Hewlett Packard Enterprise

ProLiant Update

Hybrid IT Category Manager
서 유 덕 부장

3 Jul 2018

HPE ProLiant Gen10 서버를 소개합니다

Security

Next Generation Compute Innovation

증가하고 있는 사이버 공격

99 일

탐지되기 전까지 공격자가 시스템 내부에 머무르는 평균 시간[1]

1. Mandiant M-Trends 2017

7.7 M$

사이버 범죄에 피해 입은 기관의 평균 손해 비용[2]

2. http://www.ponemon.org/

2010년 대비 확인된 공격에 대한 방어책 준비 시간 증가율[3]

2.5x

3. Ponemon Cost of Cybercrime report

1.9

공격 대상 기관에 대해 **1**주일 당 성공하는 공격의 횟수[4]

4. Ponemon Cost of Cybercrime report

공격 전선의 확장

Shift to hybrid
Mobile connectivity
Big data explosion

규제의 복잡성 증가로 비용 상승

Data sovereignty
Data privacy
Industry regulations

정교해지는 공격 기법

Growing threats
More frequent
More damaging

Hewlett Packard Enterprise

펌웨어가 새로운 공격 대상으로 부상

공격 기술의 발전으로 펌웨어 공격이 현실적으로 가능해 짐

펌웨어가 취약한 이유

- 보안 및 IT 관리 부서의 관심도가 약함
- 방화벽, 침입탐지, DDoS 등에 보안 투자가 집중
- 펌웨어 공격에 대한 방어 솔루션이 많지 않음

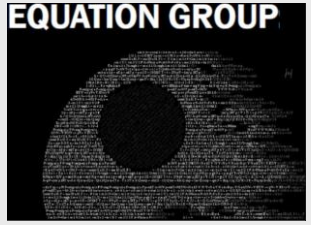
펌웨어를 공격하는 이유

- 지속성 (보안 솔루션으로 삭제 불가하여 Malware를 지속적으로 유입시킬 수 있음)
- 잠행성 (보안 솔루션은 펌웨어 검사를 할 수 없어 침입 후 장기간 활동 가능)
- 막강한 권한 확보
- 성공시 공격 대상 크게 확대 가능

주요 해킹 사례

2013

하드디스크,
라우터, 방화벽
에 백도어
설치하여 해킹



2015

유명
하드디스크
제조업체의
펌웨어에
Spyware 설치

ارامكو السعودية
Saudi Aramco

2012

35,000
하드 디스크
삭제

복구에 **5** 개월
소요

SONY
PICTURES

2014

75% servers
사용 불능

100 TB
데이터 탈취

This problem is not solvable using today's technology

Hewlett Packard
Enterprise

디지털 엔터프라이즈를 보호하기 위한 HPE 접근 방법

HPE Secure Compute Lifecycle

Protect

공격을 효과적으로 방어할 수 있는 시스템 설계

Detect & Respond

알려지지 않은 위협에 대해서도 성능에 영향 없이 시스템 내부에서 탐지하고 대응

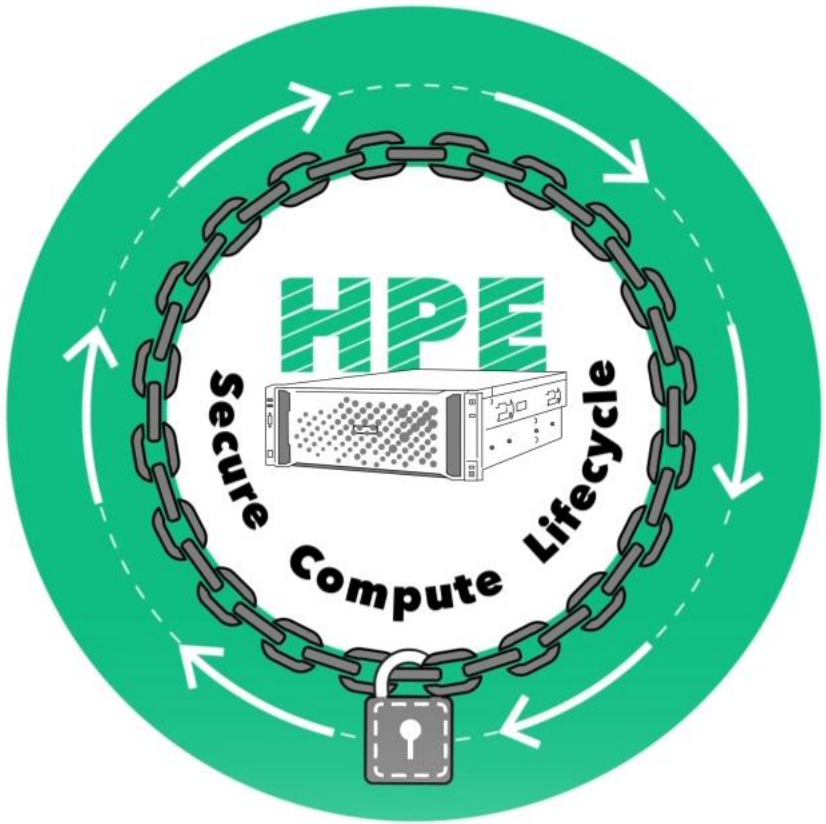
Recover

Last Known Good State로 시스템 복구

시스템 스택의 모든 구성 요소에 보안 기능을 탑재

분석 기반의 지능형 **SoC**

Hewlett Packard Enterprise



HPE Secure Compute Lifecycle은 요람에서 무덤까지
서버 전체 수명주기에 걸쳐 완벽한 보안을 제공합니다.

HPE iLO 5 – Secure server management

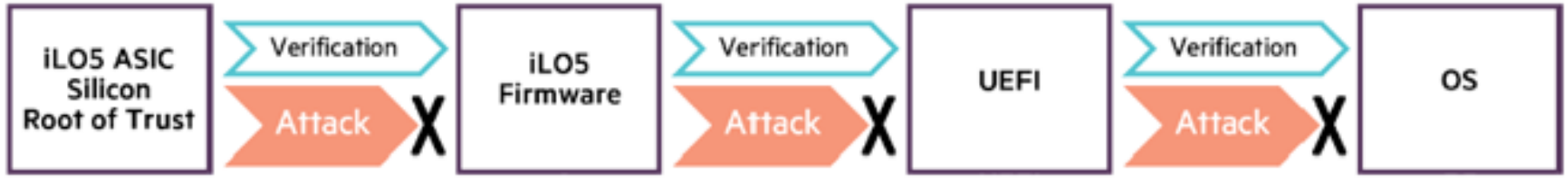
- **Silicon Root of Trust**
- 변경 불가능한 **Firmware** 인증키를 탑재
- **iLO**와 **BIOS**에 대한 **Run Time Validation**
- **Firmware** 복구 기능
- **Secure Erase** 기능
- **CNSA (Commercial National Security Algorithms)** 적용
- **Gen9 iLO4** 대비 **2배** 빠른 성능
- **Common Access Card (CAC) 2-factor** 인증

HPE ProLiant Gen10 - Silicon Root of Trust

Firmware
Root of Trust

공격 받은 Firmware 에
대해서 UEFI/OS가
탐지할 수 없음

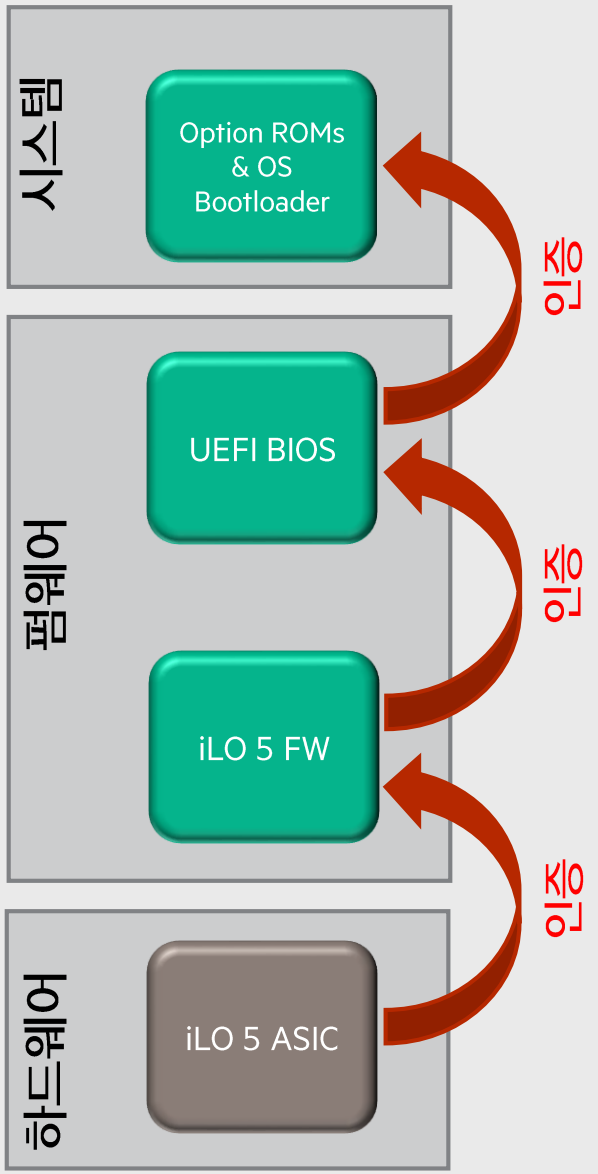
Silicon Root of Trust
Silicon칩 iLO5가
Firmware 검증



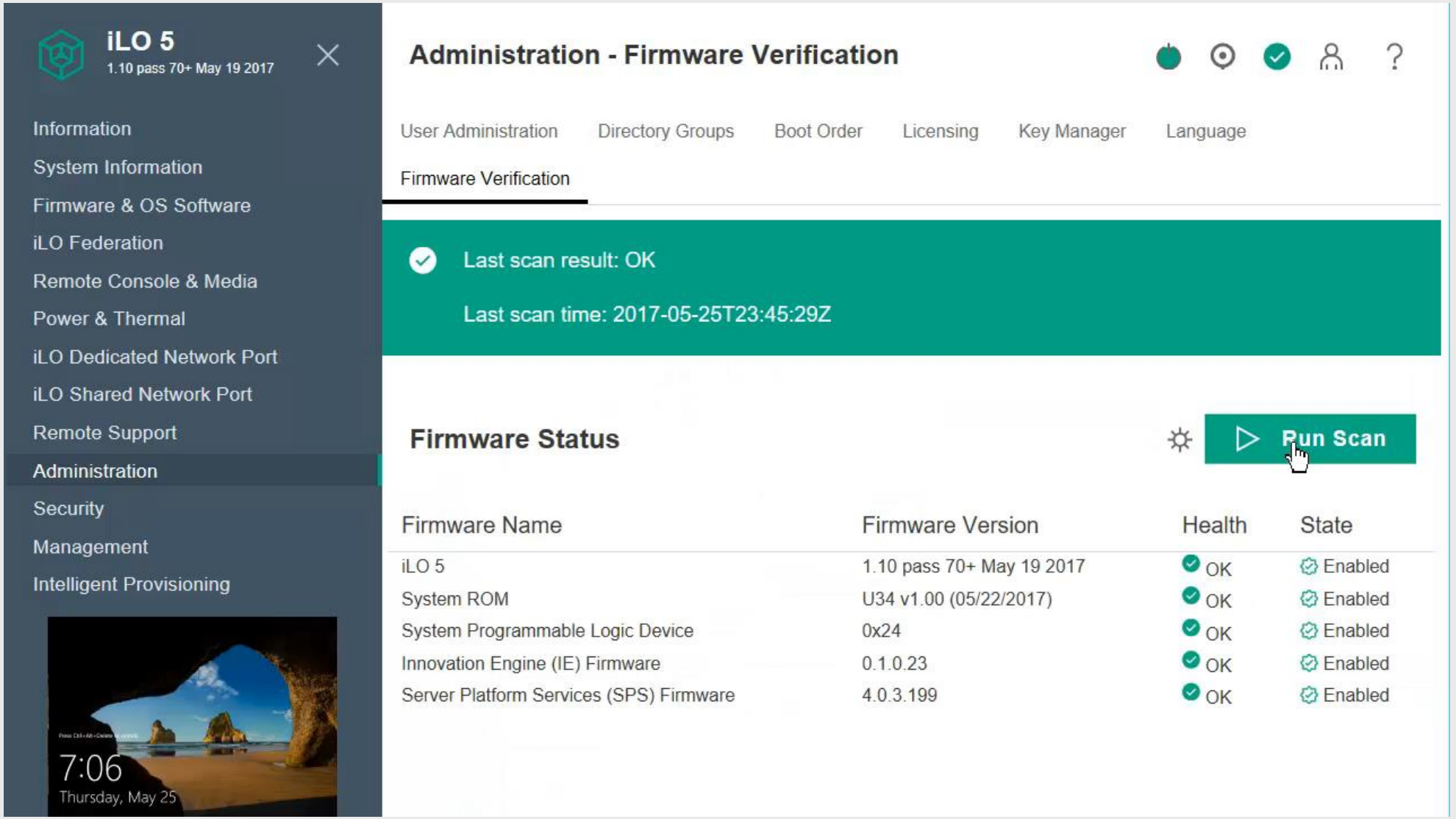
Hewlett Packard
Enterprise

HPE Secure Start

- **Silicon Root of Trust**
  - iLO Chip이 iLO 펌웨어 검증
  - iLO에 로직으로 Burn In
  - 불변 특성
- **iLO 펌웨어가 System ROM 인증**
  - 디지털 사인이 맞지 않으면 ROM 실행이 되지 않음
  - iLO 펌웨어 신뢰되었기 때문에 ROM도 신뢰됨 (Chain of Trust)
- **ROM이 Option ROMs, BIOS, OS Bootloader 인증**
  - 인증 실패시 Option ROMs / OS Bootloader 가 실행되지 않음



iLO 5 – Runtime Scan & Secure Recovery



Hewlett Packard Enterprise

Secure Recovery

- 이중화
  - ROM 과 iLO 에 이중화 내장
- 자동적인 복구
  - 공장에서 설치된 복구 옵션이 적용된 디스크
  - iLO가 iLO를 자동적으로 복구
  - iLO가 자동적으로 ROM을 복구
  - CPLD, IE, ME등을 순차적으로 복구

가장 안전한 산업 표준 서버 = HPE ProLiant

Protect

- **Silicon Root of Trust**
- **Two Factor Authentication CAC**
- **Secure Encryption**
- **Prevent Firmware Attacks from OS**
- **Secure Erase of NAND Data**
- Common Criteria & FIPS 140-2 Level1
- UEFI Secure Boot & Made in USA
- TPM 1.2 and 2.0
- NIST 800-147b BIOS

Detect

- **Detecting Compromised Firmware**
- **Firmware Runtime Validation**
- **Chassis Intrusion Detection**
- **HPE Rack Cabinet Door Detector**
- Verified Boot
- Trusted eXecution Technology
- SIEM Tool Support
- Audit Logs
- Measured Boot

Recover

- **Secure Auto Recovery**
- **Recover Operating Systems (Automatically reinstalled)**
- **Data Collection for Forensics Evaluation**
- HPE Pointnext custom recovery services

Hewlett Packard
Enterprise

Hewlett Packard Enterprise

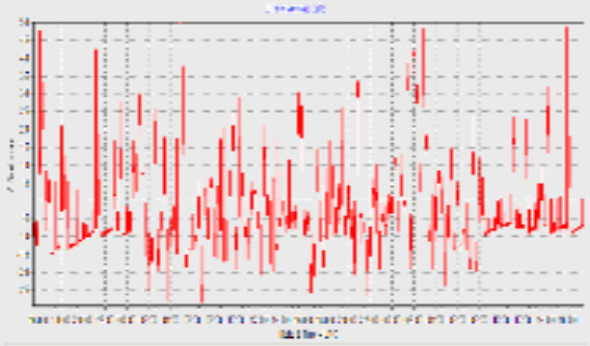
Agility

Next Generation Compute Innovation

Intelligent System Tuning

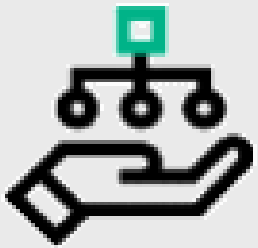
Intelligent System Tuning

Jitter Smoothing



프로세서 주파수 변동을
완화하여 터보 모드보다 전반적인
워크로드 처리량을 향상

Core Boosting



더 적은 프로세서 코어에서 더 높은
성능을 제공하여 연간 코어 기반
라이센스 비용을 획기적으로 절감

Workload Matching

내부 서버 리소스를 자동으로
조정하고 서버 기본 설정보다
최대 9 % 향상된 성능을 제공하는
사전 구성된 프로필을 활용할 수 있음

Hewlett Packard
Enterprise

Intelligent Systems Tuning – Workload Matching

Intel Turbo Boost Technology
Energy Performance Bias
Adjacent Sector Prefetch
Sub-NUMA Clustering
Intel Hyper Threading
SR-IOV
VT-x
VT-D
DCU IP Prefetcher
Channel Interleaving
DCU Stream Prefetcher
Intel DMI Link Frequency
Collaborative Power Control
Intel NIV DMA Channels (IOAT)

Minimum Processor Idle Power Core C-states
NUMA Group Size Optimization
Uncore Frequency Shifting
Thermal Configuration
Memory Refresh Rate
Power Regulator
A3DC
x2APIC
HW Prefetcher
Energy Efficient Turbo
Memory Bus Frequency
Memory Patrol Scrubbing
UPI Link Power Management
Minimum Processor Idle Power Package C-states

Intelligent Systems Tuning – Workload Matching

기본 설정 대비 최대 9% 성능 향상

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

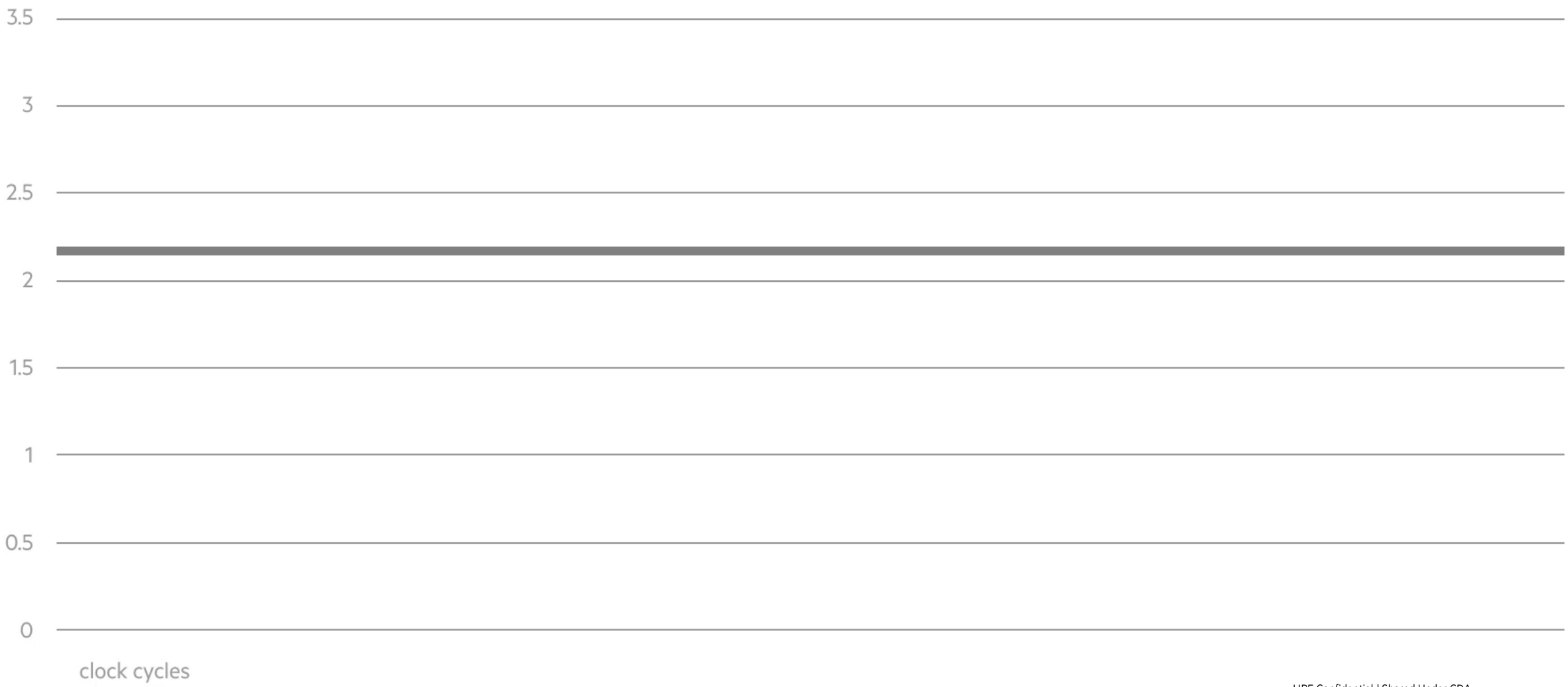
- Transactional Database
- High Performance Compute
- Decision Support
- Graphic Processing
- I/O Throughput
- Web/E-commerce
- Extreme Efficient Compute
- Custom

HPE Performance Engineering 팀의 Know-how를 담았습니다

HPE Confidential | Shared Under CDA

Jitter Smoothing

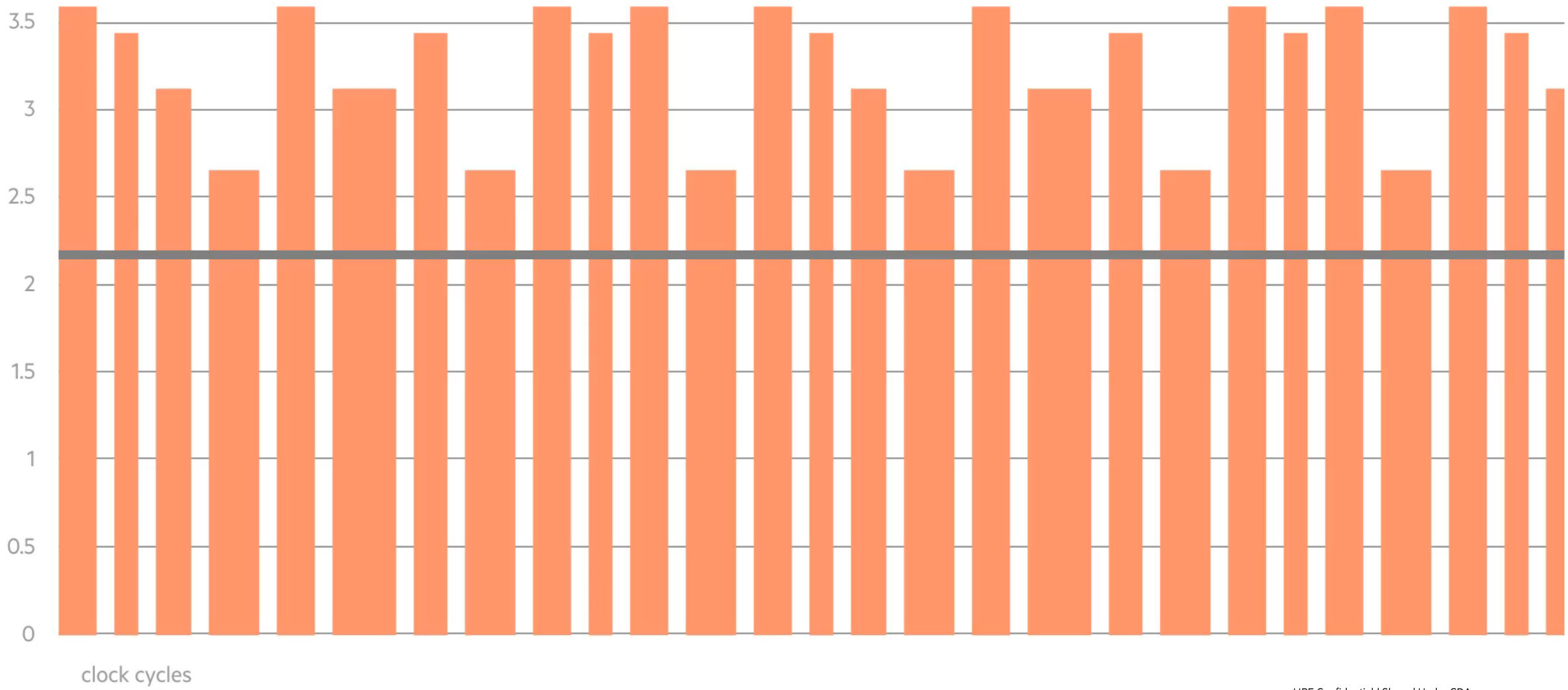
Processor Jitter Control



HPE Confidential | Shared Under CDA

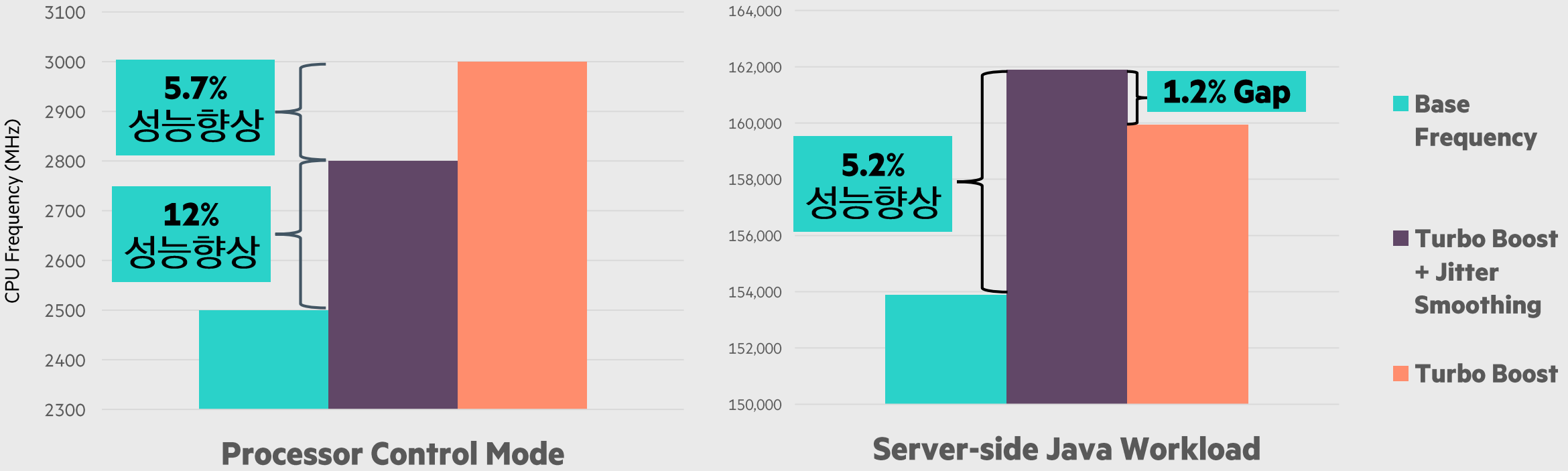
Jitter Smoothing

Processor Jitter Control



HPE Confidential | Shared Under CDA

Intelligent Systems Tuning –Jitter Smoothing

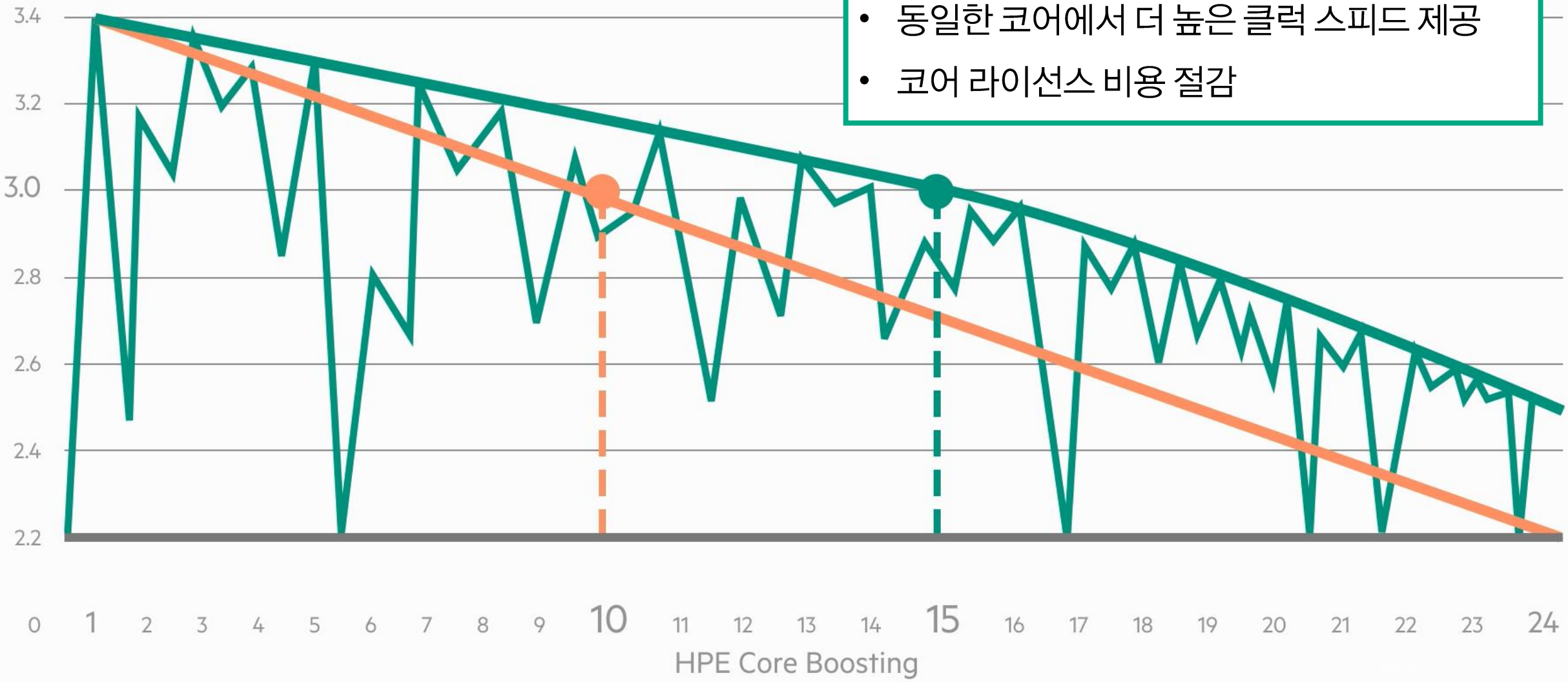


Intelligent Systems Tuning – Core Boosting

HPE Core Boosting

Opportunistic frequencies

- CPU 기본스펙 보다 더 많은 코어 활성화
- 동일한 코어에서 더 높은 클럭 스피드 제공
- 코어 라이선스 비용 절감



Next Generation Compute Innovation – Agility

We're delivering a new experience in time-to-value

Intelligent System Tuning

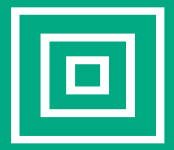
-**Jitter Smoothing**으로 Turbo Boost 대비 향상된 Latency와 성능 제공

-**Core Boosting**으로 더 많은 Active Core 제공

Scalable Persistent Memory

-**TB**급 고용량 **Persistent Memory** 스토리지 제공

-경쟁사 대비 **5**배 큰 용량 제공



Storage Density

-**58%** 향상된 내장 스토리지 제공 (최대 198TB)

-**50%** 향상된 **GPU** 확장성 **(**최대 **1,920 Tensor core)**

-Smart Array 65% 성능 향상

Server Management

-iLO 성능 향상으로 부팅 시간 67% 감소

-iLO 전용 USB 포트

-수 만대의 서버를 관리할 수 있는 **iLO Amplifier Pack**

-**OneView** 플랫폼 확장

Hewlett Packard Enterprise

Thank you

Hewlett Packard
Enterprise