CHECK POINT

Как эффективно организовать безопасный удаленный доступ и защитить устройства пользователей от современных угроз?

Турков Никита | Pre-sale инженер Check Point

15.03.2024

YOU DESERVE THE BEST SECURITY

О чем доклад?

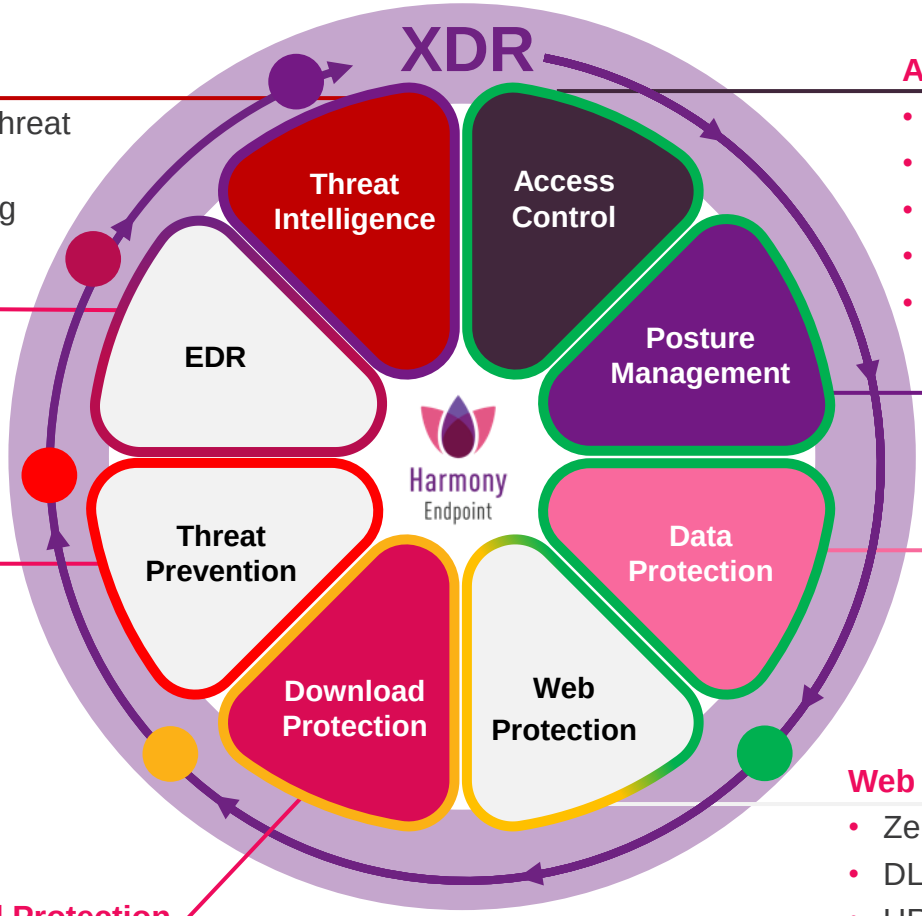
- Harmony Endpoint – защита конечных станций
- Harmony Mobile – ваш телефон уязвим
- Harmony SASE – гибридный доступ к ресурсам
- Horizon XDR – центр мониторинга и реакции на атаки
- Демонстрация
- Вопросы

01

Harmony Endpoint Защита конечных станций

Комплексная защита EPP, EDR & Zero Day Prevention

1. Сократить площадь атаки
2. Предотвратить запуск атаки
3. Защита в режиме реального времени
4. Расследование и восстановление
5. Сканирование и отчеты



ThreatCloud
- AI Powered Threat Analytics
- Threat Hunting

Detection & Response
- Incident Management
- Research Intelligence
- Automated Reaction
- Triage Tools

Next Gen AV
- Anti-Ransomware
- Anti-Bot
- Anti-Malware
- ML based NGAV
- Anti-Exploit
- Behavioral Guard
- Threat Emulation

Download Protection
- Threat Emulation
- Threat Extraction

Access Control
- Remote Access VPN
- Host Firewall
- Compliance
- Port Protection
- APP Control

Posture Management
- Zero Trust Posture Management
- Vulnerability & Patch Management

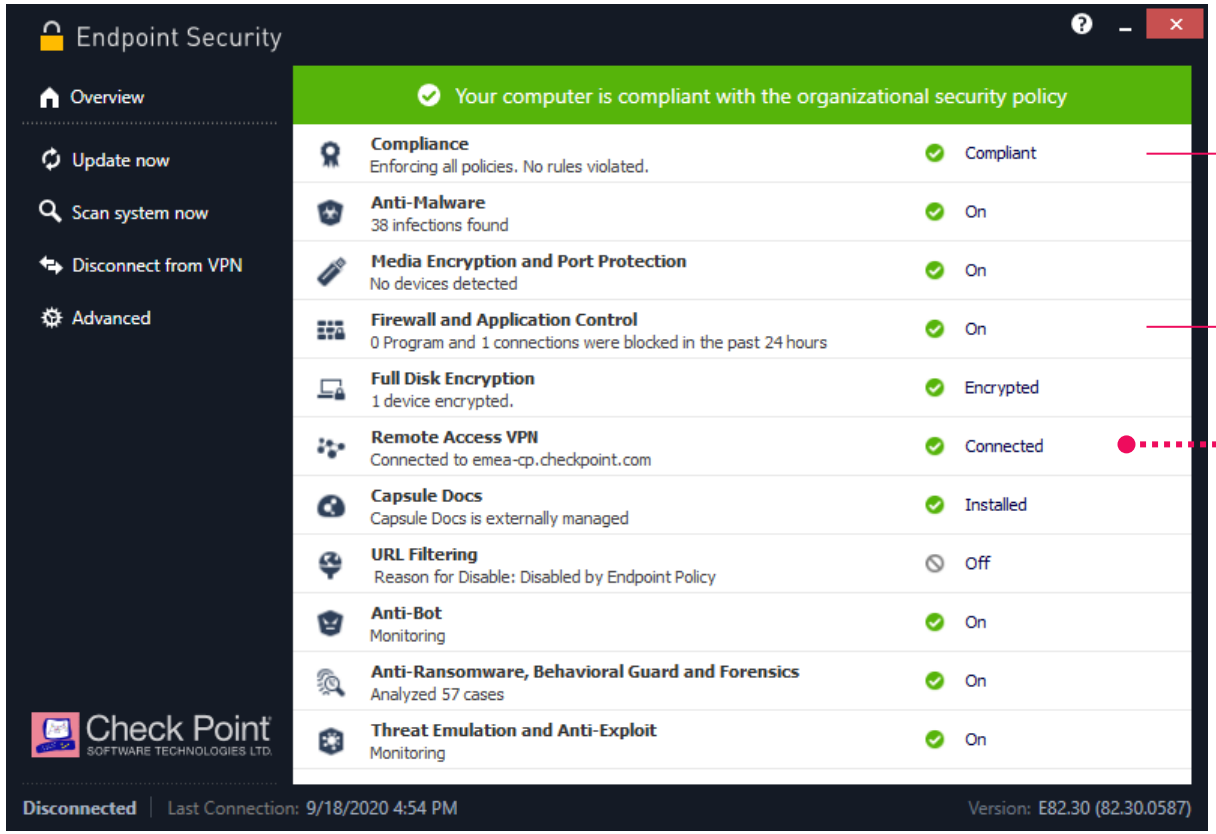
Data Protection
- Media Encryption
- Full Disk Encryption

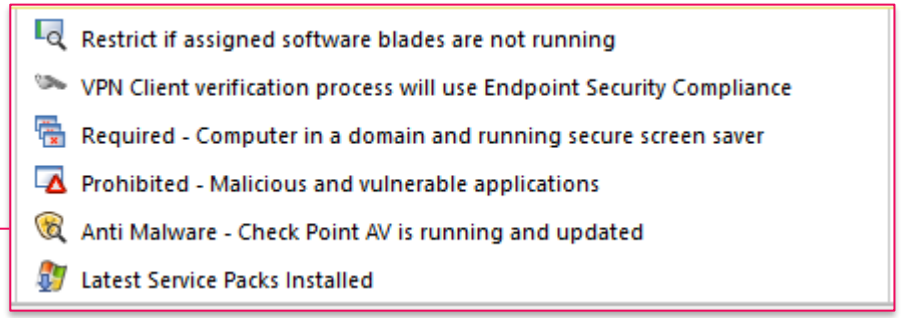
Web Protection
- Zero-day Phishing
- DLP (Data Loss Protection)
- URL Filtering
- Corporate Password Reuse Protection
- Safe Search

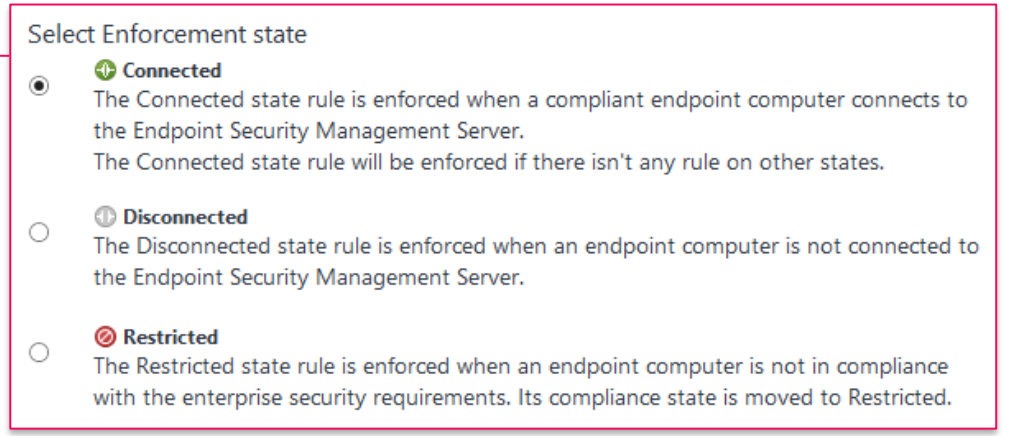
Поддержка ОС

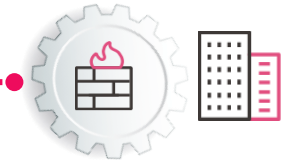
- Microsoft: Windows 7, Windows 8.1, Windows 10, Windows 11, Windows Servers
- MacOS: M1/2 chip, Catalina-Sonoma
- Linux: Ubuntu, Debian, RHEL, CentOS, Oracle, Amazon, containers
- VDI, Terminal Servers

Access Control: (Compliance и Remote Access VPN)









Предустановленный VPN-сайт, MFA

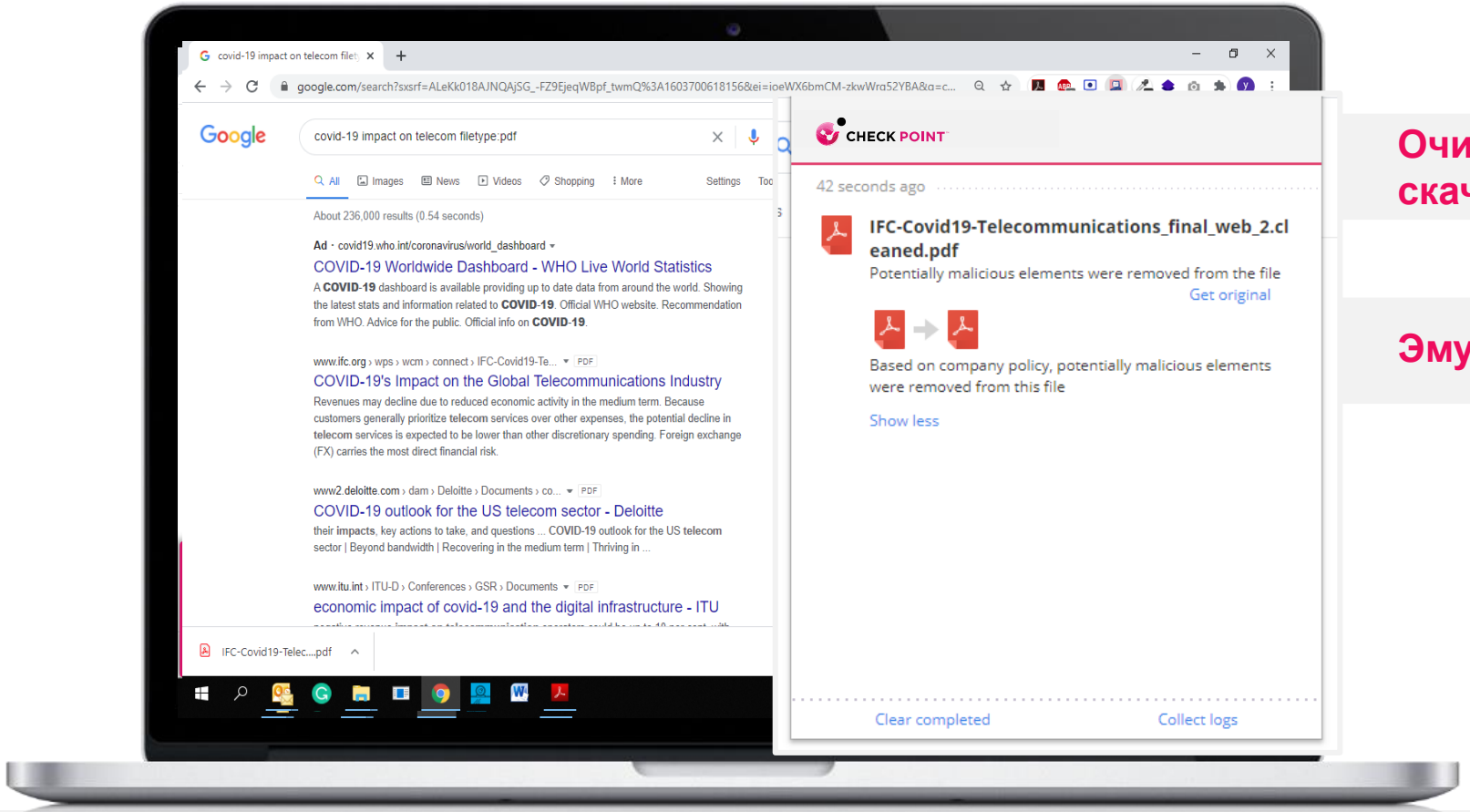
Web & File Protection: (Download Protection)

Harmony Endpoint

Сократить площадь атаки | **Предотвратить запуск атаки**

Оригинальный файл эмулируется в песочнице

Если файл не зловредный, он будет доступен для скачивания



Очищенная копия доступна для скачивания через 1.5 секунды

Эмуляция файла до 2-3 минут

Web & File Protection: (Phishing Protection)

Harmony Endpoint

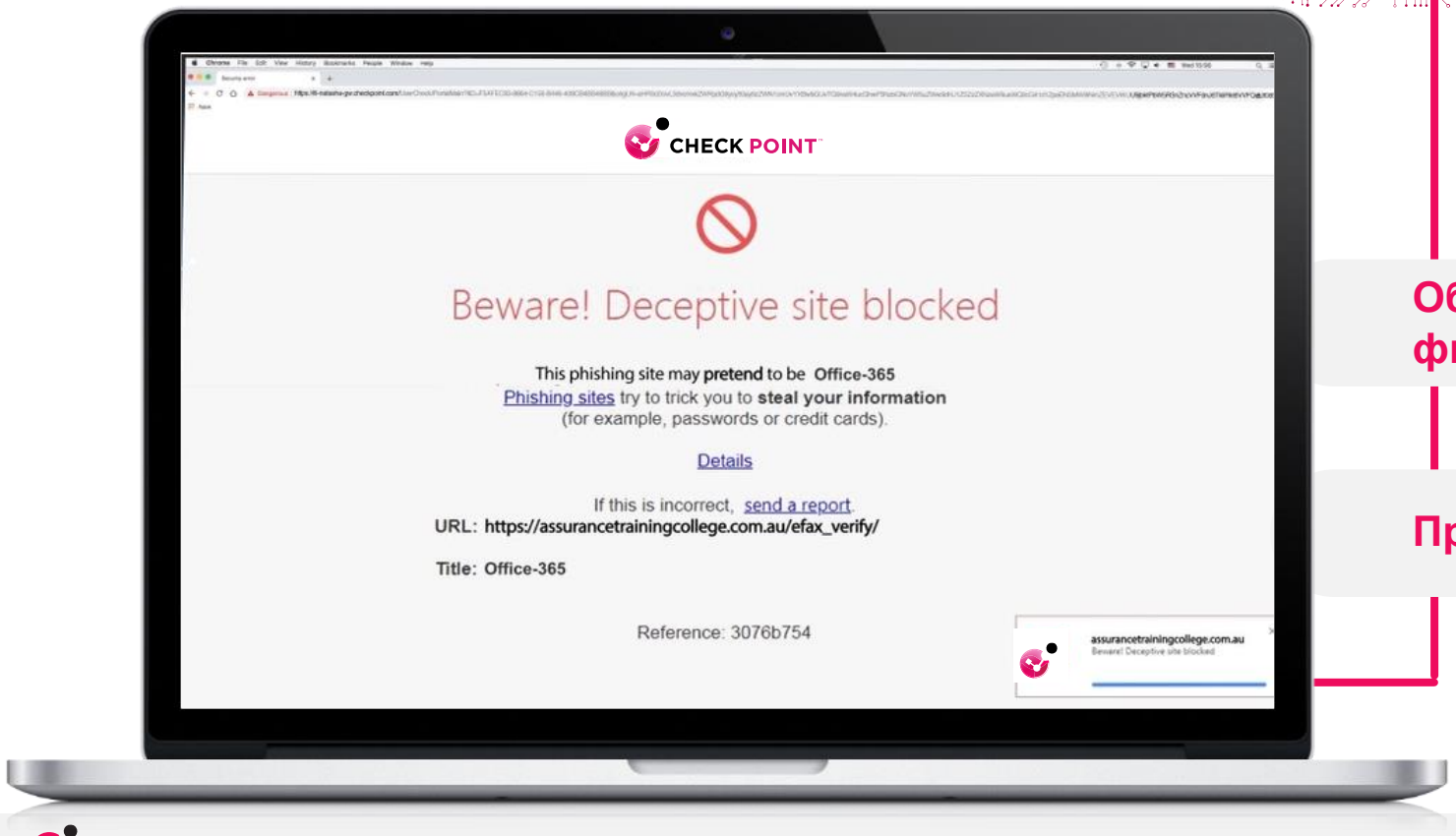
Сократить площадь атаки

Предотвратить запуск атаки

Пользователь кликает на ссылку

Браузер открывает фишинговую страницу

Harmony Endpoint сканирует формы ввода и блокирует



THREATCLOUD

- ✗ IP REPUTATION
- ✗ DOMAIN REPUTATION
- ✗ TITLE SIMILARITY
- ✓ VISUAL SIMILARITY

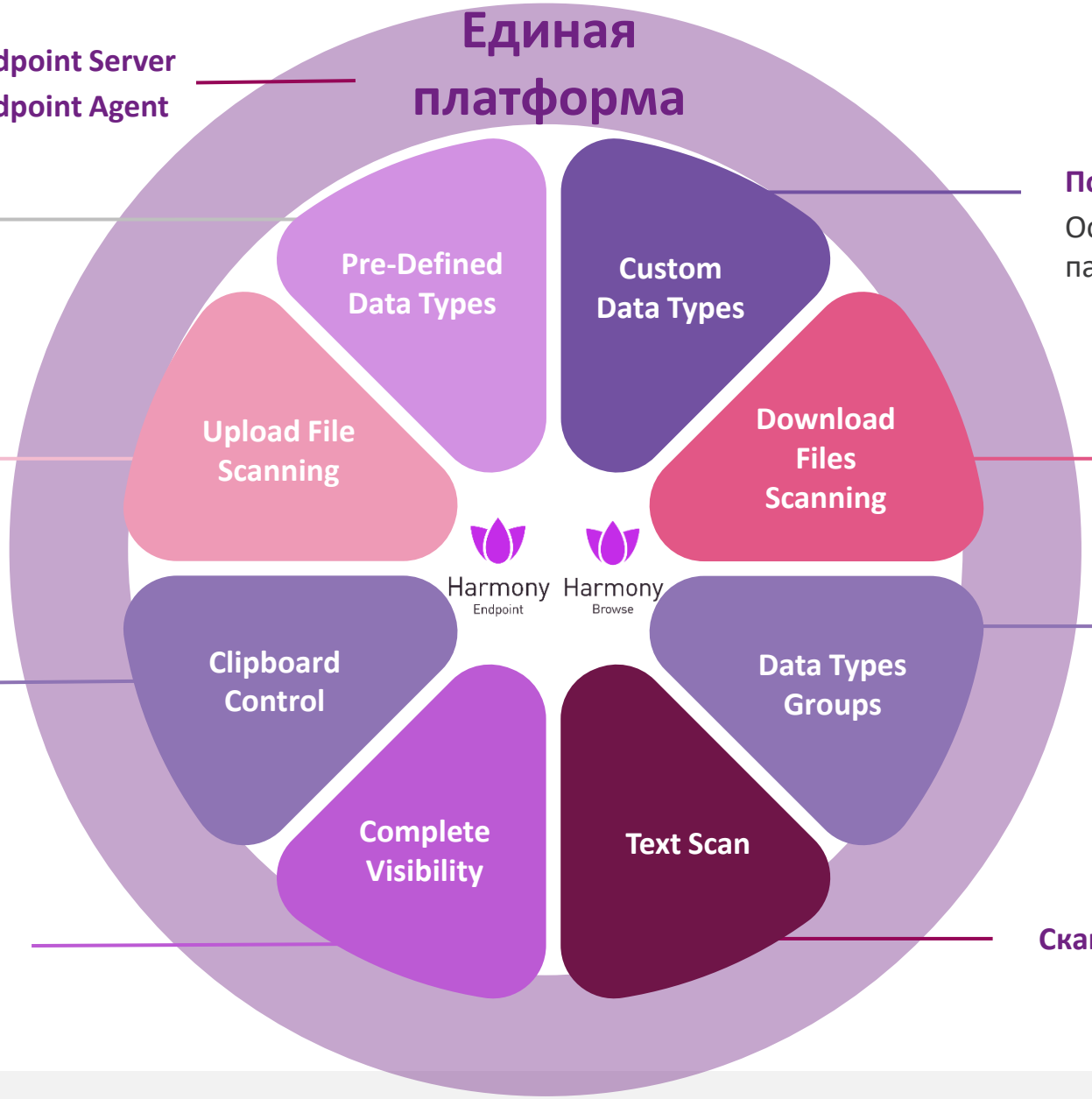
Обнаруживает и блокирует попытку фишинга менее чем через 2 секунды

- ✗ LOOKALIKE CHARACTERS

Предотвращает Zero-Phishing

- ✗ MULTIPLE TOP-LEVEL DOMAIN

Браузерный DLP (EA)



Harmony Endpoint Server
Harmony Endpoint Agent

Предустановленные объекты
Более 700 различных форматов файлов, включая встроенные

Пользовательские типы данных
Основаны на ключевых слова, паттернах, шаблонах и т.д

Сканирование выгружаемых файлов
Разрешить или запретить

Сканирование загружаемых файлов
Разрешить или запретить

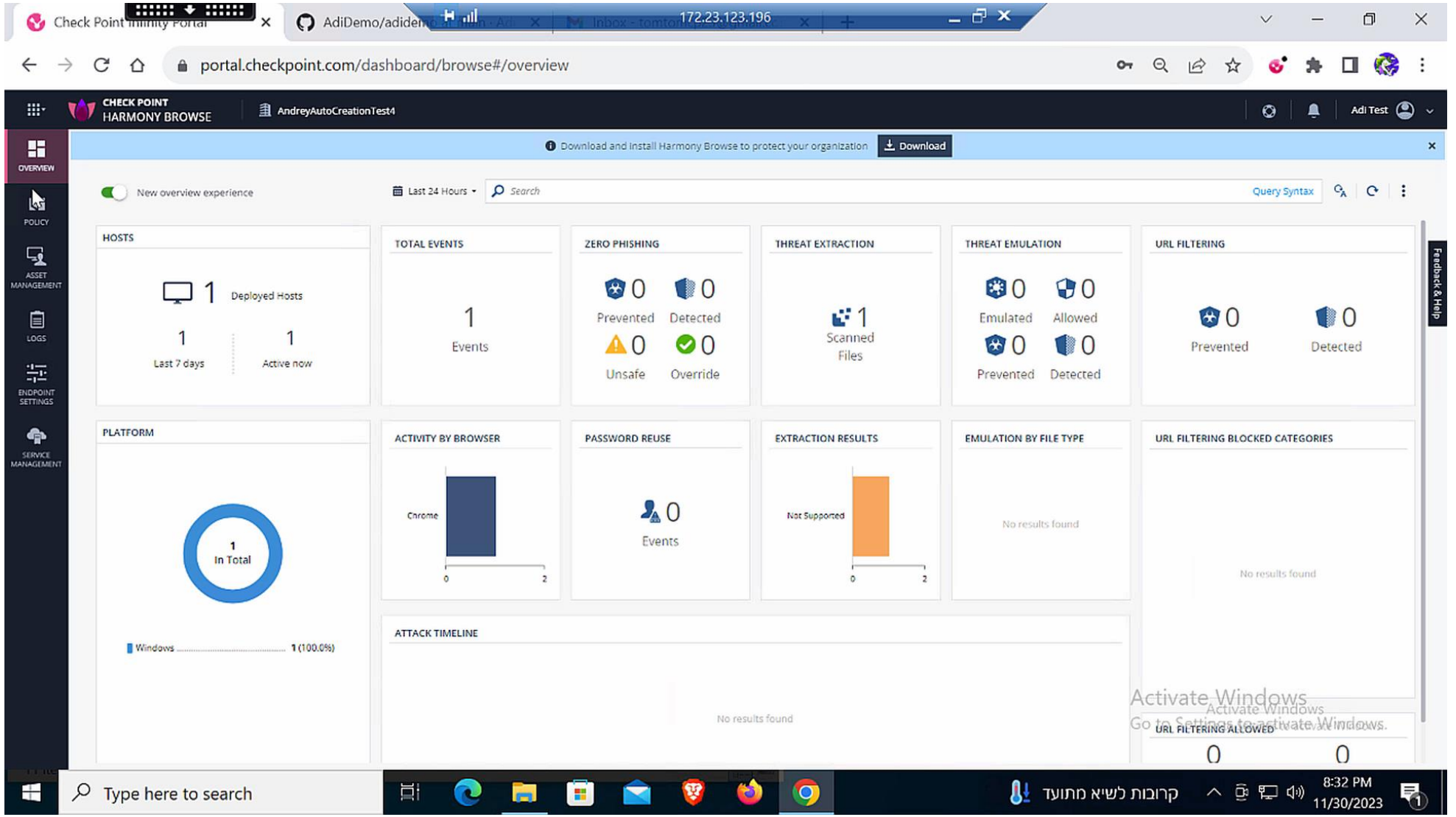
Контроль буфера
Включая Copy-Paste, Save, Print

Группы форматов
Возможность использовать специальные группы для различных задач

Мониторинг
Отчёты и логи

Сканирование запросов для AI сайтов

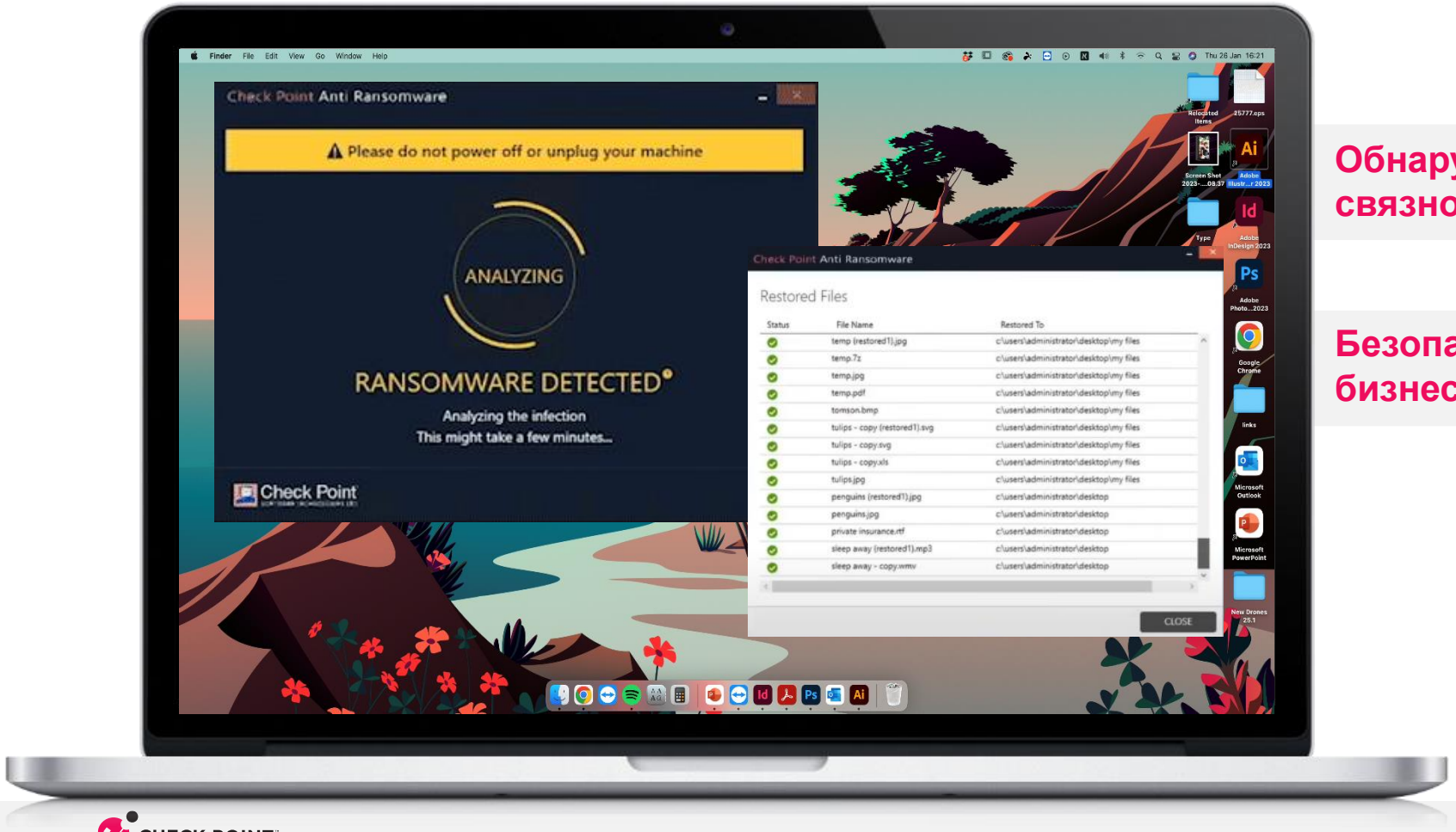
Demo



Behavioral Protection:
(Behavioral Guard & Anti Ransomware)

Harmony Endpoint

Reduce Attack Surface | Prevent Before it Runs | Run-Time Protection | Contain & Remediate | Proactive Analysis & Orchestration



Обнаружение и восстановление, даже без связности клиент-сервер

Безопасно восстанавливаются бизнес-файлы

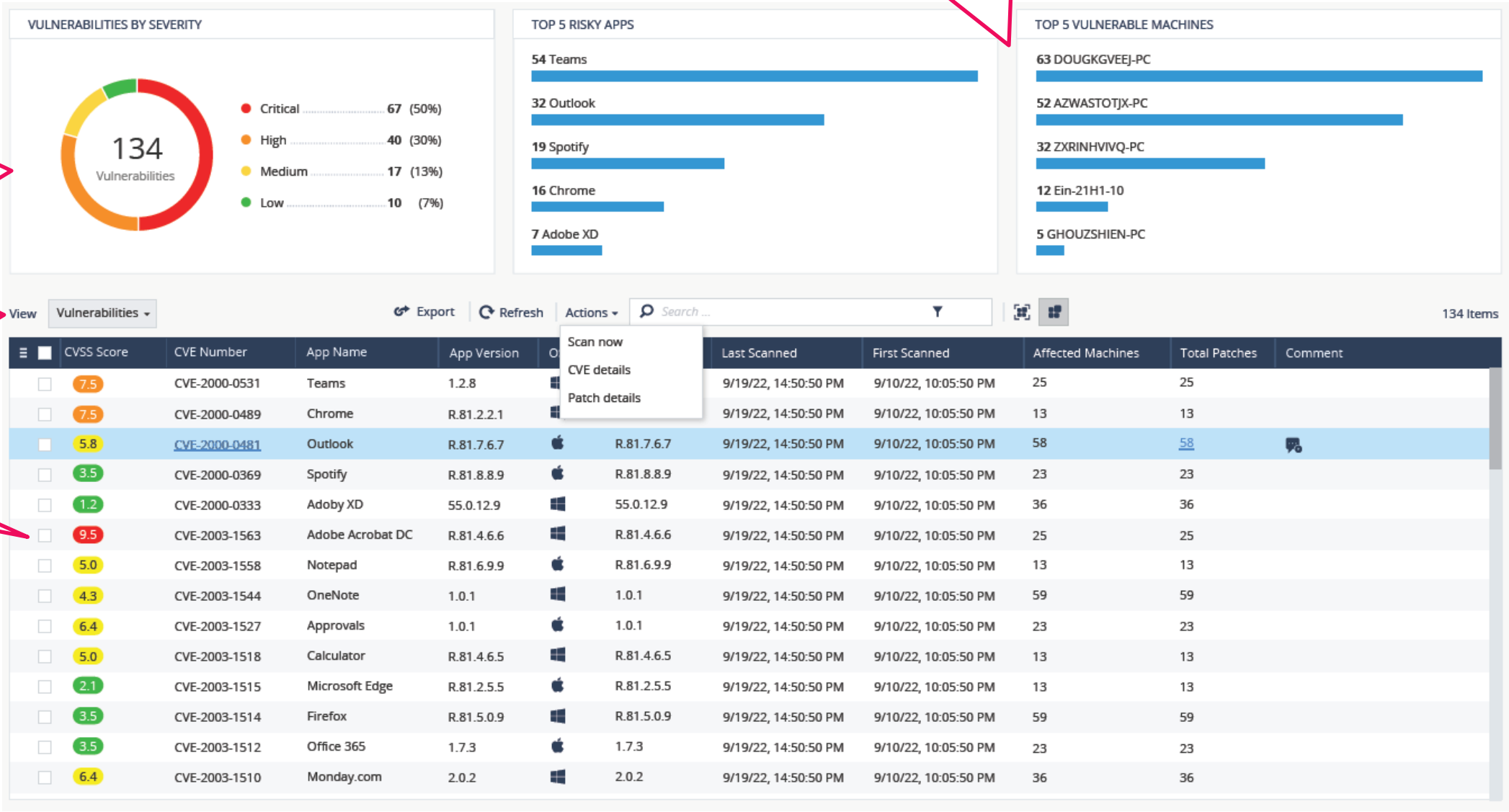
Posture Management

Фокус на наиболее уязвимые хосты в компании

Фокус на наиболее опасные уязвимости

Просмотр всех уязвимостей внутри организации

Сортировка по CVSS

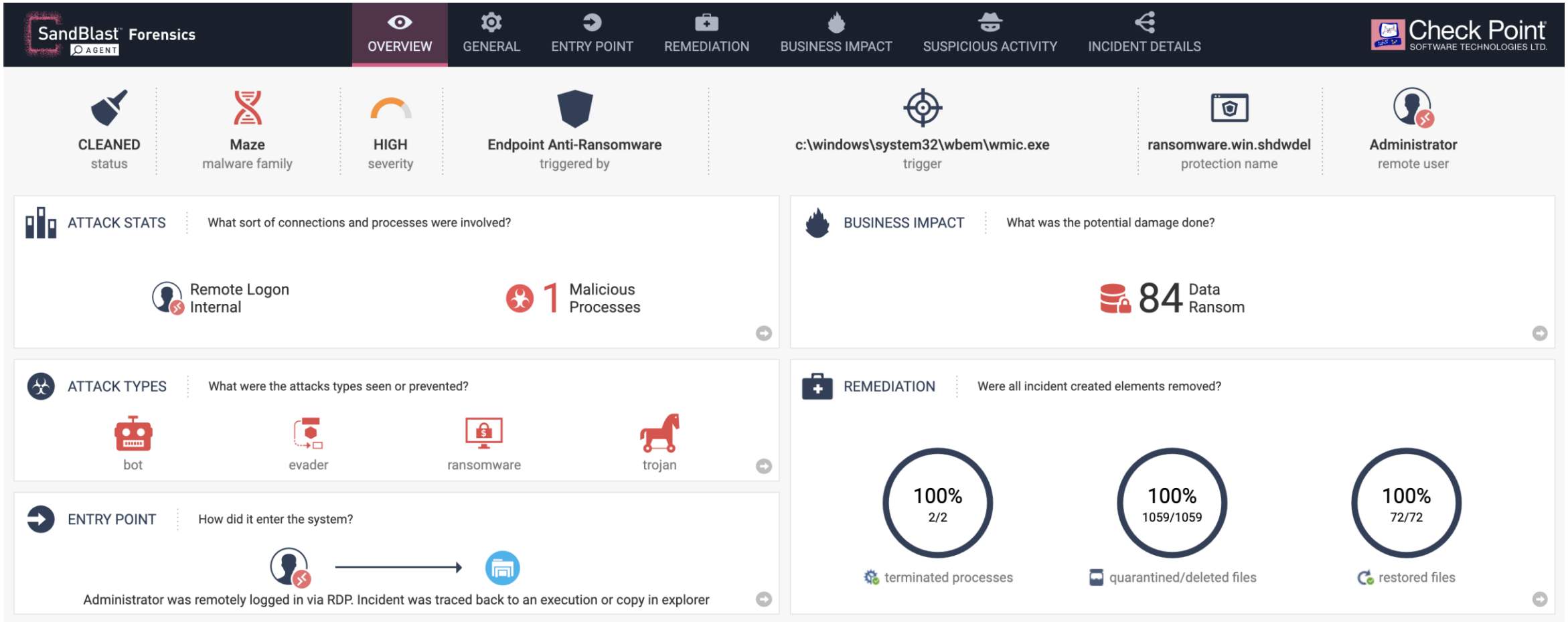


CVSS Score	CVE Number	App Name	App Version		Last Scanned	First Scanned	Affected Machines	Total Patches	Comment
7.5	CVE-2000-0531	Teams	1.2.8		9/19/22, 14:50:50 PM	9/10/22, 10:05:50 PM	25	25	
7.5	CVE-2000-0489	Chrome	R.81.2.2.1		9/19/22, 14:50:50 PM	9/10/22, 10:05:50 PM	13	13	
5.8	CVE-2000-0481	Outlook	R.81.7.6.7	R.81.7.6.7	9/19/22, 14:50:50 PM	9/10/22, 10:05:50 PM	58	58	
3.5	CVE-2000-0369	Spotify	R.81.8.8.9	R.81.8.8.9	9/19/22, 14:50:50 PM	9/10/22, 10:05:50 PM	23	23	
1.2	CVE-2000-0333	Adoby XD	55.0.12.9	55.0.12.9	9/19/22, 14:50:50 PM	9/10/22, 10:05:50 PM	36	36	
9.5	CVE-2003-1563	Adobe Acrobat DC	R.81.4.6.6	R.81.4.6.6	9/19/22, 14:50:50 PM	9/10/22, 10:05:50 PM	25	25	
5.0	CVE-2003-1558	Notepad	R.81.6.9.9	R.81.6.9.9	9/19/22, 14:50:50 PM	9/10/22, 10:05:50 PM	13	13	
4.3	CVE-2003-1544	OneNote	1.0.1	1.0.1	9/19/22, 14:50:50 PM	9/10/22, 10:05:50 PM	59	59	
6.4	CVE-2003-1527	Approvals	1.0.1	1.0.1	9/19/22, 14:50:50 PM	9/10/22, 10:05:50 PM	23	23	
5.0	CVE-2003-1518	Calculator	R.81.4.6.5	R.81.4.6.5	9/19/22, 14:50:50 PM	9/10/22, 10:05:50 PM	13	13	
2.1	CVE-2003-1515	Microsoft Edge	R.81.2.5.5	R.81.2.5.5	9/19/22, 14:50:50 PM	9/10/22, 10:05:50 PM	13	13	
3.5	CVE-2003-1514	Firefox	R.81.5.0.9	R.81.5.0.9	9/19/22, 14:50:50 PM	9/10/22, 10:05:50 PM	59	59	
3.5	CVE-2003-1512	Office 365	1.7.3	1.7.3	9/19/22, 14:50:50 PM	9/10/22, 10:05:50 PM	23	23	
6.4	CVE-2003-1510	Monday.com	2.0.2	2.0.2	9/19/22, 14:50:50 PM	9/10/22, 10:05:50 PM	36	36	

Analysis & Remediation + XDR

Harmony Endpoint

Reduce Attack Surface | Prevent Before it Runs | Run-Time Protection | Contain & Remediate | Proactive Analysis & Orchestration



02

Harmony Mobile
Ваш телефон уязвим

Кейсы с взломом телефона

40% всех устройств уязвимы на аппаратном уровне

400+ уязвимостей найдено в чипсетах Qualcomm

SAMSUNG LG SONY

Lenovo ONEPLUS xiaomi Google Pixel

Маркетплейсы публикуют приложения с вредоносным кодом

Банки, мессенджеры – фейки

Google play

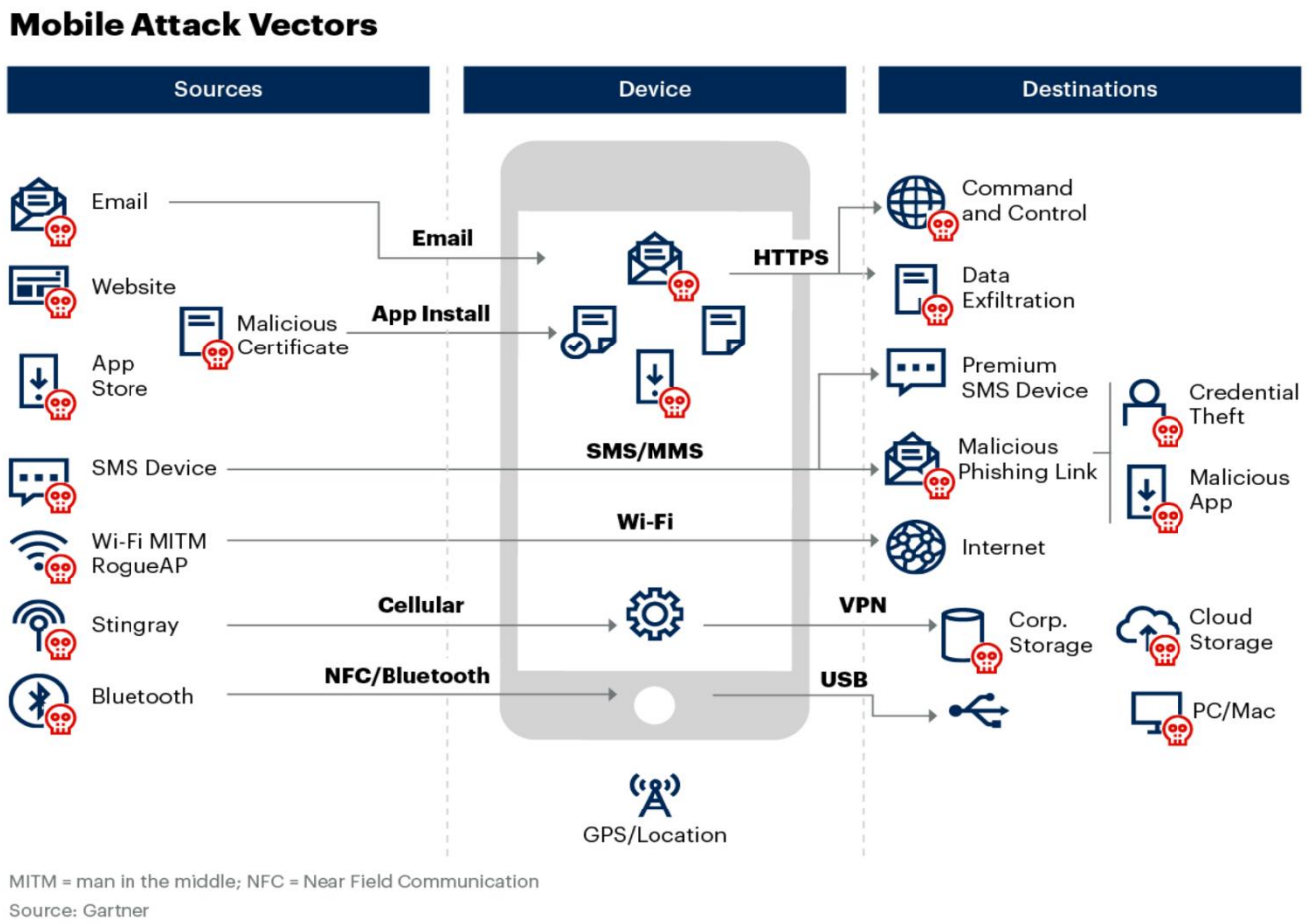
МОБИЛЬНЫЕ ШИФРОВАЛЬЩИКИ

‘Black Rose Lucy’ Вредоносный Ботнет с возможностью шифрования

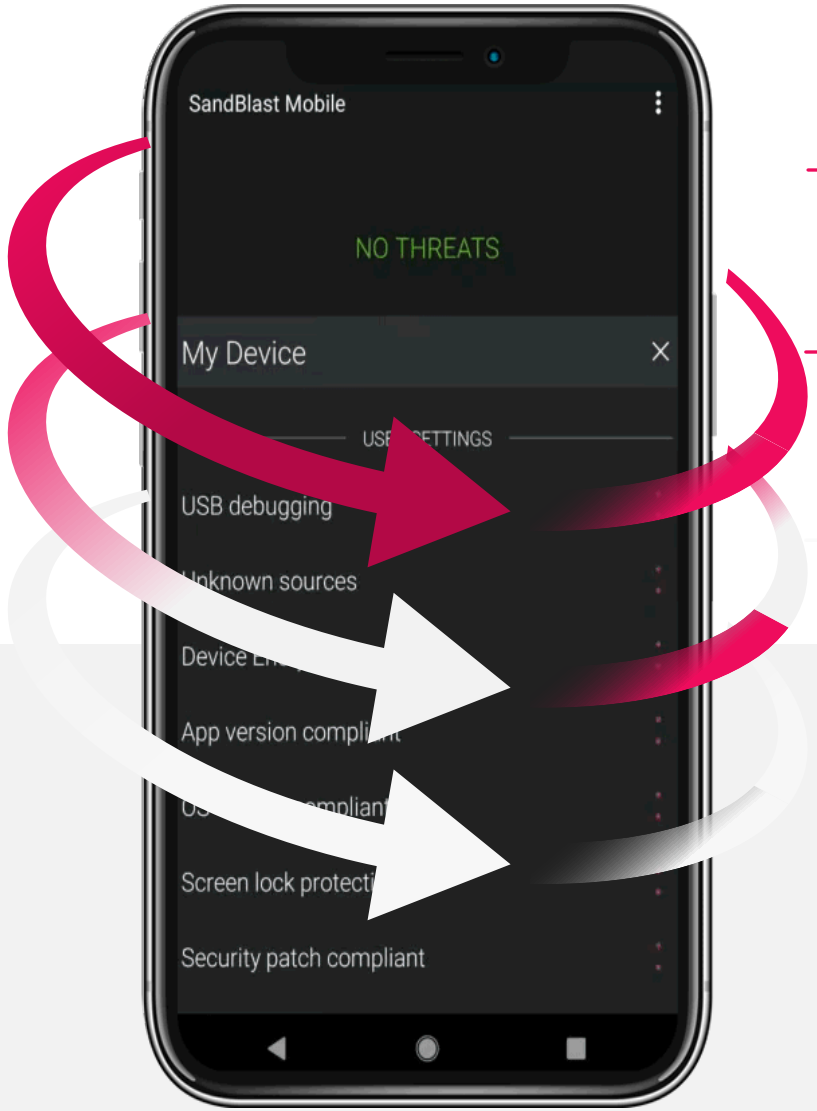
КРИТИЧЕСКИЕ УЯЗВИМОСТИ

Gartner описал техники взлома: **MOBILE THREAT DEFENSE (MTD)**

Класс решений MTD позволяет в полной мере защищать мобильные устройства, в отличие от UEM.



Защита на всех уровнях мобильного устройства



01 ПРИЛОЖЕНИЯ

02 СЕТЬ

03 УСТРОЙСТВО & ОС

Harmony Mobile

01
BEHAVIORAL RISK ENGINE

Real-time analysis
Malicious side-loading prevention
App vetting service

02
- Anti-phishing, safe browsing
- File reputation, sandboxing, CDR
- Conditional access
- Anti-bot
- URL filtering
- Protected DNS
- Wi-Fi security (MITM)

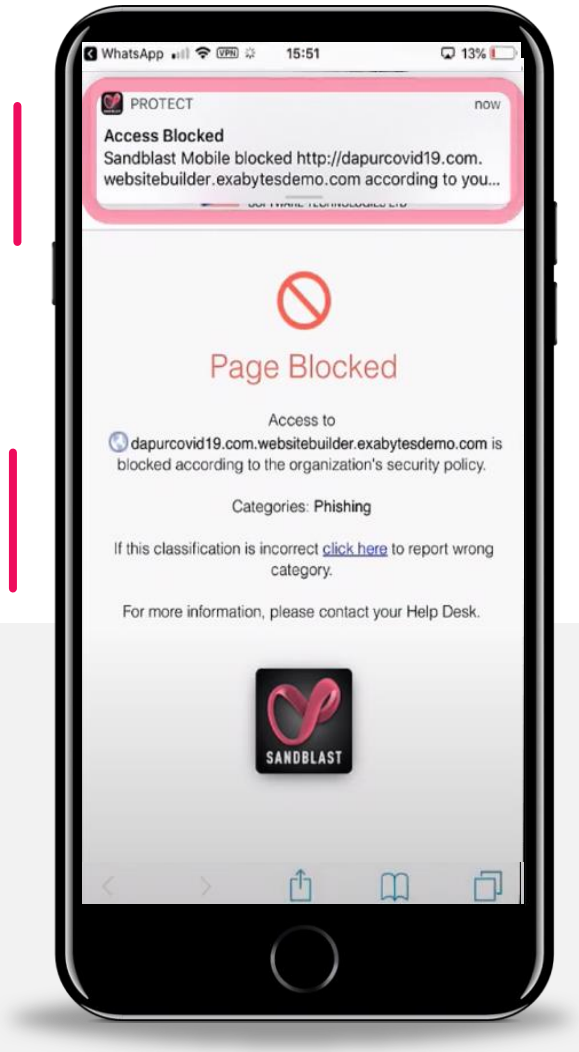
03
Device risk assessment:
- OS vulnerabilities
- Device-level exploits
- Risky configurations
- Advanced rooting
- Jailbreak detection

PHISHING PROTECTION

Предотвратить открытие вредоносных ссылок

Пользователь открывает ссылку

URL обнаружена как вредоносная и заблокирована



THREATCLOUD

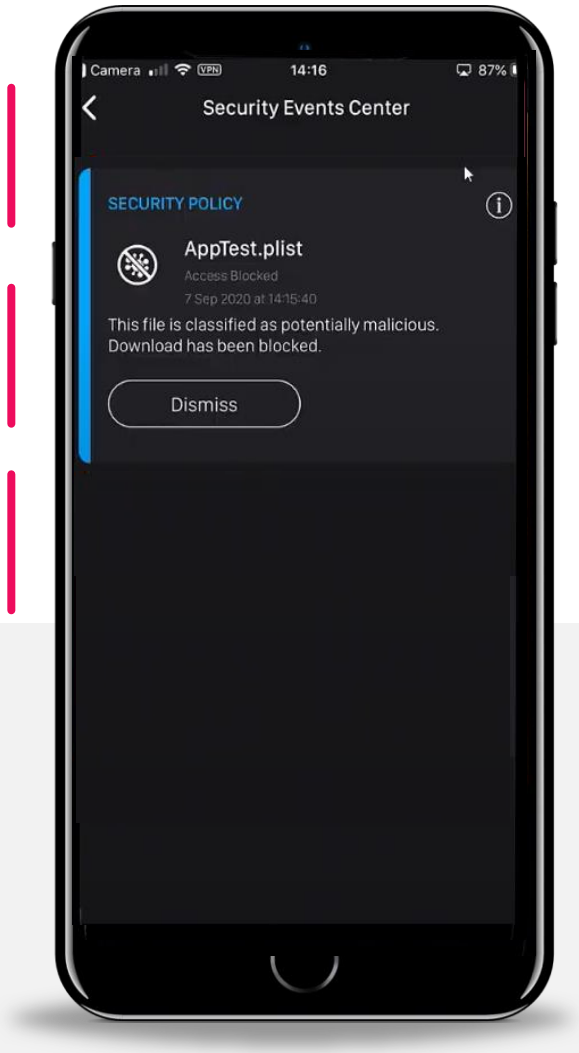
Anti-phishing движок постоянно анализирует ссылки

Сканирование загружаемых приложений

Пользователь пытается загрузить установщик через QR-код

Подозрительное содержимое блокируется

Отчет об инциденте предоставляется пользователю



FILE PROTECTION – AI POWERED ENGINES

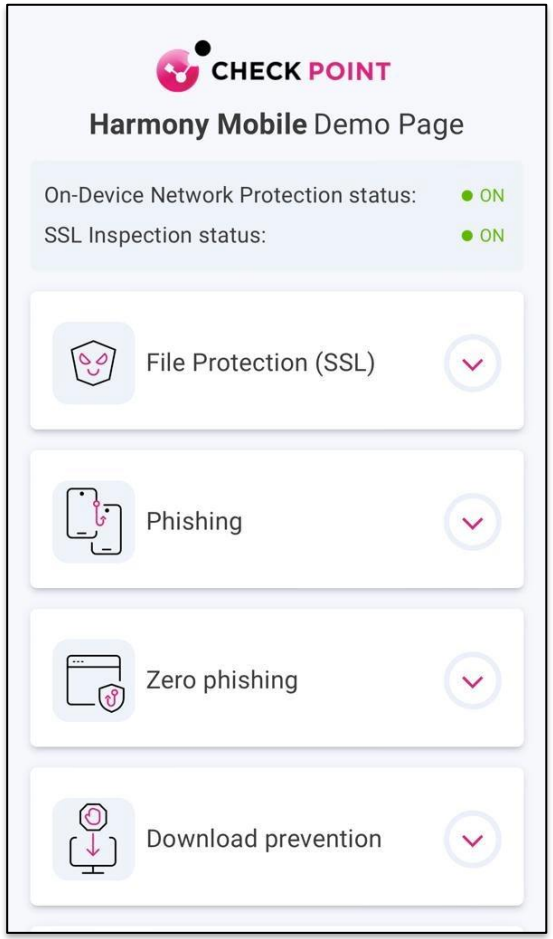
Пользователь пытается загрузить файл

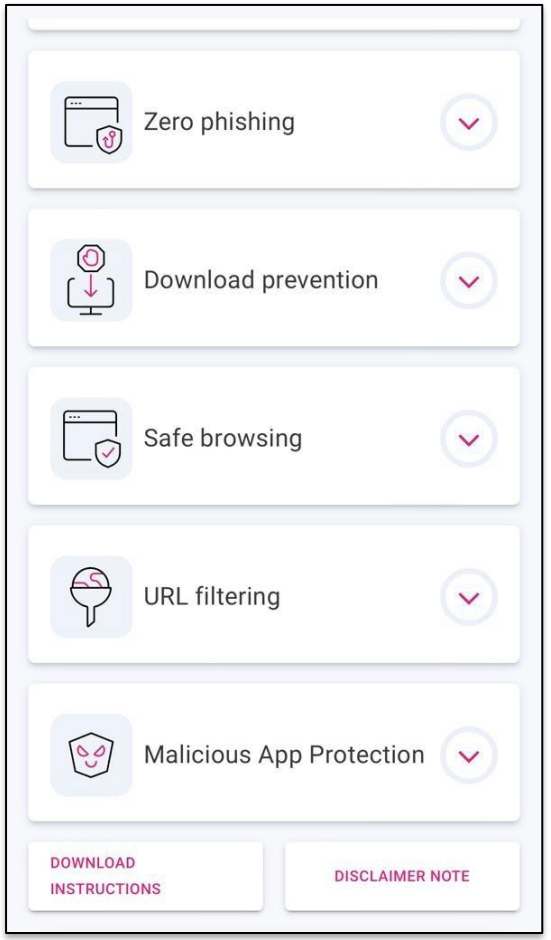
Файл перехватывается агентом

Файл загружается в облако для эмуляции

Информация по файлу у пользователя

Тестировать проще, отдельный портал





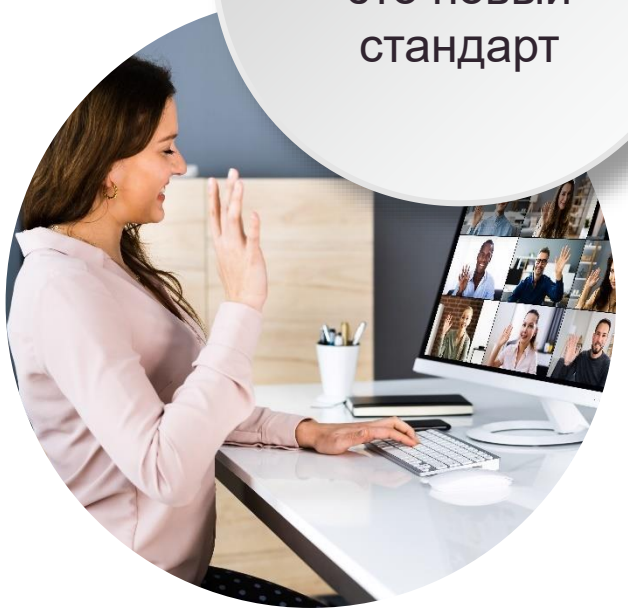
Проверь!

03

Harmony SASE Гибридный доступ к ресурсам

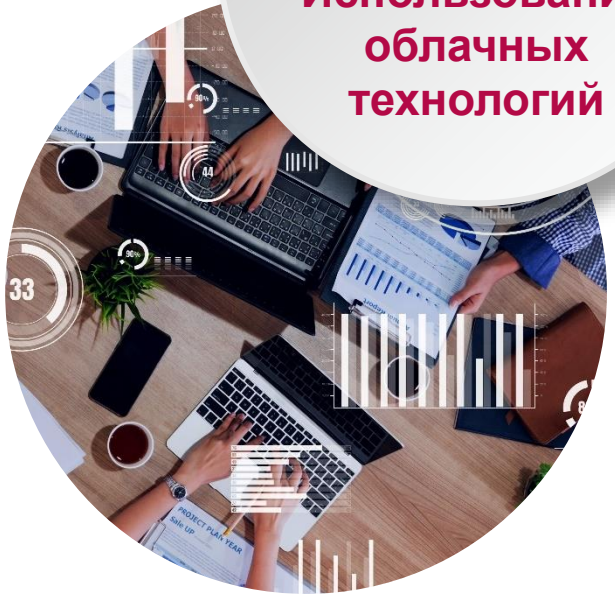
Интернет – это новая корпоративная сеть

Гибридная работа это новый стандарт



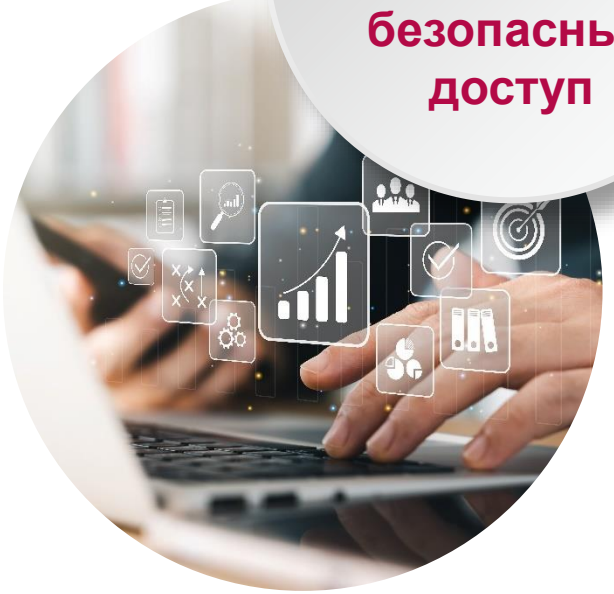
Цифровая трансформация

Использование облачных технологий



Организации необходим

Стабильный и безопасный доступ



Компании рассматривают Secure Access Service Edge (SASE) как решение для …

- Безопасный доступ в Интернет для пользователей с любых устройств
- Реализация концепции Zero Trust для доступа к приложениям
- Подключение филиалов в единую корпоративную сеть с оптимизацией пропускной способности

Быстро и гибко внедряется силами ИБ-отдела

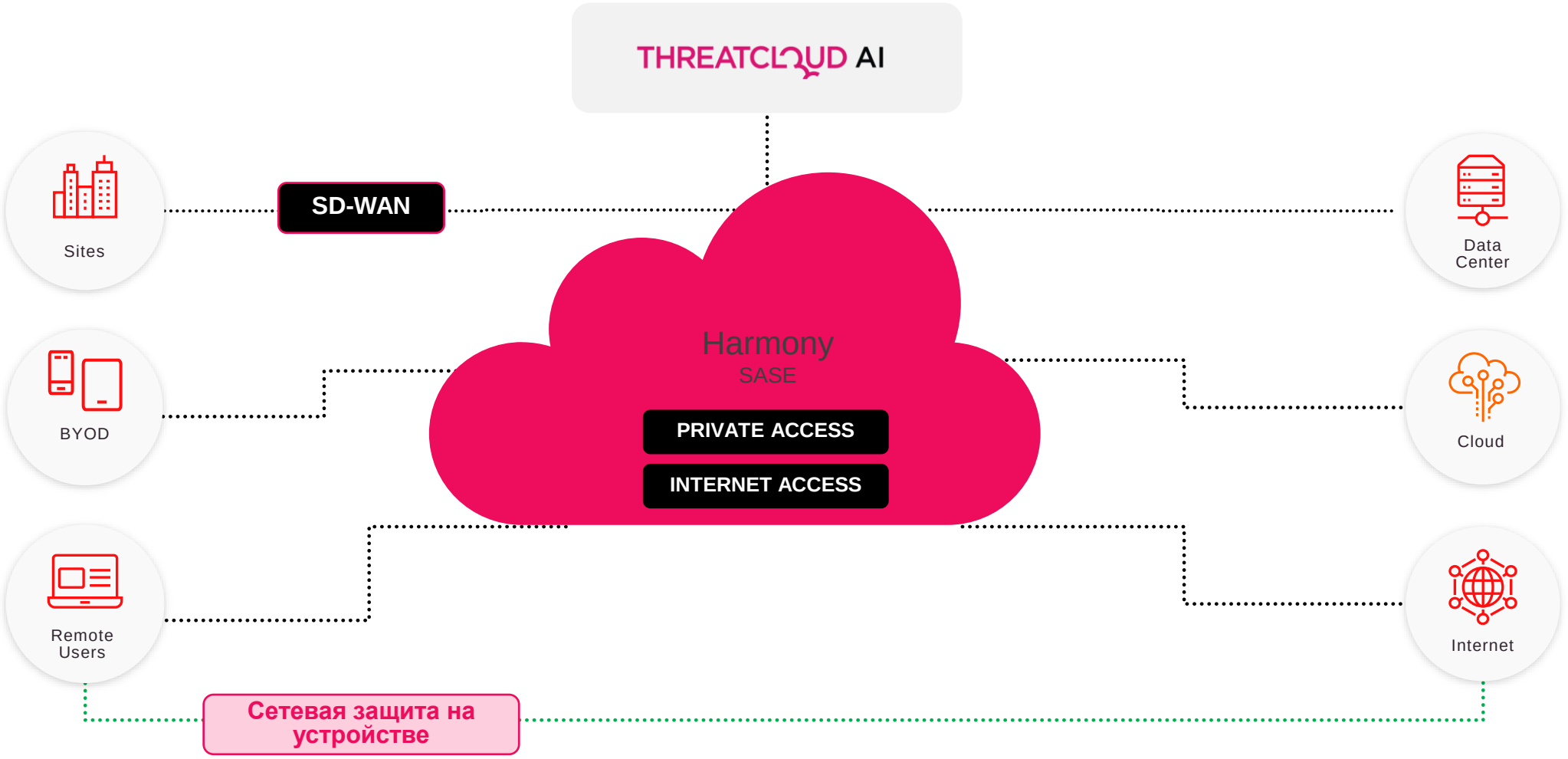
Текущие SASE решения **обладают рядом проблем**

Инспекция трафика только в облаке влияет на приватность, задержки.

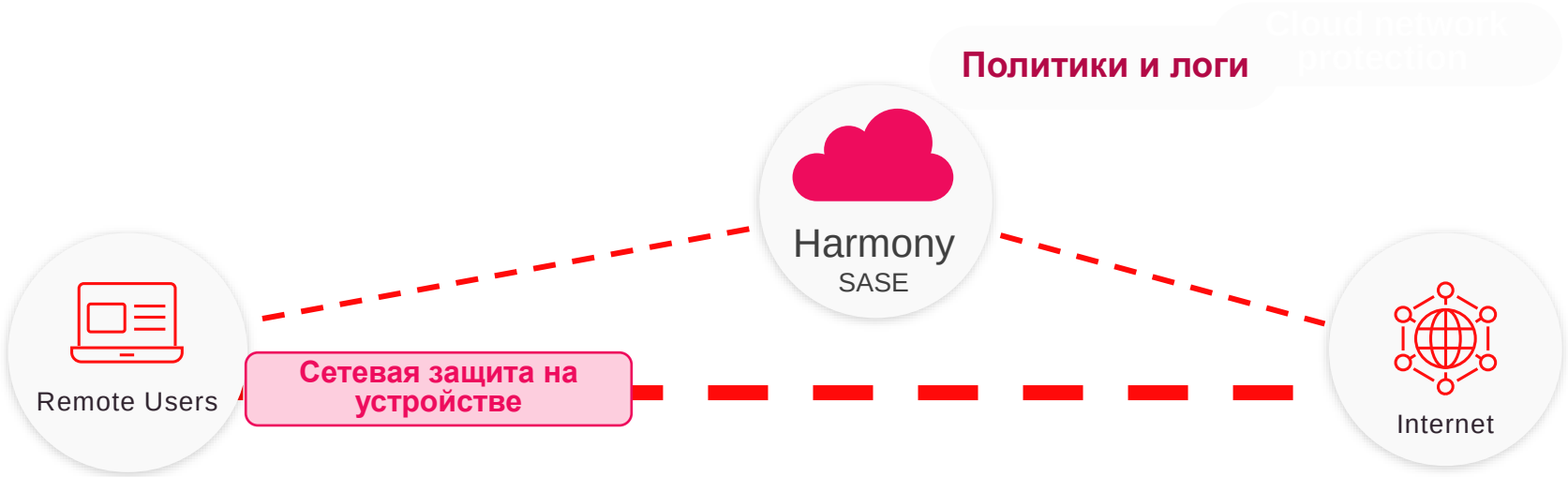
Этап развертывания, децентрализованное управление с помощью нескольких консолей

Безопасность устройства и процесса получения доступа

SASE от Check Point с единым управлением и Threat Prevention



Инспекция трафика с помощью агента



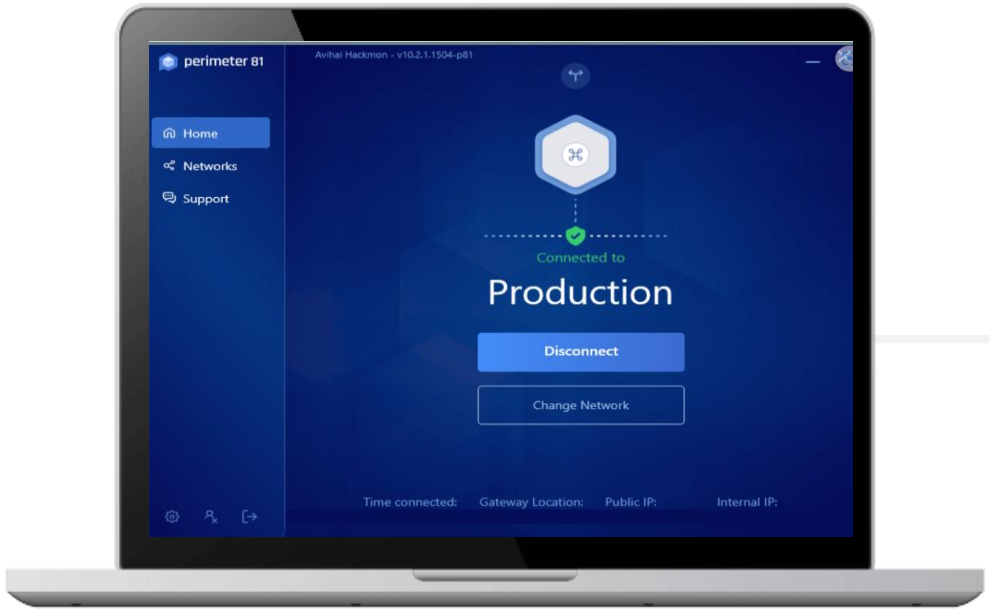
Пользователи и их приватность

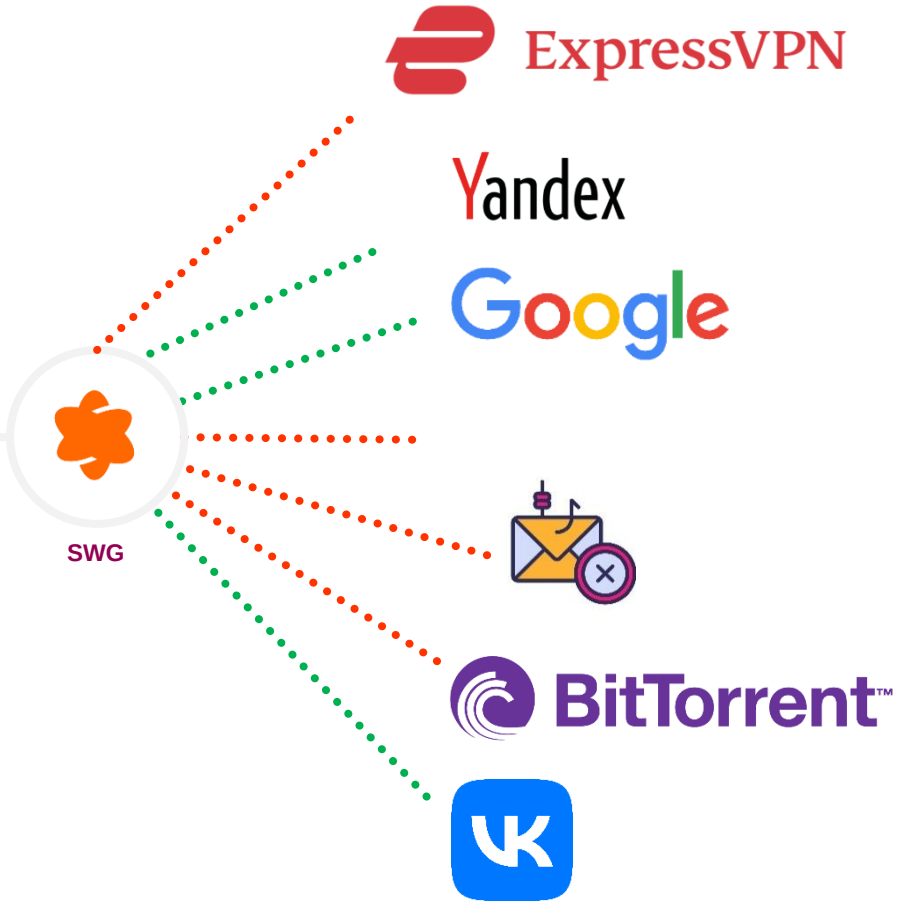
- On-device network protections
  Трафик не маршрутизируется в Интернет для инспекции

Движки защиты

- HTTPS инспекция
- Web / DNS фильтрация
- Антивирус
- Защита публичных Wi-Fi

Сценарий использования Internet Access





SWG – правила, агент – обработка трафика

Пользователи

- BYOD
- Контракторы
- Аутсорсеры

Платформы

- Windows
- Mac OS
- Linux
- Android
- iOS

Возможности

- Контроль трафика
- Bypass
- Двухфакторная аутентификация

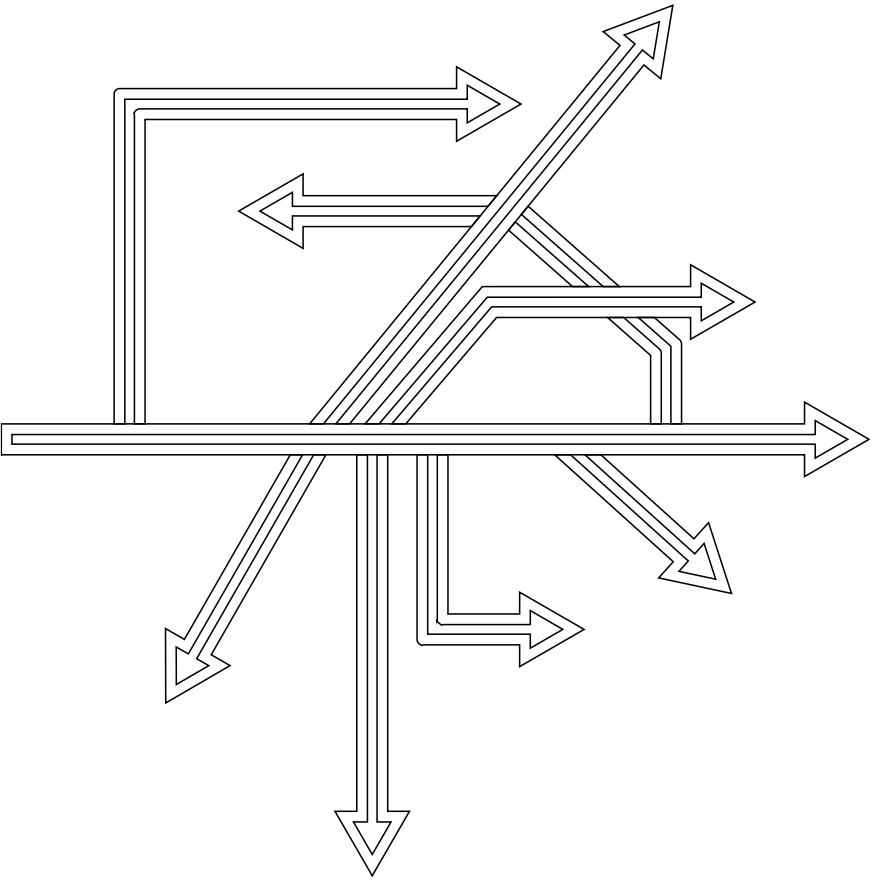
Безопасный доступ к любому сетевому ресурсу компании

Zero Trust

Full Mesh Network

Гибкий доступ

Концепция Zero Trust



Обеспечьте доступ к приложениям с минимальными привилегиями

- В зависимости от User Identity
- В зависимости от Device Posture

Подключите всех пользователей и их устройства

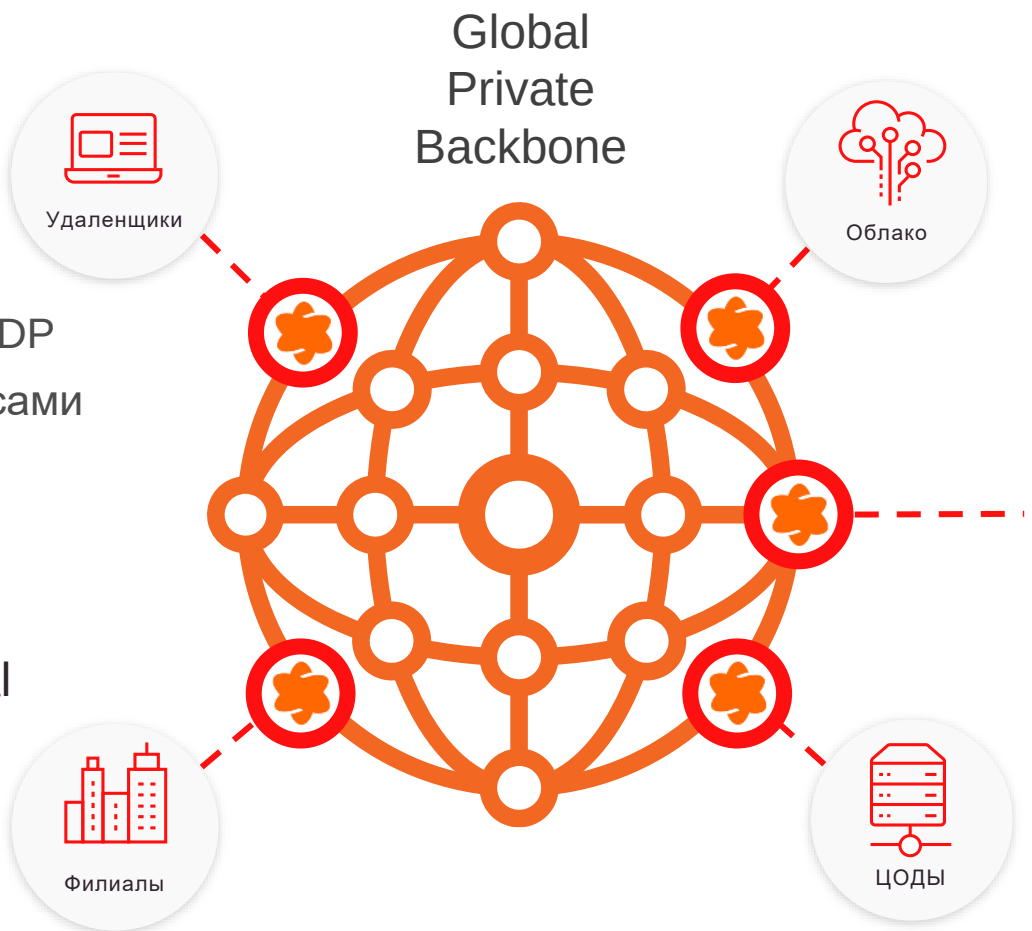
- Легкий агент для всех платформ
- Альтернатива – доступ в браузере (HTTPS)

Сократите площадь атаки

- Сетевая сегментация
- Обфускация трафика

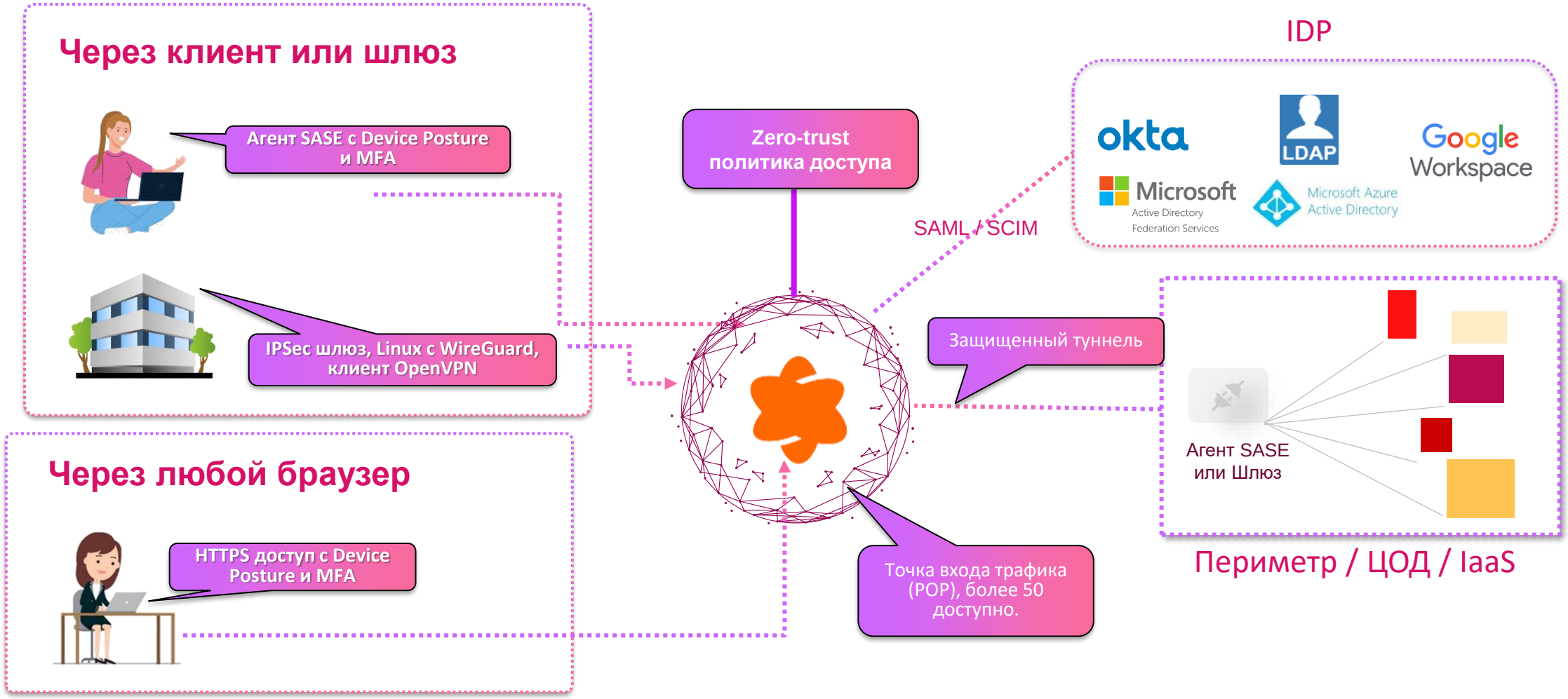
Гибридная схема подключения Full Mesh

- Full mesh **т.е каждый с каждым**
  - сотрудник IT подключается к персоналу по RDP
  - организация VoIP между филиальными офисами
  - обмен трафиком между серверами компании
- Гибкая альтернатива классическому S2S
- Высокая производительность через global private backbone



⚠ *Другие вендоры не предлагают Full Mesh подключение*

Сценарий использования Private Access (Remote Access)



04

Horizon XDR
Центр мониторинга и реакции на атаки

Много срабатываний – много работы. Как увидеть инцидент в целом?

Необходимо коррелировать события и классифицировать по критичности – не пропускаем важное!

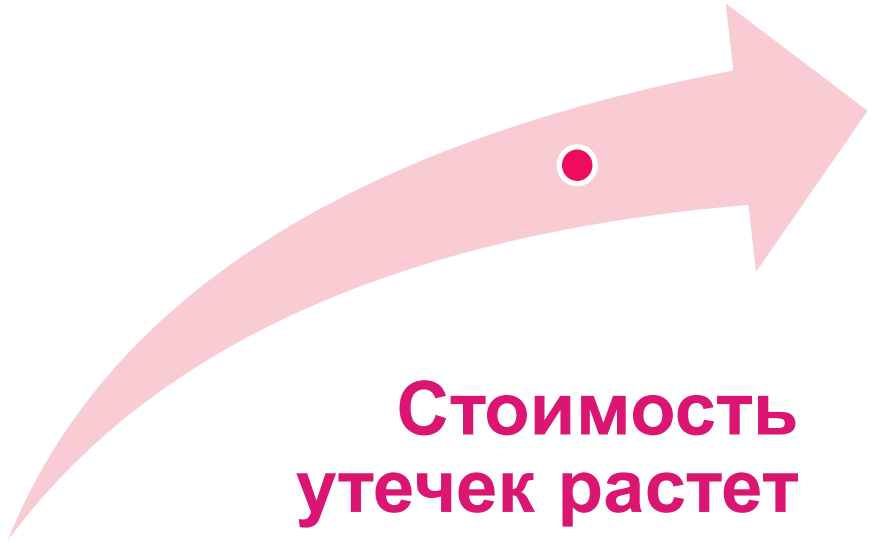
*(IBM report 2021)

Угроза может долго оставаться незамеченной

277 дней может пройти до обнаружения

Необходимо останавливать атаки до распространения!

- Много ложных срабатываний
- Разные инструменты
- Не хватает контекста
- Не хватает спецов/знаний

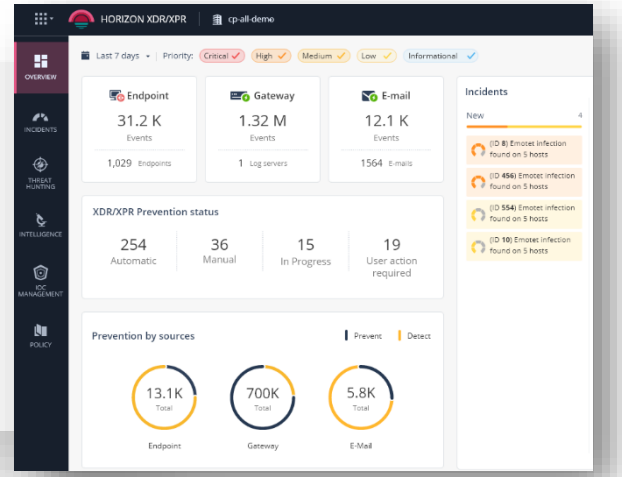


Стоимость утечек растет

*(IBM report 2021)

Подход «Предотвращение прежде всего»

Предотвращение угроз
по всей инфраструктуре **благодаря продвинутой** корреляции



CloudGuard
Secure the Cloud

Quantum
Secure the Network

Harmony
Secure Users & Access

aws
Azure
Microsoft Active Directory

Microsoft Defender
Azure Active Directory

Office 365
Google Workspace
slack
Dropbox

XDR – в чем ценность для заказчиков?

- **XDR** с момента начала разработки – ориентирован на предотвращение угроз
- **Полноценная работа** с любыми источниками данных - сеть, облако, эндпойнт, мобильное устройство, почта
- **ThreatCloud** – глобальная база данных угроз
- **Немедленное распространение IOC** по всем подключенным продуктам
- **Встроенные** реакции и плейбуки
- **Возможно** использовать даже заказчикам, имеющим только шлюзы

Комплексная защита от угроз

XPR позволяет предпринимать действия немедленно

Интеграция со шлюзами, эндпойнтами, защитой почты

Статусы реакций и источники

Новости и расследования CP<R> - персонализация

Итоги

- Реализация безопасности устройств и их удаленного доступа сложный и комплексный процесс
- Минимум доверия, максимум проверок
- Каждый продукт доступен для пилота
- Russia@checkpoint.com

CHECK POINT™

Спасибо за внимание!

YOU DESERVE THE BEST SECURITY