

# A NEW COMPUTE EXPERIENCE

PROLIANT SERVER, MANAGEMENT AND SECURITY

**SASCHA NEFF**

TECHNICAL CONSULTANT

HEWLETT PACKARD ENTERPRISE



**Hewlett Packard**  
Enterprise

# A New Compute Experience

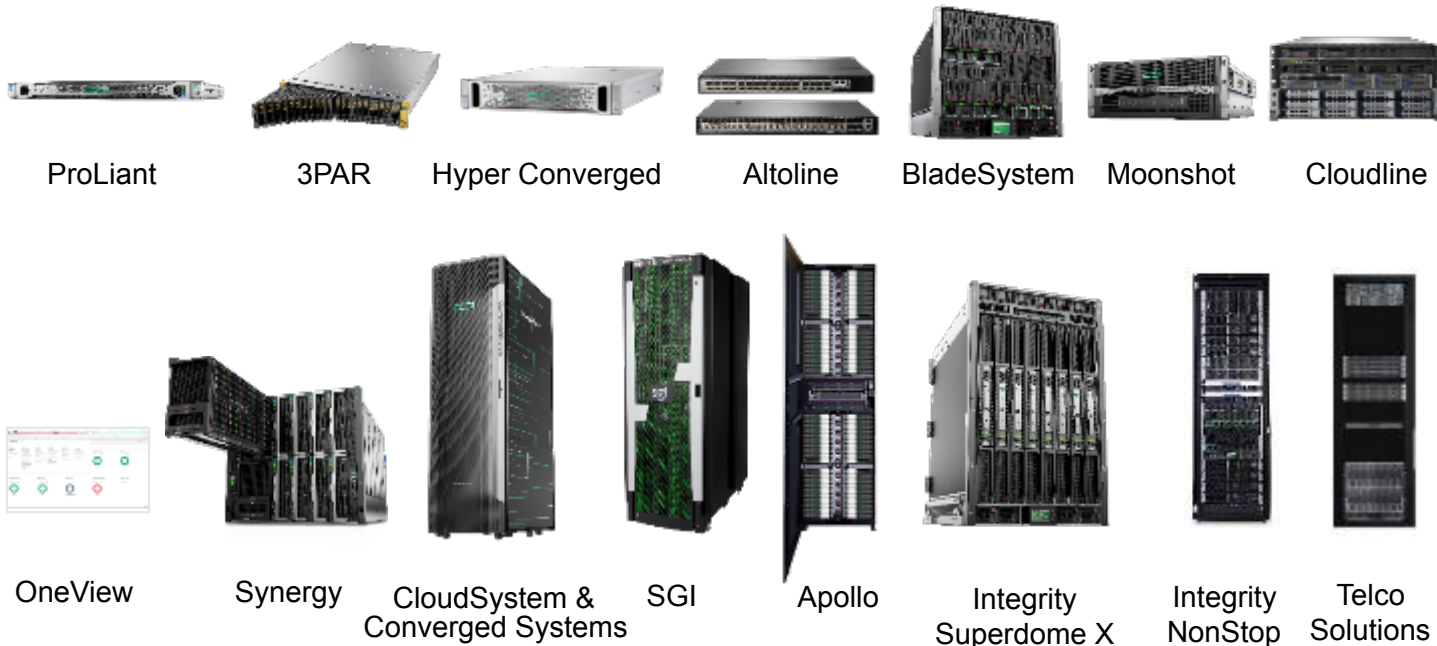
ProLiant Server, Management and Security

Sascha Neff – Technical Consultant  
[sascha.neff@hpe.com](mailto:sascha.neff@hpe.com)



# HPE ecosystem to deliver your right mix

## Key offerings



## Key partnerships



**#1** in Private Cloud infrastructure<sup>1</sup>

**#1** in Servers<sup>1</sup>

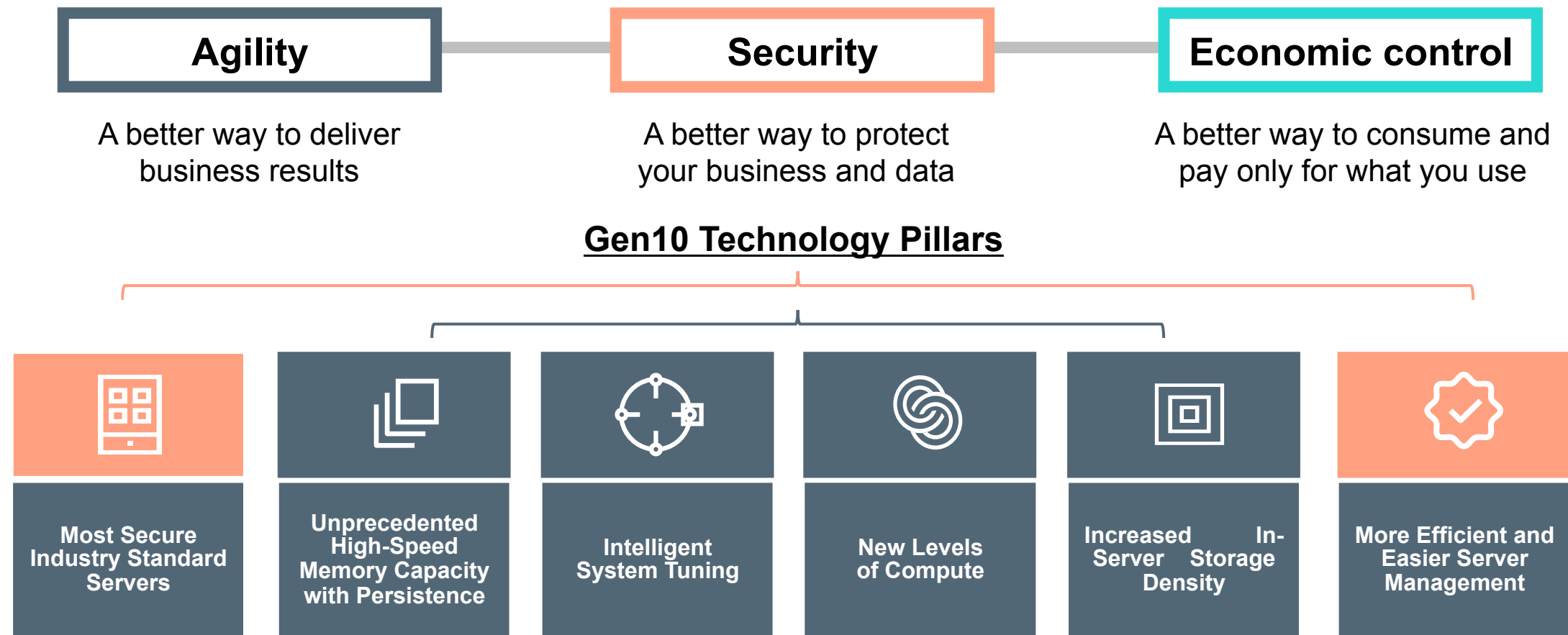
**#1** in Cloud build infrastructure<sup>2</sup>

**#1** in Total storage<sup>3</sup>

**#2** in External storage<sup>3</sup>

**#2** in Integrated platform<sup>4</sup>

# A new Compute Experience powered by HPE Gen10 innovations







# AGILITY

- ProLiant DL380 Gen10 Server

# DL380 Gen10 example, 2-SFF NVMe & 16-SFF SAS/SATA



2 Socket Server, 24 DIMMM Slots (3TB),

# DL380 Gen10 example, 18-SFF NVMe, 6-SFF SAS/SATA 2 CPUs needed



# DL380 Gen10, optioned up example 30-SFF SAS/SATA



SFF Chassis: 6 Rear SFF HDD's + 2 FHHL PCI slots

# DL380 Gen10 optioned up example, 8-LFF/2-SFF NVMe with DVD





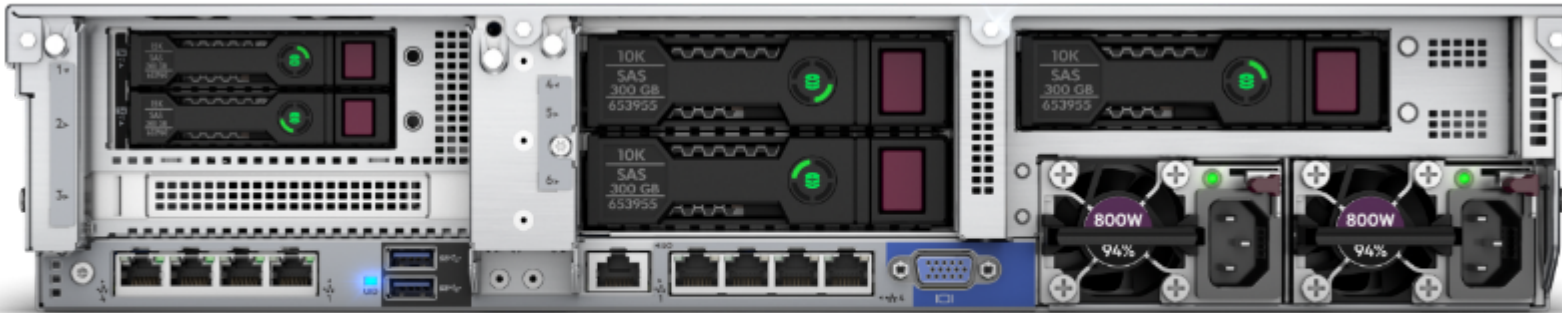
# DL380 Gen10, 12-LFF



# Max with 12 LFF chassis with internal 4 LFF and the LFF/SFF rear drives

2 SFF HDD's

3 LFF Drives



4 internal  
LFF Drives



# HPE ProLiant DL380 Gen9 to Gen10 Comparison

Primary and Tertiary Riser



Up to 3 Double Wide GPU's

Primary/Secondary Riser with 2 SFF Rear Cage

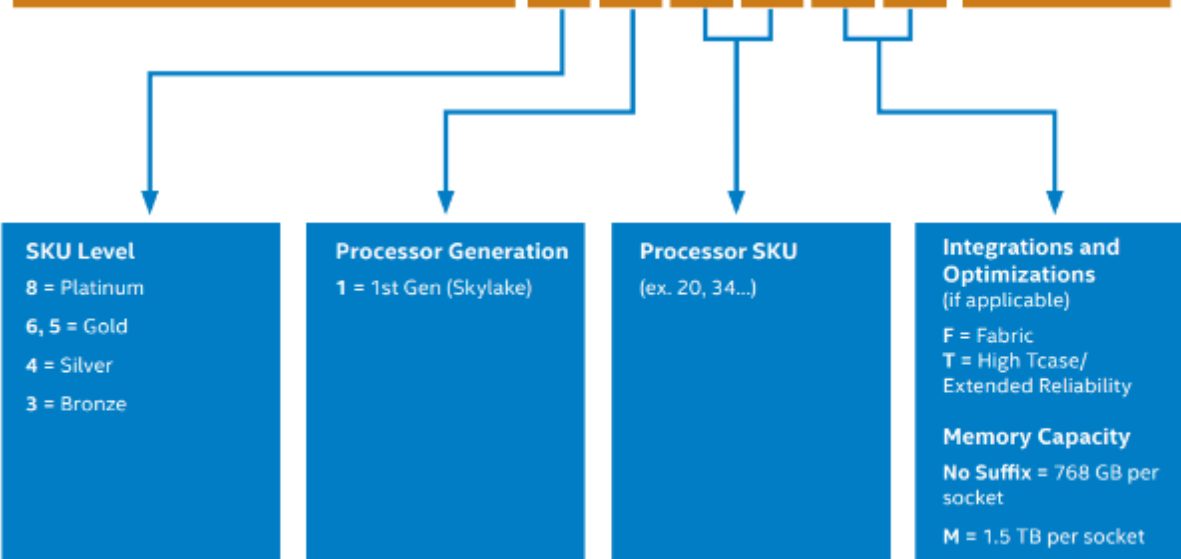


Up to 2 Double Wide GPU's



# Intel Xeon Scalable Processors Family

Intel® Xeon® Platinum	8	1	#	#	α	α	processor
Intel® Xeon® Gold	6	1	#	#	α	α	processor
Intel® Xeon® Gold	5	1	#	#	α	α	processor
Intel® Xeon® Silver	4	1	#	#	α	α	processor
Intel® Xeon® Bronze	3	1	#	#	α	α	processor



## BEST PERFORMANCE, MOST SCALABLE, BEST BUSINESS AGILITY



Intel® Xeon® Platinum  
Processor 8XXX Family

- Best choice for mission-critical, real-time analytics, machine learning, and artificial intelligence workloads
- Best workload-optimized performance for general purpose compute and hybrid-cloud deployments
- Best performance for the most demanding storage and networking workloads
- Best memory bandwidth and 2, 4, 8+ socket scalability

## GREAT PERFORMANCE, FAST MEMORY, AND MORE INTERCONNECT/ACCELERATOR ENGINES



Intel® Xeon® Gold  
Processor 6XXX Family

- Significant workload-optimized performance improvements for general purpose compute
- Significant improvements for demanding storage and networking workloads
- Highest memory speed, highest memory capacity, and enhanced Intel AVX-512
- Enhanced 2-4 socket scalability and performance

## BETTER PERFORMANCE, ADVANCED RELIABILITY



Intel® Xeon® Gold  
Processor 5XXX Family

- Improved performance for compute-bound workloads
- Affordable Advanced RAS and 4-socket scalability
- Suitable for a wider range of workloads

## EFFICIENT PERFORMANCE AT LOW POWER



Intel® Xeon® Silver  
Processor 4XXX Family

- Solid compute capability (Hyper-Threading, Turbo Boost)
- Improved memory speed, energy efficiency
- Suitable for a moderate range workloads

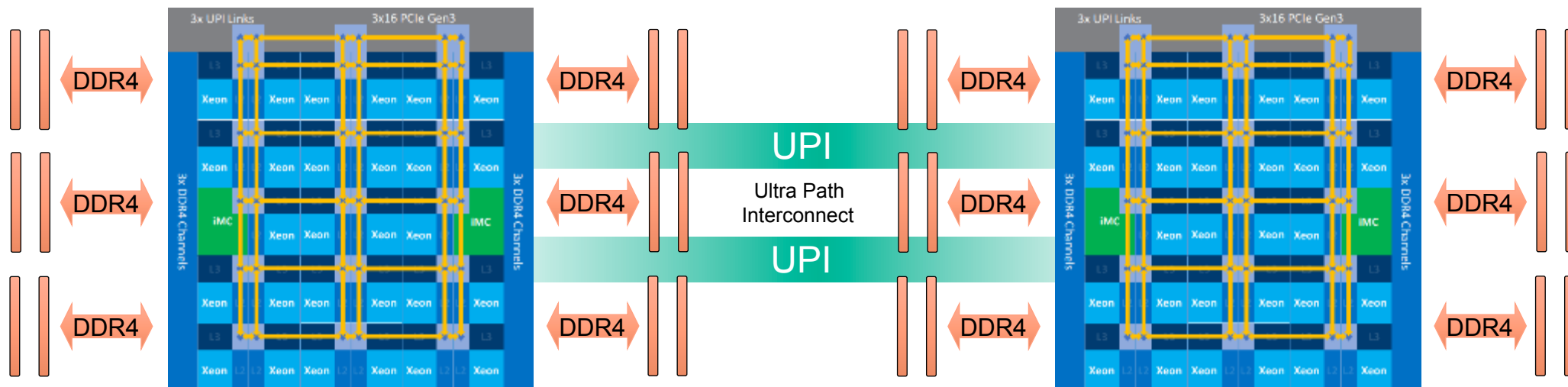
## ENTRY-LEVEL PERFORMANCE AND HW-ENHANCED SECURITY



Intel® Xeon® Bronze  
Processor 3XXX Family

- Affordable, entry-level 2-socket support suitable for light-range workloads
- Reliable upgrade versus Intel® Xeon® processor E3 product family

# Intel Xeon Scalable Processors



## UPI:

$10.4 \text{ GT/s} \cdot 20 \text{ Bit/T} = 208 \text{ GBit/s} = 26 \text{ GByte/s Brutto}$   
 $10.4 \text{ GT/s} \cdot 16 \text{ Bit/T} = 166.4 \text{ GBit/s} = \mathbf{20.8 \text{ GByte/s Netto}}$

$20.8 \text{ GByte/s per direction} \times 2 = 41.6 \text{ GB/s total transfer per link}$

$2 \times \text{UPI} = \mathbf{83.2 \text{ GB/s CPU - CPU Communication}}$

## CPU:

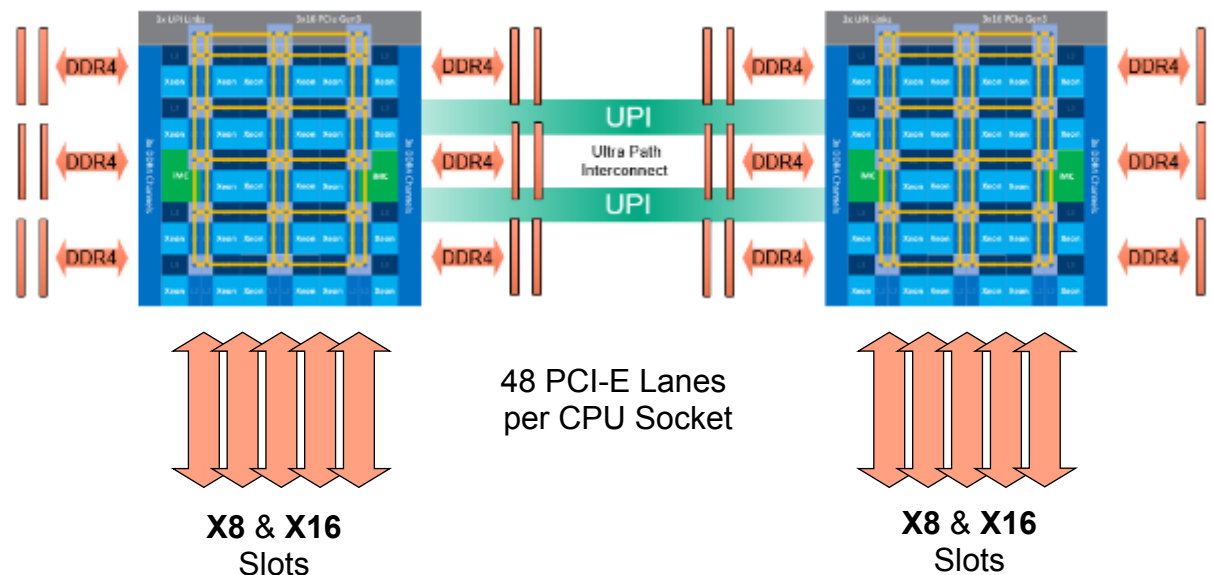
- 8 – **28 Cores**
- 1.7 GHz – 3.6 GHz
- Up to **1.5 TB RAM** (2133 – 2666 MHz)
- 48 PCI-E Lanes



# PCI-E Gen3

PCI-E bandwidth per direction:

	PCI-E 1.0	PCI-E 2.0	PCI-E 3.0
x1	250 MB/s	500 MB/s	1'000 MB/s
x2	500 MB/s	1'000 MB/s	2'000 MB/s
x4	1'000 MB/s	2'000 MB/s	4'000 MB/s
x8	2'000 MB/s	4'000 MB/s	8'000 MB/s
x16	4'000 MB/s	8'000 MB/s	16'000 MB/s



## PCI-Express Generation 3:

PCI-E is a full duplex protocol.

PCI-E 3.0 - x16 = 16GB/s per direction \* 2 = **32GB/s** per x16 slot

# HPE Memory Speeds

HPE Server Memory Speed: Intel Xeon Platinum/Gold 81xx/61xx Processors				
	8GB	16GB	32GB	64GB
1 DIMM per Channel	2666 MT/s	2666 MT/s	2666 MT/s	2666 MT/s
2 DIMM per Channel	2666 MT/s	2666 MT/s	2666 MT/s	2666 MT/s
HPE Server Memory Speed: Intel Xeon Gold/Silver 51xx/41xx Processors				
	8GB	16GB	32GB	64GB
1 DIMM per Channel	2400 MT/s	2400 MT/s	2400 MT/s	2400 MT/s
2 DIMM per Channel	2400 MT/s	2400 MT/s	2400 MT/s	2400 MT/s
HPE Server Memory Speed: Intel Xeon Bronze 31xx Processors				
	8GB	16GB	32GB	64GB
1 DIMM per Channel	2133 MT/s	2133 MT/s	2133 MT/s	2133 MT/s
2 DIMM per Channel	2133 MT/s	2133 MT/s	2133 MT/s	2133 MT/s



# AGILITY

- Intelligent System Tuning

# HPE Intelligent Systems Tuning

Agility



## Jitter Smoothing\* :

Smooths fluctuations in processor frequency as customers increase performance. For multiple segments, particularly financial institutions and live streaming applications

## Core boosting\* :

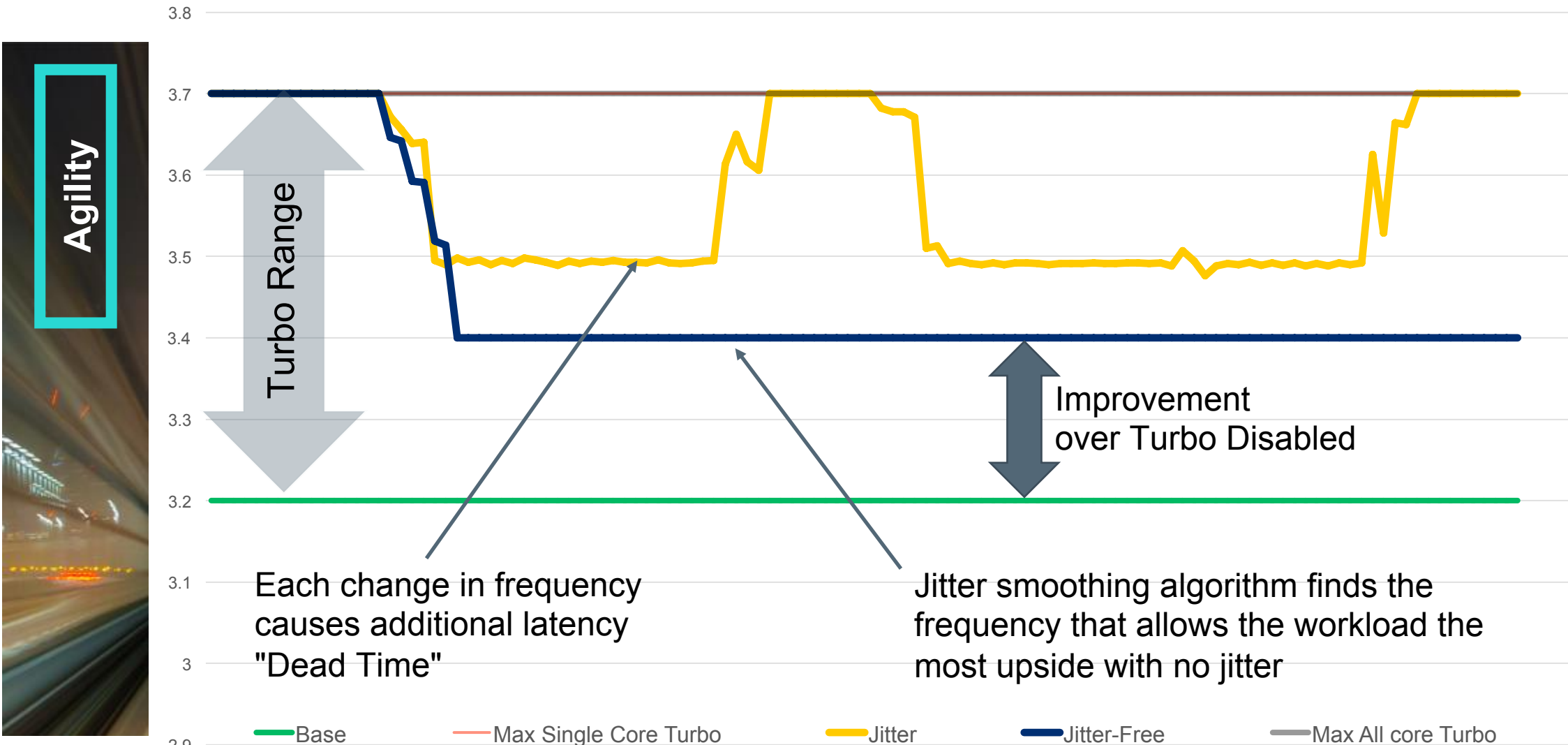
Unique ability to dynamically modulate frequency and performance  
Reduce application core charges through greater performance with fewer processor cores – **available in future release**

## Workload matching :

Custom profiles on ProLiant Server systems match the more common customer workloads, automatically matching internal resources to those typical needs

\* Available with iLO Advanced and iLO Advanced Premium Security

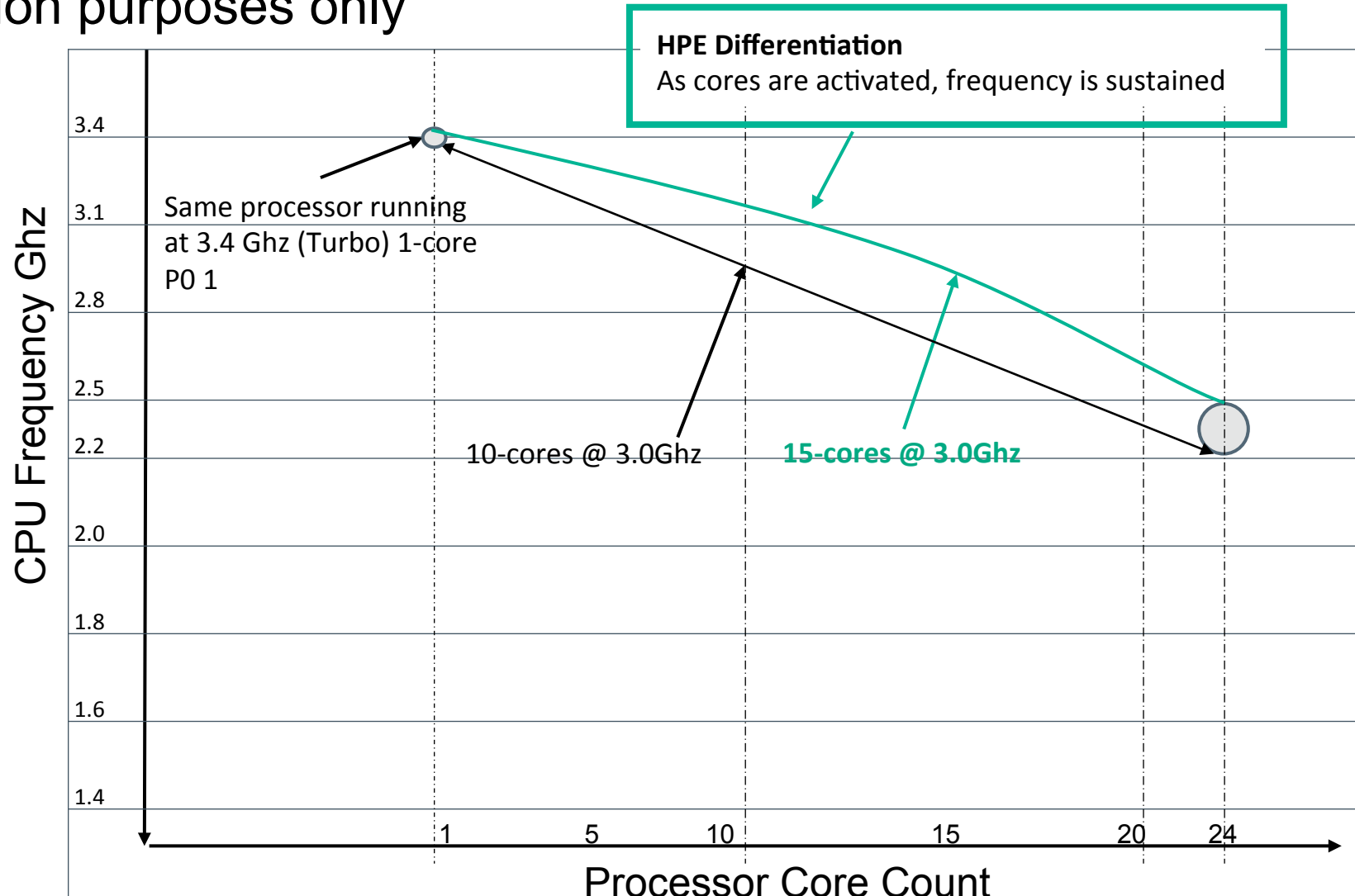
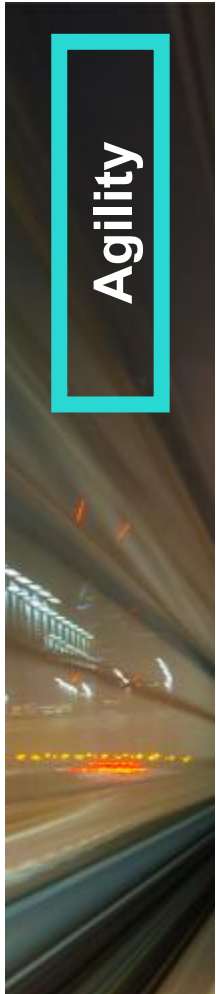
# Jitter Smoothing - illustration





# Core Boosting: Performance

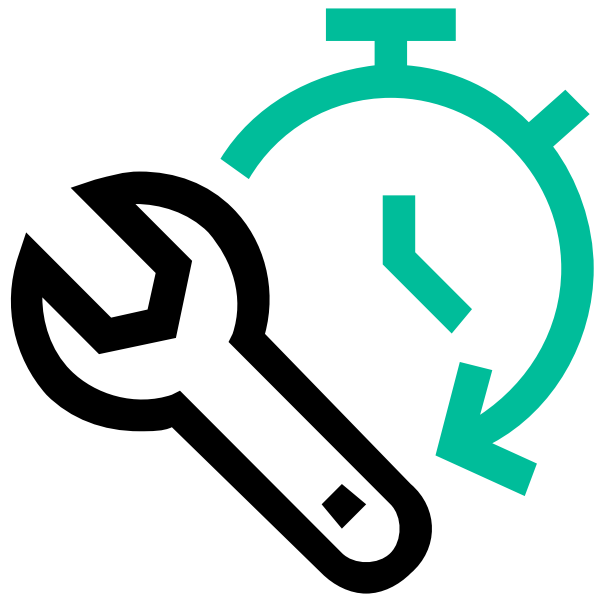
Illustration purposes only



- Core Boosting on selected platforms
- 8c/155W
- 16c/205W
- 24c/205W
- Standard High Performance fans
- Available @ September 2017

# Workload Profiles

Server Tuning Variables to Optimize Performance and/or efficiency



# Workload Matching

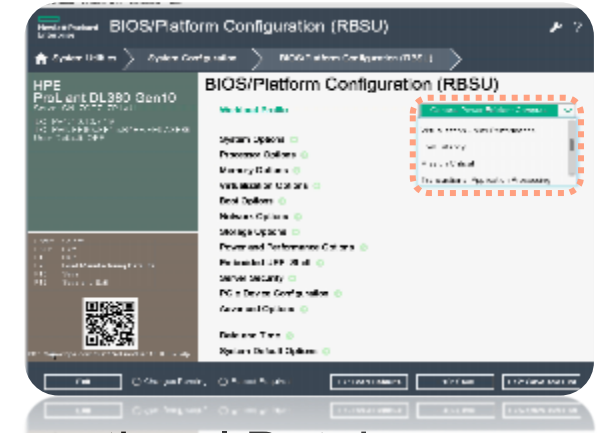
## Simplifying Performance Optimization for Key Workloads

Agility

- General Power Efficient Compute
- General Peak Frequency Compute
- General Throughput Compute
- Virtualization – Power Efficient
- Virtualization – Max Performance
- Low Latency
- Mission Critical



- Transactional Database
- High Performance Compute
- Decision Support
- Graphic Processing
- I/O Throughput
- Web/E-commerce
- Extreme Efficient Compute
- Custom



**Leverage the experience of HPE's Performance Engineering Team**



# AGILITY

- HPE Persistent Memory

# Ultra-fast HPE Persistent Memory at speed of Compute

## New Gen10 Persistent Memory Product Portfolio

Agility

**Performance:** Memory speeds (DRAM)  
**Persistence:** Flash-backed  
**Endurance:** Up to 10 trillion times higher than Flash

### HPE NVDIMMs



#### HPE 16GB NVDIMMs

max.192GB capacity (12 x 16GB NVDIMM)

### HPE Scalable Persistent Memory



#### 1 TB in 2 socket Server

Large in-memory compute  
Checkpoints and Restores  
HTAP- Real Time Analytics  
Large Databases  
VSAN and Storage Spaces Direct  
Big Data, Service Providers, Performance Tier, and Virtualizations

Database Storage Bottlenecks  
OLTP logs  
index files  
Caching

Small (100s of GB)    Large (Terabytes)

Database Workloads

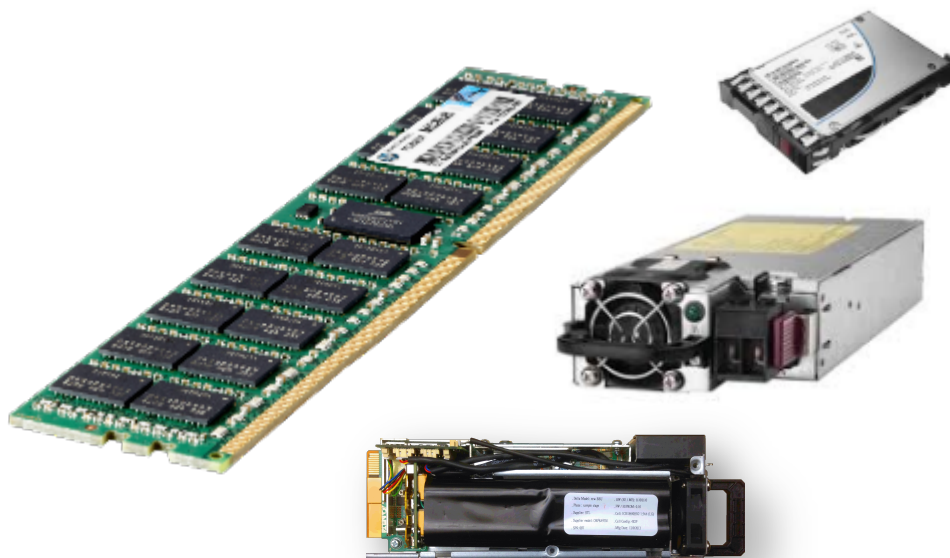
Industry leading persistent memory technology delivers performance, resiliency, scale and efficiency required of data intensive applications



# HPE delivers TB-scale persistent memory at DRAM speeds

## HPE Scalable Persistent Memory

Agility



### Key Features:

- Large capacity & fast persistent memory with up to 1TB capacity
- Delivers data resiliency
- Highest performing persistent memory in the market running at DRAM speeds

### Key Benefit:

- Ideal for in-memory compute, large databases and analytics workloads needing terabyte scale capacity and the highest levels of performance.
- Up to **20x reduction** in database recovery time, up to **27x faster checkpoints**





# AGILITY

- Increased In-Server Storage Density
- New Levels of Compute

# Boost storage performance, scalability and resiliency

## HPE Smart Array Gen10 Controllers

Agility



### Key Features:

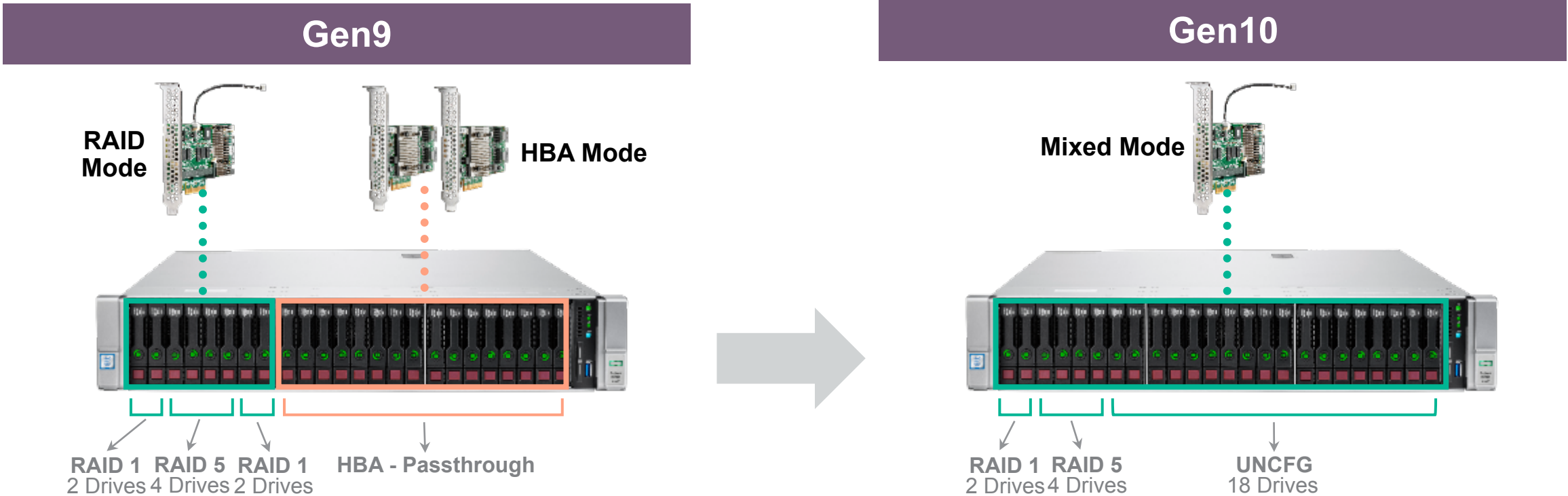
- **Mixed Mode** for Smart Array Controllers
- Performance with up to **1.6M IOPS**

### Key Benefit:

- Offers the flexibility to use both HBA and RAID modes simultaneously on a single controller, freeing up a PCIe slot

# Smart Array Gen10 Mixed Mode

Illustration purposes only



---

# HPE Gen10 Smart Array Controllers New Features

Enterprise-class RAID protection to maximize performance, data availability and capacity

## Hybrid Mode

Flexibility to **use both HBA and RAID mode simultaneously** on a single controller, freeing up a PCIe slot for other uses

## Better Performance

Gen10 controllers deliver up to 1.5M IOPS (4KB random reads), **50% more performance compared to Gen9 controllers**

## Less Power

Gen10 controller ASIC uses up to **47% less power** than Gen9 ASIC, resulting in power and cooling savings

## Security

**HPE Smart Array SR Secure Encryption** provides encryption for data-at-rest on all SAS/SATA drives

## Caching Solution

**HPE Smart Array SR SmartCache** accelerates access to your data on HDDs by up to 4x by caching the hot data on SSDs

## UEFI Configuration Tool

**New UEFI Configuration Tool** reduces the time it takes to configure simple RAID volumes on an unconfigured server

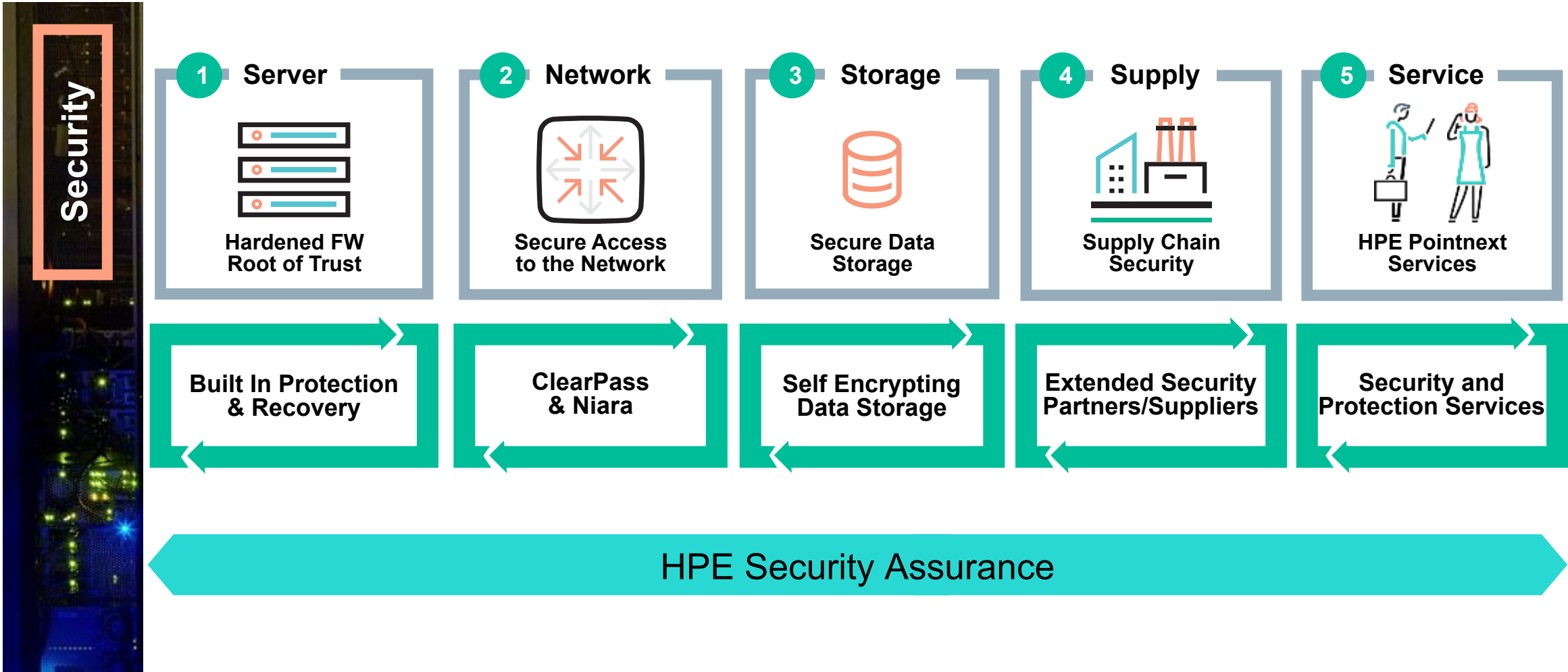
---



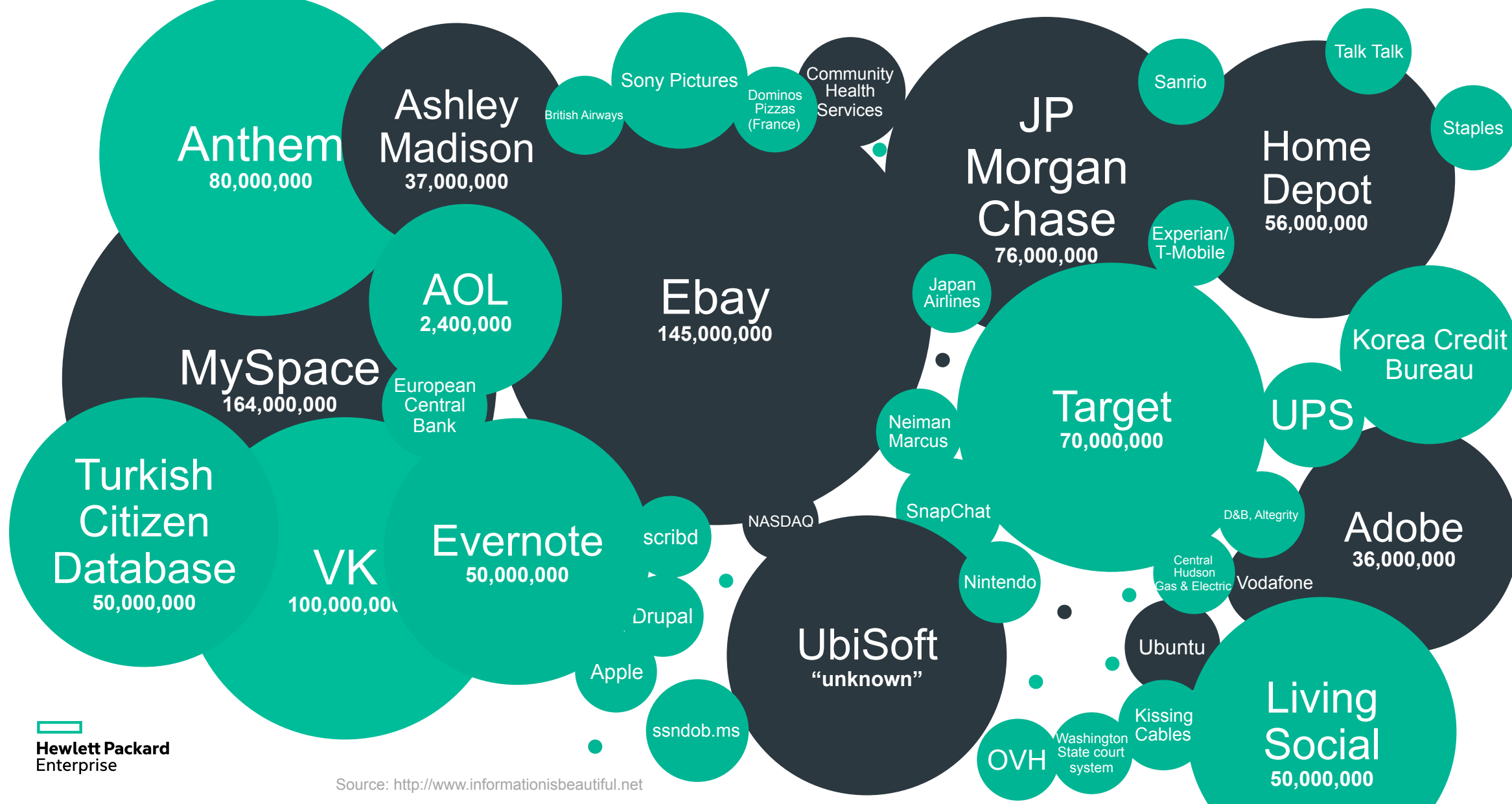


# SECURITY

# The HPE Security Portfolio







Ma

River City Media  
1,370,000,000



99 days

2017 ...March April May June July August...

Average time cyber criminals are inside before detection<sup>1</sup>

2017: 99 days  
2016: 146 days  
2015: 229 days

1. Mandiant M-Trends 2017

84%

of breaches occur at the **application layer**<sup>2</sup>

2. <http://www.neowin.net/news/hp-discover-startling-security-statistics> and HPE Research

Since 2010, time to resolve an attack **has grown**<sup>3</sup>

2.5x

3. Ponemon Cost of Cybercrime report

“As cyber attacks become more sophisticated, the potential for BIOS or other **firmware attacks** is growing”<sup>4</sup>

4. National Institute of Standards and Technology (NIST) Special Publication 800-147b, 2014, updated 2017

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

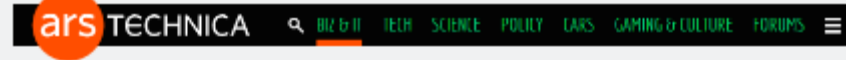
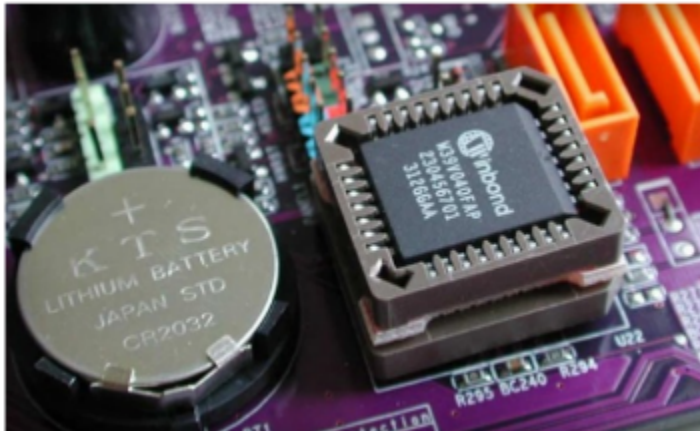
# Can you trust your hardware vendor?



## Rakshasa: The hardware backdoor that China could embed in every computer

By Sebastian Anthony on August 1, 2012 at 8:45 am | 31 Comments

0 shares     



## Apple deleted server supplier after finding infected firmware in servers [Updated]

Report: Siri, internal development servers affected by fake firmware patch.

SEAN GALLAGHER - 2/24/2012, 5:49 PM



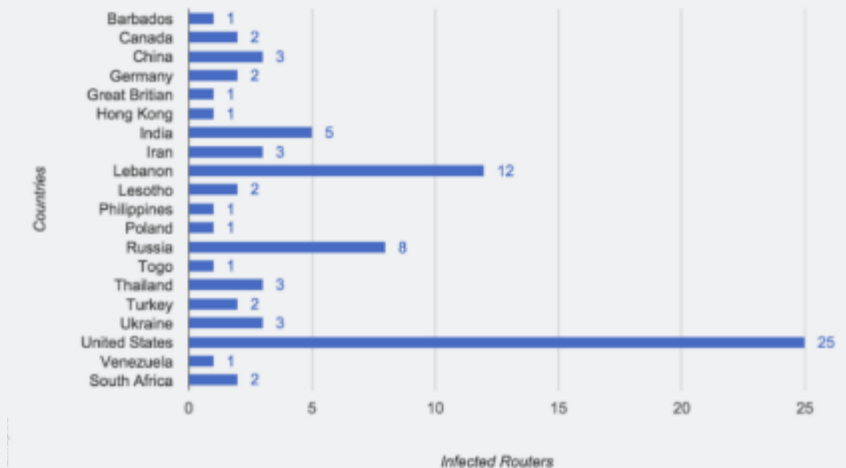
Racks of servers that populate Apple's \$1 billion data center in Maiden, North Carolina



## Malicious Cisco router backdoor found on 79 more devices, 25 in the US

SYNful Knock Implant appears to be much bigger than first reported, researchers say.

DAN GOODIN - 9/16/2015, 4:53 PM



Sources:

<https://arstechnica.com/information-technology/2017/02/apple-axed-supermicro-servers-from-datacenters-because-of-bad-firmware-update/>

<https://www.extremetech.com/computing/133773-rakshasa-the-hardware-backdoor-that-china-could-embed-in-every-computer>

<https://arstechnica.com/security/2015/09/malicious-cisco-router-backdoor-found-on-79-more-devices-25-in-the-us/>



# HPE Integrated Lights Out 5 HPE ProLiant Security

# HPE Secure Compute Lifecycle – HPE iLO5

Security



2x the CPU MHz in iLO 5

OpenLDAP support

Open IPMI mode

Additional iLO Security modes



# HPE Secure Compute Lifecycle – HPE iLO5

Security



**Silicon Root of Trust**

**FW Runtime Validation**

**Secure Recovery**

**Commercial National  
Security Algorithms**



# HPE Secure Compute Lifecycle



## Security

### Silicon Root of Trust

- Anchoring the root of trust into the silicon
- Only HPE offers industry standard servers with major firmware anchored into the silicon
- Provides impenetrable protection through entire supply chain: manufacturing, distribution, shipping, configuration, & installation.
- Millions of lines of firmware code run before server operating system boots

### FW Runtime Validation

- Daily checking of firmware every 24 hours verifying validity and credibility of UEFI, CPLD, iLO, IE, and ME.
- Valid and secure firmware copy stored in lock-box
- Firmware on other HPE options like drives and NICs can be checked as well
- Alert of compromised code through iLO audit logs

### Secure Recovery

- Recovering firmware to known good state after detection of compromised code
- Options to recover to factory settings or last known good or not recovering at all taking server off-line
- Ability to recover other server settings, with future ability to recover operating system

### Commercial National Security Algorithms

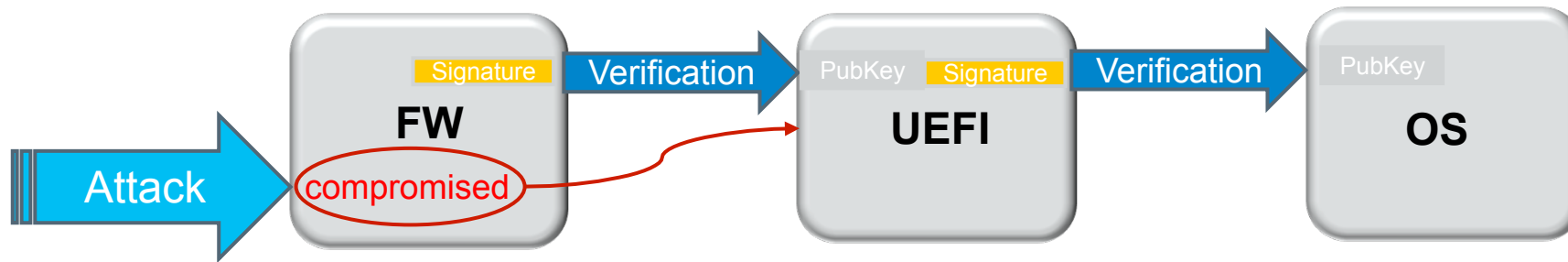
- Highest level of security not offered by any other industry server providers
- Typically used for handling the most confidential and secret information
- Uses the highest level of cryptography in the industry
- No increase in server latency



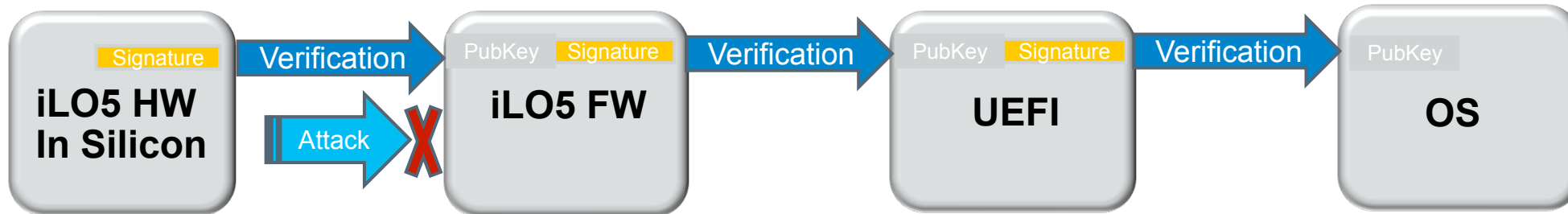
# Silicon Root of Trust & FW Verification

# HPE Silicon Root of Trust vs SW Root of Trust

## Software Root of Trust

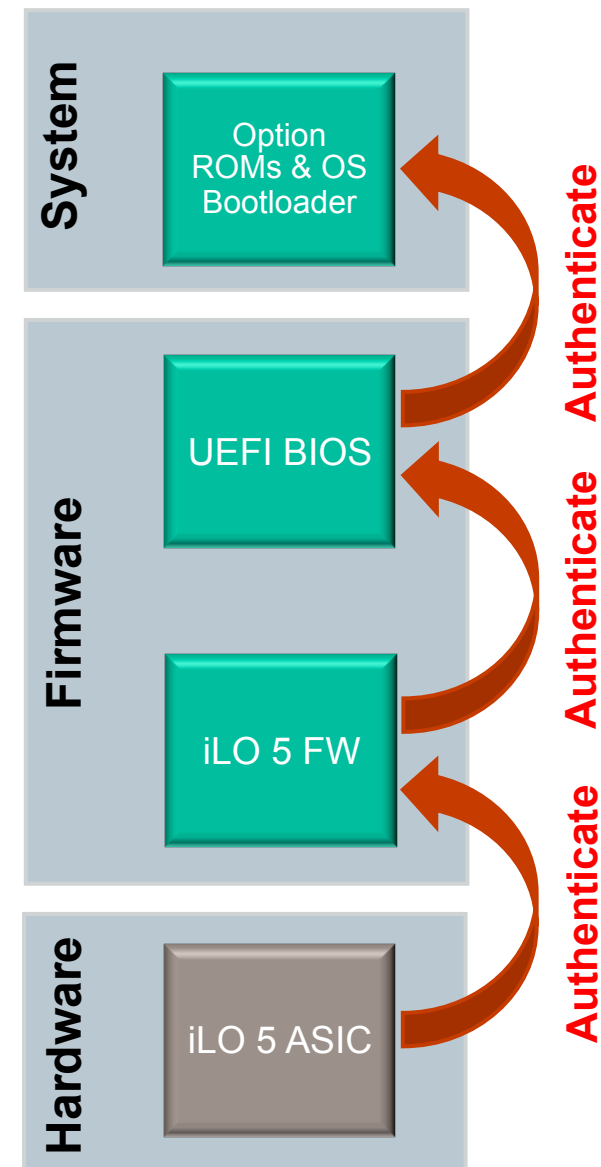


## HPE Gen10 Anchors First Crypto Key in Silicon at FAB



# Secure Start – Featuring Silicon Root of Trust

- 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.





**iLO 5**  
1.10 pass 65 May 01 2017

Information

System Information

Firmware & OS Software

iLO Federation

Remote Console & Media

Power & Thermal

iLO Dedicated Network Port

iLO Shared Network Port

Remote Support

Administration

Security

Management

Intelligent Provisioning



Administration - Firmware Verification



User Administration   Directory Groups   Boot Order   Licensing   Key Manager   Language   **Firmware Verification**

✓ **Last scan result: OK**  
Last scan time: 2017-05-29T16:50:23Z

Firmware Status

⚙️ ▶️ **Run Scan**

Firmware Name	Firmware Version	Health	State
iLO 5	1.10 May 01 2017	✓ OK	⚙️ Enabled
System ROM	U30 v1.00 (04/24/2017)	✓ OK	⚙️ Enabled
System Programmable Logic Device	0x25	✓ OK	⚙️ Enabled
Innovation Engine (IE) Firmware	0.1.0.22	✓ OK	⚙️ Enabled
Server Platform Services (SPS) Firmware	4.0.3.185	✓ OK	⚙️ Enabled

Administration - Firmware Verification

User Administration   Directory Groups   Boot Order   Licensing   Key Manager   Language   **Firmware Verification**

Scan Settings

☐ Enable Background Scan

Integrity Failure Action

☒ Log Only

☐ Log and Repair Automatically

Scan Interval (in days)

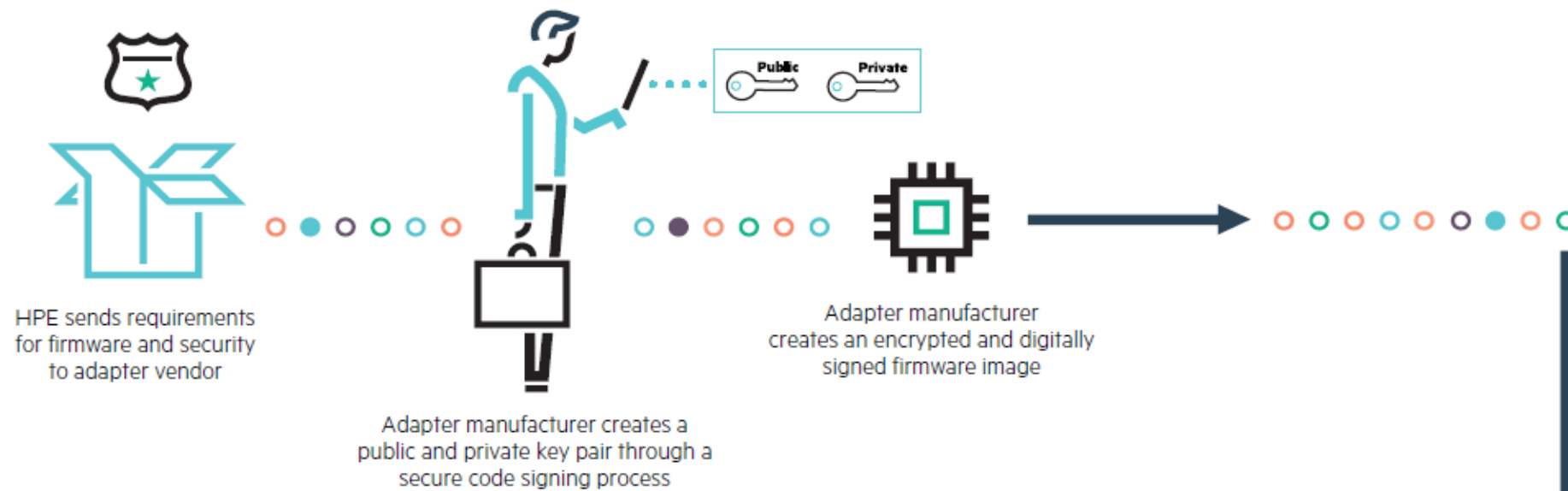
1

— +

Submit

# How the NIC Safeguards - *Inside the Server*

## Digital signing process



## Firmware update process on the NIC

### Root of trust

Creates a chain of trust for authenticating updates to firmware

### Chain of trust

Enables security features based on the root of trust with current firmware

### Authenticated updates\*

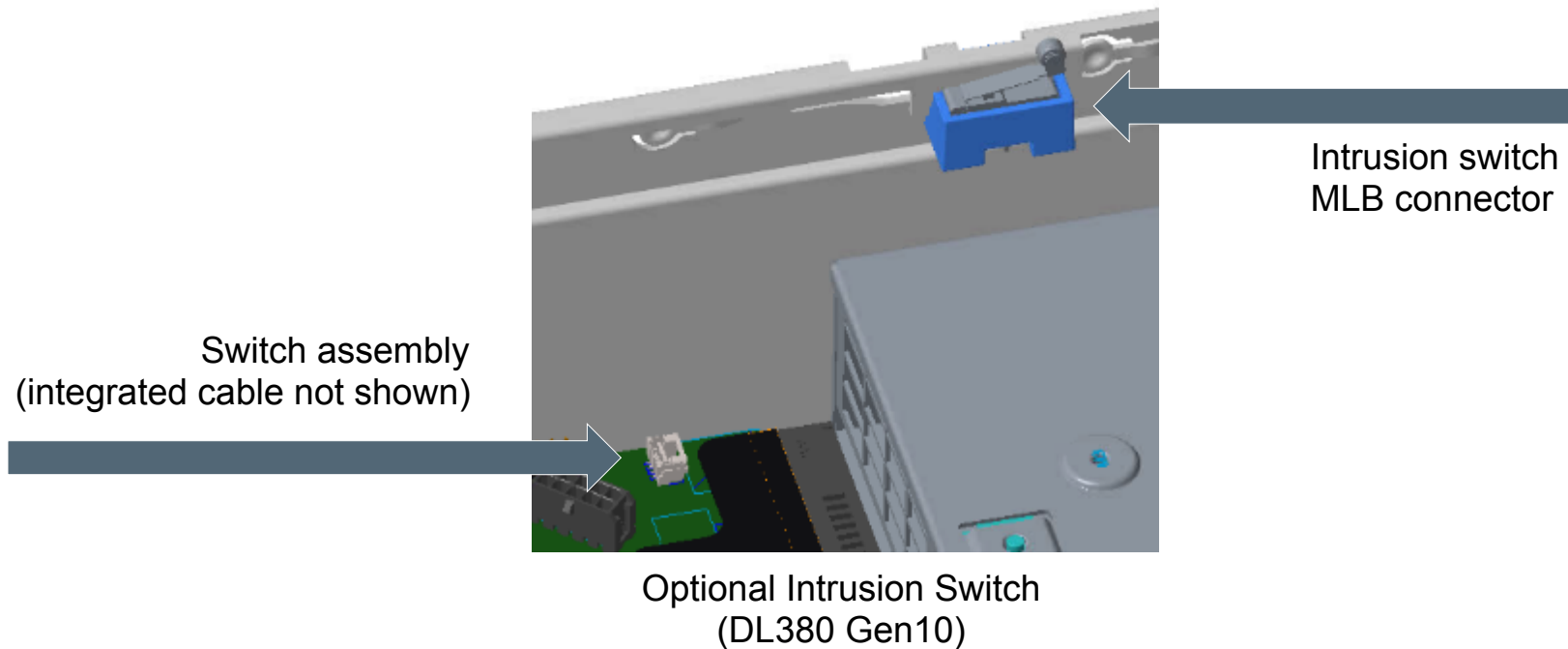
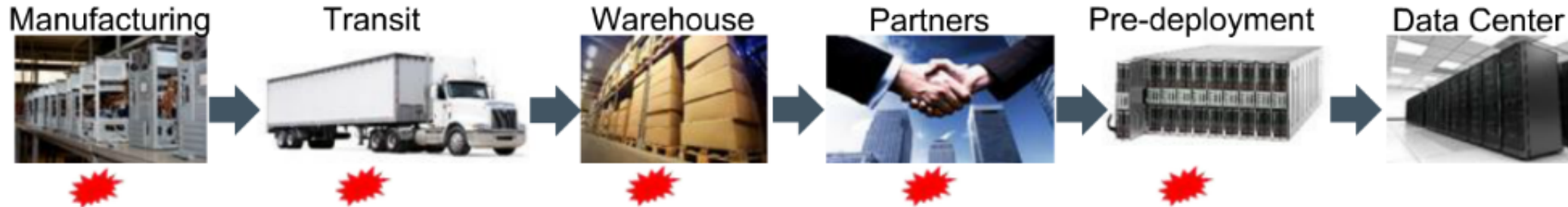
Decryption with public key to match private key and ensures that only valid, signed firmware is installed



The HPE digitally signed firmware image is loaded onto HPE branded NICs

\*Check Adapter QuickSpecs for details.

# Firmware Supply Chain Security





# Security Built into Every Level

## New iLO License Structure

Listprice  
CHF 655.-  
1y Support

### iLO Advanced Premium Security Edition

Listprice  
CHF 430.-  
1y Support

### iLO Advanced

### iLO Standard

Single Sign-On  
Common Criteria, FIPS  
Validation  
Remote Firmware Update  
Agentless Management

Remote Console  
Virtual Media  
SIEM Connectivity (ArcSight)

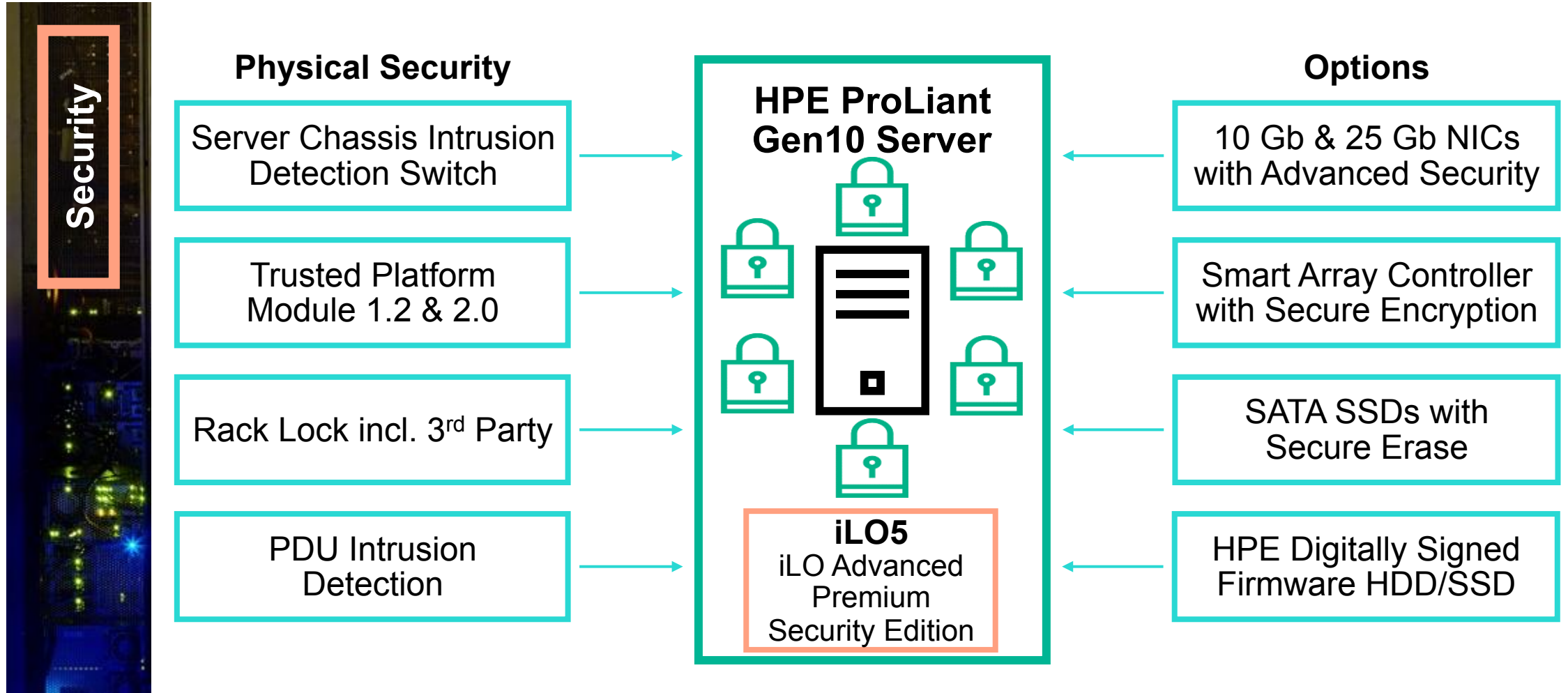
Payment Card Industry  
Standards  
UEFI Secure Boot  
Measured Boot  
Authenticated Updates

CNSA  
Secure Erase of NAND Data  
Runtime FW verification (iLO &  
UEFI)  
Secure Start w/ Recover  
(Automatic)

2-factor Kerberos and CAC  
Directory Services  
Enterprise Security Key  
Manager  
Remote System Logs  
Silicon Root of Trust/Secure  
Start  
Trusted eXecution Technology  
FW Supply Chain Attack  
Detection  
NIST 800-147b BIOS Protection

Key Features

# World's Most Secure Industry Standard Servers



# HPE Rack & Power Infrastructure

Advanced security for your critical physical infrastructure



## HPE G2 Series Racks

- Support for a variety of secure and managed door locking mechanisms including digital and **biometric** locks
- Flush-mount side panels for secure baying of racks
- 3 Factor Authentication
  - *Who you are*
  - *What you have*
  - *What you know*



## HPE G2 Power Distribution Units

- Remote management of power outlets to secure power control of IT devices
- Optional environmental sensors including rack intrusion sensors



## HPE KVM Switches

- Provides Common Access Card (CAC) support which is a key component for datacenters that require two-factor authentication

Providing enhanced infrastructure security

# Secure Sourcing

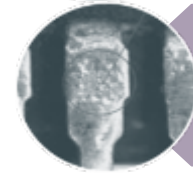
Building security into every aspect of the product



Regulatory & Standards Compliance



Component Provenance and Sourcing Origin & Traceability



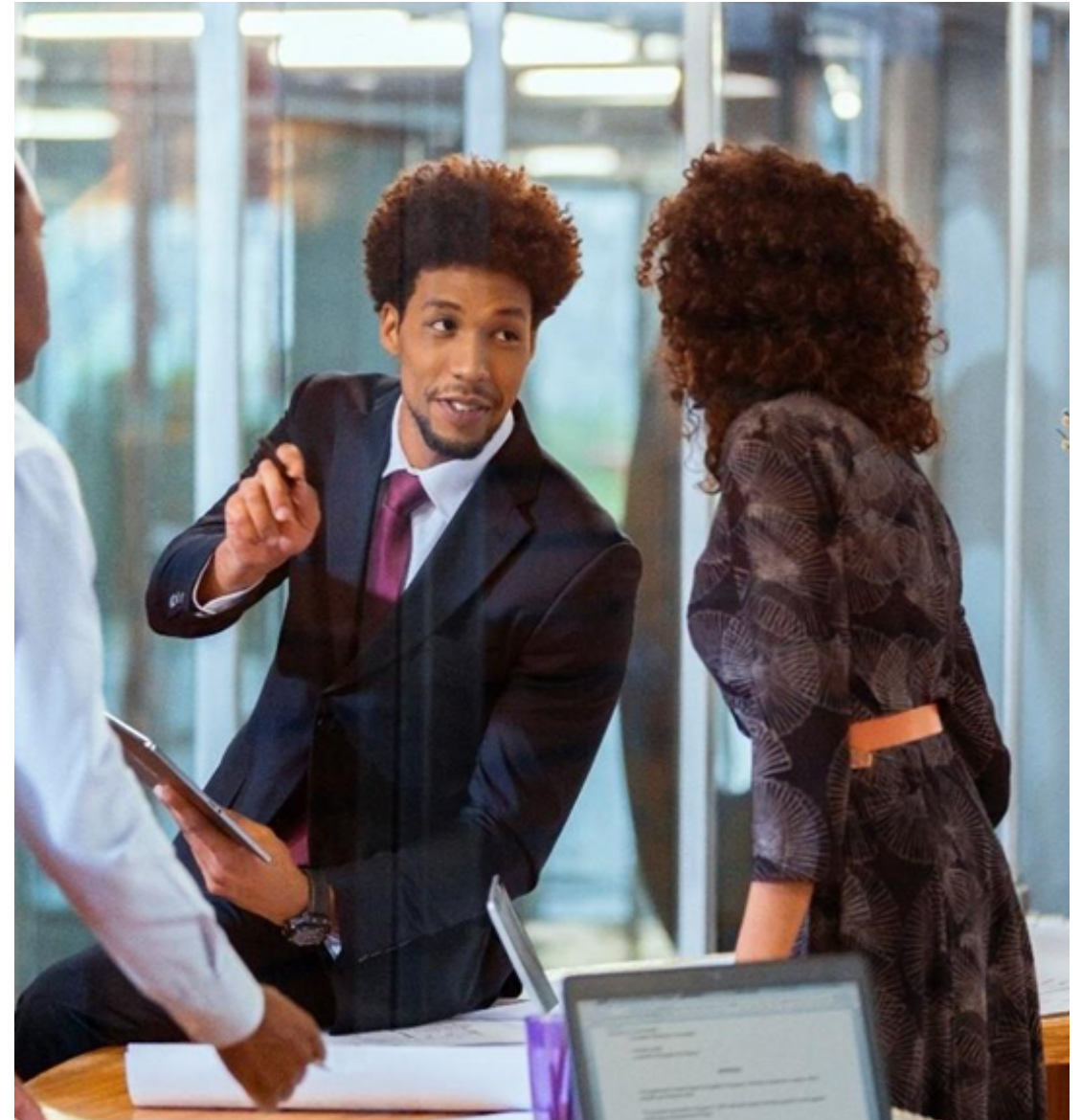
Secure Product Measures, Controls, Features



Customer/Supplier Authentication

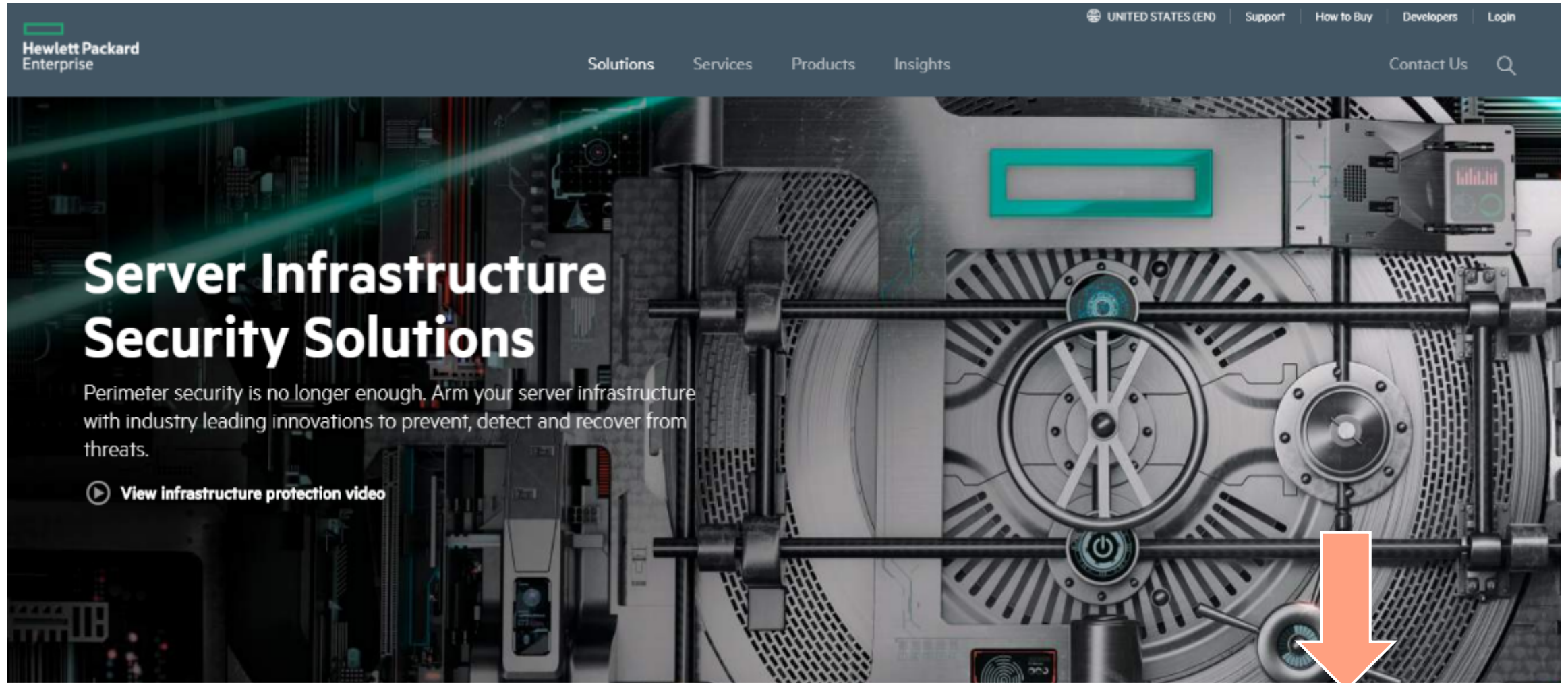


Security Labeling & Packaging & Anti-Counterfeiting






# Server Infrastructure Security Site





# Intelligent Provisioning

**iLO 5**  
1.10 pass 65 May 01 2017

×

Information

System Information

Firmware & OS Software

iLO Federation

Remote Console & Media

Power & Thermal

iLO Dedicated Network Port

iLO Shared Network Port

Remote Support

Administration

Security

**Intelligent Provisioning**

## Intelligent Provisioning

Intelligent Provisioning is now Always On. Access Intelligent Provisioning from the iLO browser user interface anytime without having to reboot your server. Clicking Always On to access Intelligent Provisioning has the same capabilities as accessing Intelligent Provisioning by pressing F10 from the POST screen. You can review in-depth hardware configuration and perform software deployments from almost anywhere.

Click Always On to display Intelligent Provisioning through a secure web-based interface that consolidates the management and deployment of individual servers.

**Intelligent Provisioning version** 3.00.335  
:

**Always On**



# Intelligent Provisioning

World's most advanced server configuration software

EXPRESS OS INSTALL

PERFORM MAINTENANCE

## Perform Maintenance

Maintain your device with powerful tools



Attempt Firmware Update



Intelligent Provisioning Preferences



Deployment Settings



BIOS Configuration (RBSU)



System Erase and Reset



BIOS Configuration (RBSU)

BIOS/Platform Configuration (RBSU)

[VIEW CHANGE](#)

[UPDATE](#)

1

- System Options
- Processor Options
- Memory Options
- Virtualization Options
- Boot Options
- Network Options
- Storage Options
- Power and Performance Options
- Embedded UEFI Shell
- Server Security
- PCIe Device Configuration
- Advanced Options
- Date and Time
- System Default Options
- Language Settings

ROM Information



U30 v1.00 (04/24/2017)

BiosAttributeRegistryU30.v1\_1\_00



Pending settings are NOT valid and may not be applied after reboot

Please click 'Update' to submit new config which is auto-corrected by this tool or 'reset' pending settings



1 items has been changed automatically according to dependency rules

items has been changed automatically according to dependency rules



Reset BIOS

Click to reset BIOS back to default

Workload Profile

General Power Efficient Compute





# RED HAT FORUM

Europe, Middle East & Africa

# Thank you