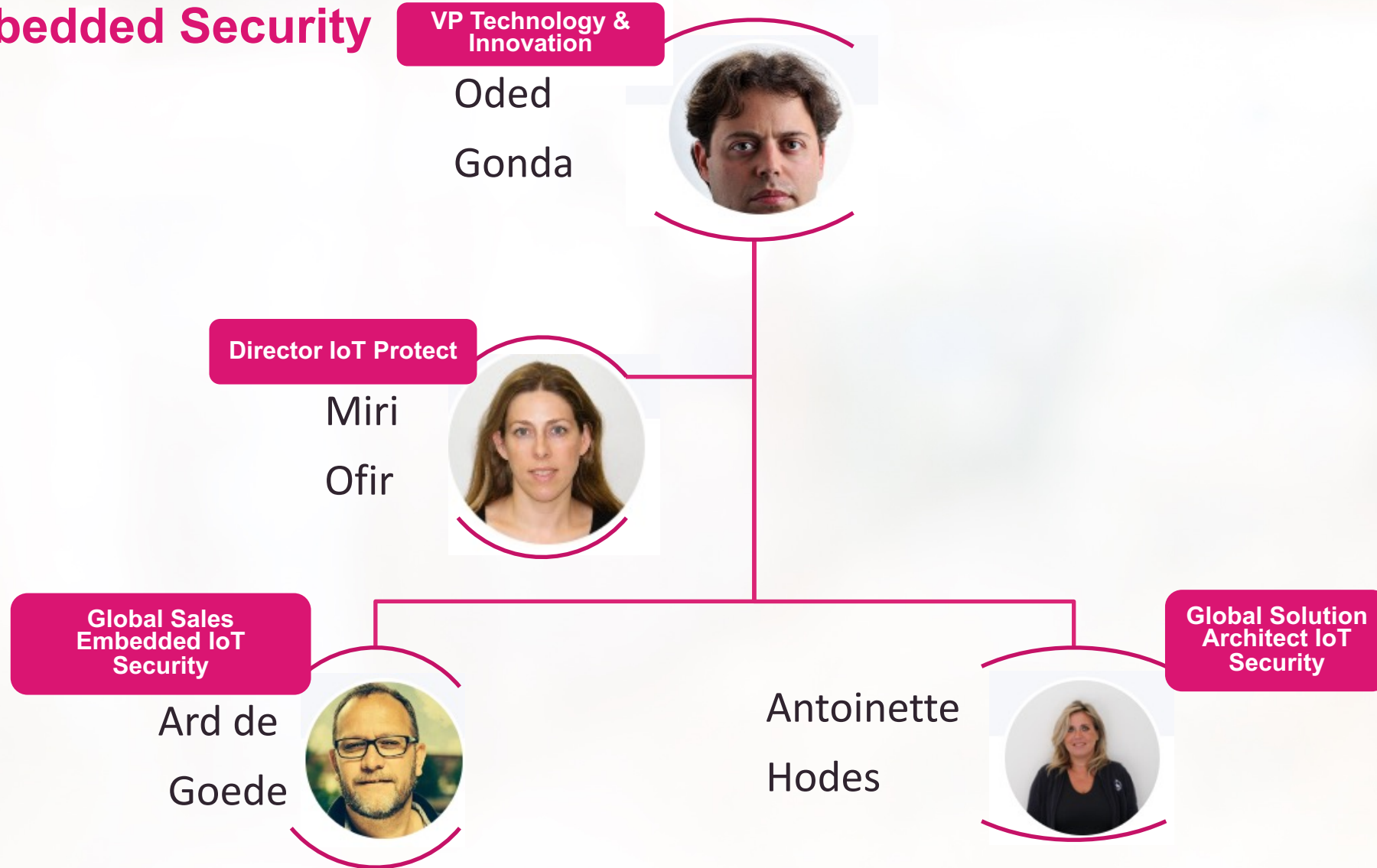


Antoinette Hodes | Global Solution Architect - IoT  
Evangelist - Office of The CTO

YOU DESERVE THE BEST SECURITY

# Meet the team

## IoT Embedded Security



# Antoinette Hodes

## Global Solution Architect - IoT

- Experienced Solution Architect with a demonstrated history (**25+ years**) of working in the cyber security industry
- **Stephen knight!** (Stephen King fan)
- Technical Security **Evangelist** at **Office of the CTO**
- **CCSA & CCSE**
- Passionate about technology!
  
- **Personal Mission** | Making Internet a better place for our children!

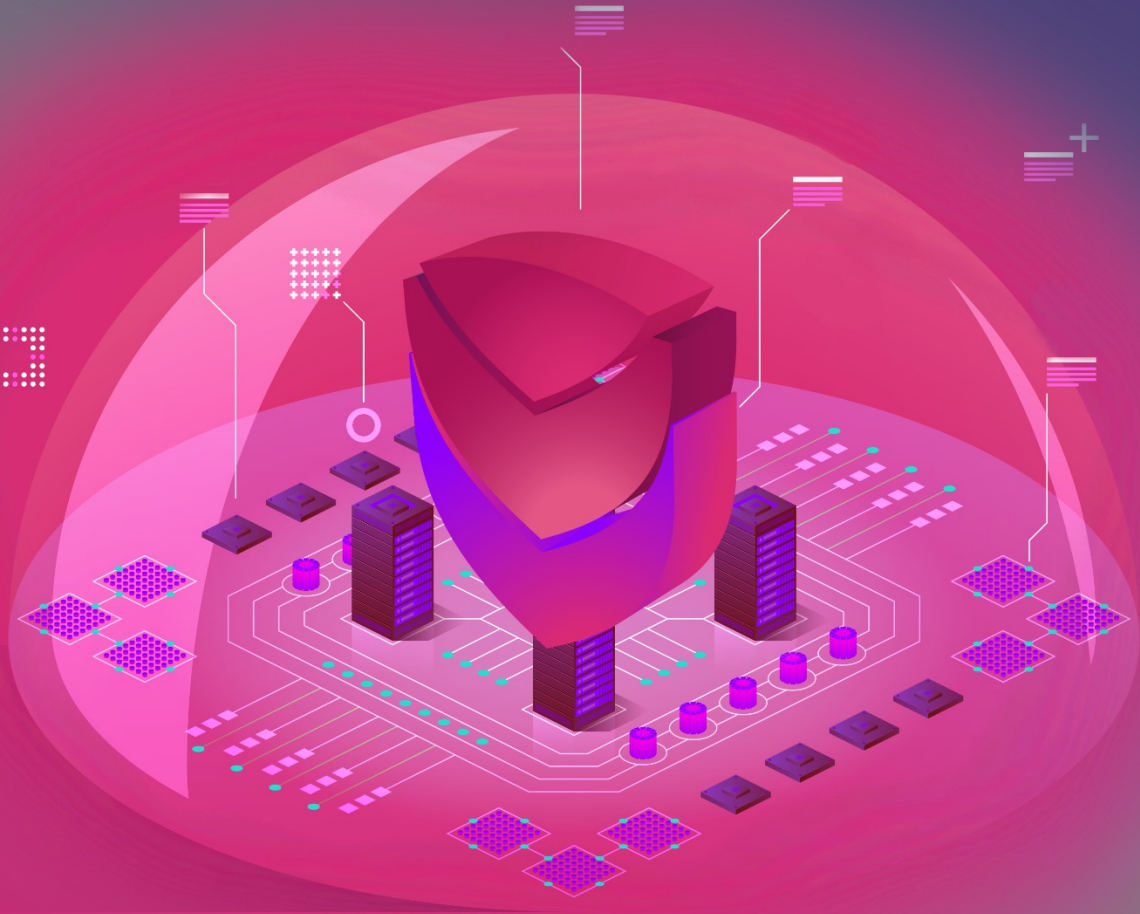


#pinkhat #iotspartan #otsecurity #CTF #nerdcandy #womenintech  
#womenincyber #WICCA\_NL #WiCS #cybersecurity #criticalinfra  
#missioncritical #criticalinfrastructures #industrial #manufacturing  
#nanotech #ICS #SCADA #OT #IoT #IIoT #IoMT #XIoT  
#youdeservethebestsecurity #threatprevention #cybersecurity  
#stepuptogen6 #zerotrust #zerotolerance #zerowaste #nanosecurity  
#iotembedded #hiddenfactory #greenfactory #smartfactory

## The Check Point Ethos

# PREVENTION NOT DETECTION

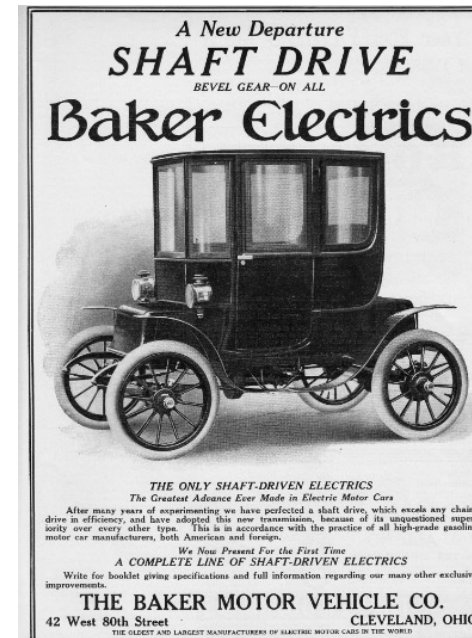
Once Malware is inside,  
it is already too late



# Fun Fact

## How old are electrical cars?

- ✓ Charging an electrical car in 1911
- ✓ This car was produced by the [Baker Motor Vehicle Company](#)



# Today...



Vulnerabilities could let hackers remotely shut down EV chargers,  
steal electricity

# Why

IoT asset designs is focused on connectivity rather than security

# Why OT/IoT Devices are the Weakest Link?



No Built-in Security



Limited Resources



High TCO on Vendors



Impossible/  
Difficult to Patch



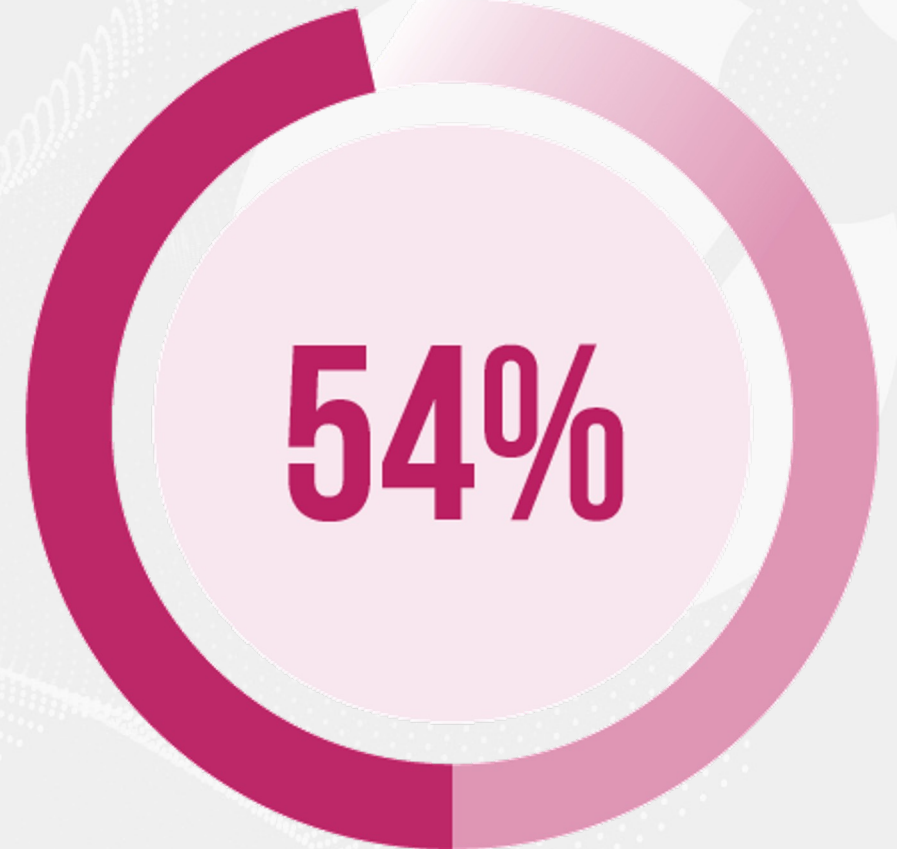
Vast Deployment Shadowed, Unmanaged



Highly Vulnerable Devices



ON AVERAGE, EVERY WEEK  
**54% OF ORGANIZATIONS**  
SUFFER FROM ATTEMPTED CYBER  
ATTACKS TARGETING IOT DEVICES



SOURCE: [Q1 2023 CYBER REPORT, CHECK POINT](#)

# Europe

Average of 70 IoT attacks per organization weekly

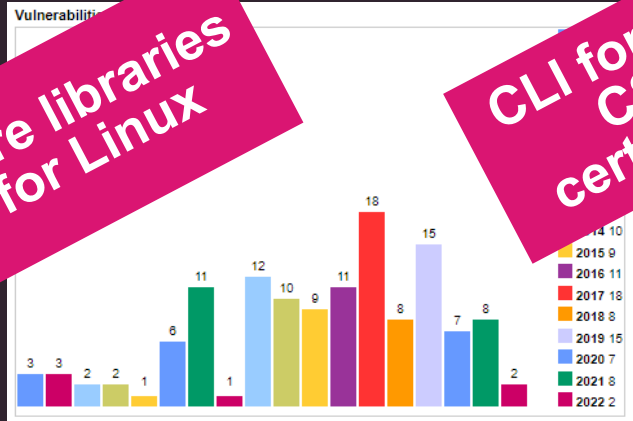


# Common components

## Popular vulnerabilities

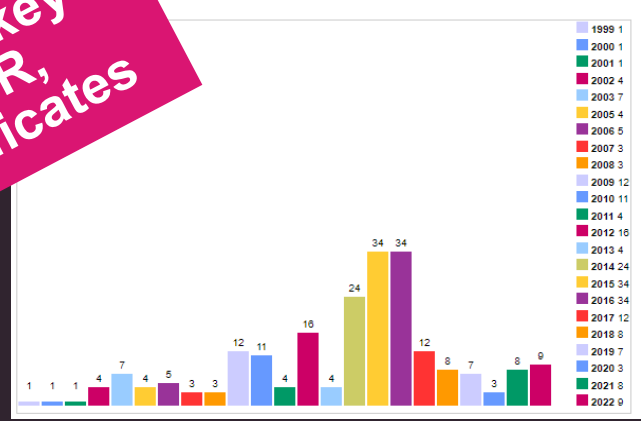
Glibc

Core libraries for Linux

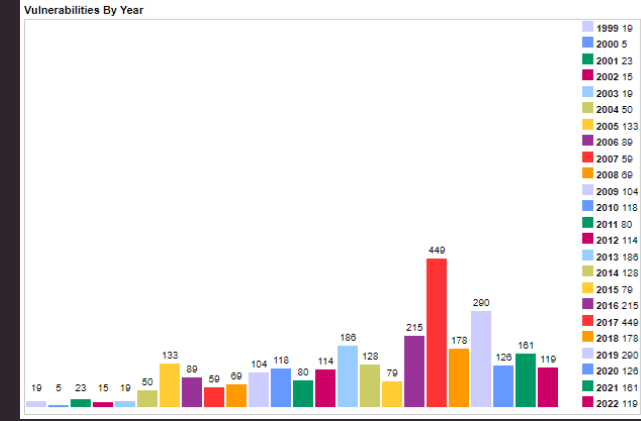


OpenSSL

CLI for keys, CSR, certificates



Linux kernel



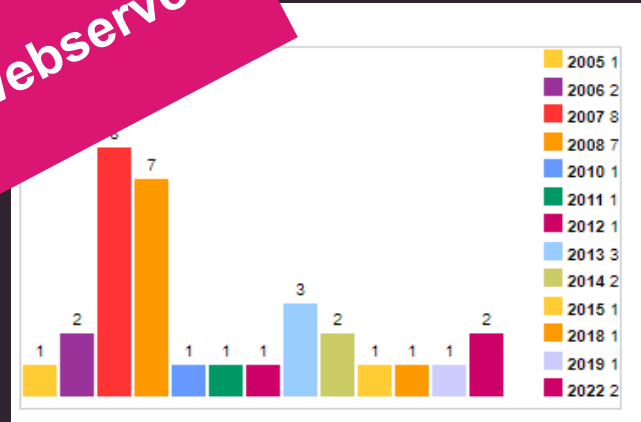
OpenSSH

Remote login

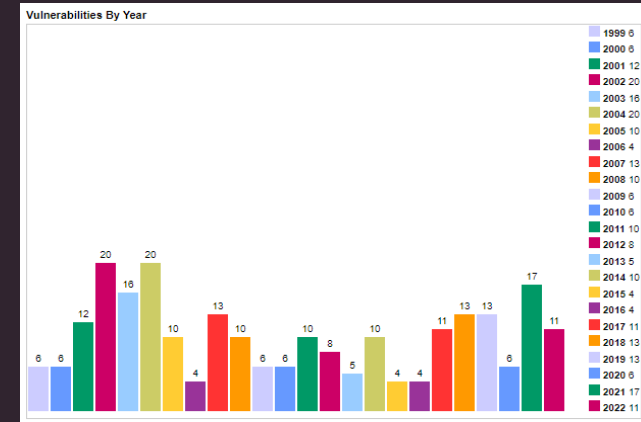


lighttpd

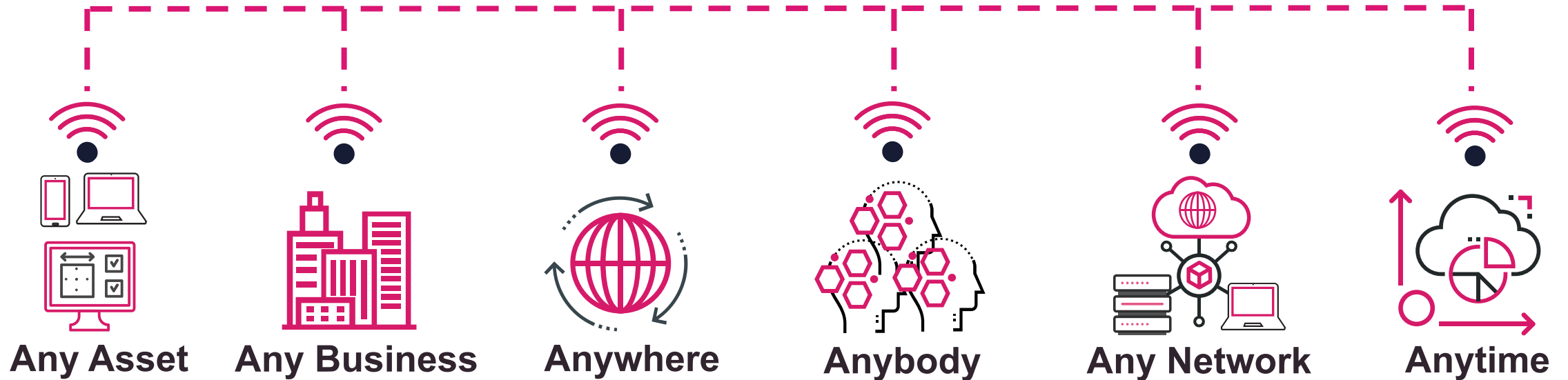
Webserver



Apache httpd



# Internet of “Any” Things



# IloT | Hacktivism example

## The first encrypted RTU



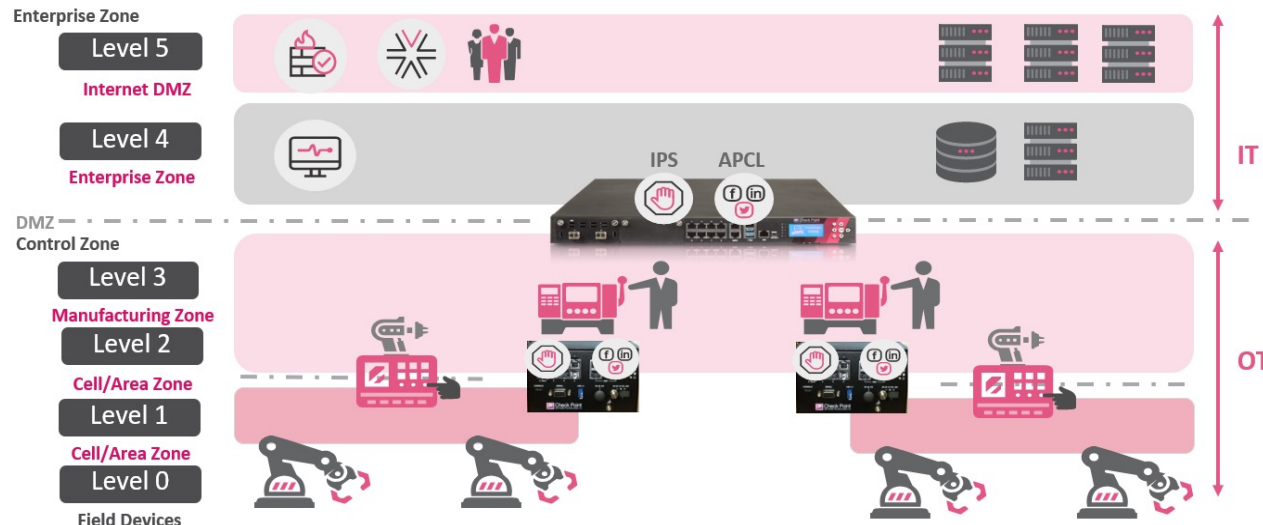
RTU Teleofis 968

```
1 config dropbear
2   option PasswordAuth 'on'
3   option RootPasswordAuth 'on'
4   option Port '22'
5   # option BannerFile '/etc/banner'
```

```
root@TELEOFIS-RTU968V2:~# ls /bin
ash          dnsdomainname  login          ping
board_detect.fuckPutin  echo            login.sh.fuckPutin  ping6
busybox      egrep           ls             pingcontrol.fuckPutin
```



# Hacktivism

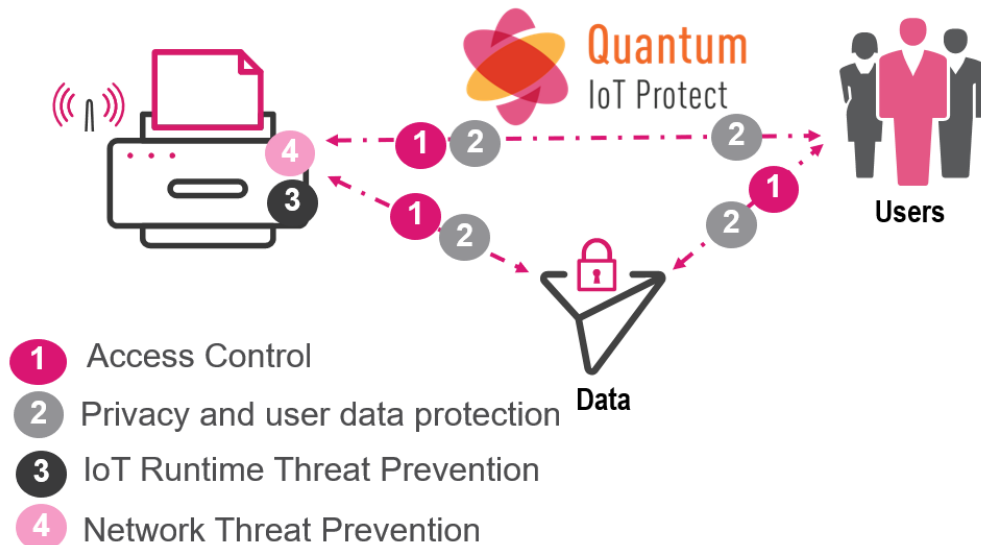


- In this example GhostSec is claiming to be the first to encrypt an RTU, Remote Terminal Unit using ransomware
- An RTU is a critical asset in the OT/SCADA environment. An RTU is situated at **level 1** of the **Purdue model**
  - A Hacktivist group with political attribution exploited the weak preconfigured root password

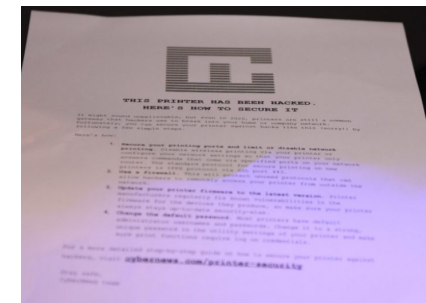
# Enterprise IoT | A real hijack example

27.000 hacked printers

## White Hat research



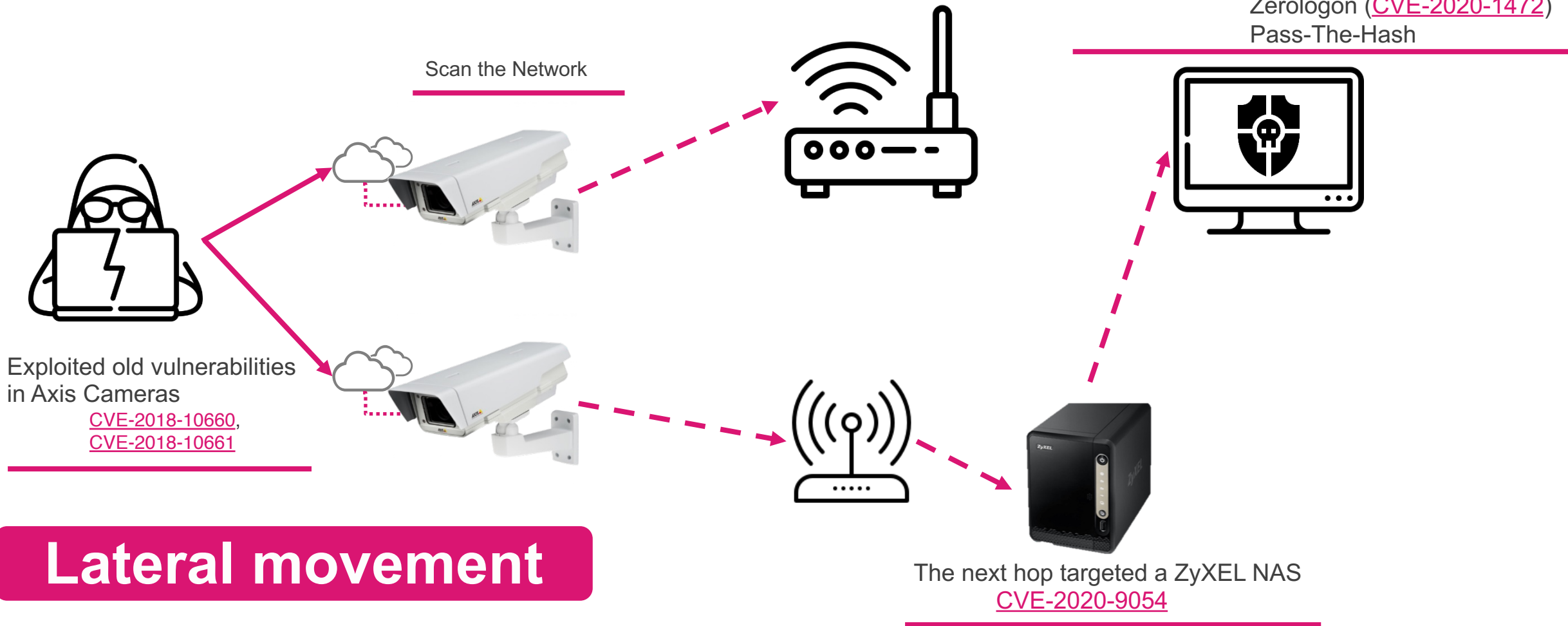
- Experts at Cybernews hijacked 27.044 printers to create awareness
- After they compromised the printer, they forced a print job
- The print job: **“A 5-step guide how to secure a printer!”**



source <https://cybernews.com/security/we-hacked-28000-unsecured-printers-to-raise-awareness-of-printer-security-issues/>

# How It Works In The Real World

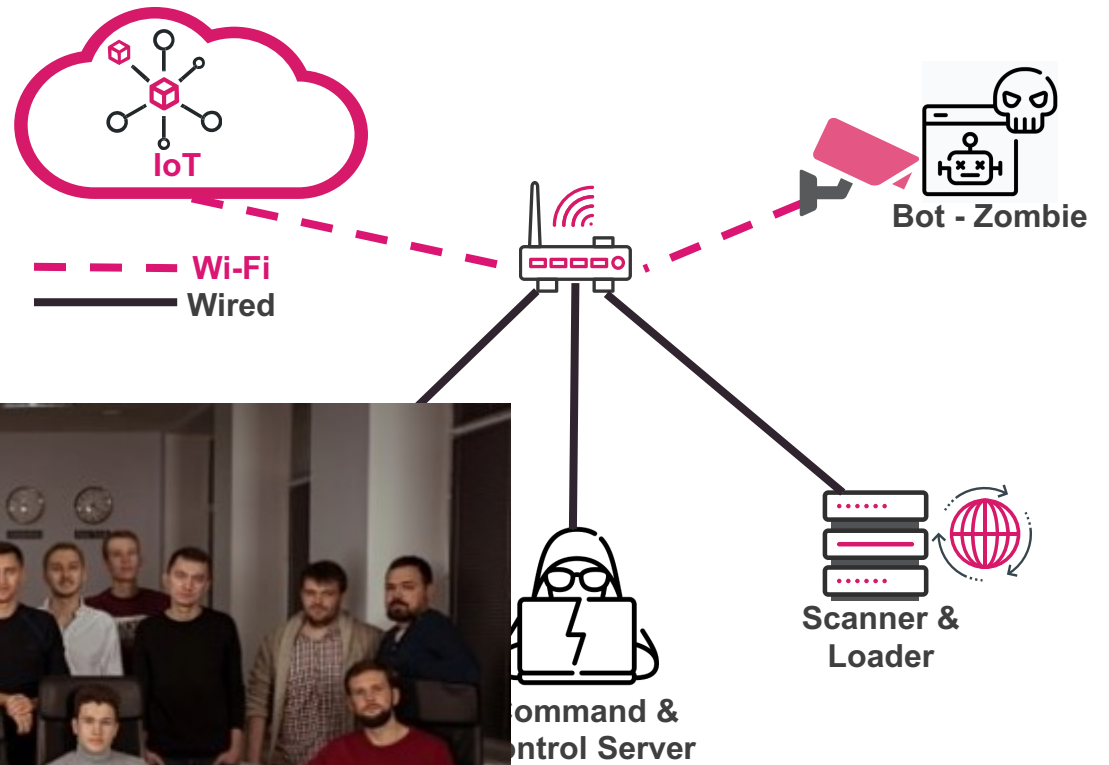
## R4IoT - Ransomware for IoT attack



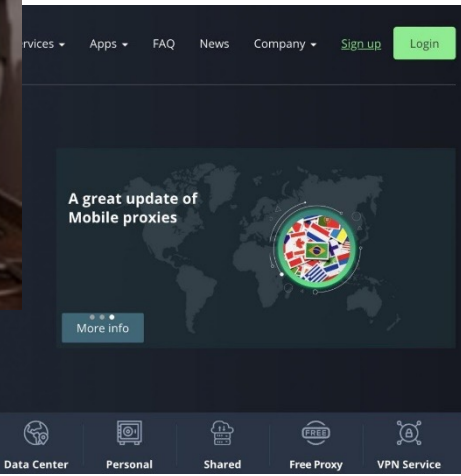
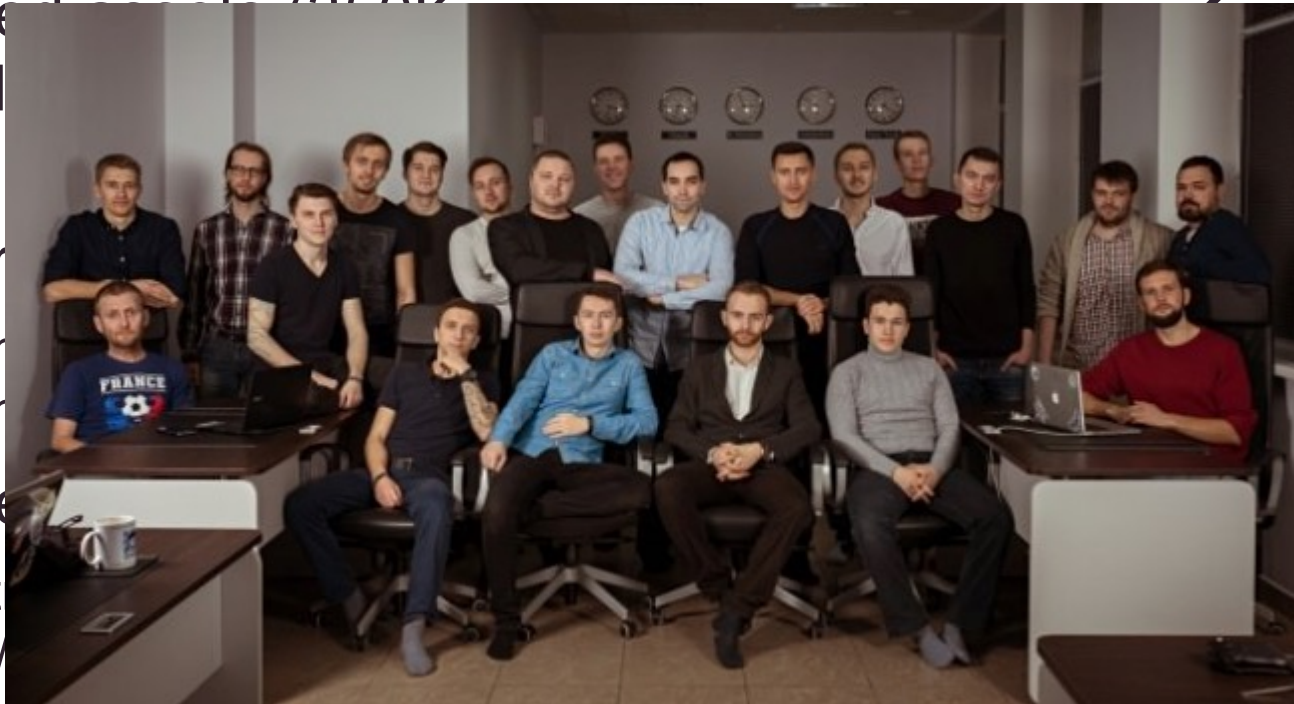
source <https://borncity.com/win/2022/09/02/ransomware-auf-iot-anderer-sicherheitsansatz-bei-iot-gerten-erforderlich/>

# IoT | A real example

## RSOCKS Proxy Botnet



- Seized by the FBI in June 2022
- Compromised devices (950K assets) sold as “proxies”
- Threat actor
  - Exploiting known weak credentials
- Compromised devices: Industrial controllers, routers, audio devices, and smart garage door openers



## Propagation attack

source <https://krebsonsecurity.com/2023/01/administrator-of-rsocks-proxy-botnet-pleads-guilty/>



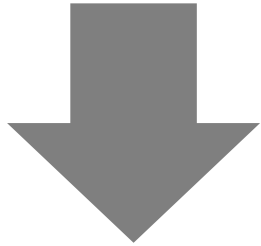
# IoT asset manufacturing

## Device and market challenges

### IoT asset manufacturing challenges



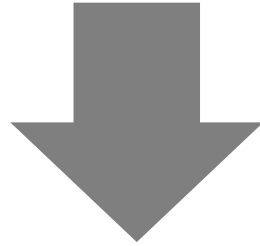
Factory



- Development
- Programming
- Testing
- Source Repos
- Build & Release Management
- Factory Automation



Device Security



- Secure Debug Lock
- Root of Trust
- Communications Stack
- Secure Key Storage
- Hardware Acceleration
- Secure Identity



## LAWS AND REGULATIONS

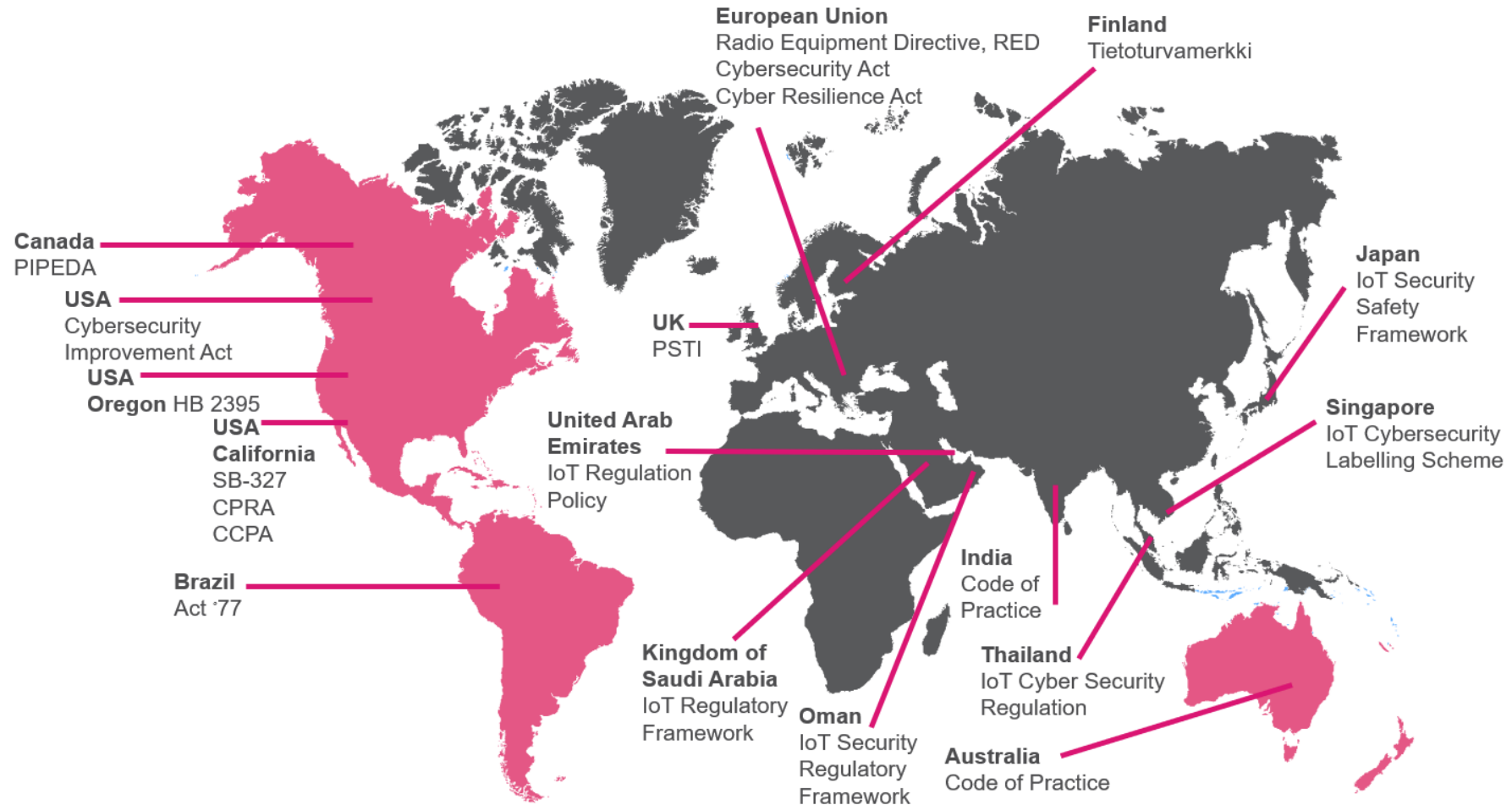
# Global Regulations and Jurisdiction

## The Nano Agent addresses all regulatory key elements

### Mandatory legislations

#### Europe |

- Cyber Security Act (CSA)
- Cyber Resilience Act (CRA)
- GDPR
- Radio Equipment Directive - RED
- ETSI EN 303 645
- NIS Directive
- Swedish Data Act



[https://www.cybertalk.org/wp-content/uploads/2023/03/IoT-Solutions-Brief\\_031523](https://www.cybertalk.org/wp-content/uploads/2023/03/IoT-Solutions-Brief_031523)

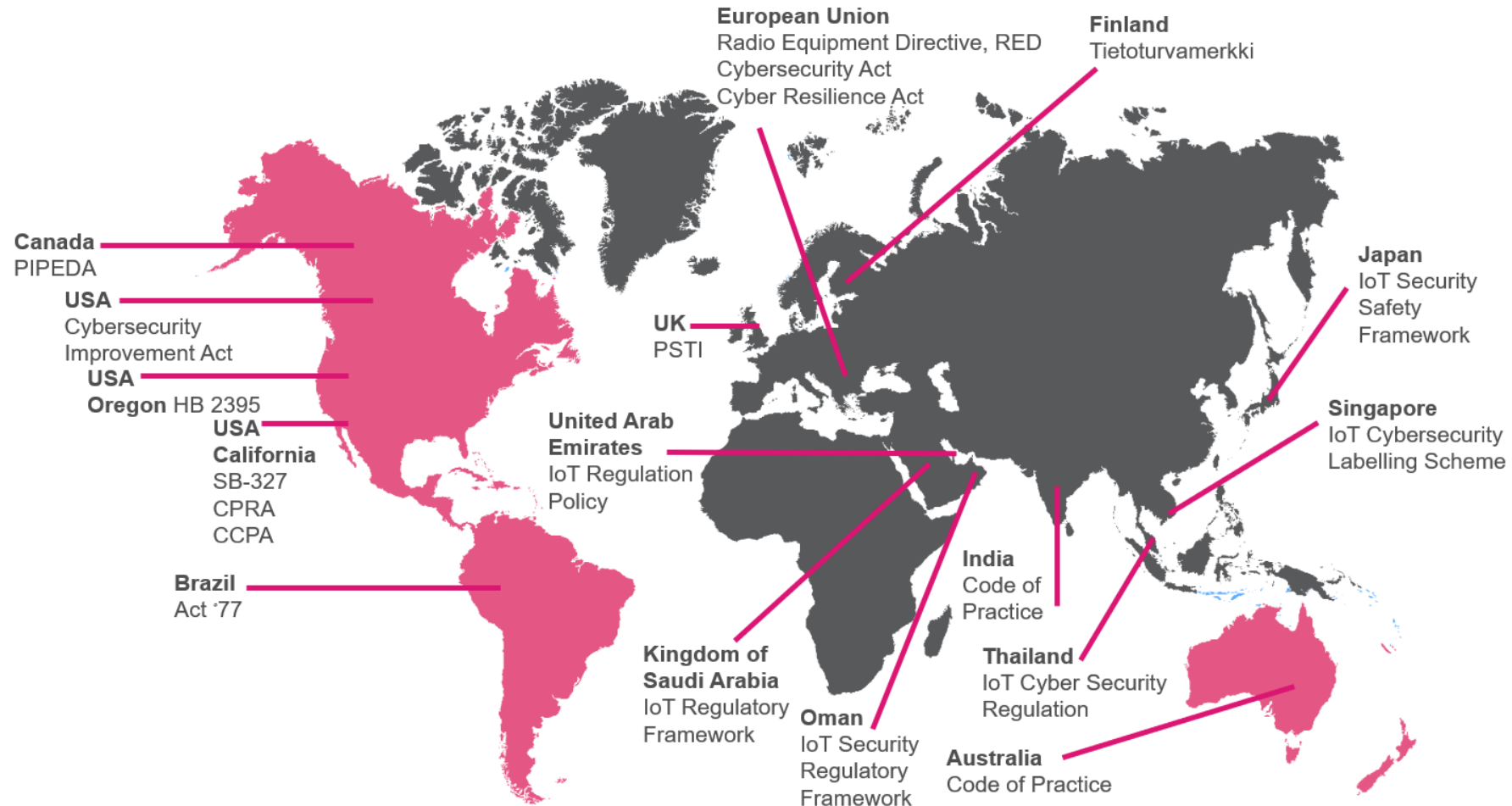
# Global Regulations and Jurisdiction

## The Nano Agent addresses all regulatory key elements

### Mandatory legislations

#### US |

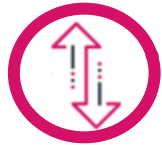
- IoT Cybersecurity Improvement Act
- Biden-Harris Administration New Cybersecurity Strategy
- California Senate Bill 327 Information privacy
- Oregon House Bill 2395
- Federal Exchange Data Breach Notification Act
- California Consumer Privacy Act 1121 (CCPA)
- California Privacy Right Act (CPRA)



[https://www.cybertalk.org/wp-content/uploads/2023/03/IoT-Solutions-Brief\\_031523](https://www.cybertalk.org/wp-content/uploads/2023/03/IoT-Solutions-Brief_031523)

# Regulations and standards

## Key Elements



### Secure Access and Access Control

- Permissions
- Access Control List



### Authentication and Authorization

- Login Protection
- Password Policy
- Brute-force Login Protection



### Vulnerabilities Management and Reporting



### Data Protection

- User Data (GDPR)
- Sensitive security parameters



### Secure Connections

- HTTPs
- Allowed domains




### Secure Software update

- Regular patch management
- Vulnerability patching



<https://www.cybertalk.org/2023/03/13/the-2-biggest-regulatory-challenges-for-the-internet-of-any-thing-iot/>

# Levels of IoT Security Rating (UL MCV1376)



**CHECK POINT™**  
**EMBEDDED**



- DIAMOND**  
Comprehensive security capabilities
- Hardware root of trust
  - Unknown vulnerability testing
  - Extensive interface and service documentation



- PLATINUM**  
Extensive security capabilities
- Sophisticated runtime hardening
  - Known vulnerability testing
  - Strong input sanitization



- GOLD**  
Advanced security capabilities
- Secure out-of-the-box settings
  - Hardware design hardening
  - Least privilege principle



- SILVER**  
Enhanced security capabilities
- Password complexity enforcement
  - Credential recovery
  - Device safety considerations



- BRONZE**  
Essential security capabilities
- No default passwords
  - Secure update mechanism
  - Secure reset
  - Secure communications

These levels map to different Standards/guidelines, e.g.:

**NIST8259A** maps to Bronze Level

**DLC** maps to Silver Level

**EN 303 645** maps to Gold Level

\*For Gold+, products earn certification against EN 303 645. In the absence of a formal certification authority, a letter of attestation is issued.



# What



Scan me!

- Our offering consists of 2 parts |
  - 1. Firmware Risk Assessment
  - 2. Embedded Nano Agent

# Solution 1 | Quantum IoT Embedded – Firmware Risk Assessment

## Solution



IoT Embedded – Firmware Risk Assessment

Assessing the **Cyber Security Immune System**, **Cyber Hygiene** and the **security posture** of the associated firmware

Delivering results with recommended actions in |

- ✓ PDF report or
- ✓ API in JSON format (CI/CD pipeline)



## Target Audience

IoT device manufactures, vendors, developers and operators

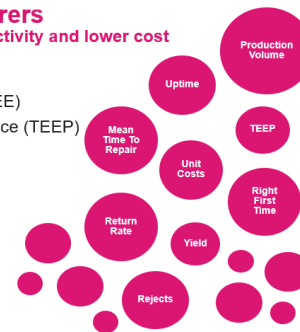
- ✓ **Security value proposition** | Risk assessment
- ✓ **Business value proposition** | Improving the daily operation

### KPIs IoT Device Manufacturers

Improve customer satisfaction, productivity and lower cost

IoT device manufactures KPIs:

- Overall Equipment Effectiveness (OEE)
- Total Effective Equipment Performance (TEEP)
- Downtime
- Yield, cost and throughput
- Lead time to customer
- Customer rejects
- Inventory turns
- Maintenance metrics



## Deployment Type

- ✓ **Security type** | Static firmware scan
- ✓ **Cloud service** for manufactures, vendors, developers and operators hosted by Check Point's Infinity Portal



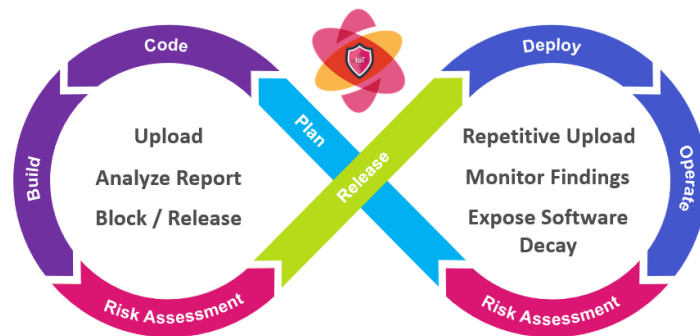
- Weak/Known Credentials
- Known Vulnerabilities (CVEs)
- SW Misconfigurations
- Suspicious Listed Domains
- Unsecured Private Key

# Combining Firmware Risk Analysis within CI/CD

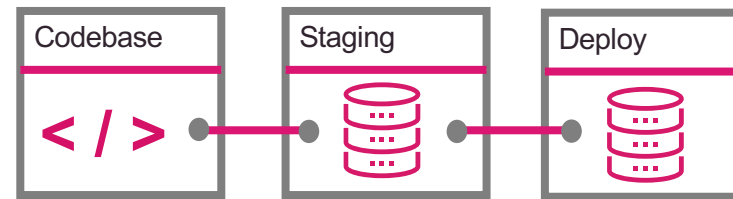
## Firmware Risk Analysis service automated

### CI/CD

- Continuous Integration and Continuous Deployment



### CI/CD is a DevOps practice



### CI/CD benefits

- Increased safety and security
- Higher efficiency and increased productivity
- Reduced risk of defects and problems



Scan me!



# NANO AGENT FOOTPRINT



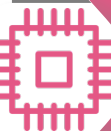
Scan me!

OS

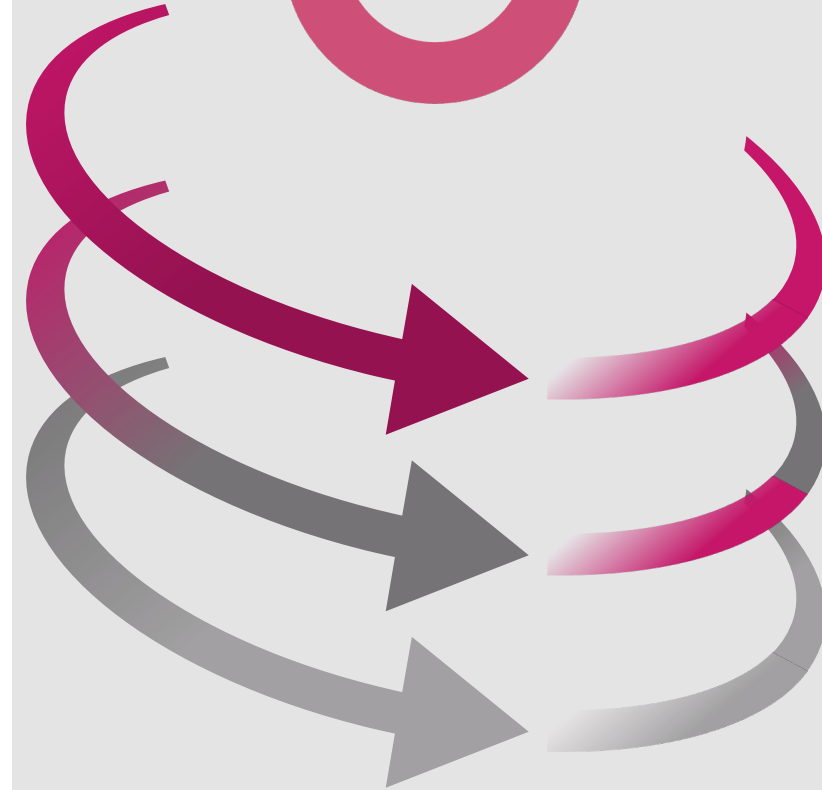
ANY Linux OS



Storage & RAM Starting at 1MB



CPU ARM 32/64bit, X86 64bit, MIPS




# Use Case 2 | Quantum IoT Embedded – Nano Agent

## Solution



On device zero-day runtime protection. Using the principles of zero trust and zero tolerance. Harden the device from within

- ✓ Solution is deployed by manufacturer during device development
- ✓ Perfect for Industry 4.0   
Field device
- ✓ Ideal for **air-gapped\*** environments such as OT, Operational Technology

\* Air-gap is a security measure isolating an asset/network, preventing it from establishing an external connection

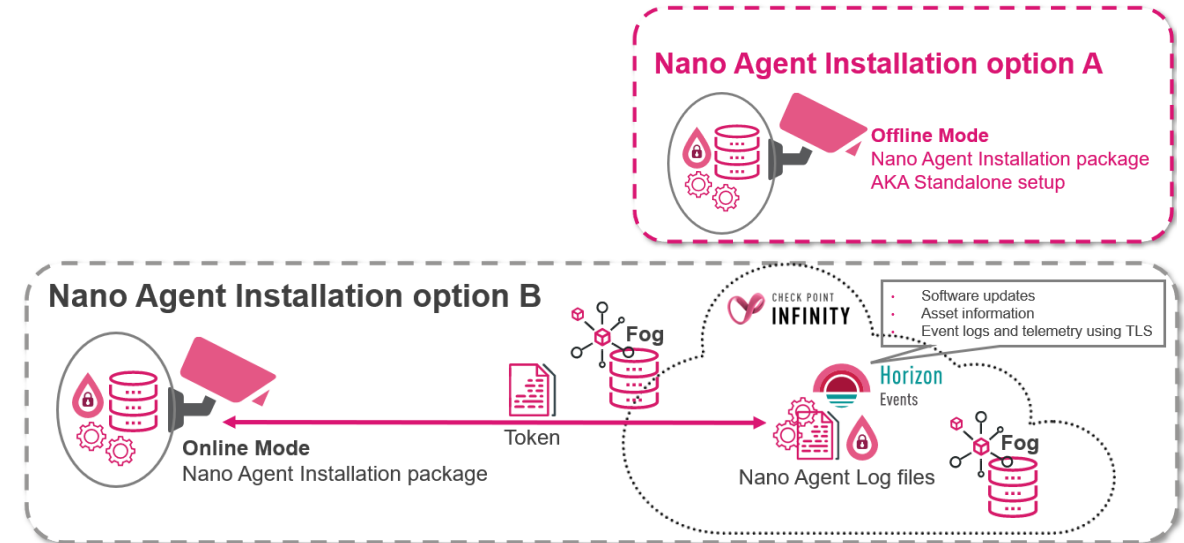
## Target Audience

IoT device manufactures, vendors, developers and operators

- ✓ **Security value proposition** | Prevention of known and unknown (zero-day) attacks
- ✓ **Business value proposition** | Brand & Reputation protection

## Deployment Type

- ✓ **Security type** | Device level protection
- ✓ **Optional Cloud service** for manufactures, vendors, developers and operators hosted by Infinity Portal



# Base and advanced protections Nano Agent



Scan me!

**Embedded Nano Agent**  
Mitigating device level attacks

Base protection

**Embedded Nano Agent**  
Mitigating device level attacks

Base protections

**Embedded Nano Agent**  
Mitigating device level attacks

Advanced protections

Track by pr for m to exp contr

Imp Pr

**Embedded Nano Agent**  
Mitigating device level attacks

Advanced protections

**Embedded Nano Agent**  
Mitigating device level attacks

Advanced protections

**Control-Flow Integrity**



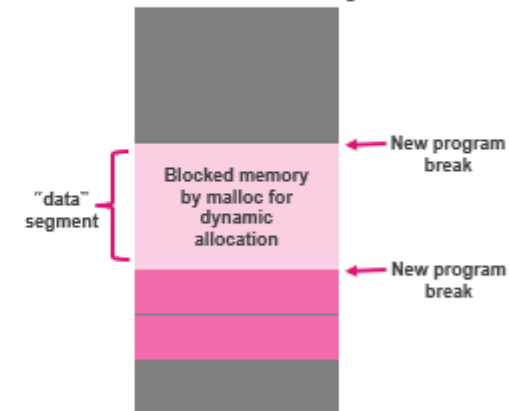
- Common implementation
- These functions through a is a function
- Function inherently takeover exploited
- Runtime protection is using Control Flow Integrity, to protect all binaries, scripts and libraries on the IoT asset
- CFI prevents malware attack from redirecting the flow of execution (the control flow) of program

**Dynamic-Memory Protection**



- Software uses dynamic memory when handling data
- This protection tracks every dynamic memory allocation and writes
- Offering exploit protection by malicious actors

**Virtual Memory**



Dynamic-Memory Protection

# Use Case and Success Story

## RAISING THE BAR ON CCTV CYBER SECURITY



# Success Stories

## Quantum IoT Embedded – Nano Agent

### Nano Agent



<https://www.esix.co/en>



<https://www.altatechnologies.com/>



<https://bbt.live/>



<https://xsquareiot.com/>

### Firmware Risk Assessment

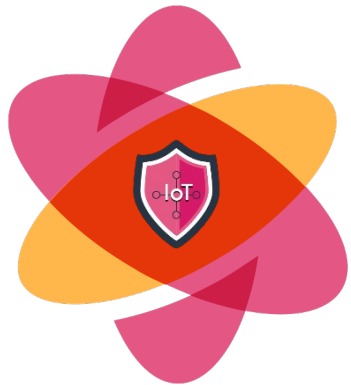


**MOTOROLA**



Scan me!

# Summary



Quantum  
IoT Embedded

[iot-device-security@checkpoint.com](mailto:iot-device-security@checkpoint.com)

- Help manufacturers build **secure-by-design** IoT devices
  - 1. Firmware Risk Assessment
  - 2. Embedded Nano Agent
- The **Nano Agent** improves the daily operation by delivering a higher efficiency, increased safety and security. All in a cost-effective manner
- **Complete end-to-end solution**, for all firmware security needs
- **Assess, harden and manage** security at the device level with a very low footprint



Scan me!

**Robert Mueller, former Director of the FBI**

**There are only two types of companies:**

**Those that have been hacked and those that will be hacked**

**Check Point is adding third one:**

**Those that have been hacked but still don't know**



**Thank you!**

YOU DESERVE THE BEST SECURITY