



**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

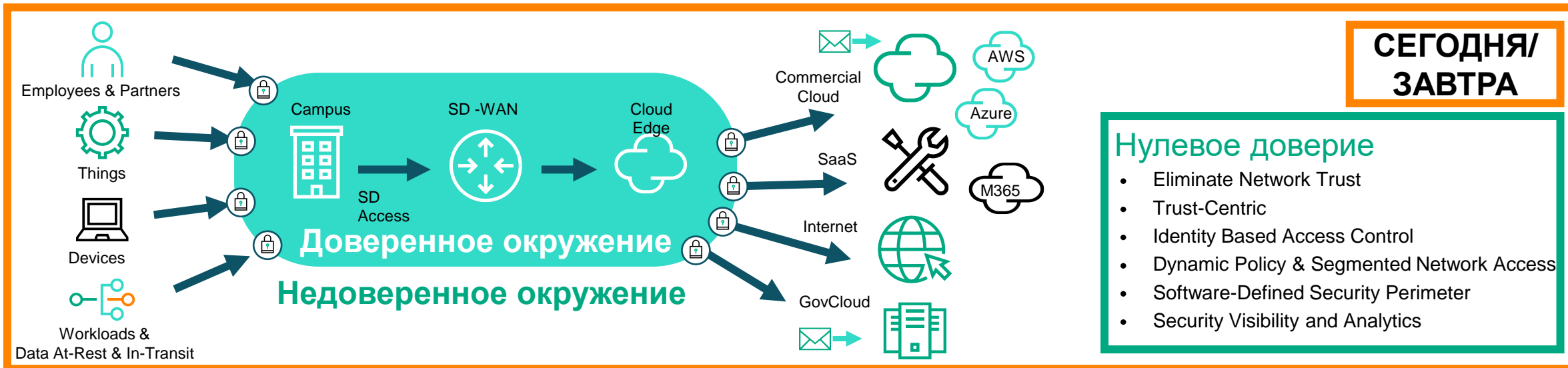
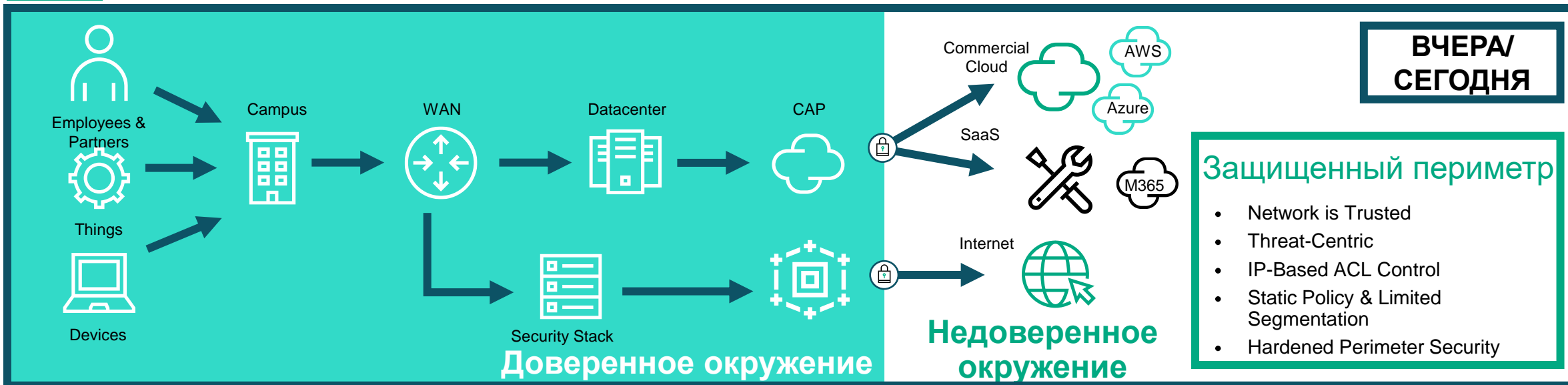
---

- 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

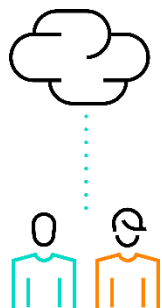


# НРЕ использует модель «нулевого доверия»

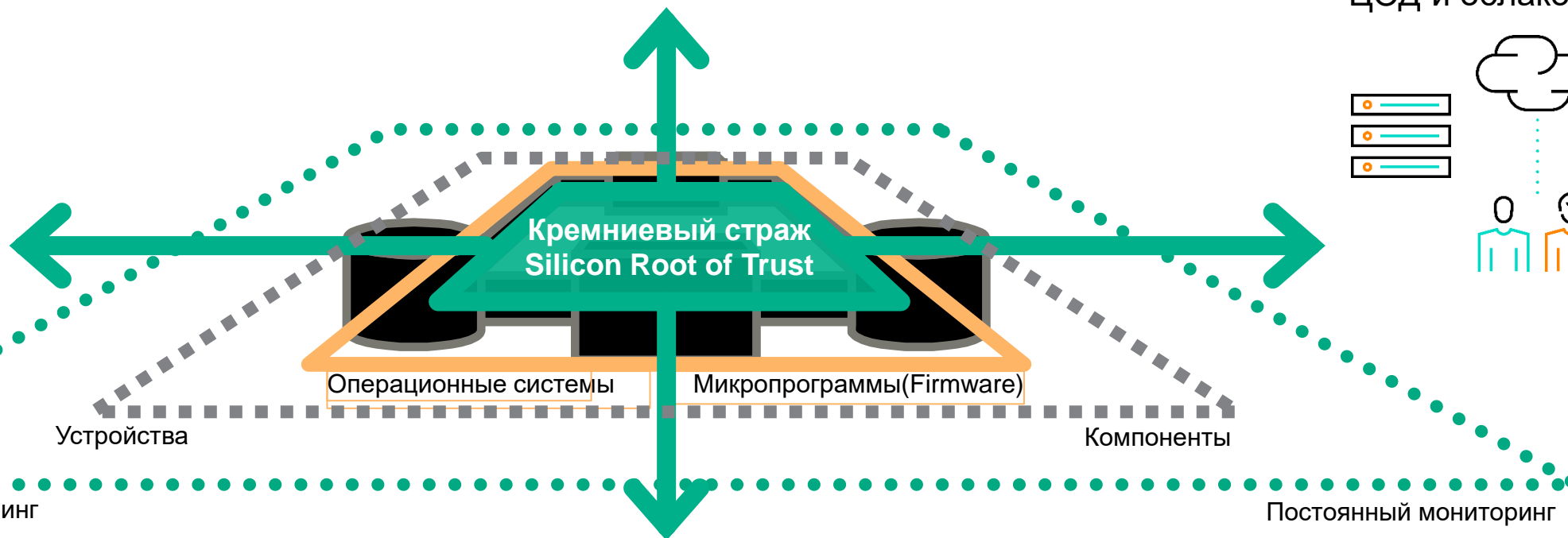
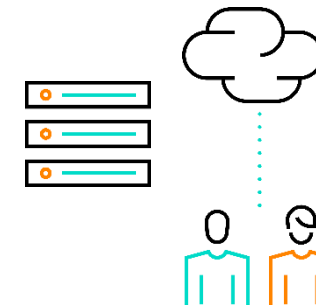
## Модель «нулевого доверия»

Никому не доверять, постоянно проверять, автоматически реагировать

Много границ,  
ЦОД и облаков



Много границ,  
ЦОД и облаков



Постоянный мониторинг

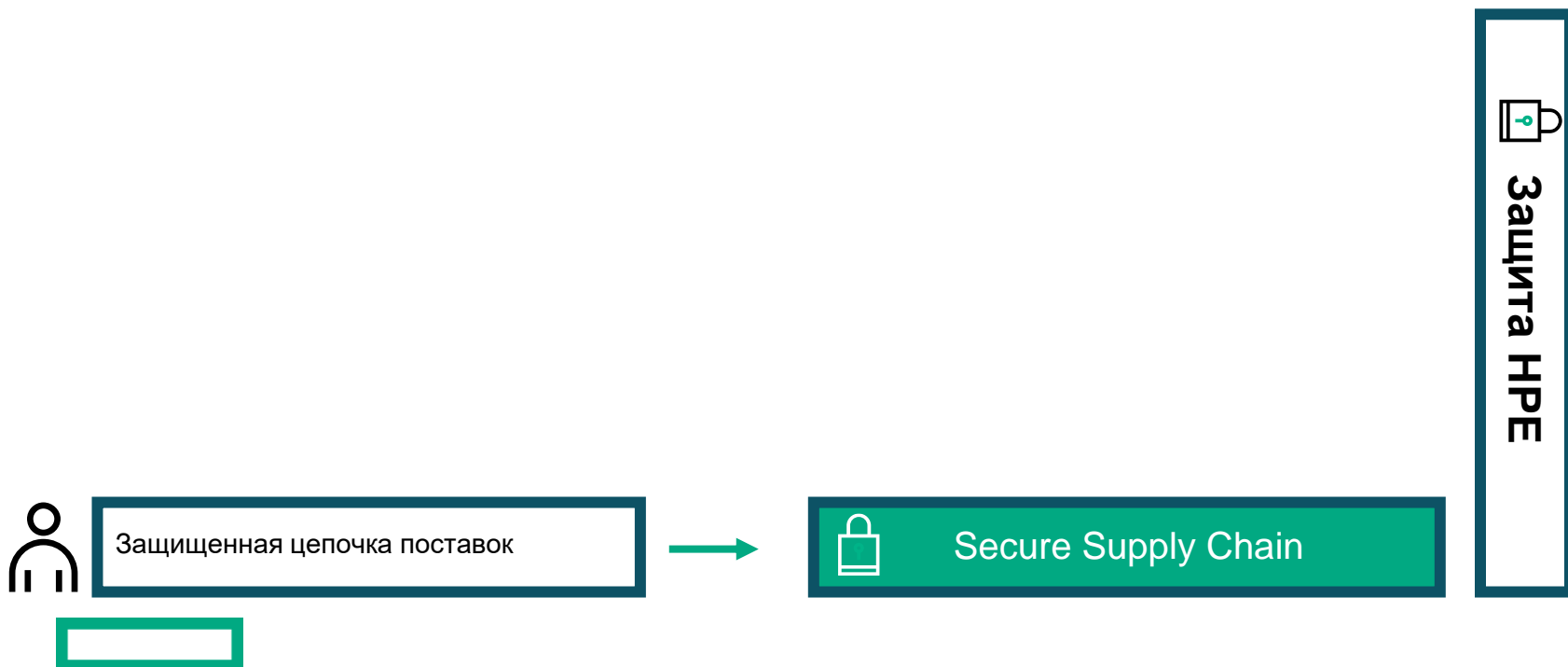
Постоянный мониторинг

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



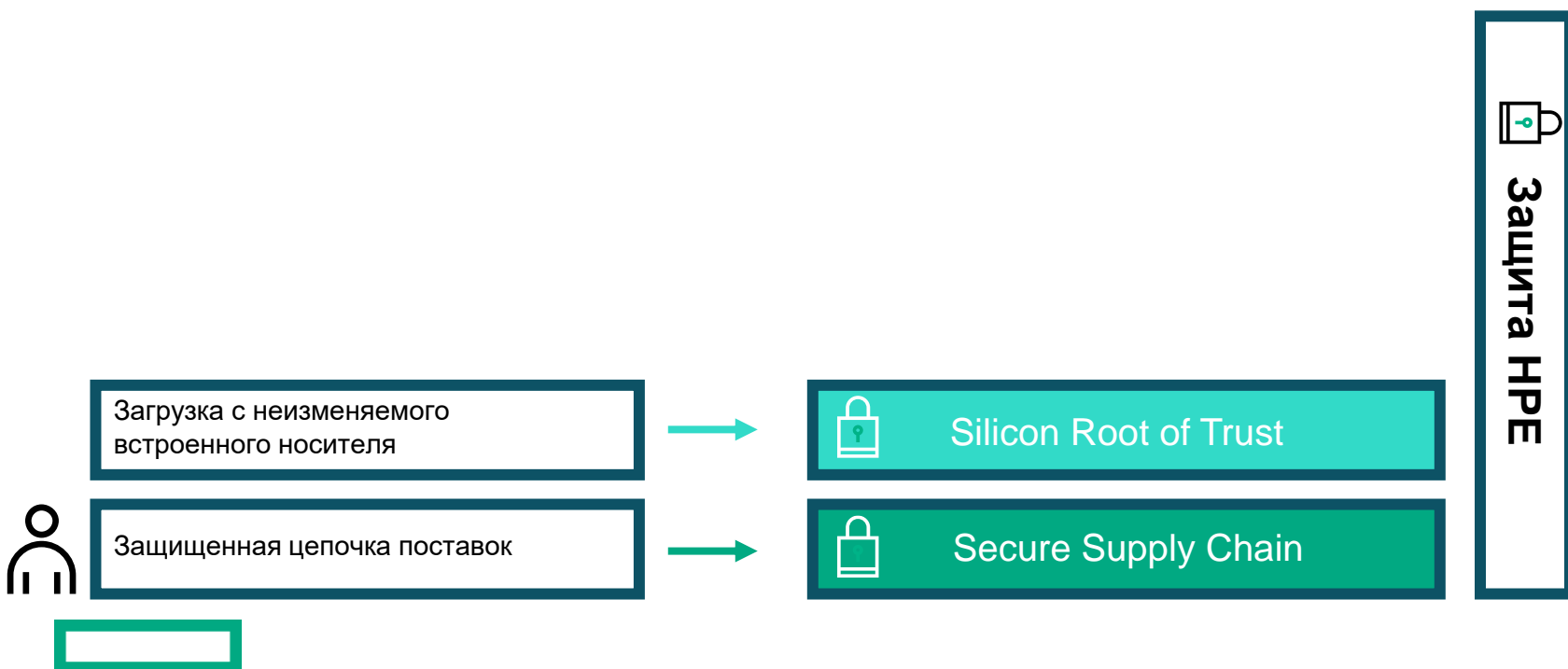
# Безопасность инфраструктуры критична для модели нулевого доверия

Безопасность  
обеспечивается только  
тогда, когда защищён  
уровень ниже точки атаки



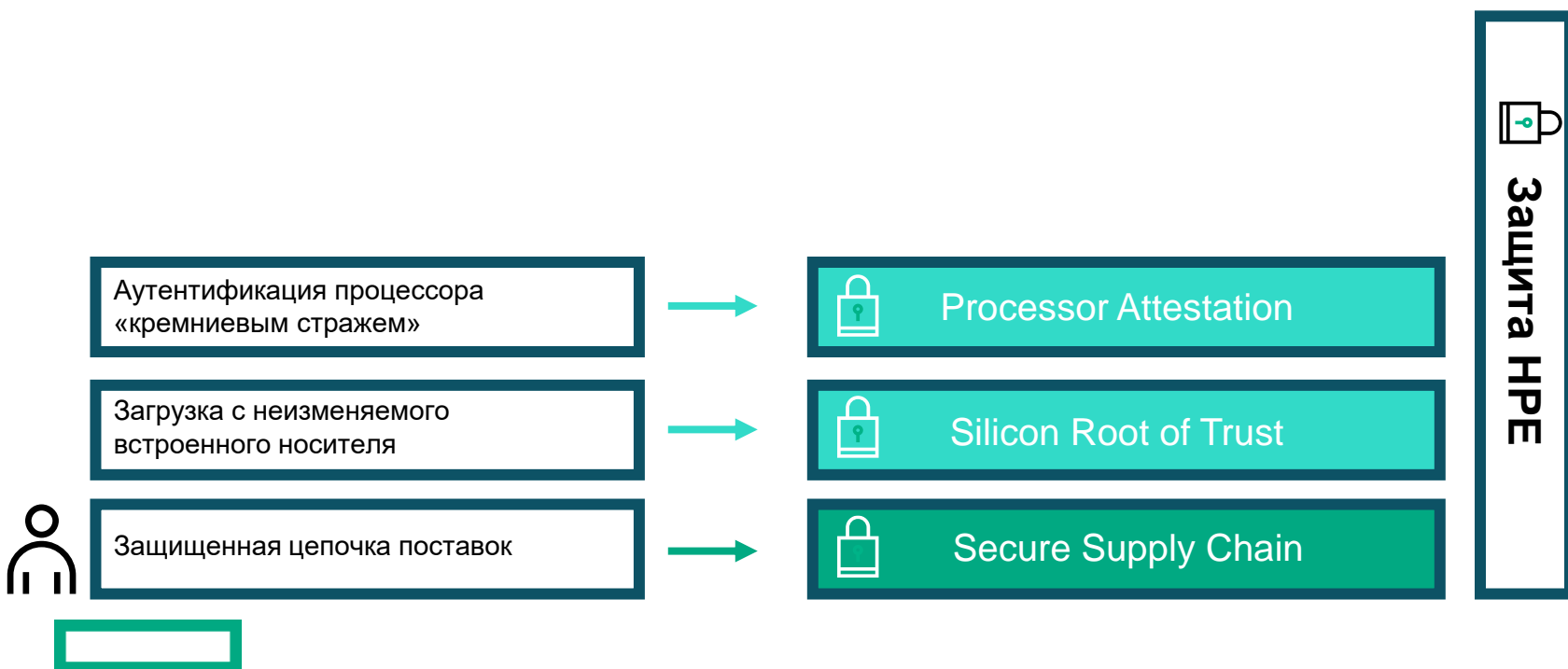
# Безопасность инфраструктуры критична для модели нулевого доверия

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

Постоянная проверка во время работы систем


Аутентификация процессора «кремниевым стражем»


Загрузка с неизменяемого встроенного носителя

Защищённая цепочка поставок



 UEFI/BIOS/firmware

 Processor Attestation

 Silicon Root of Trust

 Secure Supply Chain

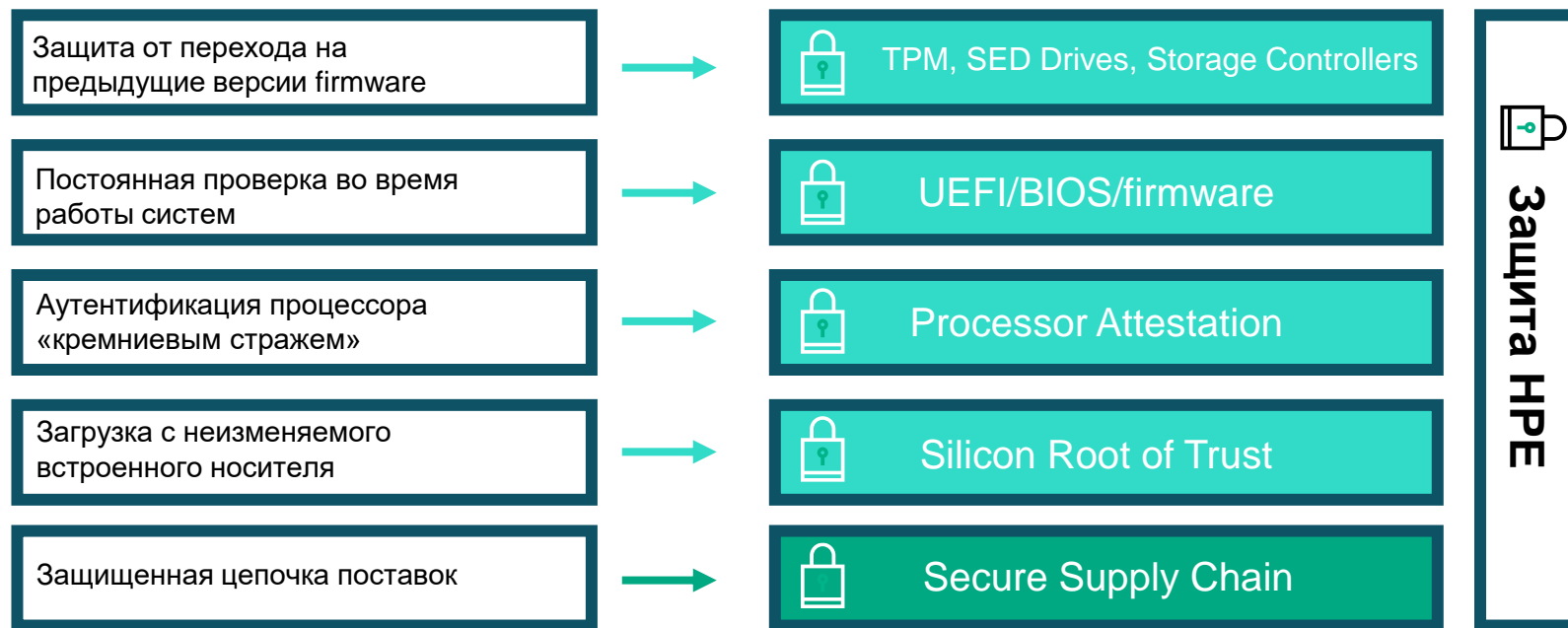
 **Защита NPE**





# 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

Защита от перехода на предыдущие версии firmware

Постоянная проверка во время работы систем

Аутентификация процессора «кремниевым стражем»

Загрузка с неизменяемого встроенного носителя

Защищенная цепочка поставок



Приложения

Платформы

Операционные системы



TPM, SED Drives, Storage Controllers



UEFI/BIOS/firmware



Processor Attestation



Silicon Root of Trust



Secure Supply Chain

Защита по  
«проекту Аврора»

Защита NPE

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

Защита от перехода на предыдущие версии firmware

Постоянная проверка во время работы систем

Аутентификация процессора «кремниевым стражем»

Загрузка с неизменяемого встроенного носителя

Защищенная цепочка поставок



Приложения

Платформы

Операционные системы



TPM, SED Drives, Storage Controllers



UEFI/BIOS/firmware



Processor Attestation



Silicon Root of Trust



Secure Supply Chain

Защита по «проекту Аврора»

Защита NRE

Ransomware, malicious insider, malware, phishing, theft, trojan horse, user error, water-holing, zero day attack

DOS, DDOS, user error, worms

Ransomware, man in the middle, user error, worms

Malware, data theft, malware, theft of hard drives.

Root kit, boot kit, booting into alternate OS, phlashing

Boot Kit, root kit, tampering, data theft

Malware (firmware), unvalidated firmware updates, theft of data (w/EPYC)

Counterfeit materials, malware, tampering, theft, malware, root kit, boot kit

Типы Атак

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**



Больше защиты

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

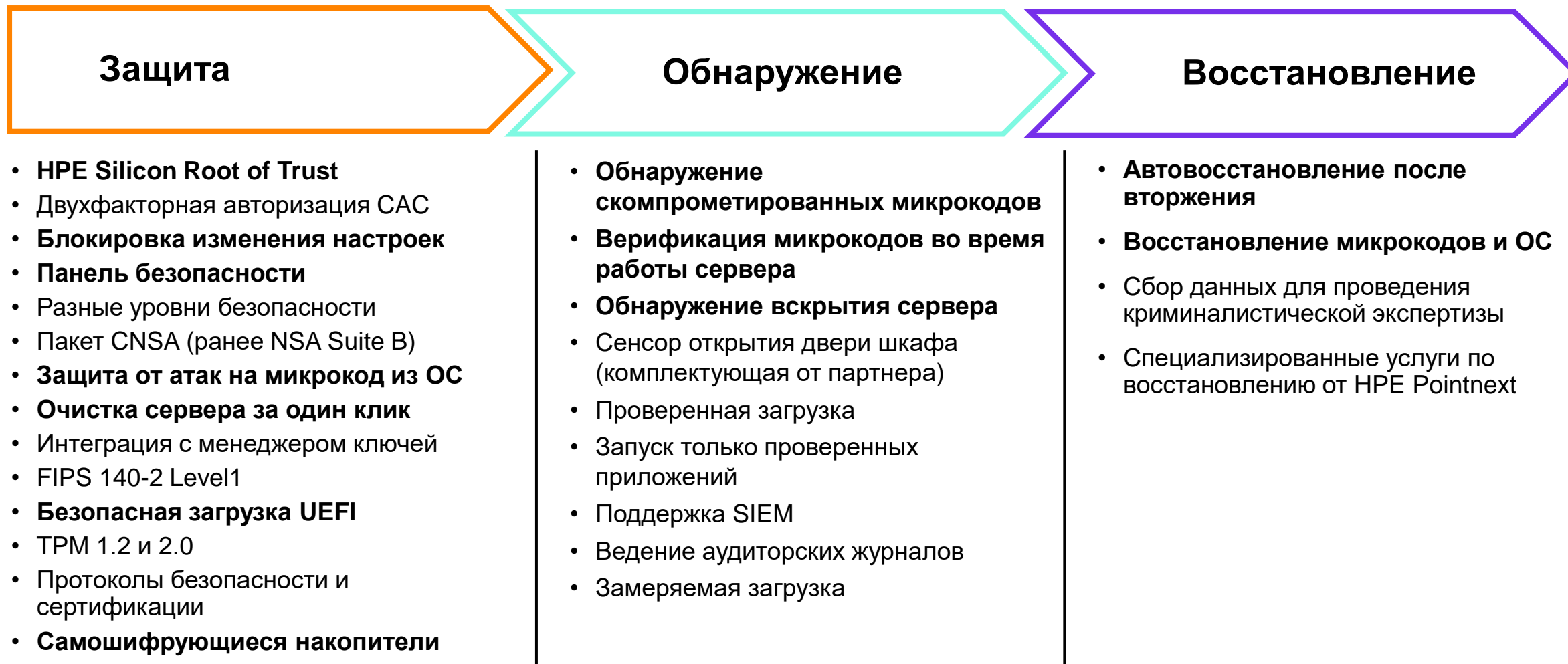


Каждый уровень проверяет и защищает вышестоящий уровень

\* 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

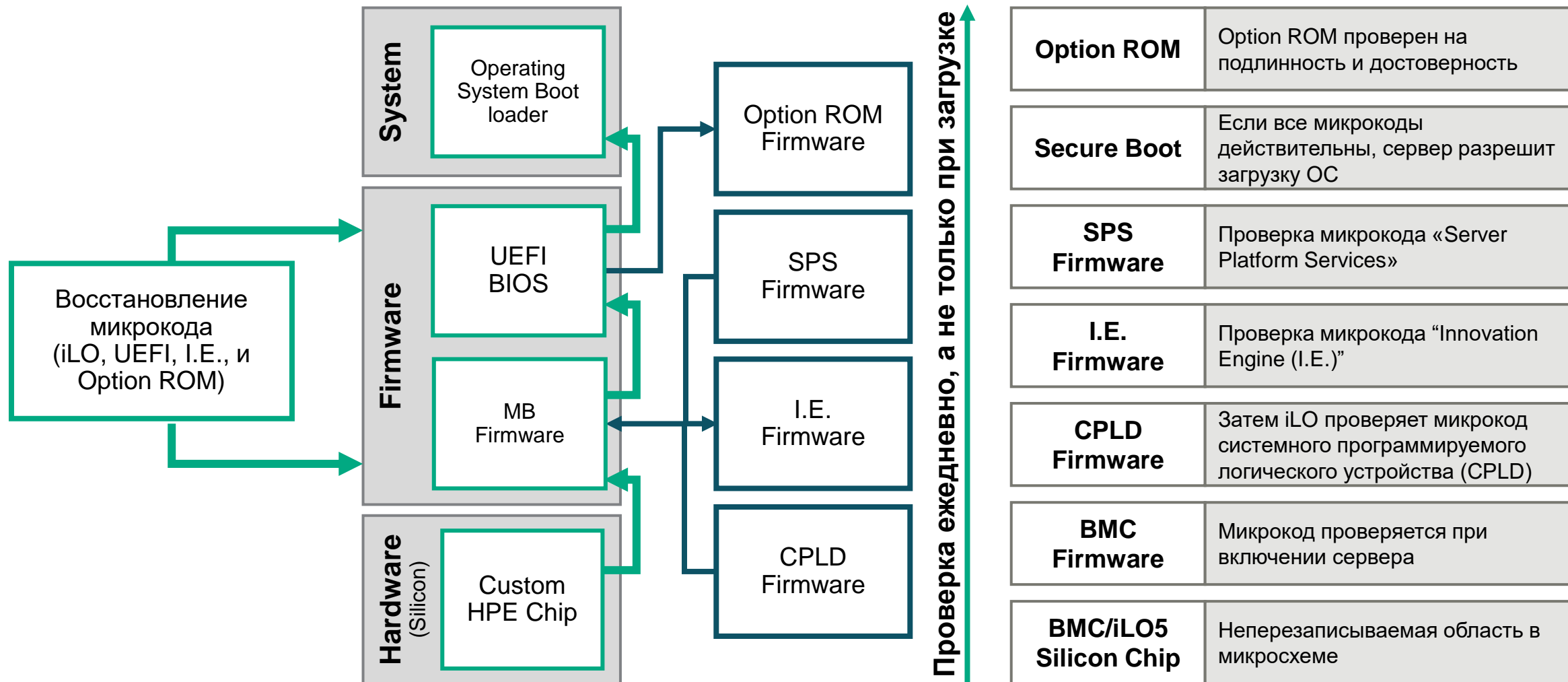
Самый безопасный сервер в мире\*



\*Based on testing of multiple server platforms by InfusionPoints



# Технология Silicon Root of Trust и Firmware Verification в серверах HPE



# 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

The screenshot displays the iLO 5 Lifecycle Management - Decommission interface. The left sidebar shows the navigation menu with 'Lifecycle Management' selected. The main content area shows the 'Decommission' tab active, with a table of decommissioned devices. The table columns are Device Type, Location, Serial Number, Status, Erase Type, Start Time, and End Time. The status for all devices is 'Success'. Below the table, it lists devices not impacted by secure erase: USB Drives, SD Cards, and iLO Virtual Media.

**iLO 5** [Redacted]

### Lifecycle Management - Decommission

Decommission | Backup & Restore

Server Serial Number: CN7932042D  
Initiated By: admin

Device Type	Location	Serial Number	Status	Erase Type	Start Time	End Time
SATA Drives	SATA Drive Box 4 Bay 2	ZFA0KVLZ	Success	Purge	02/17/2021 11:44:53	02/17/2021 13:29:24
SATA Drives	SATA Drive Box 4 Bay 4	ZFA0KVNZ	Success	Purge	02/17/2021 11:44:53	02/17/2021 13:32:24
SATA Drives	SATA Drive Box 1 Bay 3	ZFA0S63M	Success	Purge	02/17/2021 11:44:52	02/17/2021 13:33:24
SATA Drives	SATA Drive Box 1 Bay 2	ZFA0KV1Y	Success	Purge	02/17/2021 11:44:51	02/17/2021 13:35:24
SATA Drives	SATA Drive Box 4 Bay 3	Z8G XK006FQPE	Success	Purge	02/17/2021 11:44:53	02/17/2021 15:10:24
SATA Drives	SATA Drive Box 1 Bay 1	Z8FGK0XEFQPE	Success	Purge	02/17/2021 11:44:51	02/17/2021 15:23:24
SATA Drives	SATA Drive Box 1 Bay 4		Success	Purge	02/17/2021 11:44:52	02/18/2021 00:54:54
SATA Drives	SATA Drive Box 4 Bay 1	79V0A0ATFDBG	Success	Purge	02/17/2021 11:44:53	02/18/2021 07:02:54
UEFI Store	N/A	N/A	Success	Clear	02/18/2021 07:04:04	02/18/2021 07:04:24
Embedded NAND Flash	N/A	N/A	Success	Purge	02/18/2021 07:09:49	02/18/2021 07:13:15
NVRAM	N/A	N/A	Success	Clear	02/18/2021 07:14:51	02/18/2021 07:14:51

Following devices are not impacted by secure erase:

- USB Drives
- SD Cards
- iLO Virtual Media

# iLO Security Dashboard – контроль настроек iLO

## Information - iLO Overview

Overview Security Dashboard Session List iLO Event Log Integrated Management Log

Active Health System Log Diagnostics

Information		Status	
<b>Server Name</b>	WIN-6A1A1HBL5NN	<b>System Health</b>	✔ OK
<b>Product Name</b>	ProLiant DL560 Gen10	<b>iLO Health</b>	✔ OK
<b>UUID</b>	30383831-332D-4E43-3737-313130445159	<b>iLO Security</b>	⚠ Risk
<b>Server Serial Number</b>	CN77110DQY	<b>Server Power</b>	● ON
<b>Product ID</b>	1880-3002	<b>UID Indicator</b>	🕒 UID OFF
<b>System ROM</b>	U34 v1.42 (06/20/2018)	<b>TPM Status</b>	Not Present
<b>System ROM Date</b>	06/20/2018	<b>SD-Card Status</b>	Not Present
<b>Redundant System ROM</b>	06/01/2017	<b>iLO Date/Time</b>	Tue Jul 24 14:24:38 2018



# 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

## Information - Security Dashboard











Overview Security Dashboard Session List iLO Event Log

Integrated Management Log Active Health System Log Diagnostics

 Overall Security Status : Ignored

Security State: High Security

Security Parameter	↓Status	State	Ignore
<a href="#">IPMI/DCMI Over LAN</a>	 Risk	Enabled	<input checked="" type="checkbox"/>
<a href="#">Minimum Password Length</a>	 Risk	< 8	<input checked="" type="checkbox"/>
<a href="#">Require Login for iLO RBSU</a>	 Risk	Disabled	<input checked="" type="checkbox"/>
<a href="#">Password Complexity</a>	 Risk	Disabled	<input checked="" type="checkbox"/>
Security Override Switch	 OK	OFF	<input type="checkbox"/>
<a href="#">Authentication Failure Logging</a>	 OK	Enabled	<input type="checkbox"/>
Secure Boot	 OK	Enabled	<input type="checkbox"/>
<a href="#">Last Firmware Scan Result</a>	 OK	Ok	<input type="checkbox"/>

# 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



## 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

- Silicon Root of Trust
- Самошифрующиеся накопители
- Защищенная цепочка поставок

## Постоянные проверки

- Обнаружение вторжений
- Полное восстановление

## Обнаружение поведенческих рисков

- Машинное обучение
- Безопасность HPE InfoSight

## Соответствие требованиям регуляторов

- Встроенные функции безопасности
- Соответствие международным стандартам

## Завершение жизненного цикла

- 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



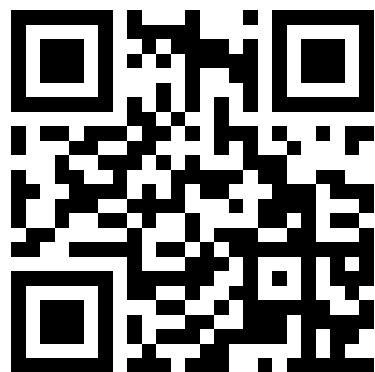
# Присоединяйтесь к каналам НРЕ в социальных сетях



**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

