Hewlett Packard Enterprise

Встроенные технологии защиты от киберугроз в серверах HPE

Александр Светлаков
Менеджер по серверным решениям, Hewlett Packard Enterprise в России

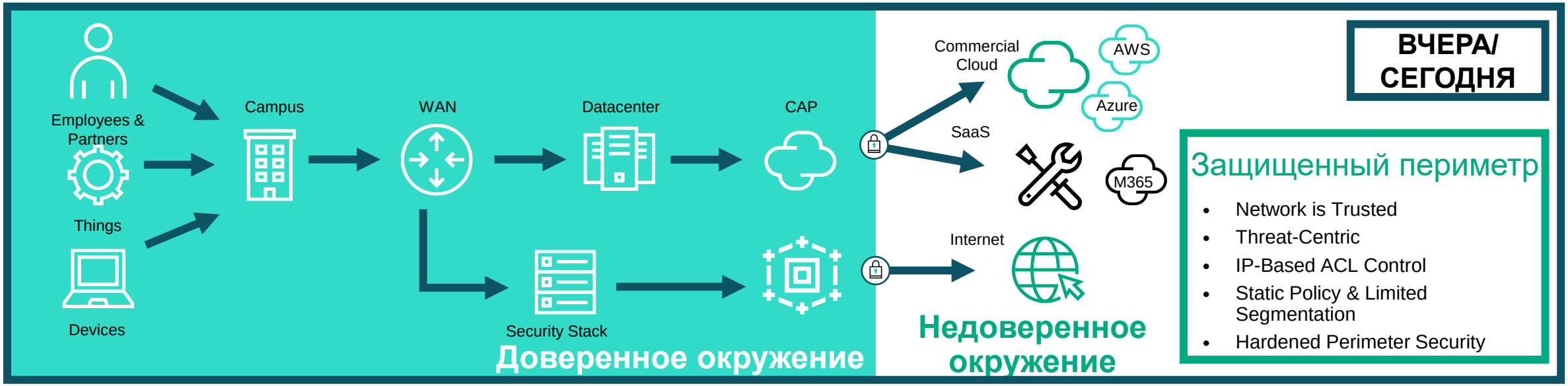
8 Февраля 2022 г.

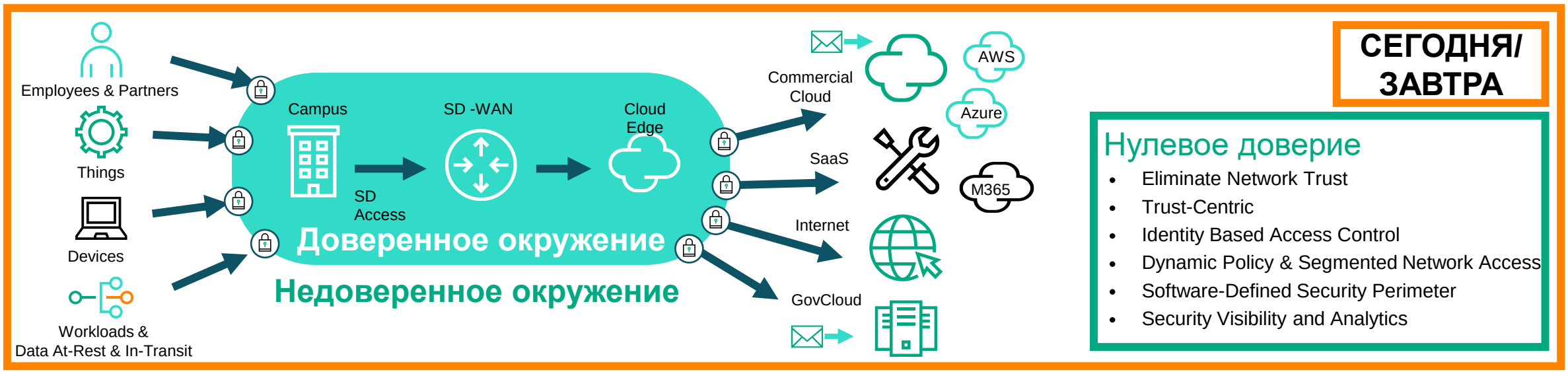
План

- 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 производителей микропроцессоров

Обеспечение информационной безопасности в модели “нулевого доверия”

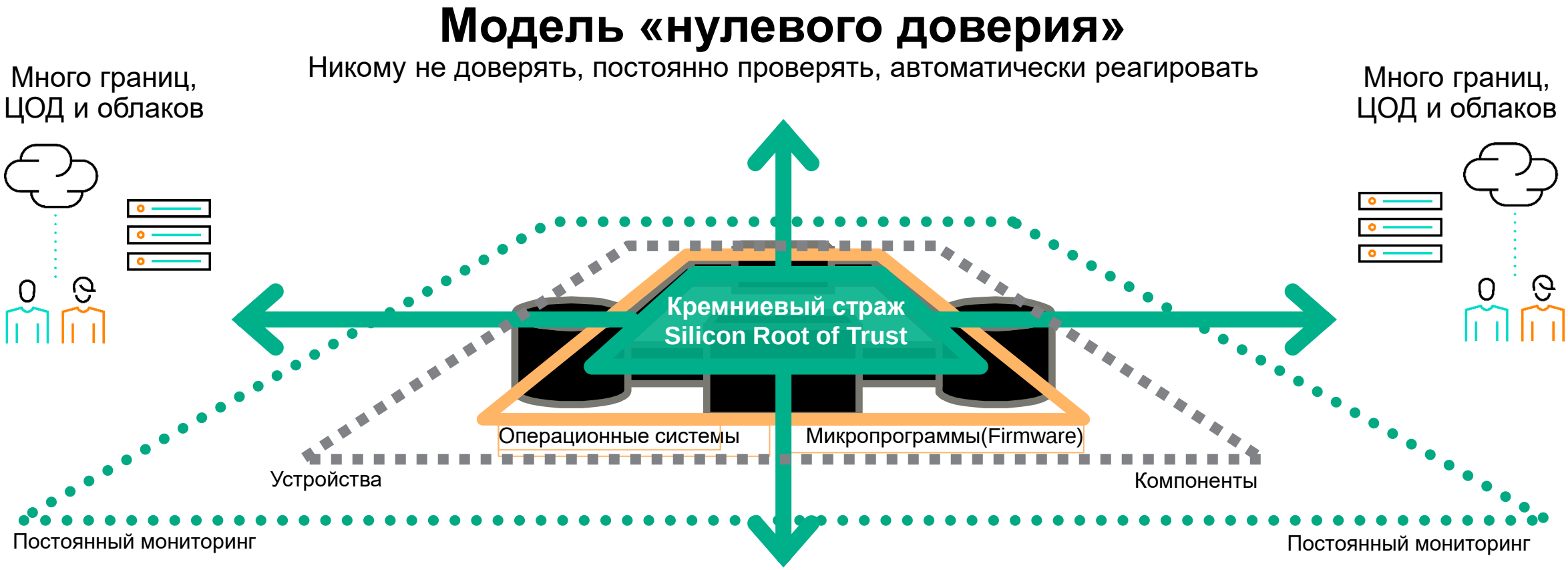
Модель “нулевого доверия” – это новый подход/архитектура обеспечения ИБ





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

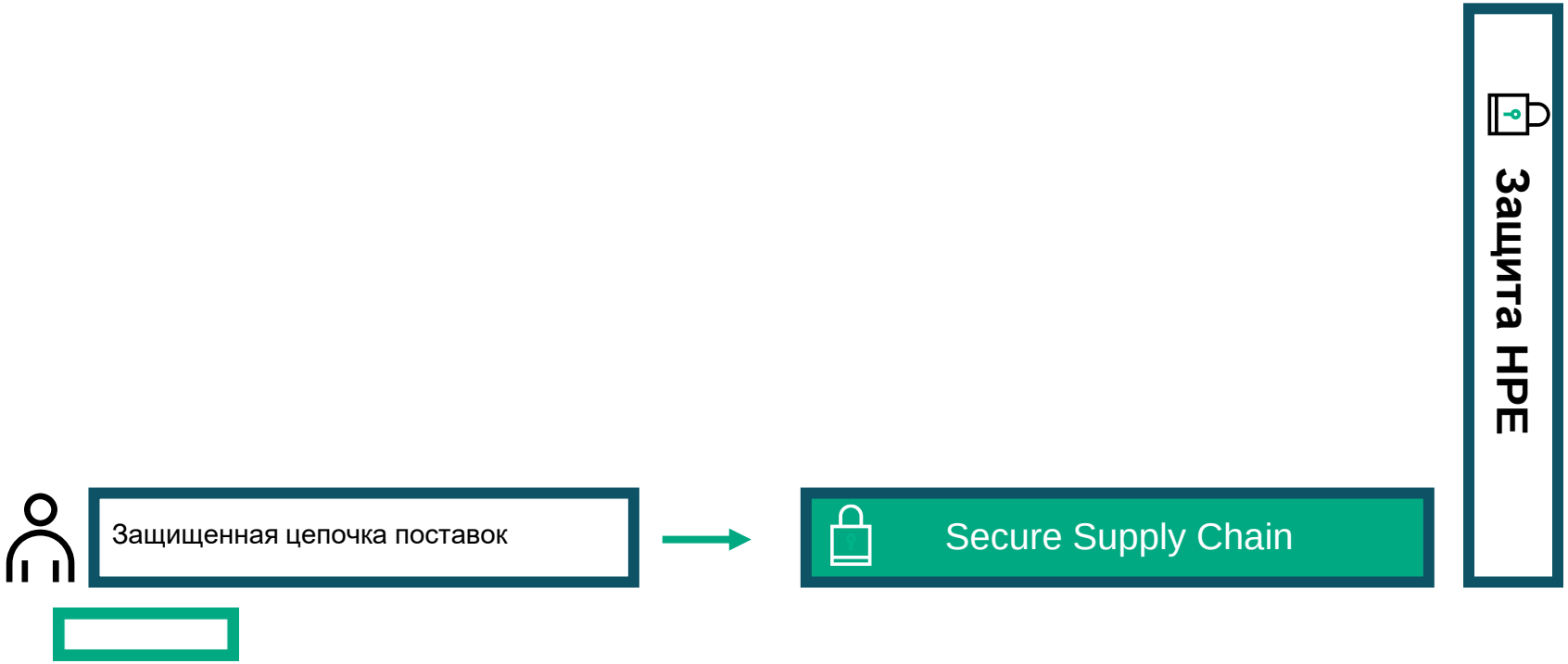
HPE использует модель «нулевого доверия»



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

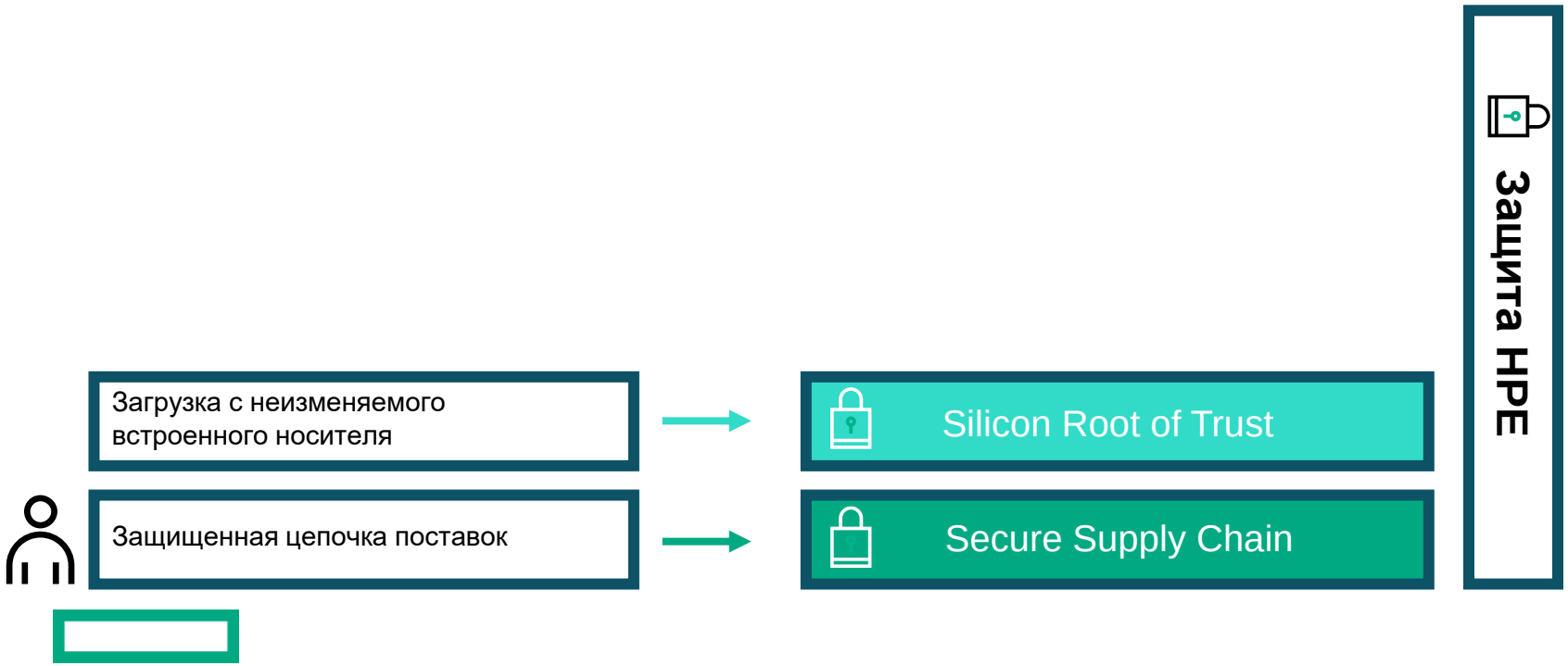
Безопасность инфраструктуры критична для модели нулевого доверия

Безопасность обеспечивается только тогда, когда защищён уровень ниже точки атаки



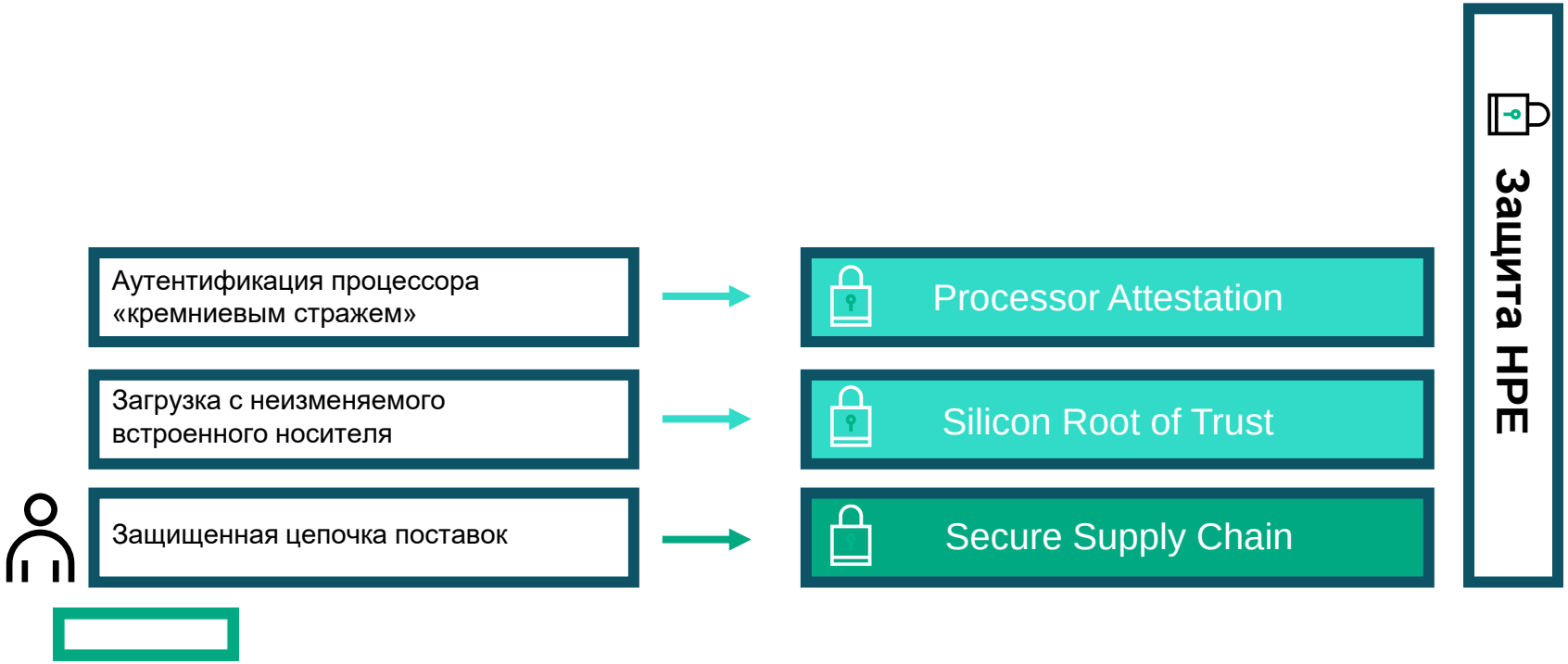
Безопасность инфраструктуры критична для модели нулевого доверия

Безопасность обеспечивается только тогда, когда защищён уровень ниже точки атаки



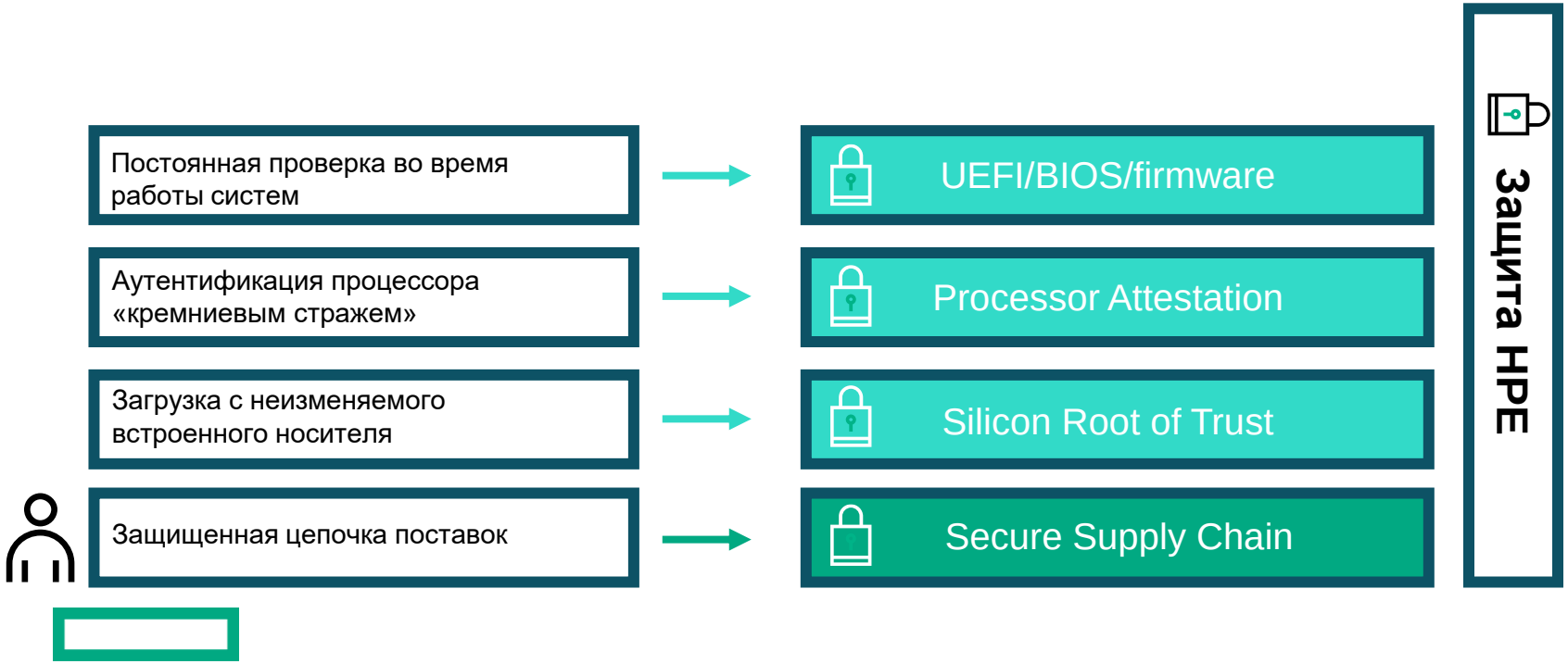
Безопасность инфраструктуры критична для модели нулевого доверия

Безопасность обеспечивается только тогда, когда защищён уровень ниже точки атаки



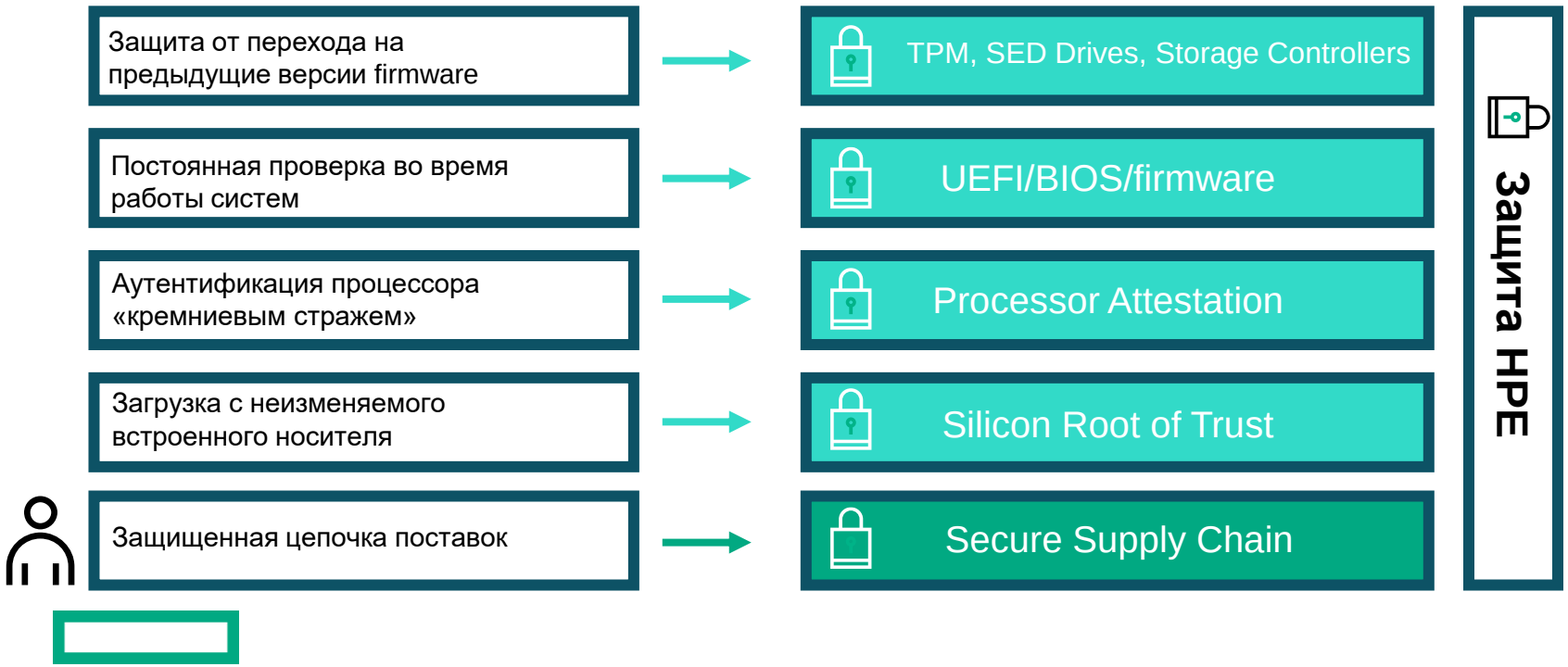
Безопасность инфраструктуры критична для модели нулевого доверия

Безопасность обеспечивается только тогда, когда защищён уровень ниже точки атаки



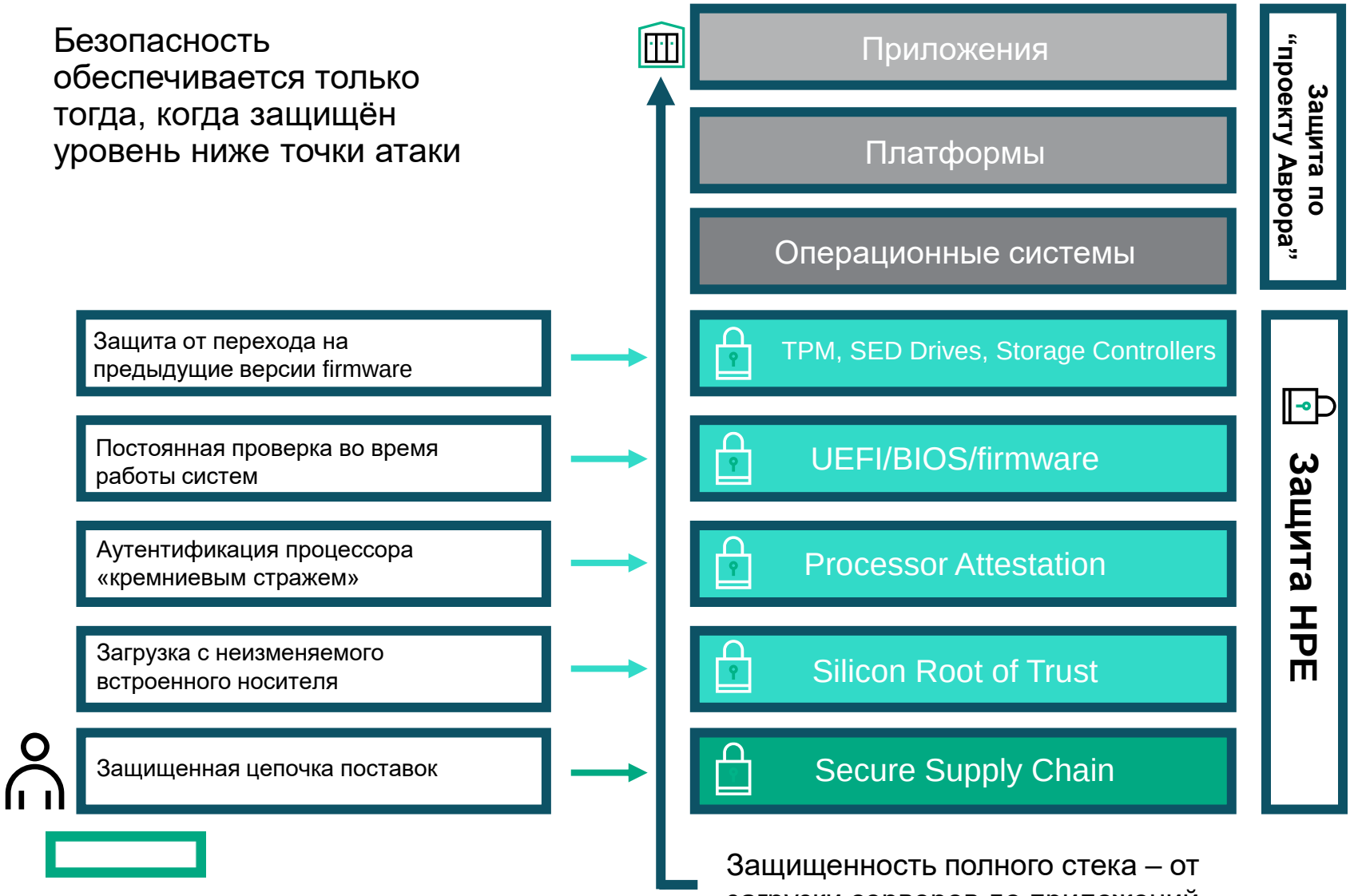
Безопасность инфраструктуры критична для модели нулевого доверия

Безопасность обеспечивается только тогда, когда защищён уровень ниже точки атаки



Безопасность инфраструктуры критична для модели нулевого доверия

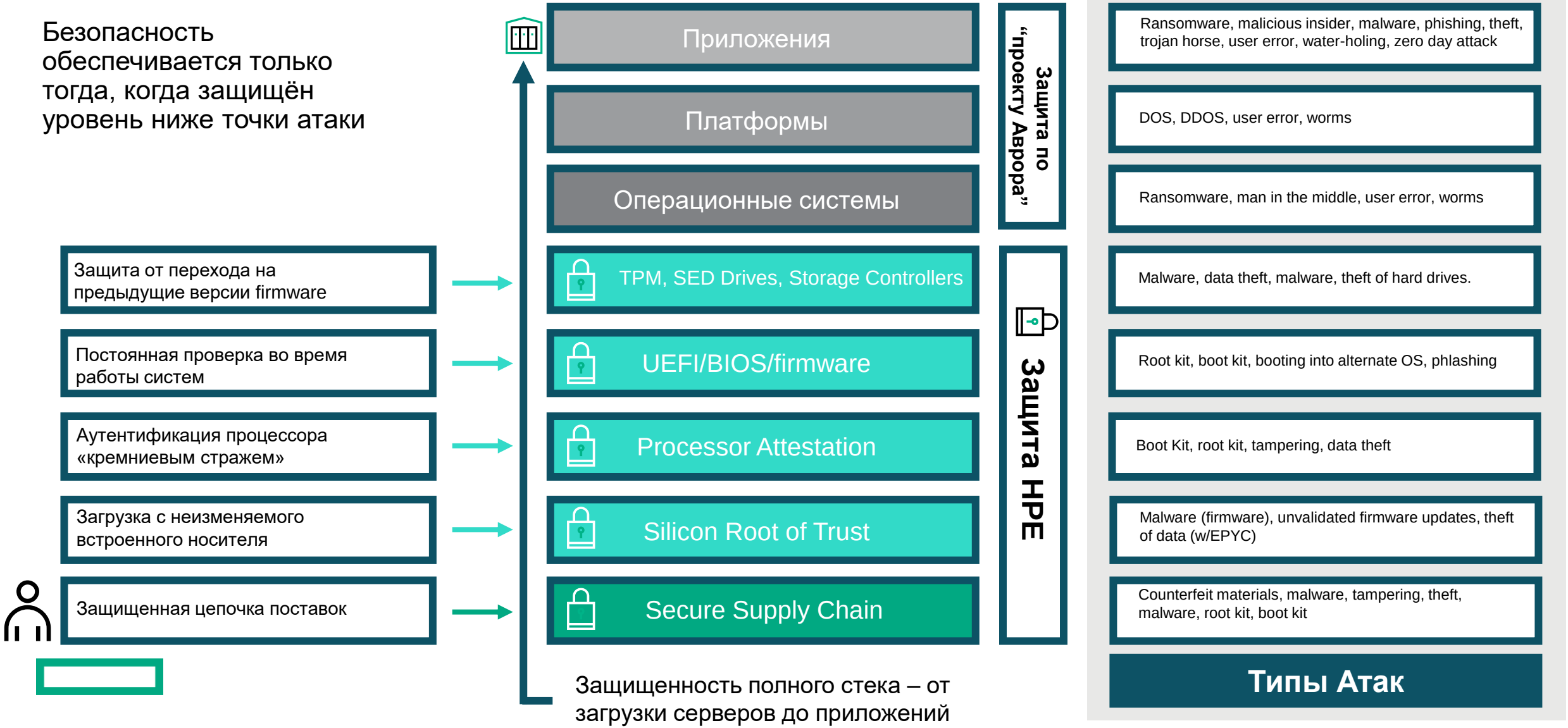
Безопасность обеспечивается только тогда, когда защищён уровень ниже точки атаки



Защищенность полного стека – от загрузки серверов до приложений

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

Инициатива HPE – “проект Аврора” призвана обеспечить защиту распределенных облачных сервисов от периферии до ЦОД/облака

Повышайте ценность данных за счет **аттестаций** и **верификаций**

Ускоряйте инновации, на базе **фундамента реализующего модель “нулевого доверия”**

Выявляйте атаки и защищайте инвестиции

Каждый уровень проверяет и защищает вышестоящий уровень

* Проект Аврора (Aurora) - набор технологий HPE (и партнеров HPE) реализующий защиту распределенных облачных сервисов в модели “нулевого доверия”. Используется/реализован в HPE GreenLake LightHouse с Gen10/Gen10 Plus серверами. Ожидаемая дата доступности – начало 2022 года. Узнай больше о проекте Аврора - https://www.hpe.com/security/projectaurora

Инициатива HPE – “проект Аврора” призвана обеспечить защиту распределенных облачных сервисов от периферии до ЦОД/облака

Повышайте ценность данных за счет **аттестаций** и **верификаций**

Ускоряйте инновации, на базе **фундамента реализующего модель “нулевого доверия”**

Выявляйте атаки и защищайте инвестиции

Каждый уровень проверяет и защищает вышестоящий уровень

* Проект Аврора (Aurora) - набор технологий HPE (и партнеров HPE) реализующий защиту распределенных облачных сервисов в модели “нулевого доверия”. Используется/реализован в HPE GreenLake LightHouse с Gen10/Gen10 Plus серверами. Ожидаемая дата доступности – начало 2022 года. Узнай больше о проекте Аврора - https://www.hpe.com/security/projectaurora

Инициатива HPE – “проект Аврора” призвана обеспечить защиту распределенных облачных сервисов от периферии до ЦОД/облака

Повышайте ценность данных за счет **аттестаций** и **верификаций**

Ускоряйте инновации, на базе **фундамента реализующего модель “нулевого доверия”**

Выявляйте атаки и защищайте инвестиции

Каждый уровень проверяет и защищает вышестоящий уровень

* Проект Аврора (Aurora) - набор технологий HPE (и партнеров HPE) реализующий защиту распределенных облачных сервисов в модели “нулевого доверия”. Используется/реализован в HPE GreenLake LightHouse с Gen10/Gen10 Plus серверами. Ожидаемая дата доступности – начало 2022 года. Узнай больше о проекте Аврора - https://www.hpe.com/security/projectaurora

Инициатива HPE – “проект Аврора” призвана обеспечить защиту распределенных облачных сервисов от периферии до ЦОД/облака

Повышайте ценность данных за счет **аттестаций** и **верификаций**

Ускоряйте инновации, на базе **фундамента реализующего модель “нулевого доверия”**

Выявляйте атаки и защищайте инвестиции

Каждый уровень проверяет и защищает вышестоящий уровень

* Проект Аврора (Aurora) - набор технологий HPE (и партнеров HPE) реализующий защиту распределенных облачных сервисов в модели “нулевого доверия”. Используется/реализован в HPE GreenLake LightHouse с Gen10/Gen10 Plus серверами. Ожидаемая дата доступности – начало 2022 года. Узнай больше о проекте Аврора - https://www.hpe.com/security/projectaurora

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

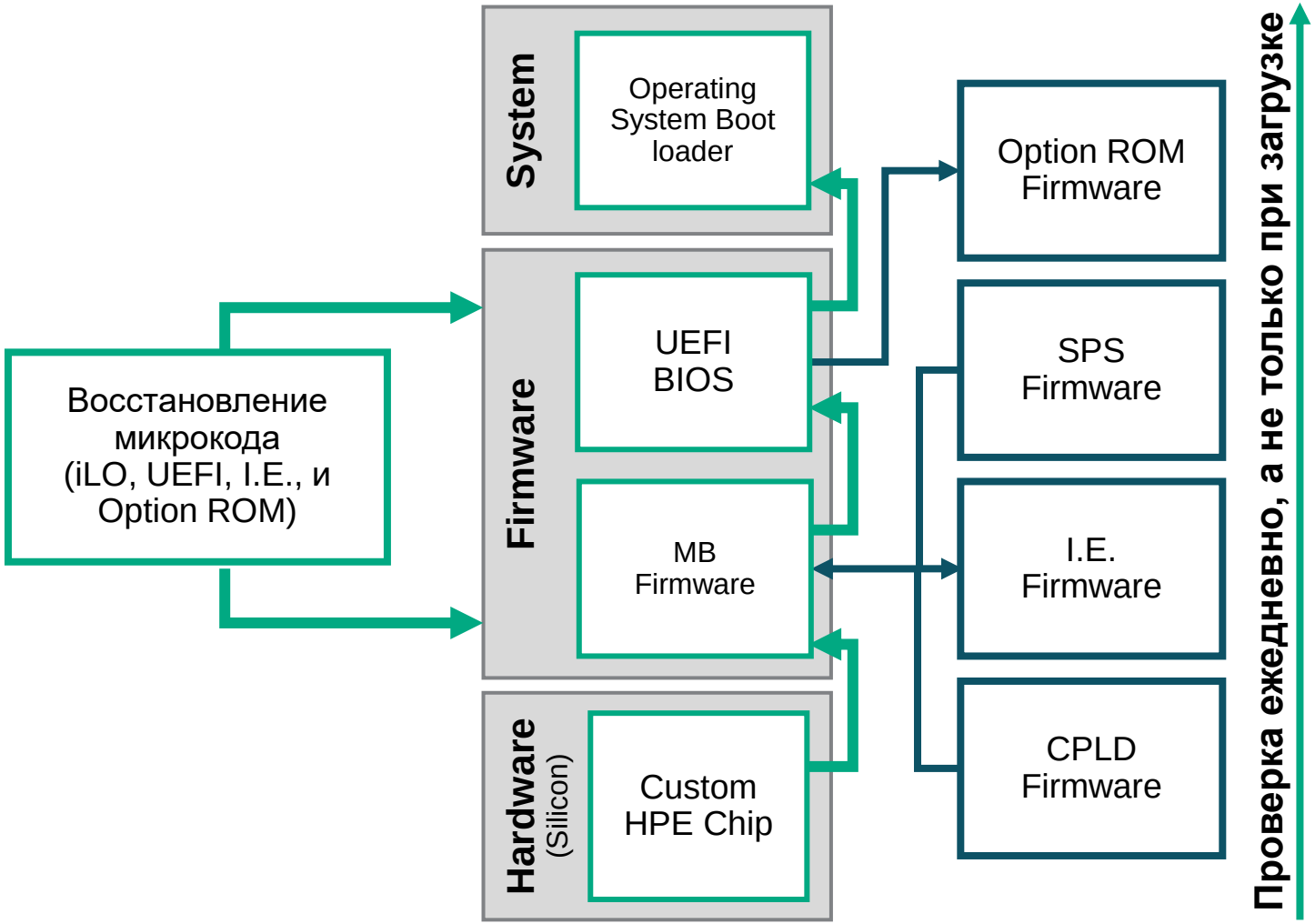
- **Обнаружение скомпрометированных микрокодов**
- **Верификация микрокодов во время работы сервера**
- **Обнаружение вскрытия сервера**
- Сенсор открытия двери шкафа (комплектующая от партнера)
- Проверенная загрузка
- Запуск только проверенных приложений
- Поддержка SIEM
- Ведение аудиторских журналов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

Технология Silicon Root of Trust и Firmware Verification в серверах HPE

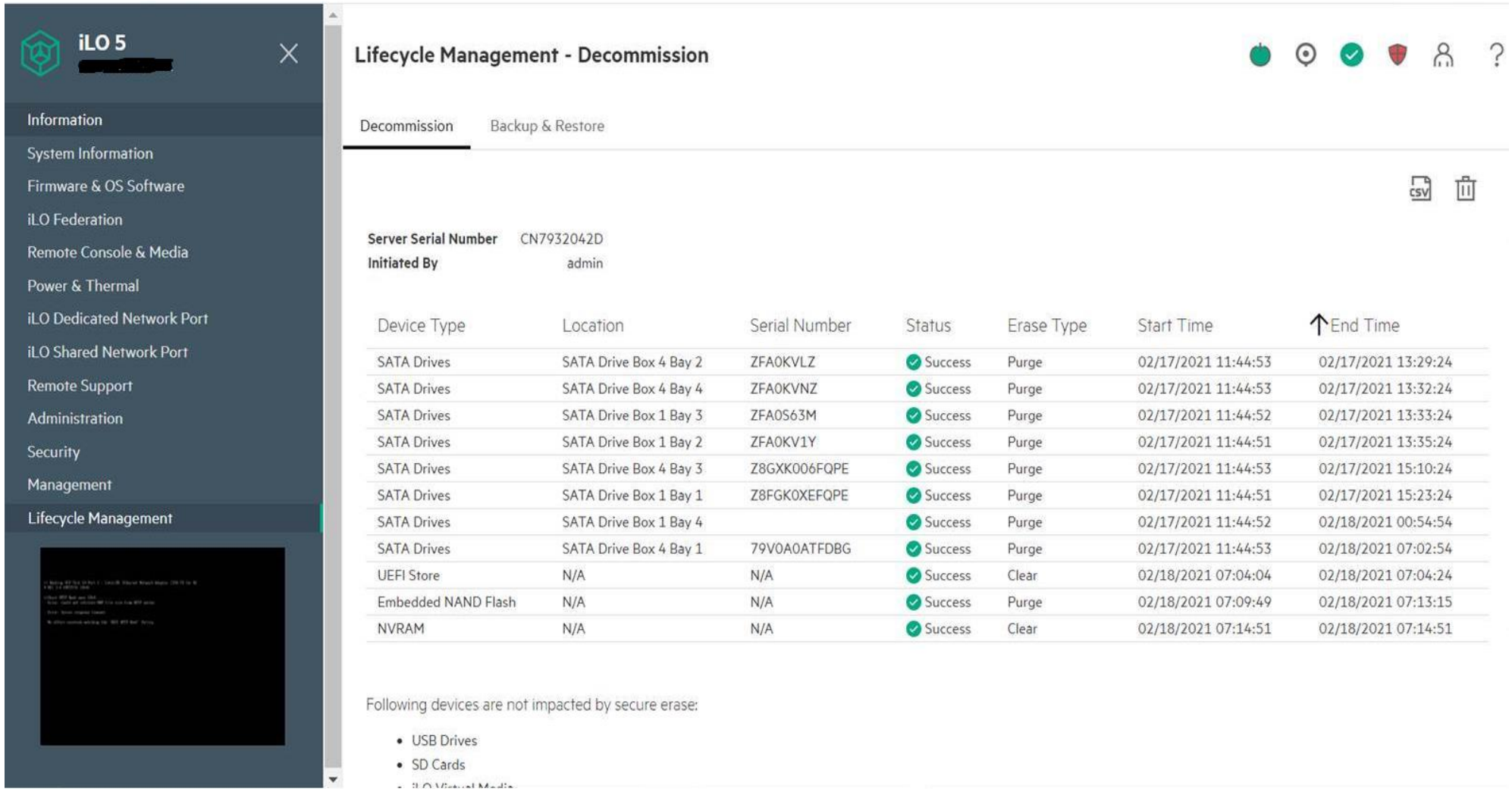


Option ROM	Option ROM проверен на подлинность и достоверность
Secure Boot	Если все микрокоды действительны, сервер разрешит загрузку ОС
SPS Firmware	Проверка микрокода «Server Platform Services»
I.E. Firmware	Проверка микрокода “Innovation Engine (I.E.)”
CPLD Firmware	Затем iLO проверяет микрокод системного программируемого логического устройства (CPLD)
BMC Firmware	Микрокод проверяется при включении сервера
BMC/iLO5 Silicon Chip	Неперезаписываемая область в микросхеме

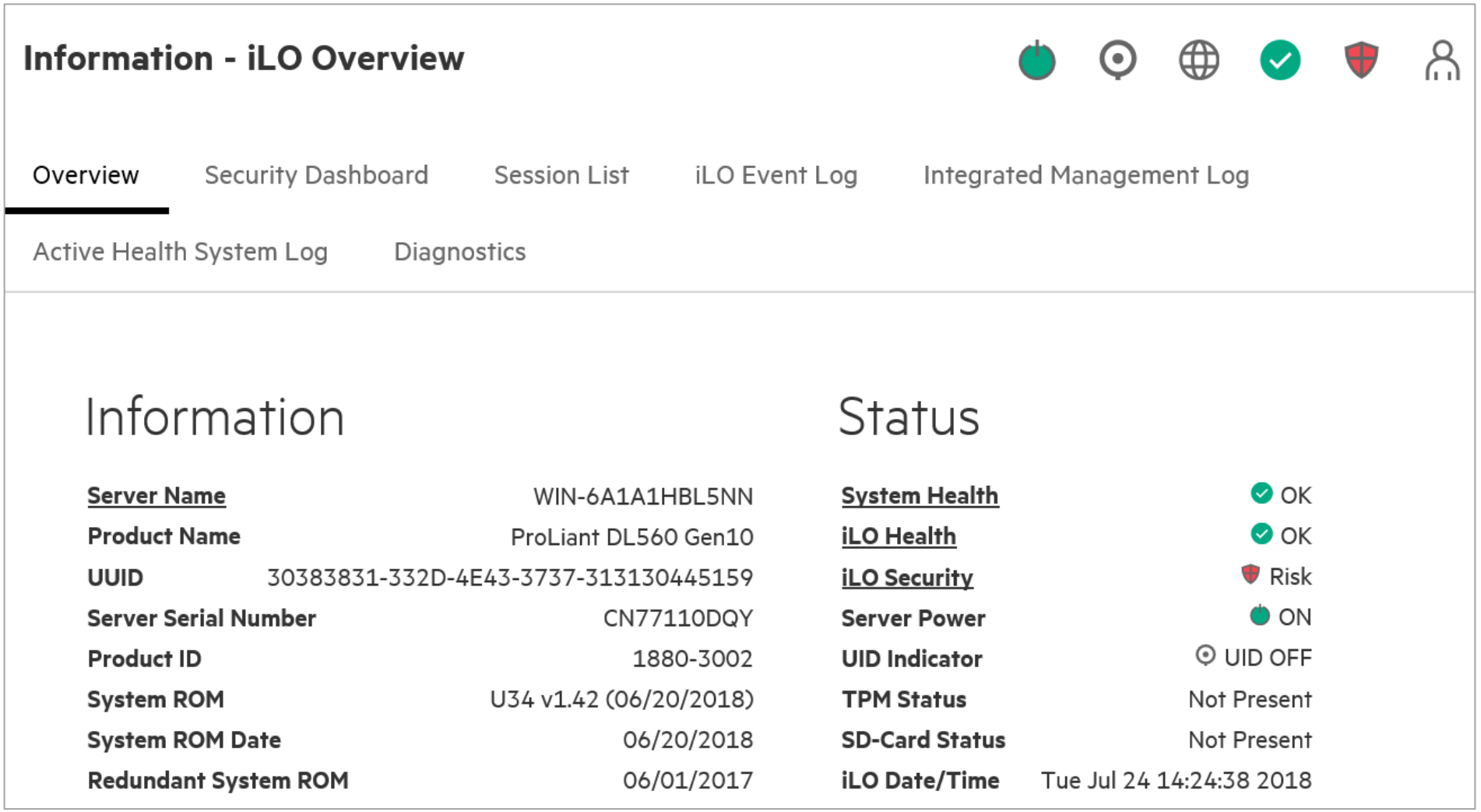
Постоянная проверка микропрограмм (firmware)

- Периодическая проверка целостности firmware.
- Репозиторий с гарантированно целостной версией firmware.
- Обнаружение компрометации firmware.
- Уведомление администратора о компрометации firmware.
- Восстановление сервера до гарантированно целостной версии firmware.

Гарантированное удаление данных – One Button Secure Erase

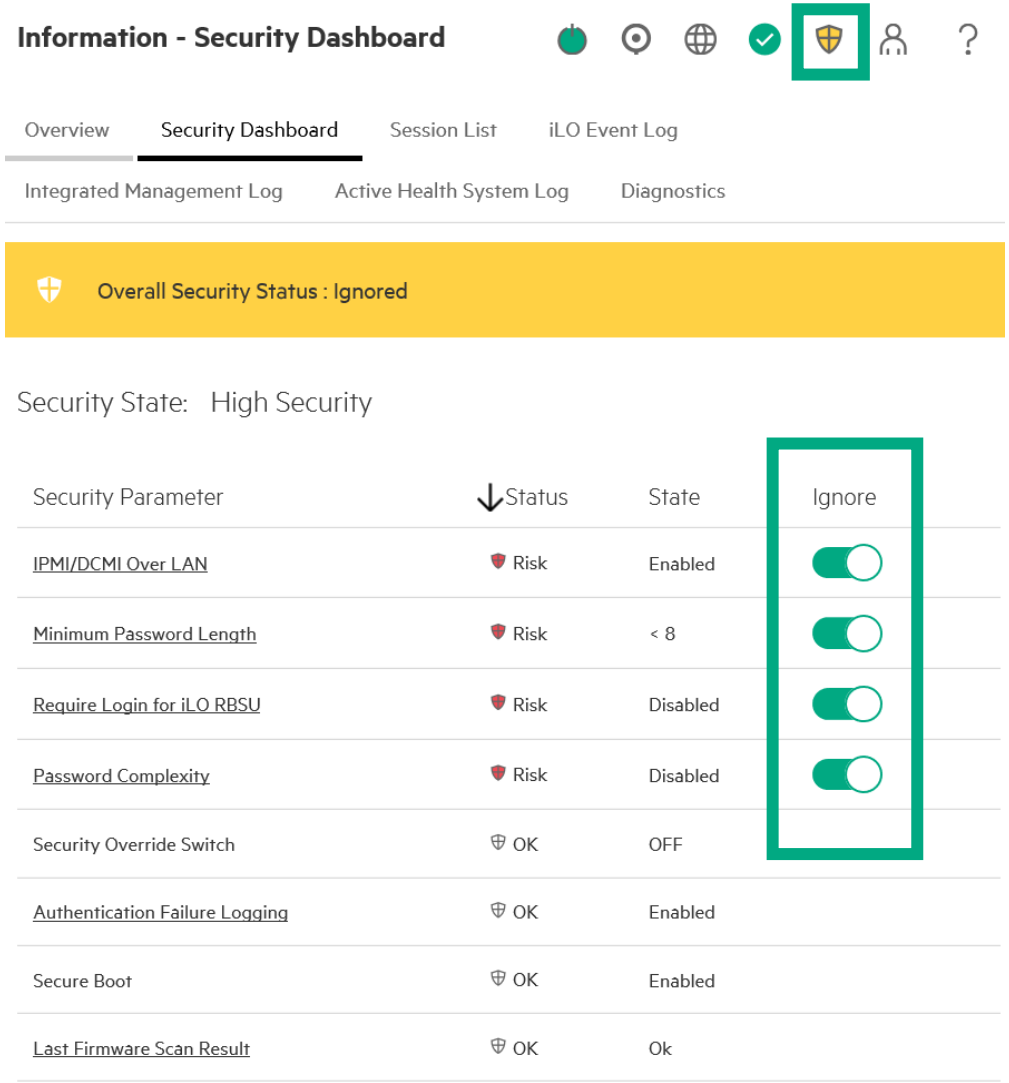


iLO Security Dashboard – контроль настроек iLO



iLO Security Dashboard

- Проверка настроек безопасности
  - Authentication Failure Logging
  - Default SSL Certificate In Use
  - IPMI/DCMI Over LAN
  - Minimum Password Length
  - Password Complexity
  - Require Host Authentication
  - Require Login for iLO RBSU
  - Secure Boot
  - SNMPv1
  - Security Override Switch
- Результаты проверок
  - Access Panel Status
  - Last Firmware Scan Result



HPE Server Configuration Lock

Защита при транспортировке и развертывании

Проблема: клиентам нужно знать, что системы, перемещаемые из одного места в другое, не подвергаются атакам при транспортировке

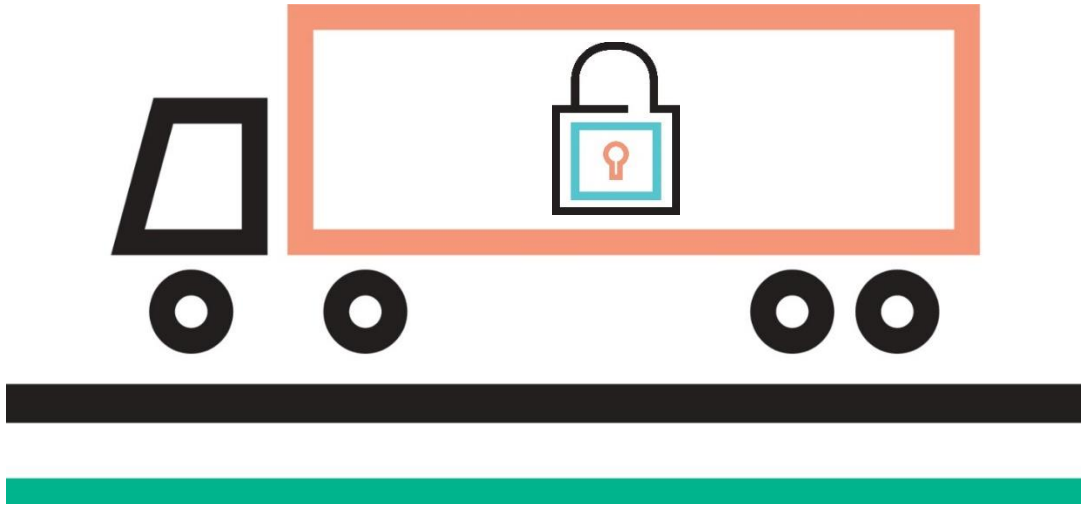
Решение: Блокировка конфигурации сервера

Модели использования:

– Доставка с завода HPE до клиента

– Транспортировка оборудования в филиальные сети

– Развертывание в небезопасной среде



HPE Server Configuration Lock

Предоставление пароля

Активация блокировки конфигурации


Создание цифрового отпечатка

Проверка цифрового отпечатка при каждой загрузке

Какие компоненты защищены цифровым отпечатком:

- Настройки конфигурации
- Версия прошивки
- Аппаратные изменения
  - Материнская плата
  - Оперативная память
  - Карты расширения PCIe
  - Процессоры

Требуется лицензия iLO Advanced

Защита данных и обеспечение информационной безопасности на протяжении всего жизненного цикла серверов HPE

Защита на уровне кремния	Постоянные проверки	Обнаружение поведенческих рисков	Соответствие требованиям регуляторов	Завершение жизненного цикла
• Silicon Root of Trust • Самошифрующиеся накопители • Защищенная цепочка поставок	• Обнаружение вторжений • Полное восстановление	• Машинное обучение • Безопасность HPE InfoSight	• Встроенные функции безопасности • Соответствие международным стандартам	• Гарантированное уничтожение чувствительной информации

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 - Silicon Root of Trust
  - Интеграция с технологиями защиты производителей микропроцессоров

Присоединяйтесь к каналам HPE в социальных сетях

TELEGRAM
@hpedigitize
https://t.me/hpedigitize

ВКОНТАКТЕ
@hperussia
https://vk.com/hperussia

- Топ-новости компании
- Информация о новых продуктах и решениях
- Расписание вебинаров и мероприятий

Спасибо!

Svetlakov@hpe.com