



**Hewlett Packard
Enterprise**

Adaptive Trust Defense for Data and IT Infrastructure



Agenda

- **IT Security risks in 2017**
- **ClearPass – Adaptive Trust Defense Security model**
- **Servers Security – Addressing security concerns**



IT Security risks in 2017

Cyber attacks are becoming more sophisticated

Firmware security risks must be part of your risk assessment

Security

Types of attack

Distributed denial of service (DDoS)

Denial of service (DoS)

Data or information theft

Application level attacks

> 500M

Records breached
in 1H, 2016¹

99 days

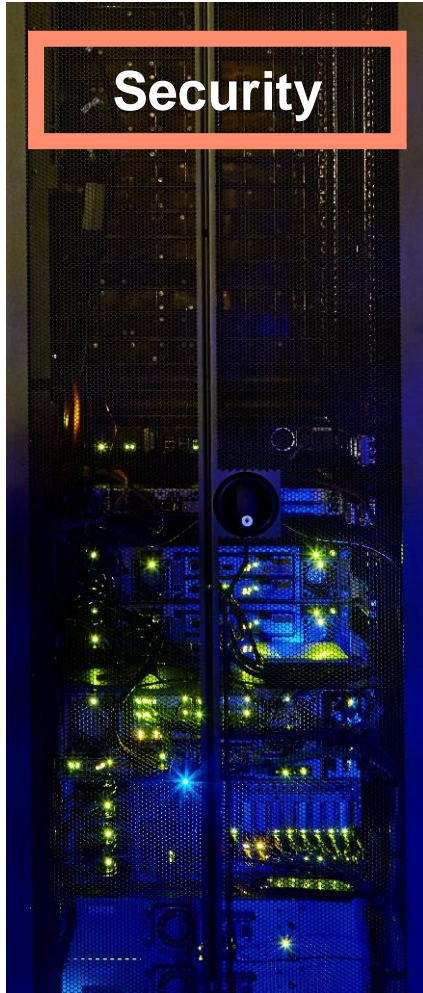
Median time to
detect breach²

“As cyber attacks become more sophisticated, the potential for BIOS or other firmware attacks is growing”³

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Companies spend 55% of their cybersecurity budget on detection and recovery⁴

Don't be in the headlines!



Hacking BIOS Chips Isn't Just the NSA's Domain Anymore

wired.com/2015/03/researchers-uncover-way-hack-bios-undermine-secure-operating-systems

aboutblank HP Designjet printer www.eagleeyenet

Wired

Hacking BIOS Chips Isn't Just the NSA's Domain Anymore

SIM ZETTER SECURITY 03.20.15 02:58 PM

HACKING BIOS CHIPS ISN'T JUST THE NSA'S DOMAIN ANYMORE

Optical illusion background © GETTY IMAGES

THE ABILITY TO hack the BIOS chip at the heart of every computer is no longer reserved for the NSA and other three-letter agencies. *Millions* of machines contain basic BIOS vulnerabilities that let anyone with moderately sophisticated hacking skills compromise and control a system surreptitiously, according to two researchers.

The revelation comes two years after a [catalogue of NSA spy tools](#) leaked to journalists in Germany surprised everyone with its talk about the NSA's efforts to infect BIOS firmware with malicious implants.

The BIOS boots a computer and helps load the operating system. By infecting this core software, which operates below antivirus and other security products and therefore is not usually scanned by them, spies can plant malware that remains live and undetected even if the computer's operating system were wiped and re-installed.

BIOS-hacking until now has been largely the domain of advanced hackers like those of the NSA. But researchers Xeno Kovah and Corey Kallenberg presented a proof-of-

SHARE

f SHARE 4728

TWEET

COMMENT

EMAIL

MOST POPULAR

CULTURE
It Was Inevitable, Really: Netflix Is Turning Into HBO
ANGELA WATERCUTTER

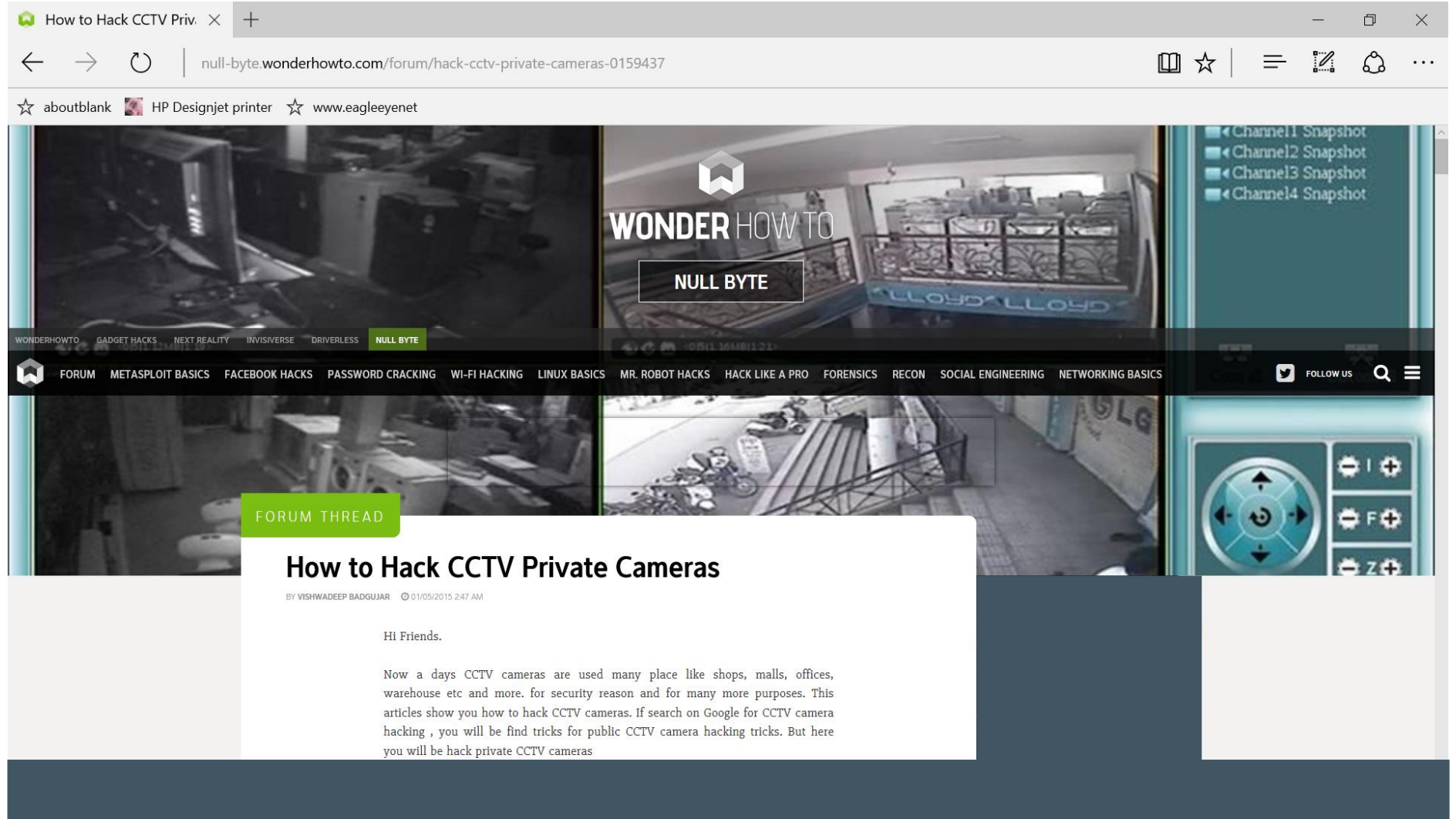
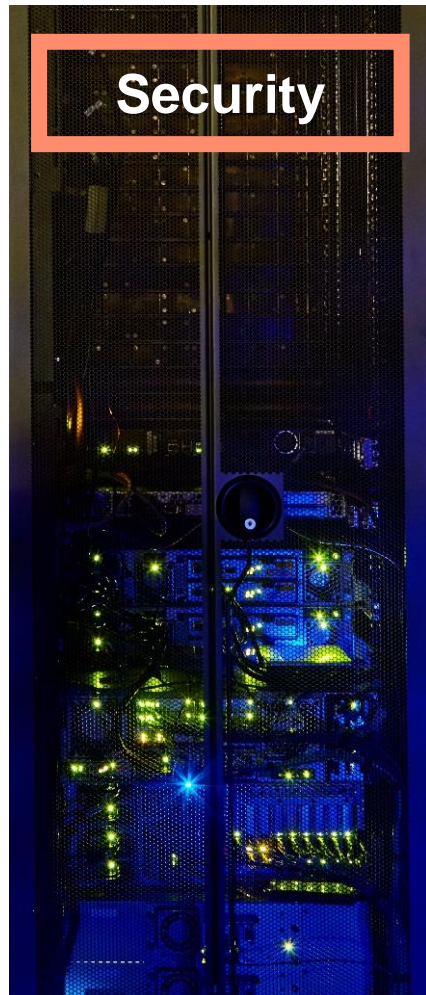
DESIGN
What's Wrong with Apple's New Headquarters
ADAM ROSE

SPONSOR CONTENT
Get and Keep Two Free Audio Books During Audible's Free Trial
WIRED

CULTURE
What Does 'Corvete' Mean? The Internet Will Define That For You.
ANGELA WATERCUTTER

MORE STORIES

Happening more often than you might think



How to Hack CCTV Priv. X +

← → ↺ | null-byte.wonderhowto.com/forum/hack-cctv-private-cameras-0159437

☆ aboutblank 🖨 HP Designjet printer ☆ www.eagleeyenet

WONDERHOWTO
NULL BYTE

WONDERHOWTO GADGET HACKS NEXT REALITY INVISIVERSE DRIVERLESS NULL BYTE

FORUM METASPLOIT BASICS FACEBOOK HACKS PASSWORD CRACKING WI-FI HACKING LINUX BASICS MR. ROBOT HACKS HACK LIKE A PRO FORENSICS RECON SOCIAL ENGINEERING NETWORKING BASICS FOLLOW US 🔍

FORUM THREAD

How to Hack CCTV Private Cameras

BY VISHWADEEP BADGUJAR 01/05/2015 2:47 AM

Hi Friends.

Now a days CCTV cameras are used many place like shops, malls, offices, warehouse etc and more. for security reason and for many more purposes. This articles show you how to hack CCTV cameras. If search on Google for CCTV camera hacking , you will be find tricks for public CCTV camera hacking tricks. But here you will be hack private CCTV cameras

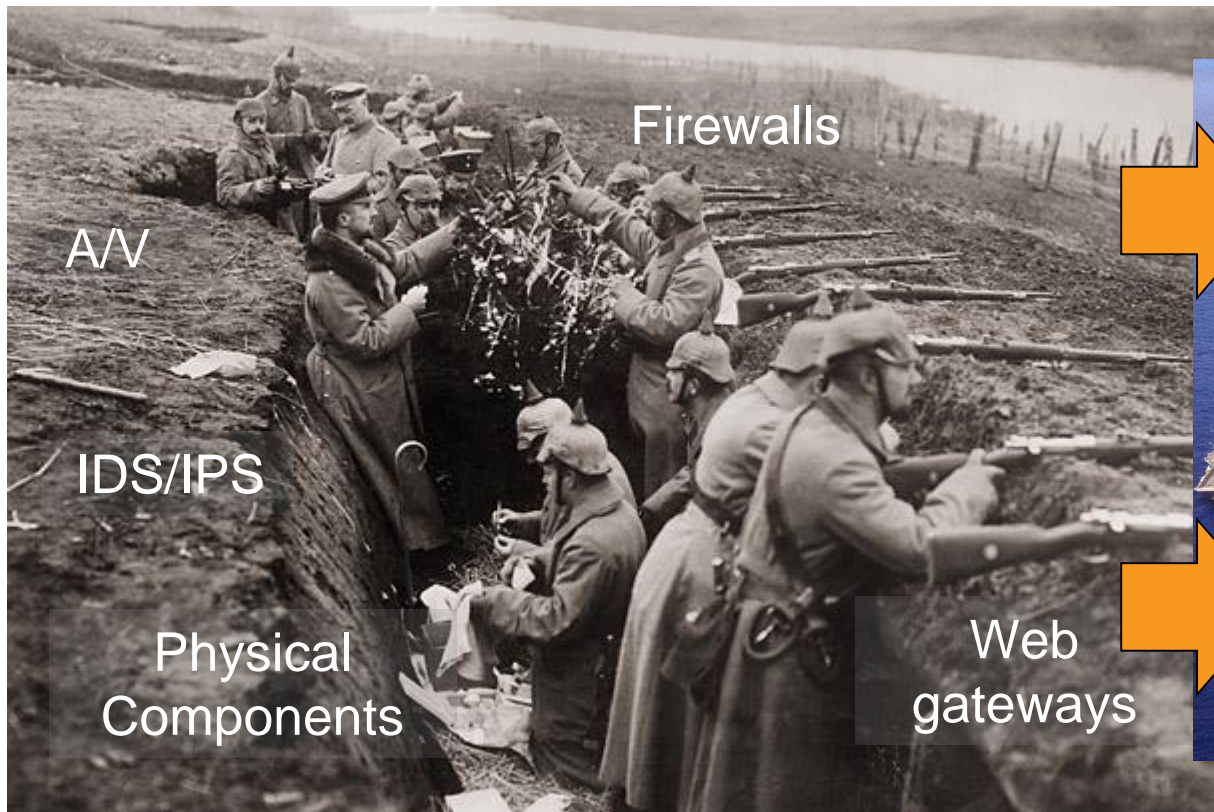


Aruba ClearPass

Time for a New Mobility Defense Model

Static Perimeter Defense

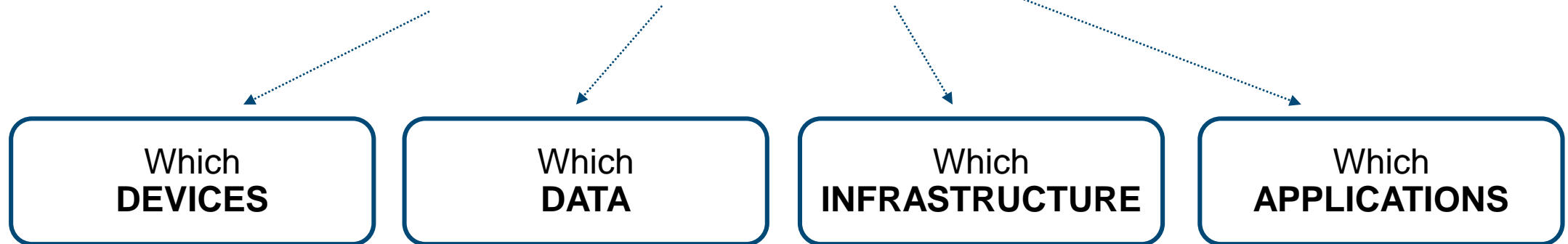
Adaptive Trust – Zero Tolerance



What does ClearPass do ?



Defines **WHO** and **WHAT DEVICES** can connect to:



Identify – Enforce – Protect

A Secure Enterprise: Identify Everything



ClearPass Identifies All Enterprise Assets



Servers



Data & Storage



Internal Applications

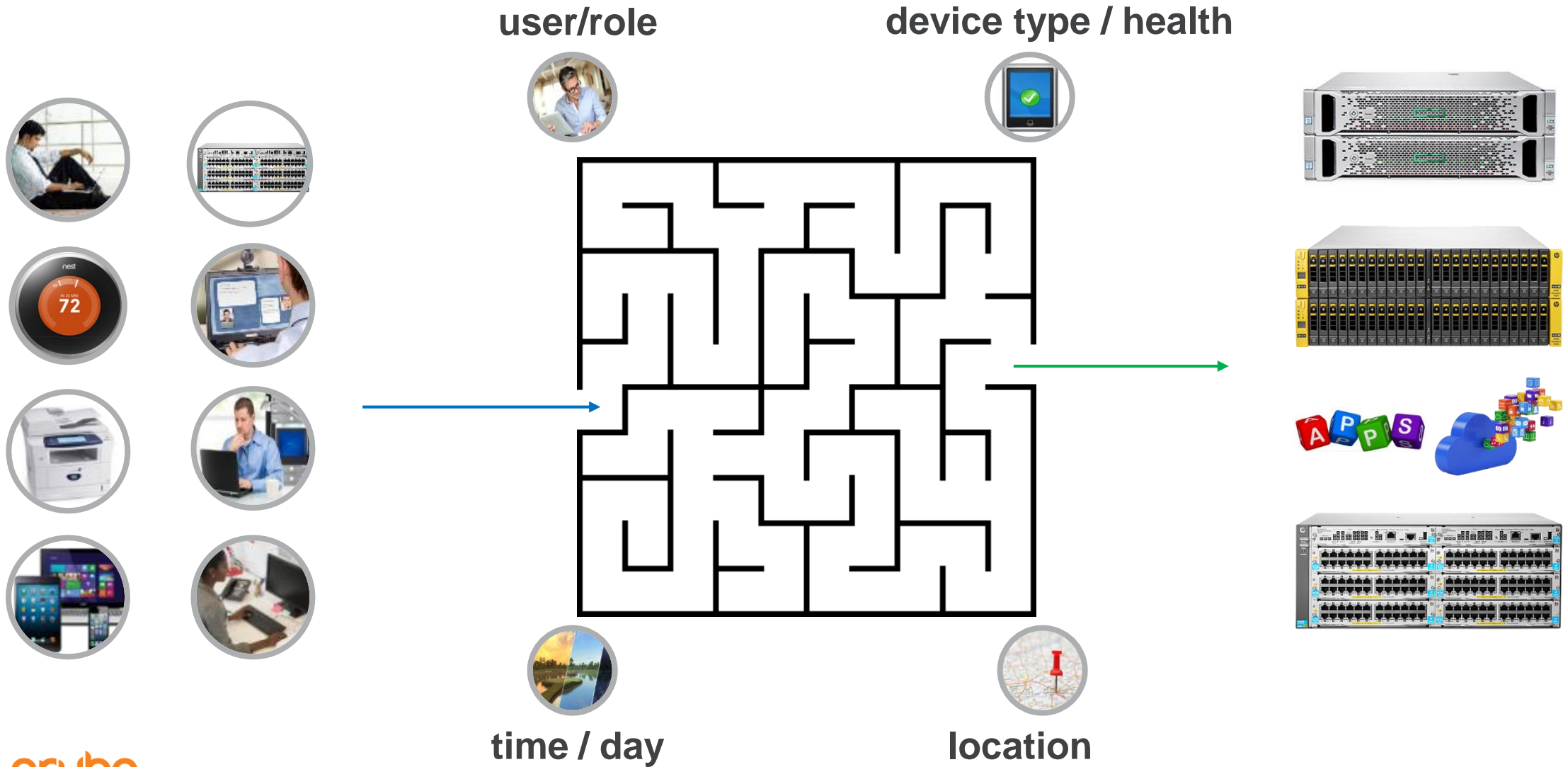


Cloud Applications



Network Infrastructure

Enforce A Per Device Policy



User and Device Access Control

CORPORATE DEVICE

Location	→	HQ
Authentication	→	EAP-TLS
TIME	→	01:00PM
SSID	→	CORP



WHAT CAN I DO TO IT



Internet and Corporate Apps

ORACLE

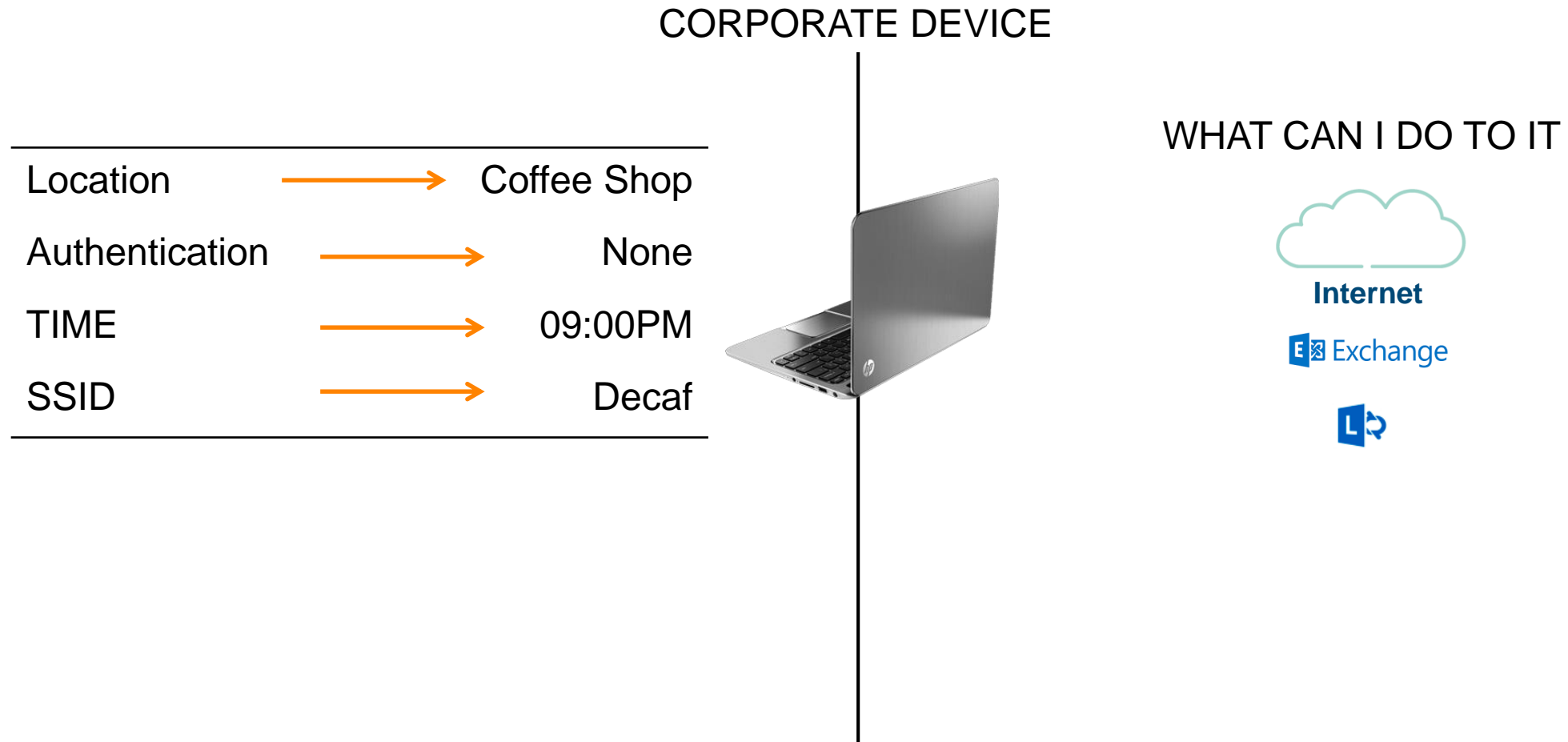
Exchange

SAP

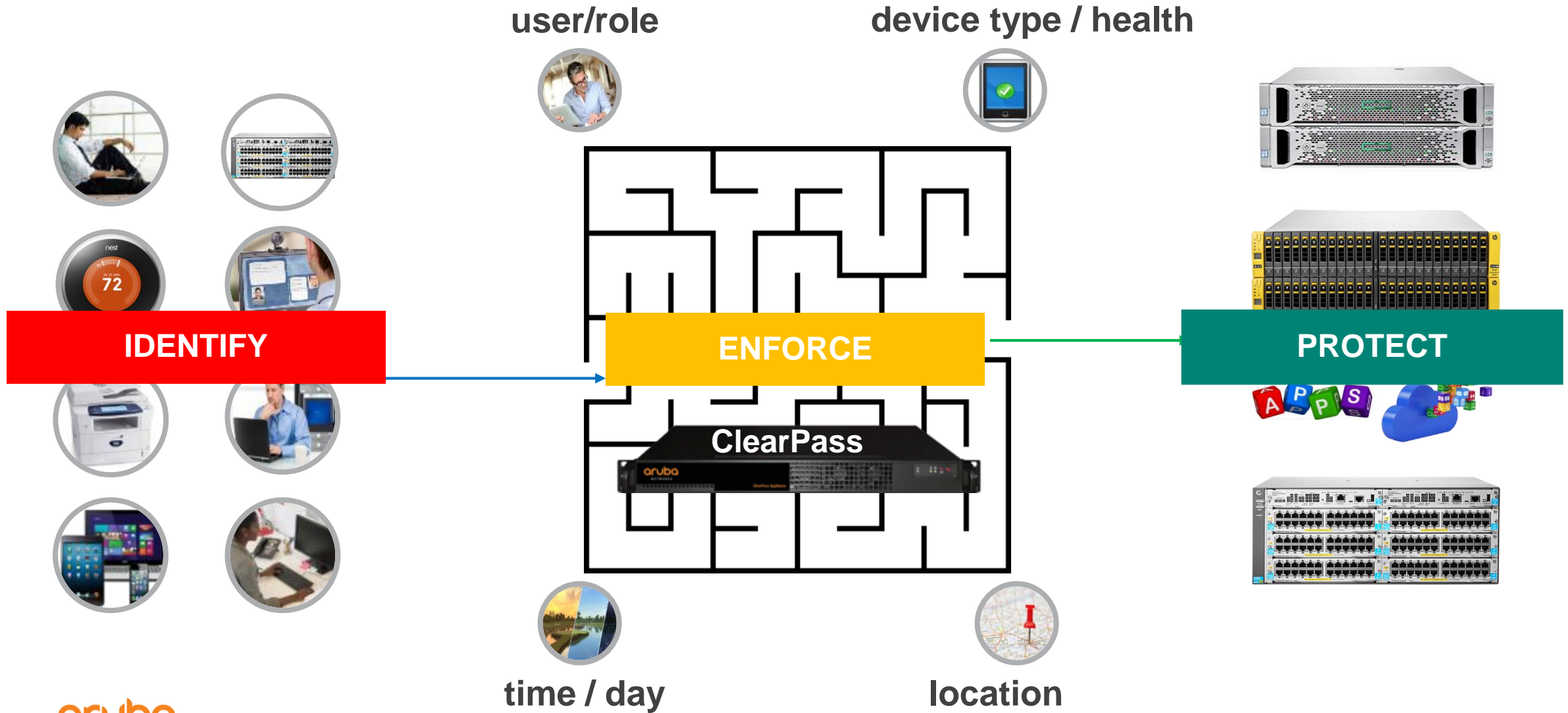


box

User and Device Access Control



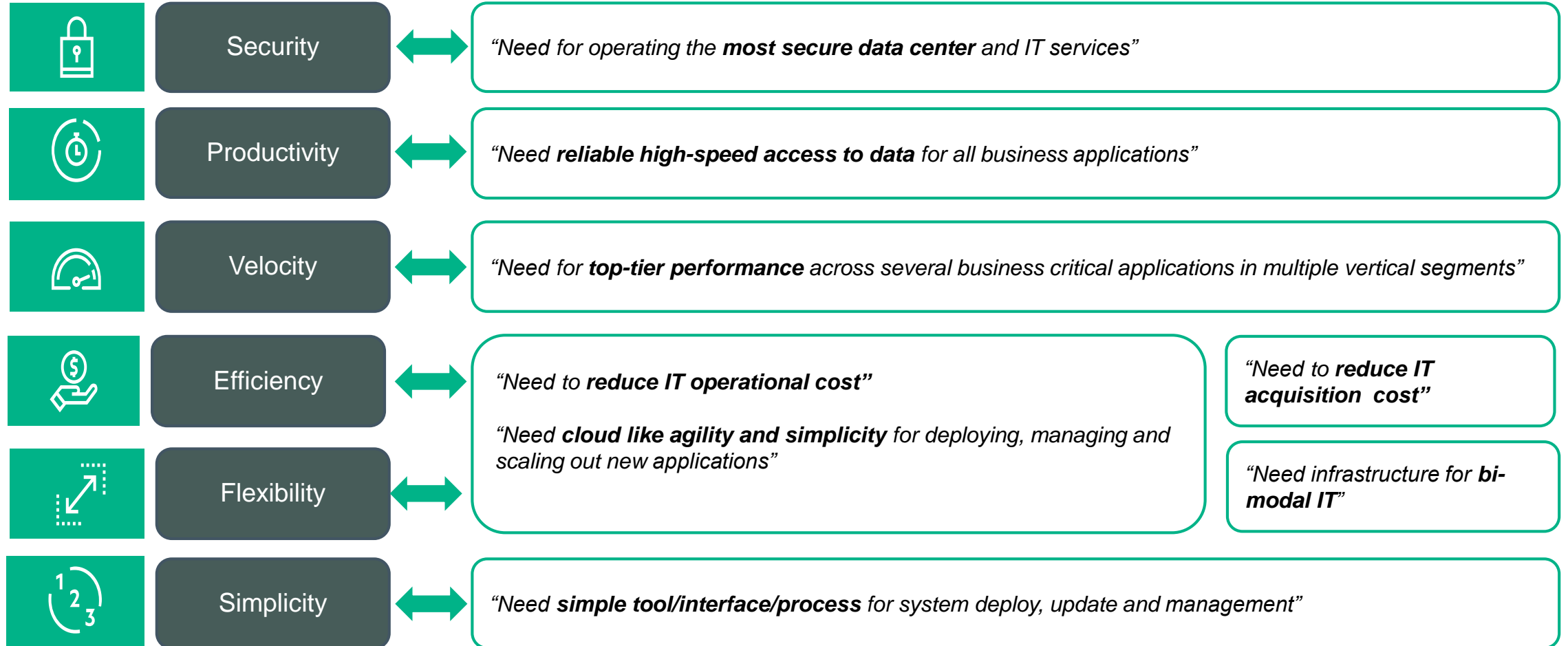
Enforce A Per Device Policy





Gen10 Servers – Addressing security concerns

Customer Requirements



HPE Servers Gen10

Introducing a new generation compute experience from HPE

Agility

A better way to deliver
business results

Security

A better way to protect
your business and data

Economic control

A better way to consume and
pay only for what you use

Powered by the world's most secure industry-standard servers

HPE Servers Gen10 - Relevant and Differentiating Innovations

Delivering the world's most secure software-defined compute and converged infrastructure to run diverse workloads and applications across traditional and multi-cloud environments



Most Secure Industry Standard Servers

Unmatched threat protection through hardware root of trust, extensive standards compliance, and supply chain attack detection.

Unparalleled ability to recover firmware and OS after denial of service attempt or detection of compromised code.



Unprecedented High-Speed Memory Capacity with Persistence

High capacity data acceleration with flash-backed Persistent Memory at TB-scale capacity for large data-intensive workloads.

Second generation of memory-centric compute innovation on the path to The Machine.



Intelligent System Tuning

Performance tuning to enable more workloads on more cores at a given CPU frequency for greater application licensing efficiency.

Predictable latency reduction and balanced workload optimization.



New Levels of Compute

Next generation industry standard CPUs with faster processing, higher speed memory access, enhanced software-defined management and security,

Enhanced GPU levels of performance and choice.



Increased In-Server Storage Density

Substantially greater NVMe capacity for large write intensive workloads needing advanced caching/tiering.

Enhanced storage density in servers with more SFF and LFF drives for collaboration and database workloads.



More Efficient and Easier Server Management

Enables large-scale FW deployment.

Improved GUI to simplify management with industry standard APIs.

Easy system debug access.

Convenient warranty entitlement validation.



Server – Security

Staying one step ahead of increasingly sophisticated attacks

A better way to protect your business and data

Security

Today's experience:

Constant worries about cybersecurity

Compliance with industry and government regulations

New threats from broader data access



Infrastructure secure from the start



An infrastructure baseline for compliance



Security standards and compliance assessment

The HPE Compute Experience

Powered by HPE ProLiant Gen10 and OneView

New protection for the entire digital enterprise

Minimizing the impacts of all forms of risk begins at the infrastructure level

Security

An infrastructure baseline for compliance

- HPE NIST 800-53 security controls applied to an infrastructure stack
- Mapping to HIPPA, NERC, ISO27001 and others



Enhanced detection of attacks from within

- Machine learning applied to behavioral analytics
- Automatic detection of attacks from inside organizations



Security standards and compliance assessment

- Security health measured against ISO27002 and HPE's unique P5 (People, Policy, Process, Product, Proof) model



Cyber Security

HPE comes to the rescue with new innovative technology just-in-time



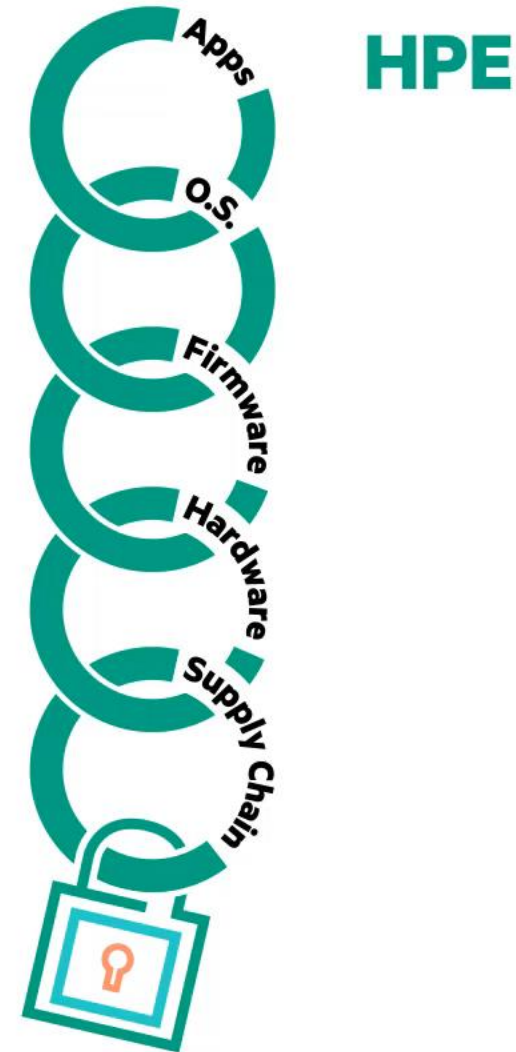
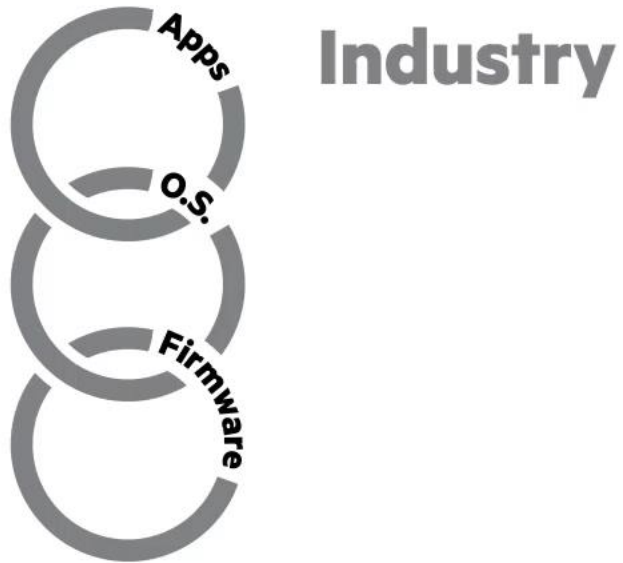
Industry



HPE

Cyber Security

HPE comes to the rescue with new innovative technology just-in-time



HPE Secure Compute

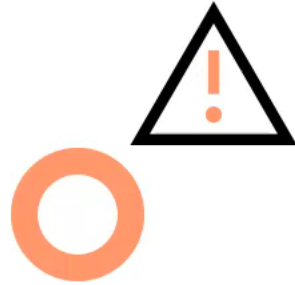
Most secure servers in the industry



 **Protect**

HPE Secure Compute

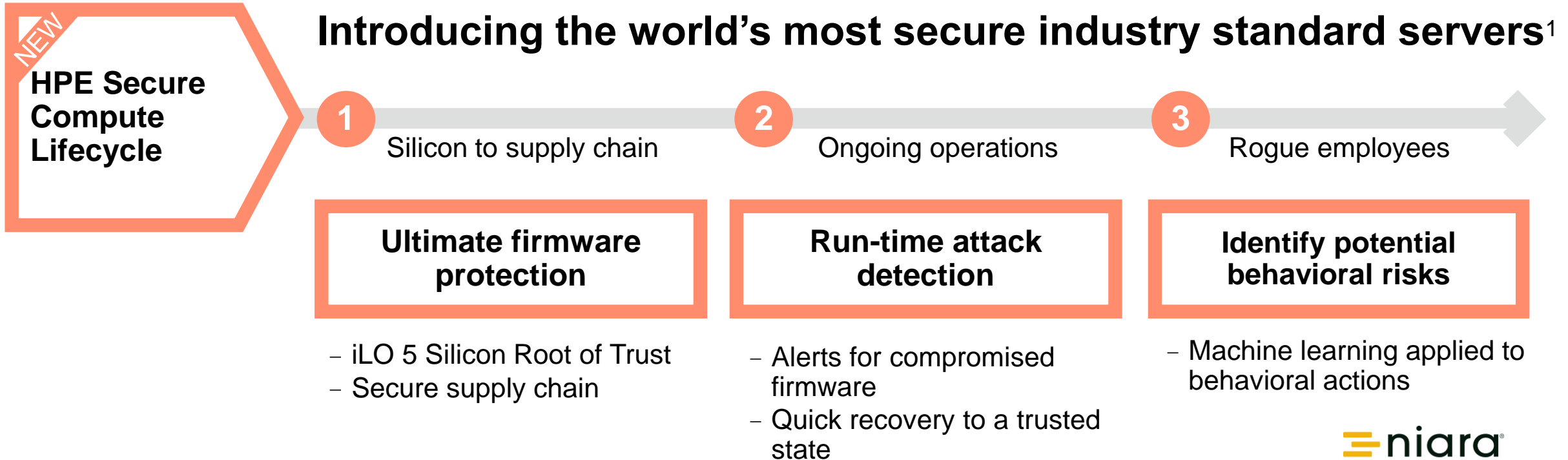
Most secure servers in the industry



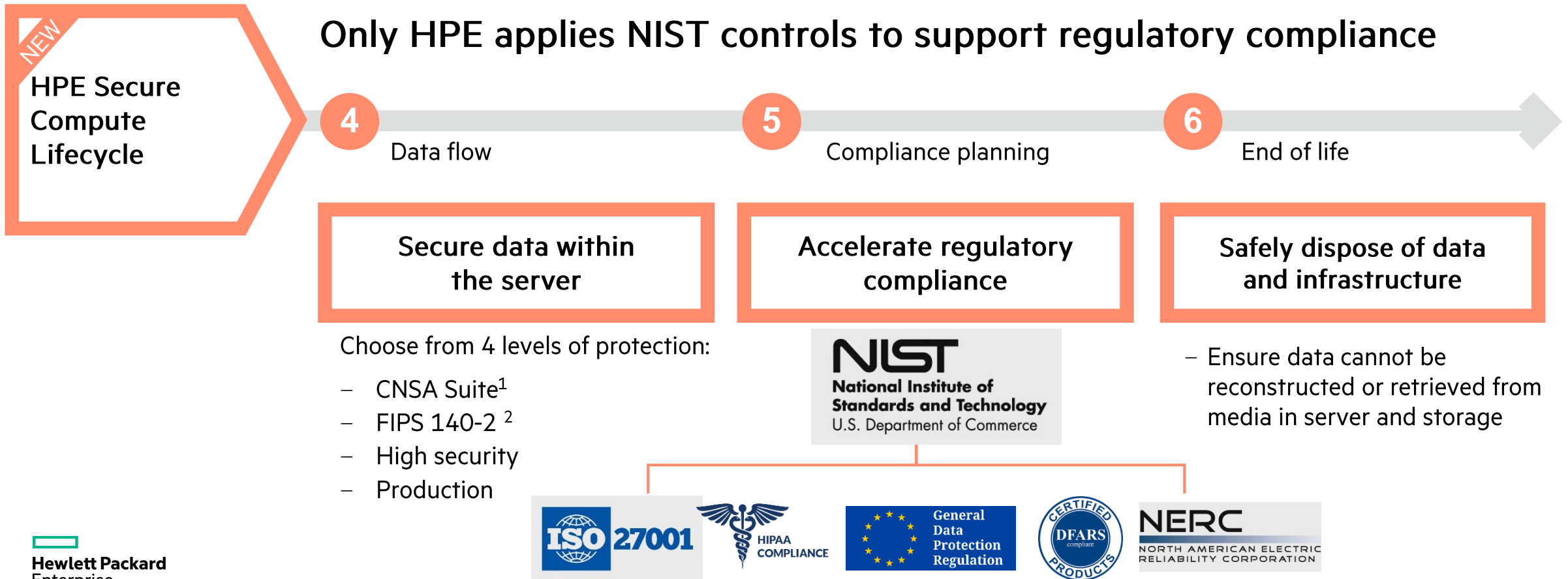
 **Protect**

 **Detect**

A new experience in server security and protection



A new experience in accelerating compliance





Server security features

UEFI Secure Boot



Industry Support

- UEFI Standard. Works with HPE and Third Party cards and major operating systems.
 - Windows 8/Server 2012+
 - SLES 11SP3+, RHEL7+, Ubuntu 12.10+, Fedora 18+, ...
 - vSphere 6.5+

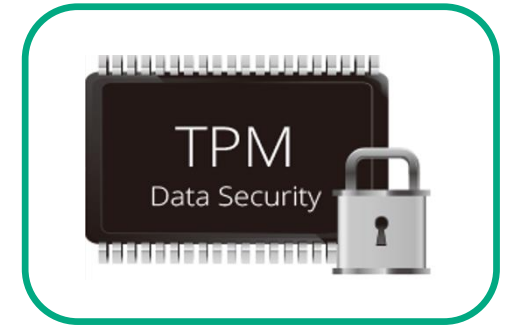
Functionality

- All UEFI Drivers, OS boot loaders, and UEFI applications are digitally signed
- Binaries are verified using a set of embedded trusted keys
- Only validated and authorized components are executed.
- Creates a chain of trust. Improved solution over TCG Trusted Boot.



Gen10 Trusted Platform Module Support

Additional Flexibility and Customer Choice



- Gen10 Supports:
 - Embedded FW-based TPM 2.0
 - Optional Discrete TPM Module configurable for TPM 1.2 or TPM 2.0.
- Embedded FW-Based TPM 2.0 called Platform Trust Technology (PTT)
 - Fully functional as TPM 2.0, but is NOT certified.
 - Does NOT support Command Response Buffer (CRB). Supports FIFO.
 - Disabled by default.
- Optional Discrete TPM
 - One module will support TPM 1.2 or TPM 2.0 mode.
 - Can be configured for FIPs mode.
 - TPM is “logically bound” to the platform by the BIOS.

Optional Server Intrusion Detection

- New Intrusion Detection sensor option for select Gen10 servers.
- iLO5 FW monitors the sensor and communicates if/ when the server hood is opened when server is powered on or on AUX power.
- Intrusion Detection even works when the server is unplugged/ AC power removed. BIOS detects any hood removal and insertions that occur when AUX power is removed.
- Competitive solution that exists on Dell Broadwell servers do NOT detect when hood is removed and AC power is not available.



iLO5 is HPE's key to Server security

iLO 5 Focus

- Security:** Raising our industry-leading bar even higher
- Firmware update technology:** Update everything through iLO network
- Agentless management:** Retiring OS-based agents
- RESTful everything:** Redfish
- At Server Management:** New innovation
- Performance:** Everything faster



Secure server management from anywhere, anytime

HPE iLO 5

Maintain complete control of your secure server, proactively managing it with ease and minimal manual intervention



Supported on MOST Gen10 ProLiant,
Apollo and Synergy servers

Customer Needs:

- **Uncompromising security**
- **Hassle-free server management** and integration into infrastructure management ecosystem using industry standards
- **Intuitive, user-friendly** server maintenance

Key New Features:

- **Immutable Silicon Root of Trust for Secure Start with ability to automatically rollback to known-good firmware**
- **Common Access Card (CAC) 2-factor authentication support**
- **OpenLDAP support**
- **Additional iLO Security modes**
- Granular control of all iLO interfaces
- **Run-time Firmware Validation** to verify integrity of iLO and BIOS
- **With 2x the CPU MHz in iLO 5, Virtual Media performance is twice as fast¹ vs iLO 4**
- **Open IPMI mode** for increased interoperability with industry IPMI tools

Secure Start

iLO and BIOS team up for a Super Hero feature

–Silicon Root of Trust

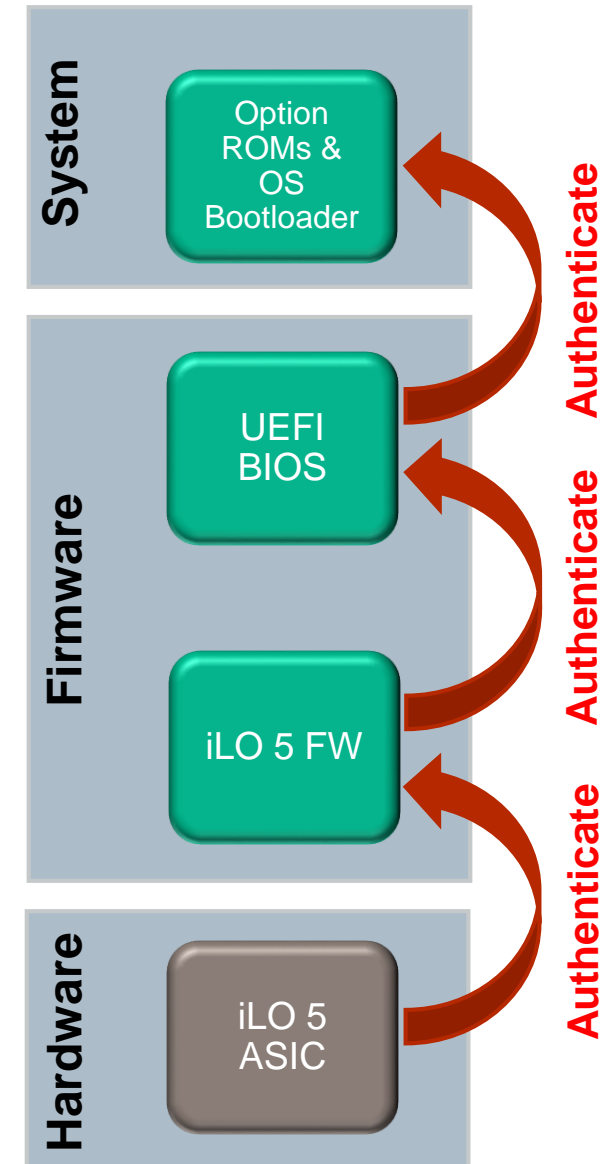
- HPE-designed logic in iLO chip validates the iLO firmware
- Burned into the iLO chip
- Immutable

–iLO firmware then validates the System ROM

- Digital signature ***must match*** or the ROM is not executed
- iLO firmware is trusted, now the ROM is trusted (Chain of Trust)

–ROM then validates Option ROMs and the OS Bootloader via UEFI Secure Boot.

- Option ROMs and OS Bootloader are NOT executed if they fail authentication.



Secure Recovery

Recovery = Priceless!

–Redundancy

- ROM and iLO have built-in redundancy

–Recovery

- Factory Installed Recovery Set on non-volatile storage
- Recovery Administrator can setup new Recovery Set
- iLO can automatically recover iLO (iLO Standard feature)
- iLO can automatically recover ROM (iLO premium feature)
- iLO can also recover CPLD, IE, ME

–Run-Time Firmware Authentication

- Background scans by iLO
- Event logs, Alerting, Web UI



iLO 5 – Runtime Scan

iLO 5
1.10 pass 64 Apr 27 2017

Information - iLO Overview

Overview Session List iLO Event Log Integrated Management Log

Active Health System Log Diagnostics

Information		Status
Server Name	WIN-9P1O6AIF27S	System Health OK
Product Name	ProLiant DL380 Gen10	Server Power ON
UUID	56303833-3250-4337-4537-303350323252	UID Indicator UID OFF
Server Serial Number	7CE703P22R	TPM Status Not Present
Product ID	380VP2-001	SD-Card Status Not Present
System ROM	U30 v1.00 (04/24/2017)	iLO Date/Time Fri Apr 28 08:37:!
System ROM Date	04/24/2017	
Backup System ROM	04/24/2017	
Integrated Remote Console	.NET Java Web Start	
License Type	iLO Advanced Premium Security Edition limited-distribution test	
iLO Firmware Version	1.10 pass 64 Apr 27 2017	
IP Address	16.85.179.52	
Link-Local IPv6 Address	FE80::FE15:B4FF:FE97:8548	
iLO Hostname	ILO7CE703P22R.americas.hpqcorp.net	

Connection to HPE

Not registered



Hewlett Packard
Enterprise

Thank you