Hewlett Packard
Enterprise

Встроенные технологии защиты от киберугроз в оборудовании HPE

Александр Светлаков

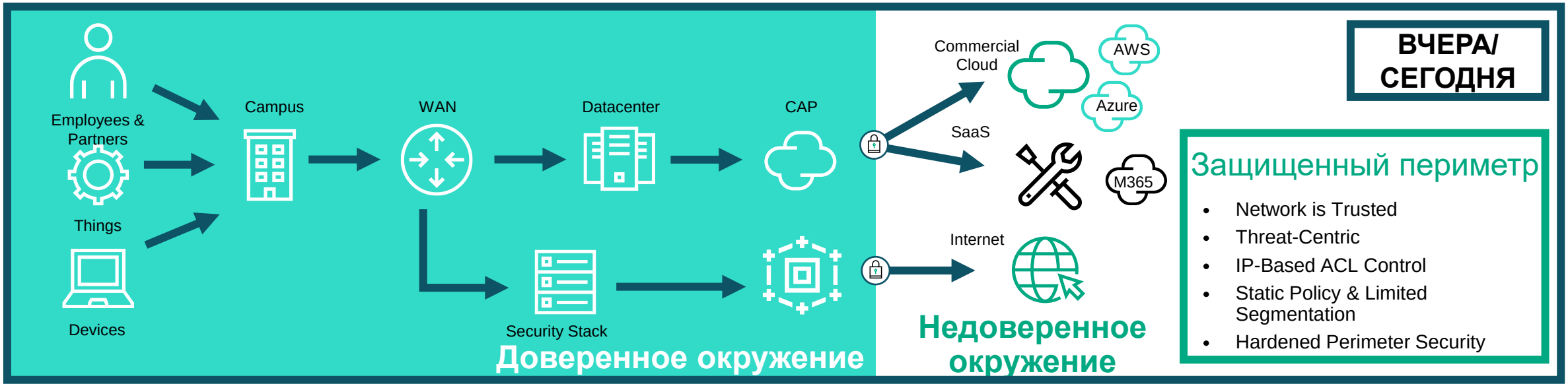
26 Ноября 2021 г.

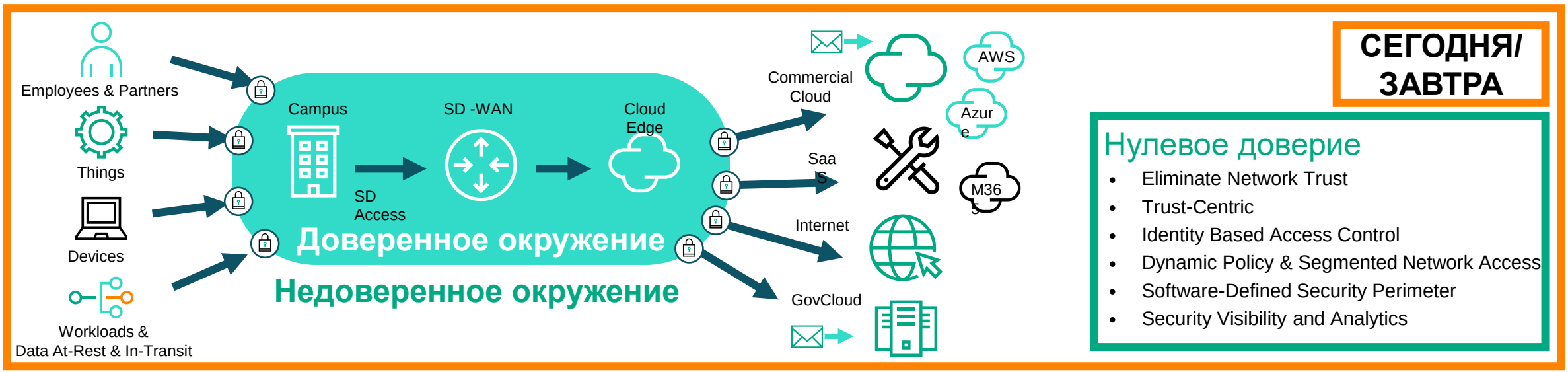
План

- Модель "нулевого доверия" от периферии до ЦОД и облака
- Комплексный подход к безопасности
- Защита на уровне кремния - Silicon Root of Trust
- Интеграция с технологиями защиты Intel и AMD

Обеспечение информационной безопасности в модели “нулевого доверия”

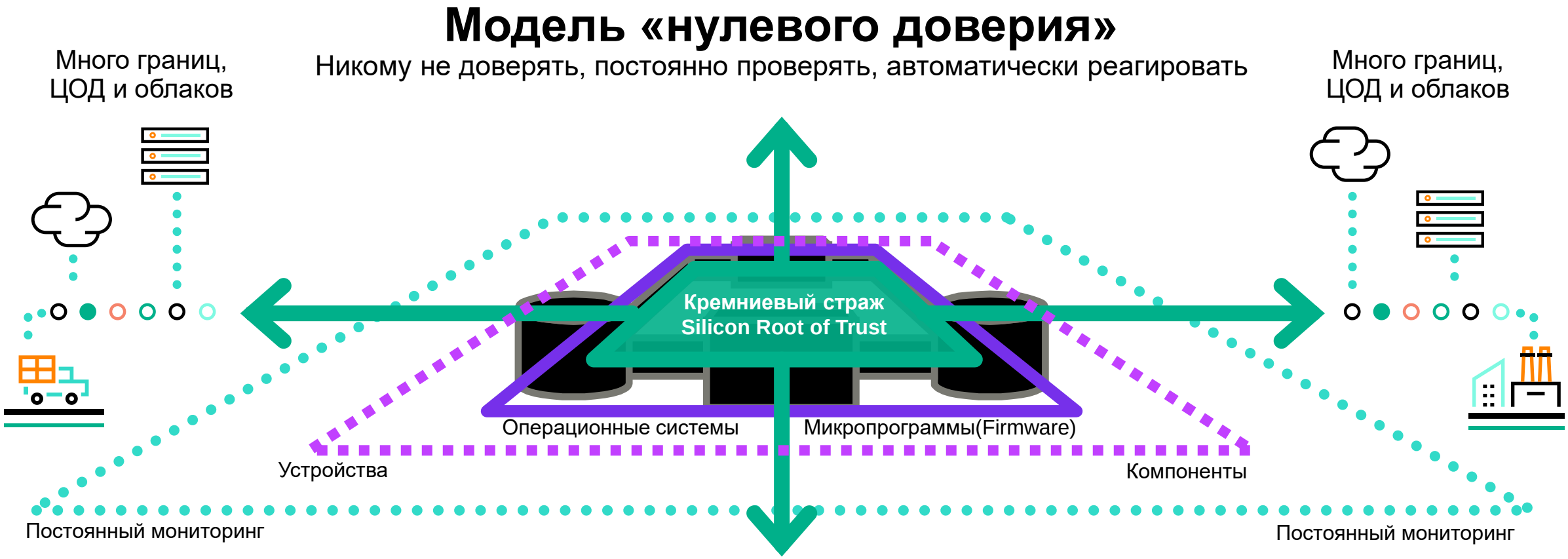
Модель “нулевого доверия” – это новый подход/архитектура обеспечения ИБ





https://www.hpe.com/us/en/insights/articles/zero-trust-makes-business-secure-by-default-2010.html

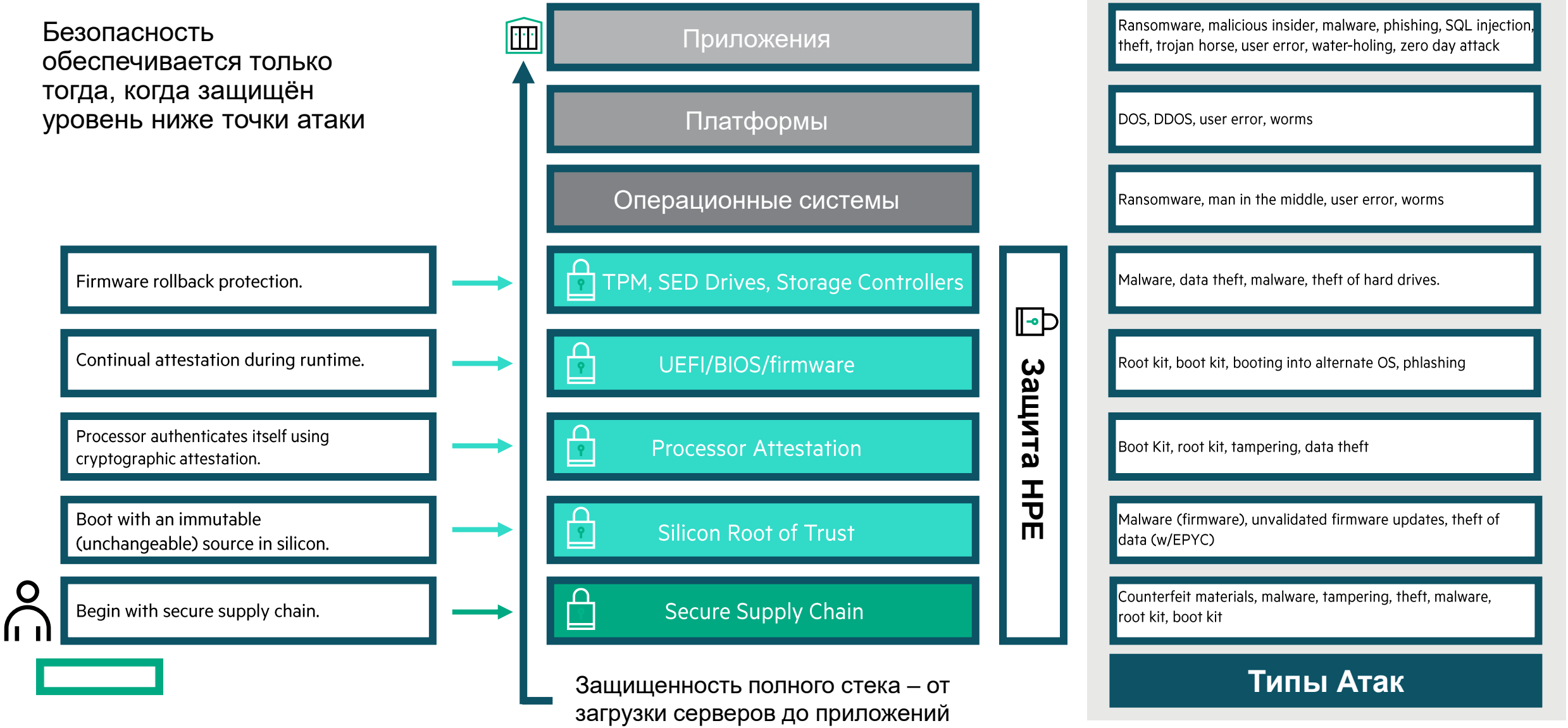
Модель «нулевого доверия» с серверами HPE



Защита изнутри от граничных устройств до ЦОД и облаков
с технологиями HPE на основе Искусственного Интеллекта

Безопасность инфраструктуры критична для модели нулевого доверия

Безопасность обеспечивается только тогда, когда защищён уровень ниже точки атаки



Защищенность полного стека – от загрузки серверов до приложений

Функции безопасности в серверах HPE ProLiant Gen10

Самый безопасный сервер в мире*

Защита

- **HPE Silicon Root of Trust**
- Двухфакторная авторизация CAC
- **Блокировка изменения настроек**
- **Панель безопасности**
- Разные уровни безопасности
- Пакет CNSA (ранее NSA Suite B)
- **Защита от атак на микрокод из ОС**
- **Очистка сервера за один клик**
- Интеграция с менеджером ключей
- FIPS 140-2 Level1
- **Безопасная загрузка UEFI**
- TPM 1.2 и 2.0
- Протоколы безопасности и сертификации
- **Самошифрующиеся накопители**

Обнаружение

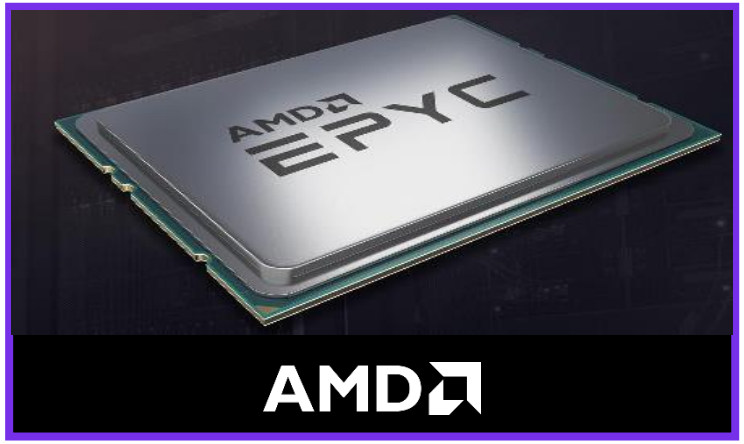
- **Обнаружение скомпрометированных микрокодов**
- **Верификация микрокодов во время работы сервера**
- **Обнаружение вскрытия сервера**
- Сенсор открытия двери шкафа (комплектующая от партнера)
- Проверенная загрузка
- Запуск только проверенных приложений
- Поддержка SIEM
- Ведение аудиторских журналов
- Замеряемая загрузка

Восстановление

- **Автовосстановление после вторжения**
- **Восстановление микрокодов и ОС**
- Сбор данных для проведения криминалистической экспертизы
- Специализированные услуги по восстановлению от HPE Pointnext

*Based on testing of multiple server platforms by InfusionPoints

HPE ProLiant Gen10 Plus на процессорах AMD



System

Option ROMs &
OS Boot loader

Firmware

UEFI
BIOS

HPE iLO 5
Firmware

Hardware
(Silicon)

HPE iLO 5 Chip

Аутентификация

Аутентификация

Аутентификация

Secure Encrypted Virtualization (SEV)

Secure Memory Encryption (SME)

AMD Secure Processor
HPE Silicon Root of Trust checks processor
& processor checks BIOS

HPE ProLiant Gen10 Plus на процессорах Intel

- Технологии Intel Software Guard Extensions (SGX) и Total Memory Encryption (TME) дополняют функции защиты HPE
- Trusted Platform Module (TPM) 2.0
- Поддержка Self-Encrypting Drive (SED)
- Zero Touch Provisioning – автоматическое развертывание новых систем*
- Аттестованная цепочка поставок*

* Доступность в России ожидается позже

Выводы

- Серверы HPE обеспечивают наивысший уровень безопасности и защищенности
  - Комплексный подход к безопасности
  - Защита на уровне кремния
  - Интеграция с технологиями защиты Intel и AMD

Спасибо!

Svetlakov@hpe.com