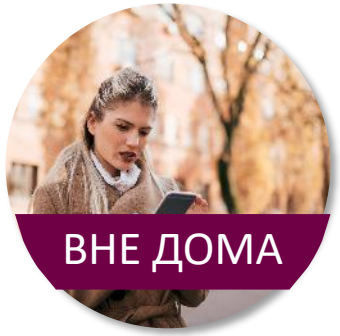
Семейства Harmony & CloudGuard в 2023 году

CPX Afteparty Partners

Турков Никита | Инженер Безопасности

nikitat@checkpoint.com

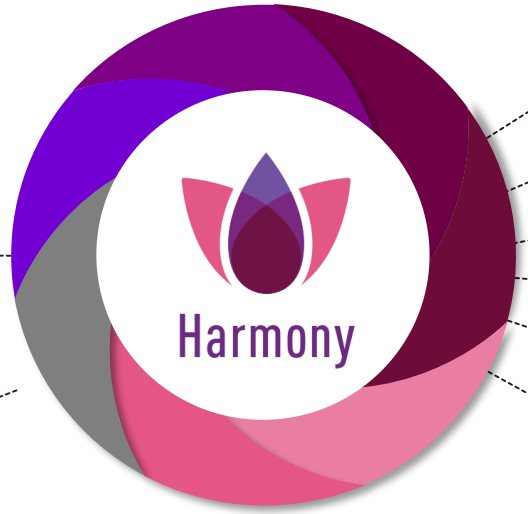
Защита пользователей и их устройств



1 Endpoint Security

2 Cloud-delivered Network Security (SASE)

3 Clientless Zero Trust Access (ZTNA)



4 Email & Office Security

5 Secure Internet browsing

6 Mobile Security

ВЕБ

WWW

ОБЛАКО

SAAS

CLOUD

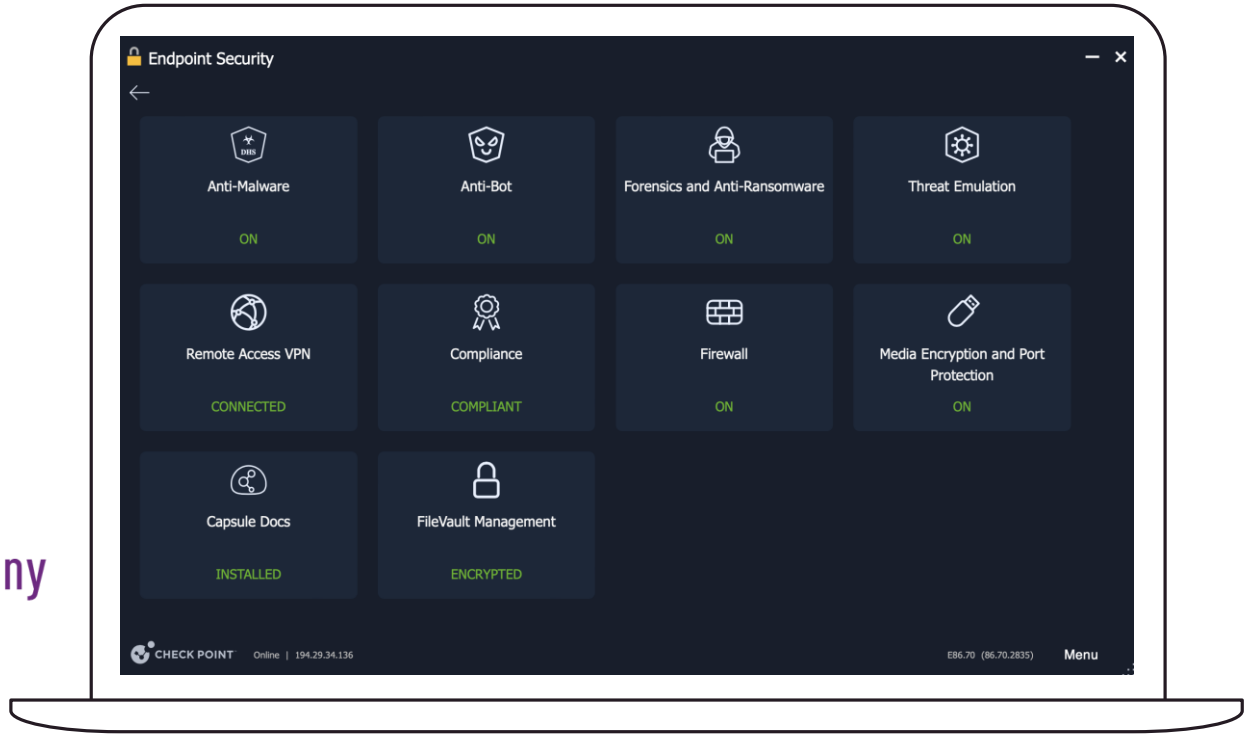
DATACENTER

ЛОКАЛЬНО

REMOTE DESKTOP

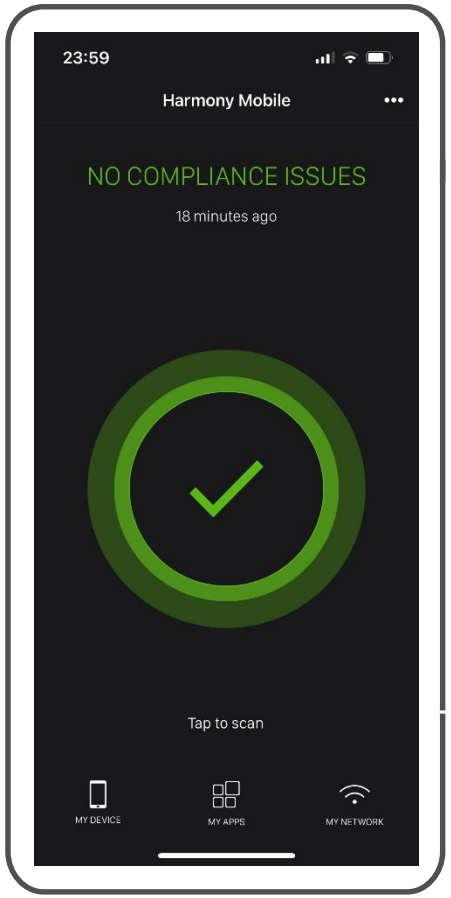
INTRANET

Агенты для защиты от атак 0-дня и других угроз



Harmony Endpoint

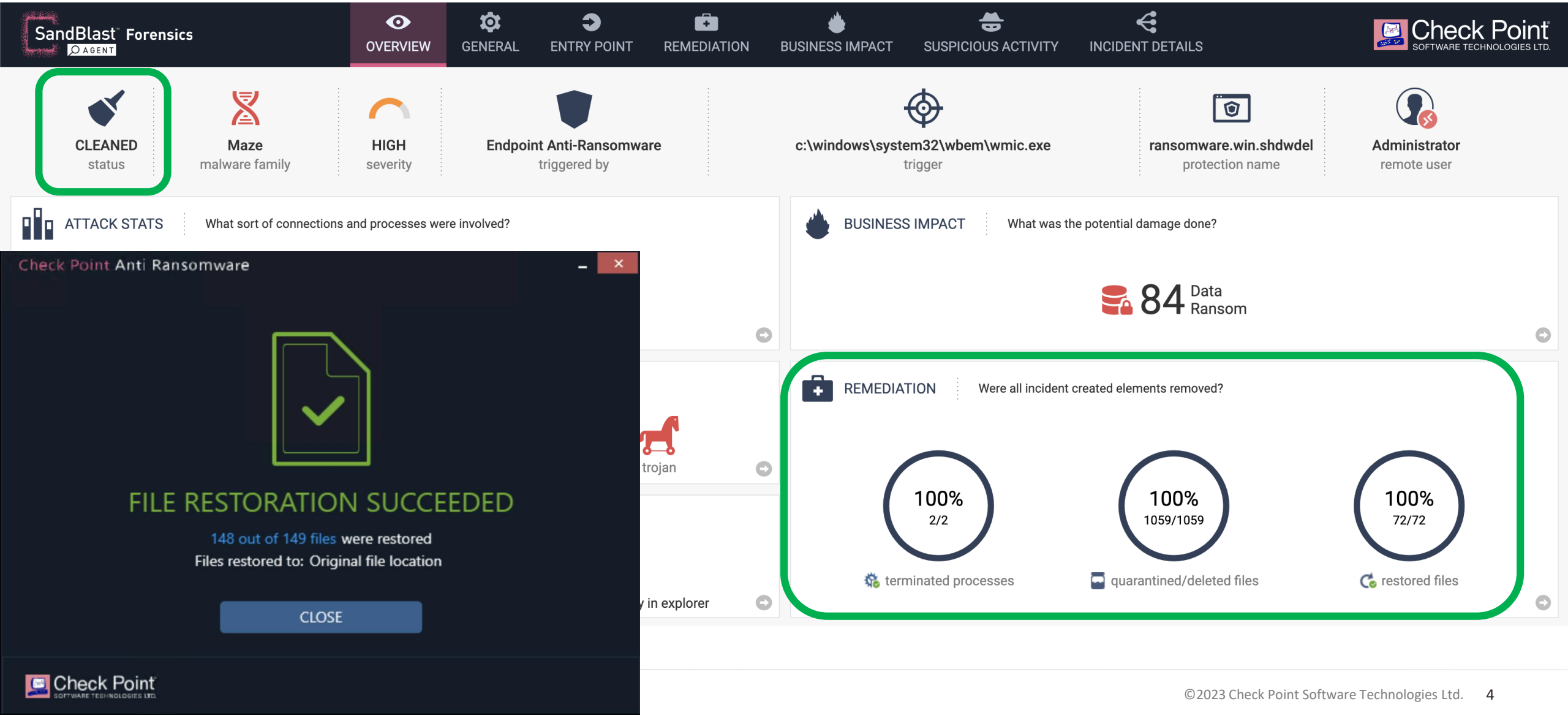
Windows (+Server), Mac OS X, VDI, TS, Linux*



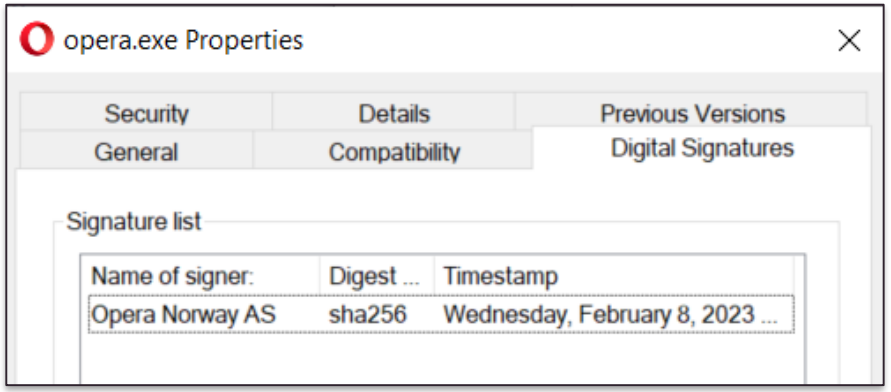
Harmony Mobile

iOS, Android

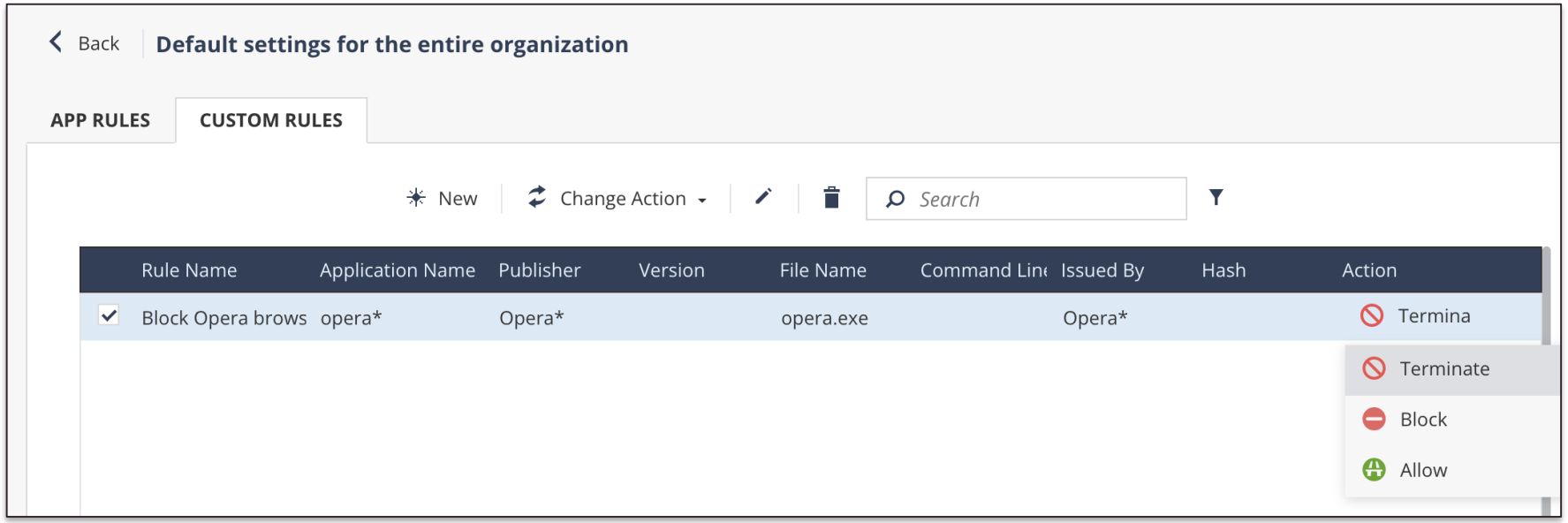
Автономная работа и отчеты для инцидентов



Новое: Application Control с Wildcard



- ✓ Блокировка всех версий одного приложения (например уязвимый браузер)
- ✓ Блокировка всех приложений от одного издателя



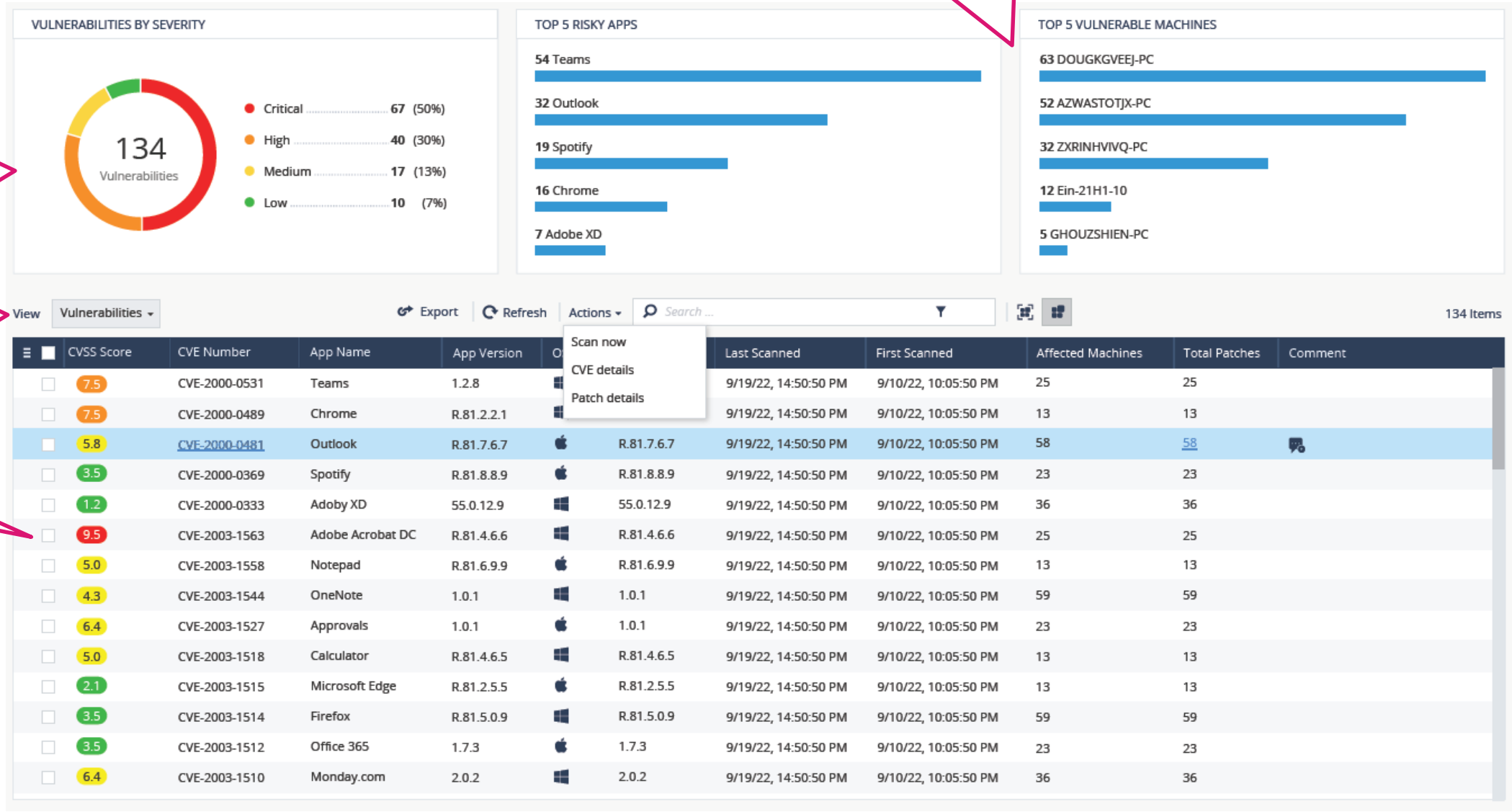
Новое: Posture Management

Фокус на наиболее уязвимые хосты в компании

Фокус на наиболее опасные уязвимости

Просмотр всех уязвимостей внутри организации

Сортировка по CVSS

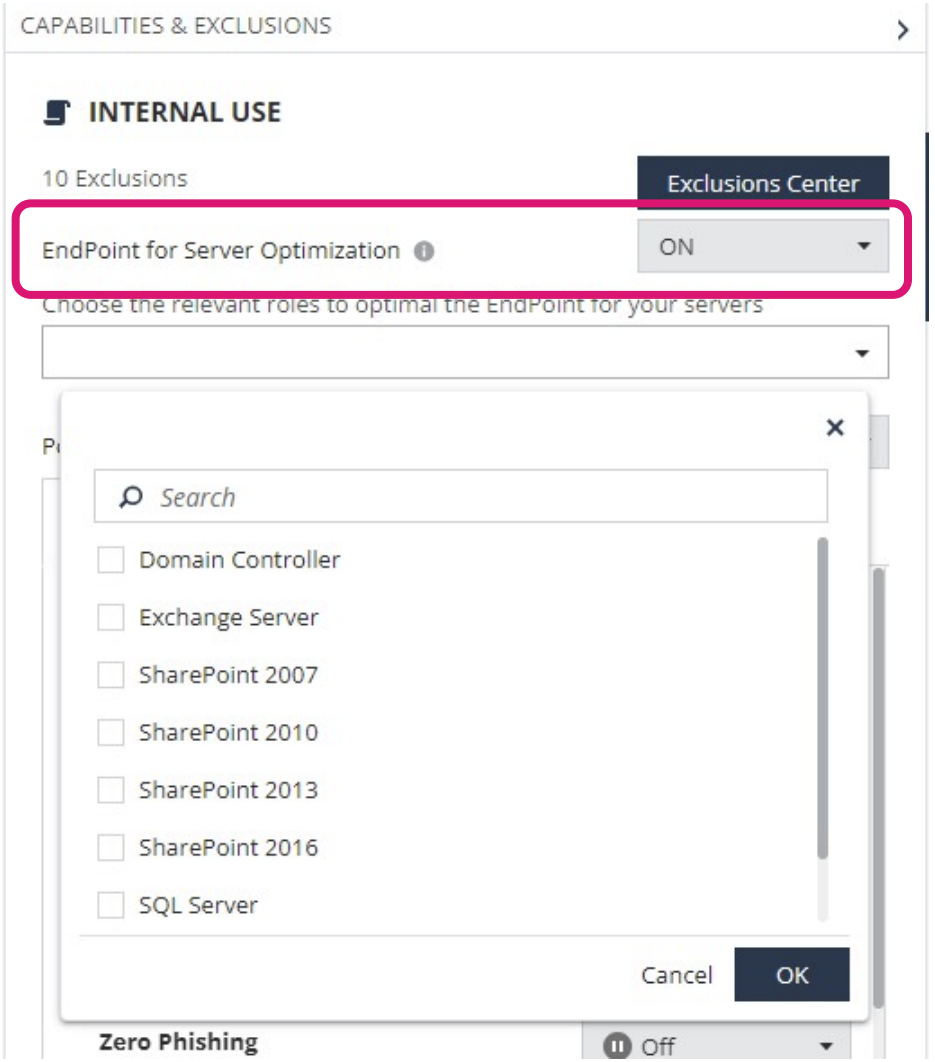


CVSS Score	CVE Number	App Name	App Version	OS		Last Scanned	First Scanned	Affected Machines	Total Patches	Comment
7.5	CVE-2000-0531	Teams	1.2.8			9/19/22, 14:50:50 PM	9/10/22, 10:05:50 PM	25	25	
7.5	CVE-2000-0489	Chrome	R.81.2.2.1			9/19/22, 14:50:50 PM	9/10/22, 10:05:50 PM	13	13	
5.8	CVE-2000-0481	Outlook	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	

Новое: оптимизация работы для серверных ОС

HEP веб-консоль предоставляет профили серверов с автоматическими Threat Prevention исключениями:

- Microsoft Exchange Server
- Microsoft SQL Server
- SharePoint Server
- Microsoft IIS
- Active Directory Server
- Terminal Server…



Запланировано добавить в On-Prem Q2-2023.

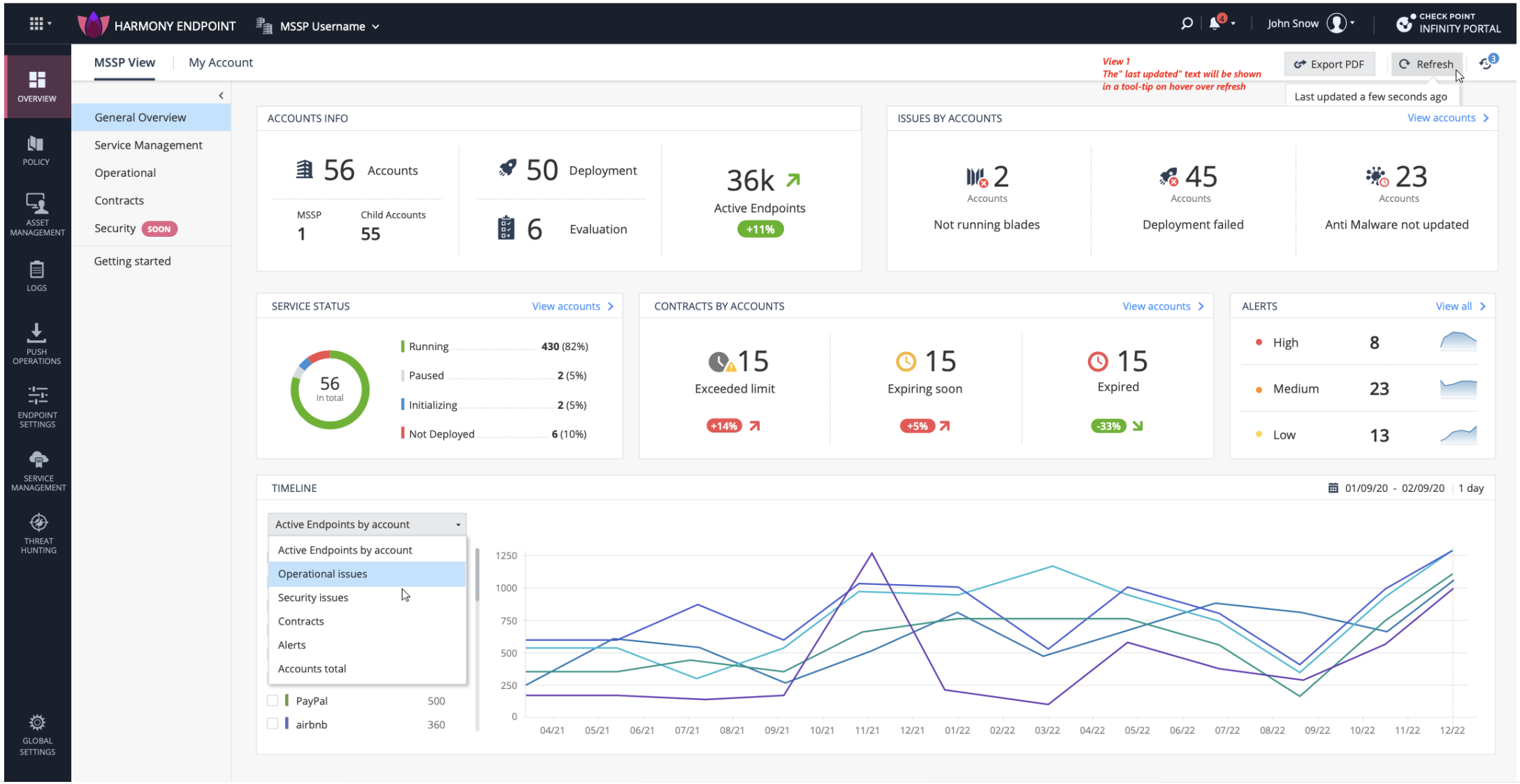
Сейчас можно добавлять из SK.

Feature type	Feature	Data Protection	Prevent	Basic	Advanced	Complete
Management	On-Premise Management Console	+	+	+	+	+
	Cloud Management Console	+	+	+	+	+
Threat Intelligence	Threat Cloud		+	+	+	+
	IOC Management		+	+	+	+
Access Control	Firewall	+	+	+	+	+
	Application Control	+	+	+	+	+
	Endpoint Compliance	+	+	+	+	+
	Remote Access VPN	+	+	+	+	+
Threat Prevention	Anti-Ransomware		+	+	+	+
	Anti-Bot		+	+	+	+
	Anti-Exploit		+	+	+	+
	Anti-Malware		+	+	+	+
	Behavioral Guard		+	+	+	+
	Port Protection	+	+	+	+	+
Attack Investigation	Forensic collection & Automated reports		+	+	+	+
	MITRE Mapping		+	+	+	+
Web Protection	Zero Phishing		-	+	+	+
	URL Filtering		-	+	+	+
	Corporate password reuse		-	+	+	+
	Safe Search		-	+	+	+
Threat Hunting	Threat Hunting		-	+	+	+
Sandboxing	Threat Emulation		-	-	+	+
	Threat Extraction & Sanitization		-	-	+	+
Data Protection	Full Disk Encryption	+	-	-	-	+
	Removable Media Encryption	+	-	-	-	+

Новый вид лицензий:
CP-HAR-EP-PREVENT

Уже доступен в каталоге!

Harmony Endpoint MSSP в Infinity Portal (EA)



Q1 2023

Best Security

- **Server Security**
- **Static analysis:**
  - ML-model for MS Office documents
- **Anti-Ransomware 2.0**
- **HTTPS inspection** (private EA)
- **E2 AM engine offline updater**
- **Web Protection:**
  - Threat Prevention for uploaded files
  - Zero Phishing – local HTML-files inspection

EDR & XDR

- **Advanced IOC Management**
- **APIs:**
  - External APIs for on-prem
  - MSSP related APIs

Posture Management

- **Vulnerability Management** (GA)
- **Patch Management** (EA)
- **Performance Diagnostics**

Q2 2023

Best Security

- **Server Security**
- **Static analysis:**
  - ML-model for PDF
- **Anti-Ransomware 2.0:**
  - Intel TDT – GPU integration
- **New remediation actions:**
  - Collect dump of process
- **Endpoint DLP:**
  - Upload & download protection (Detect & Prevent)
  - Copy-paste restriction
  - Block Print
  - Block Screenshot

EDR & XDR

- **Incident Management**
- **Research Intelligence**
- **Ticketing Management**
- **Interactive remote shell**

Posture Management

- **Patch Management** (GA)
- **Application Control**
- **Threat Hunting**

Q3 2023

Best Security

- **Server Security**
- **Static analysis:**
  - MacOS support
- **HTTPS inspection** (GA)
- **E2 AM engine feature parity**
- **Web Protection:**
  - One-time link protection
  - Block Incognito
  - HTML Smuggling

EDR & XDR

- **APIs:**
  - SDK
  - Vulnerability management
  - Audit logs

Posture Management

- **Zero-Trust Posture Management** (EA)

Q4 2023

Best Security

- **Server Security**
- **Static analysis:**
  - ML-model for HTML
- **Developer & CI/CD protection**
- **TCP/UDP protection**
- **Web Protection**

EDR & XDR

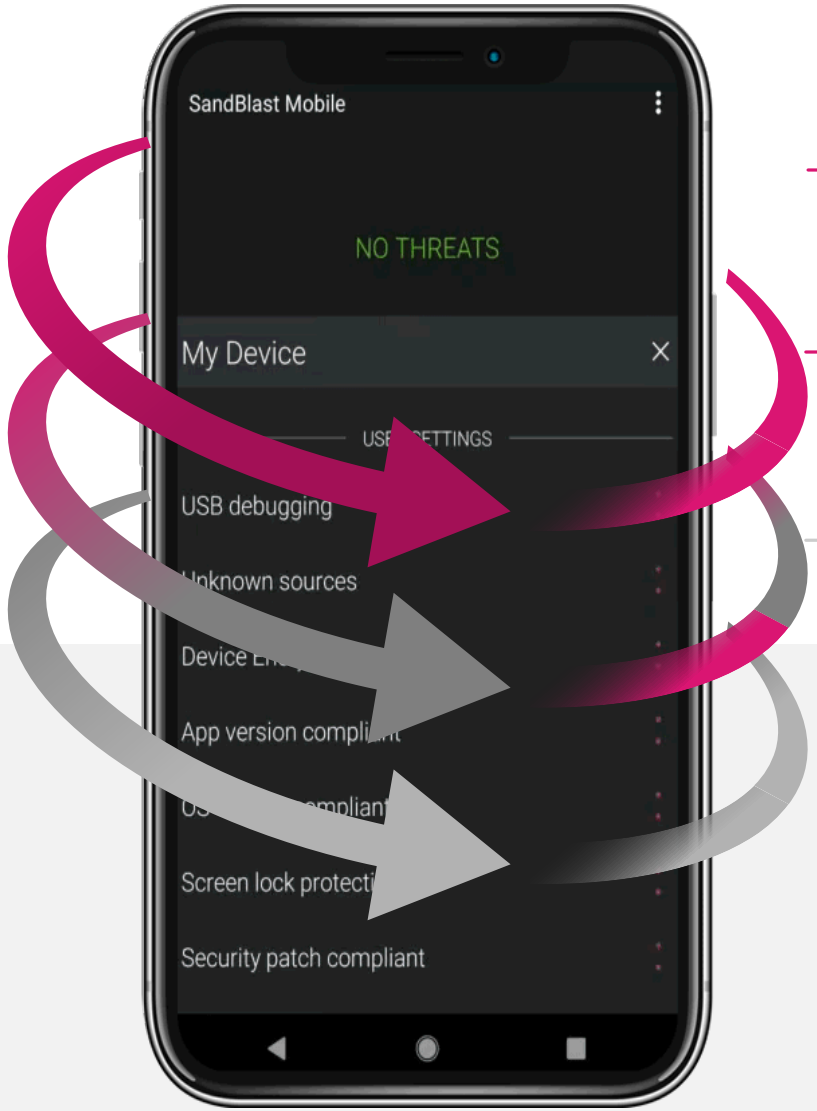
- **TBD**

Posture Management

- **Zero-Trust Posture Management** (GA)

Subject to change and may be changed by Check Point for any reason without notice

Мобильные устройства требуют защиты



01 ПРИЛОЖЕНИЯ

02 СЕТЬ

03 ОПЕРАЦИОННАЯ СИСТЕМА

Harmony Mobile MTD

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

Проверка файлов внутри приложений

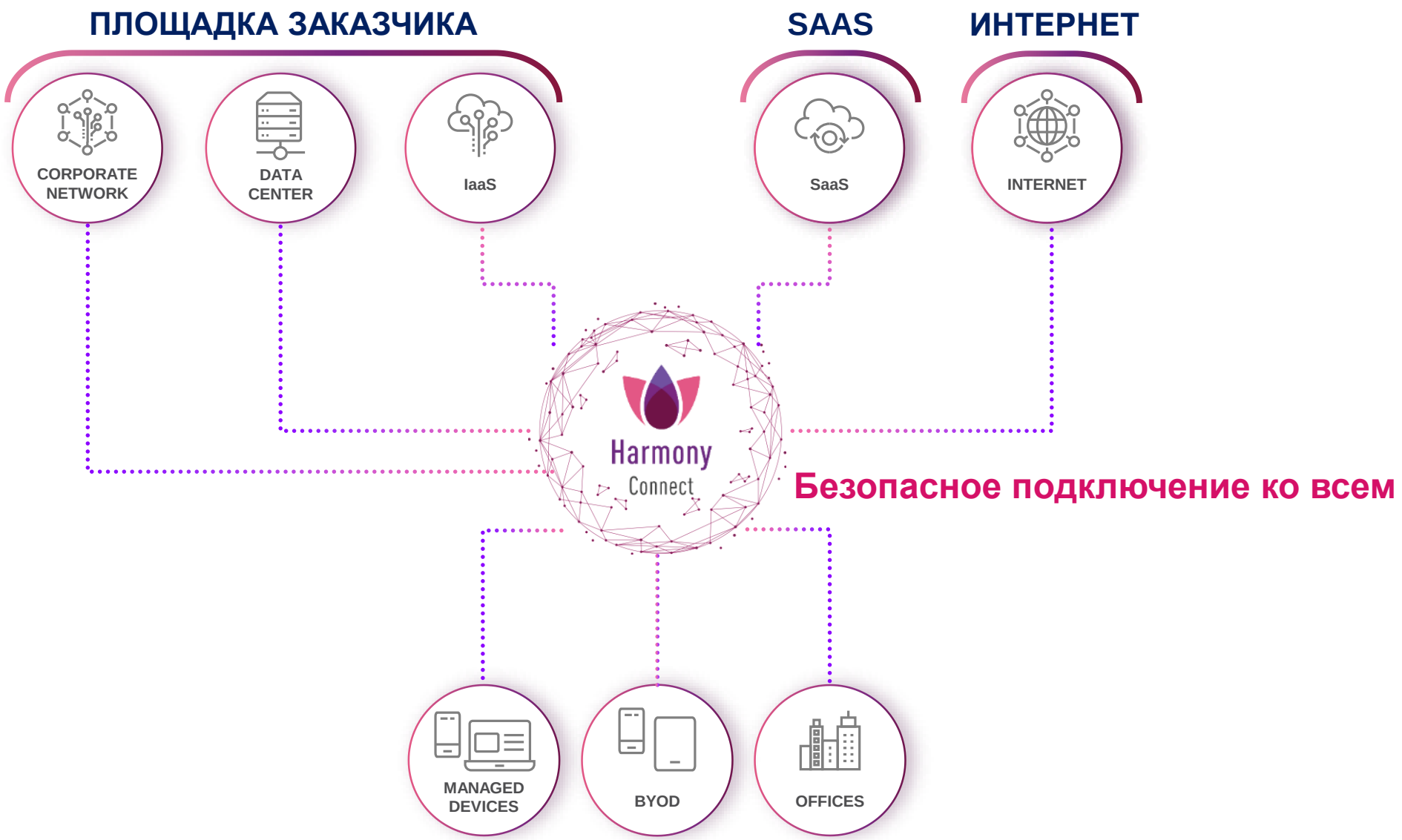
Пользователь хочет загрузить файл

Файл начинает загружаться

Файл отправляется на эмуляцию

Детали отчета доступны пользователю

Шлюз для пользователей вне периметра



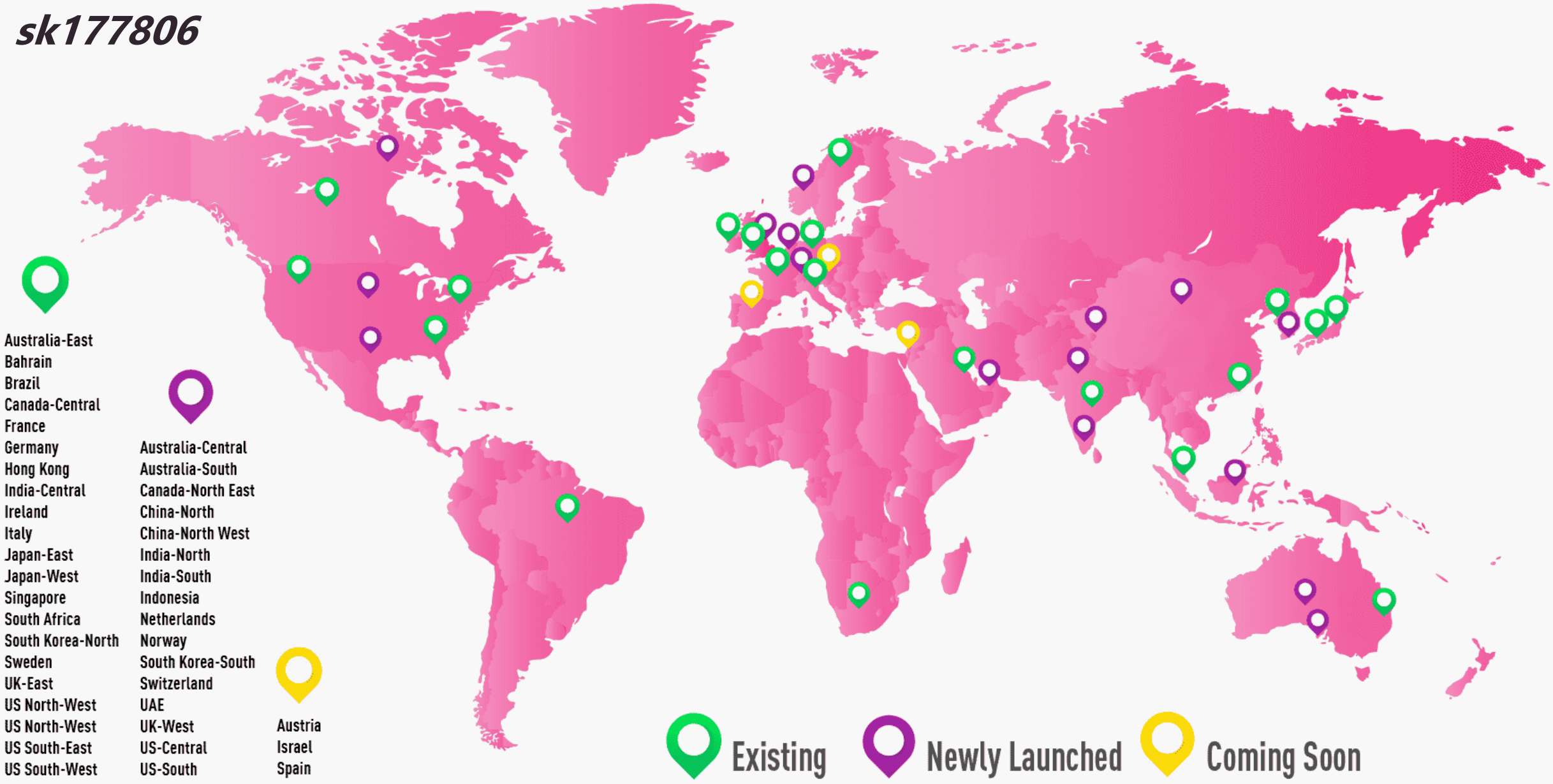
Безопасное подключение ко всем

Harmony Connect's Global PoPs

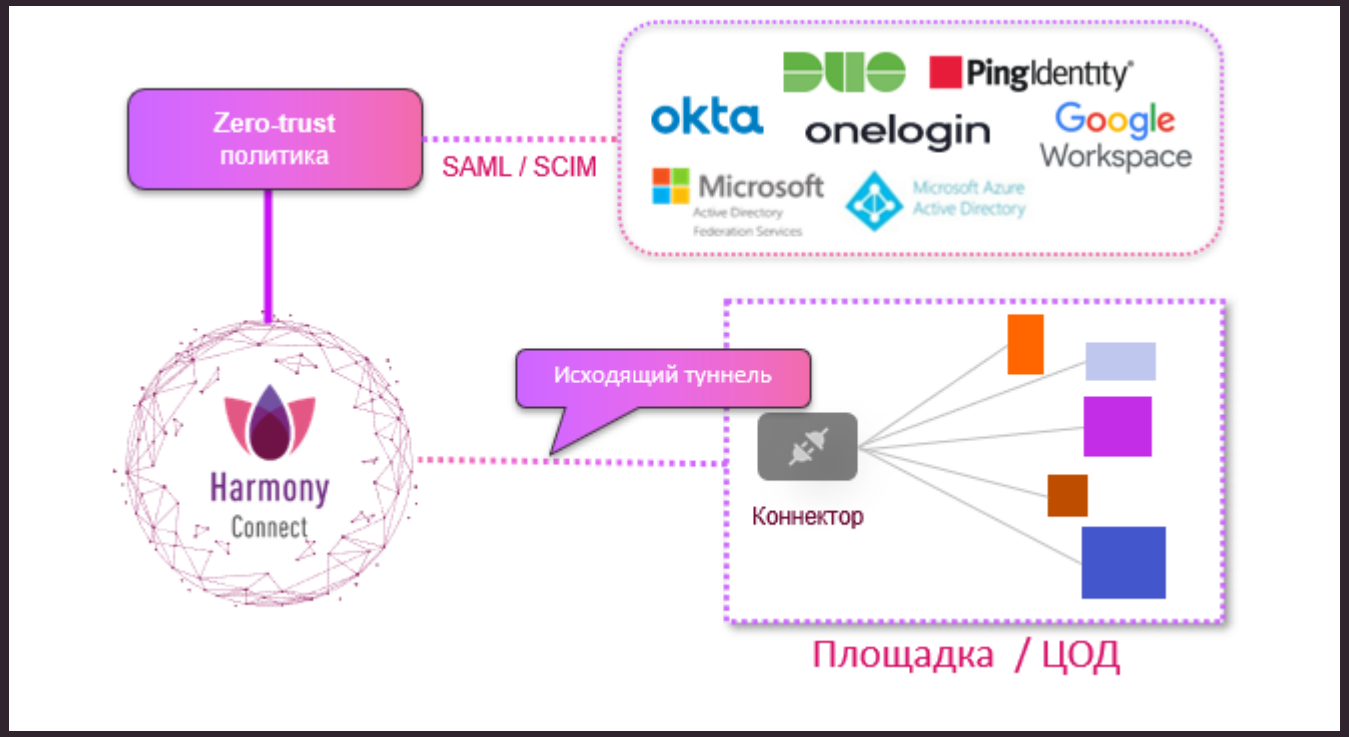
Harmony Connect (SASE)

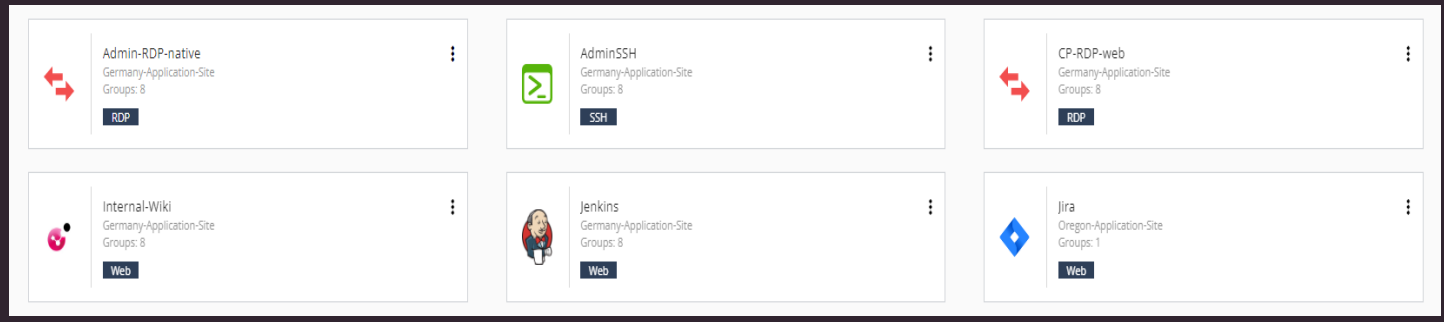
CHECK POINT
YOU DESERVE THE BEST SECURITY

sk177806



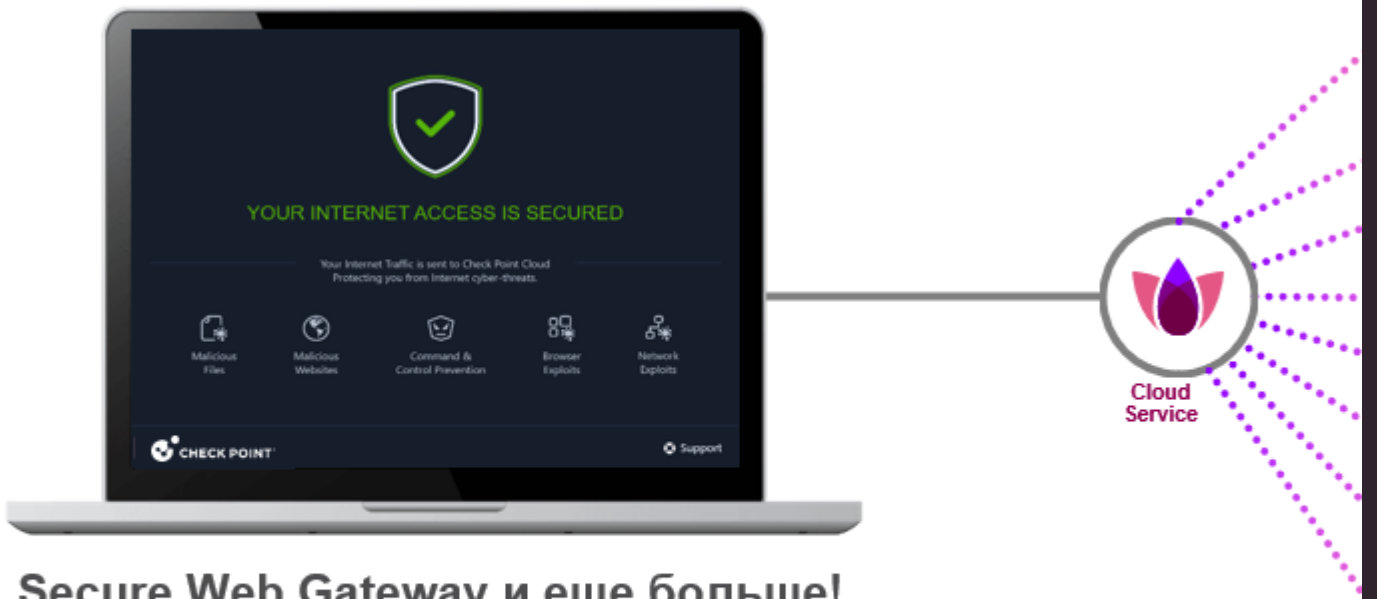
Harmony Connect: Remote Access





- Публикация ресурсов

Harmony Connect: Internet Access



Secure Web Gateway и еще больше!

Threat Prevention

- Zero-day sandboxing
- Intrusion Prevention System (IPS)
- Phishing prevention
- Malware and C2 bot prevention
- Inspects all ports & protocols (!)

Access Control

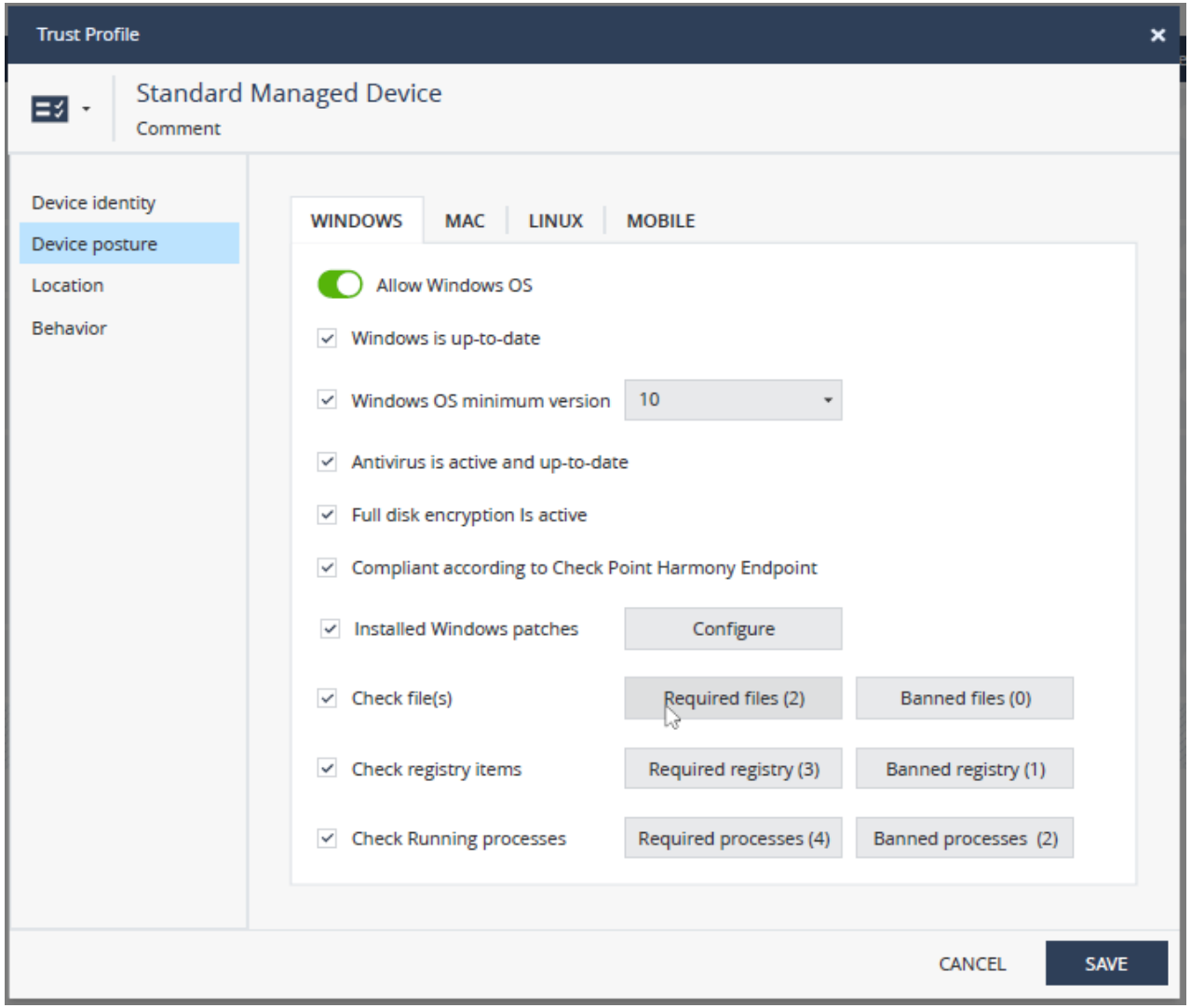
- Cloud Firewall
- URL Filtering
- Application Control

Data Protection

- Cloud DLP
- Granular policy
- Predefined data types

- Шлюз как сервис

Новое: Security Posture Validation



Фаза 1

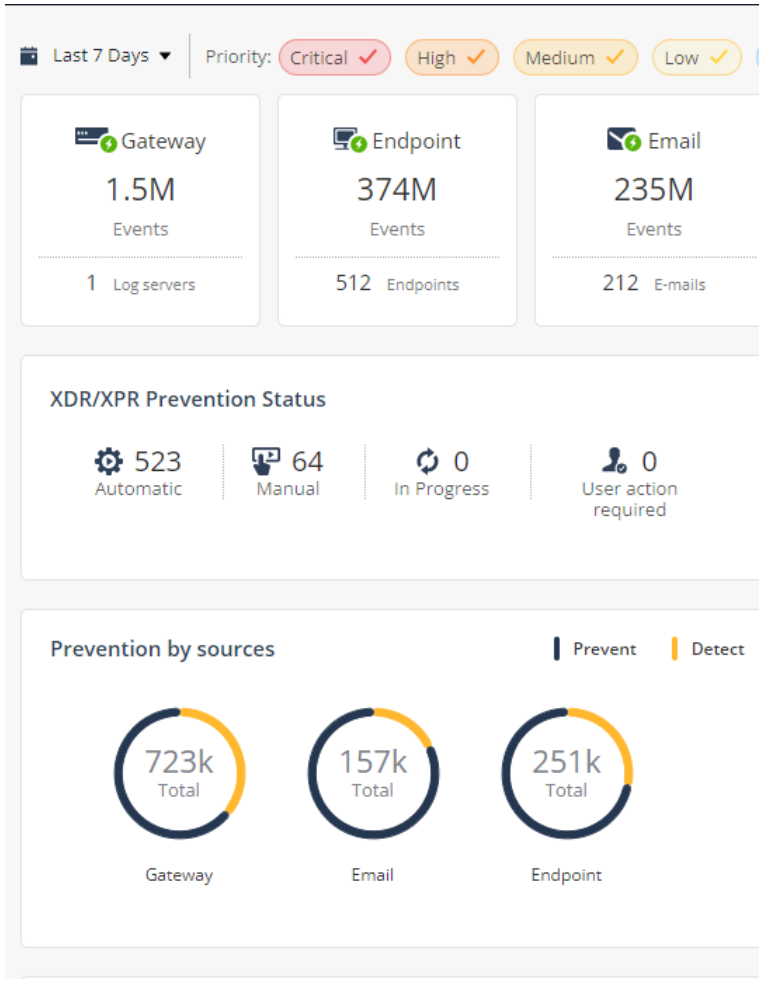
Проверка устройства на compliance-правила, валидация.

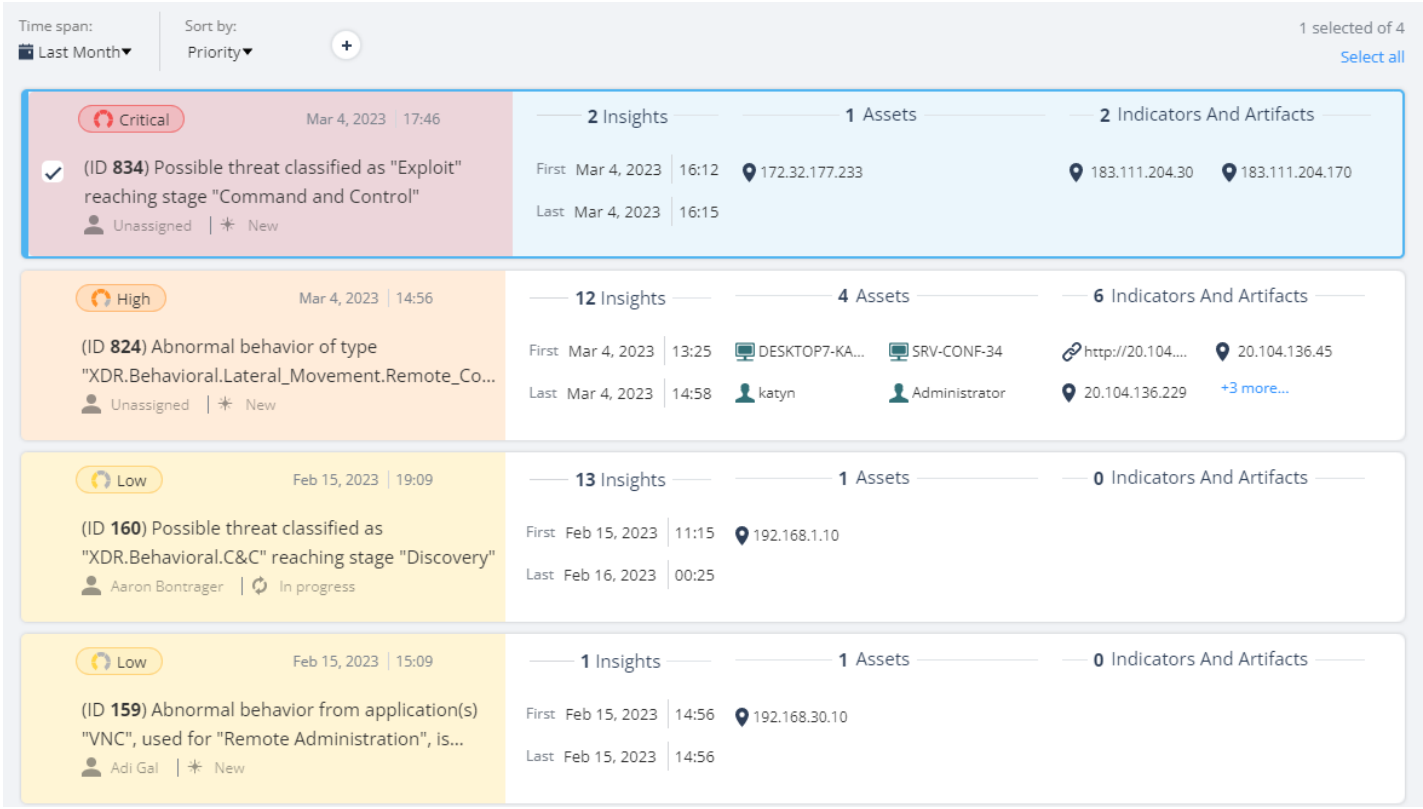
Фаза 2

Zero Trust политика, профили доверия внутри правил.

*Subject to change

Horizon XDR/MDR

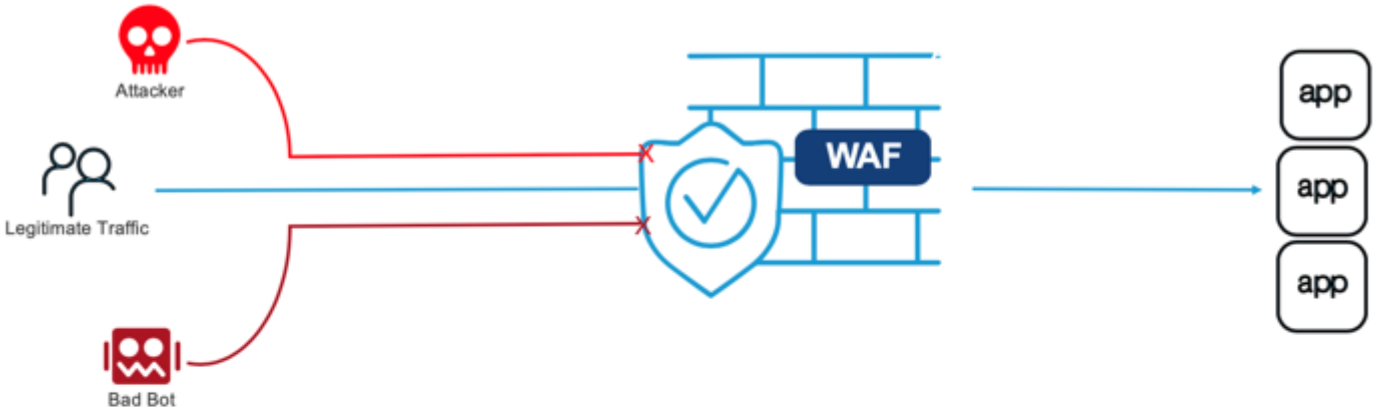




Для разработчиков и облаков

CloudGuard

Безопасность веб-приложения Appsec



Защита API

Инспектирует XML, REST и JSON запросы, блокирет нелегитимные запросы

Выявление ботов

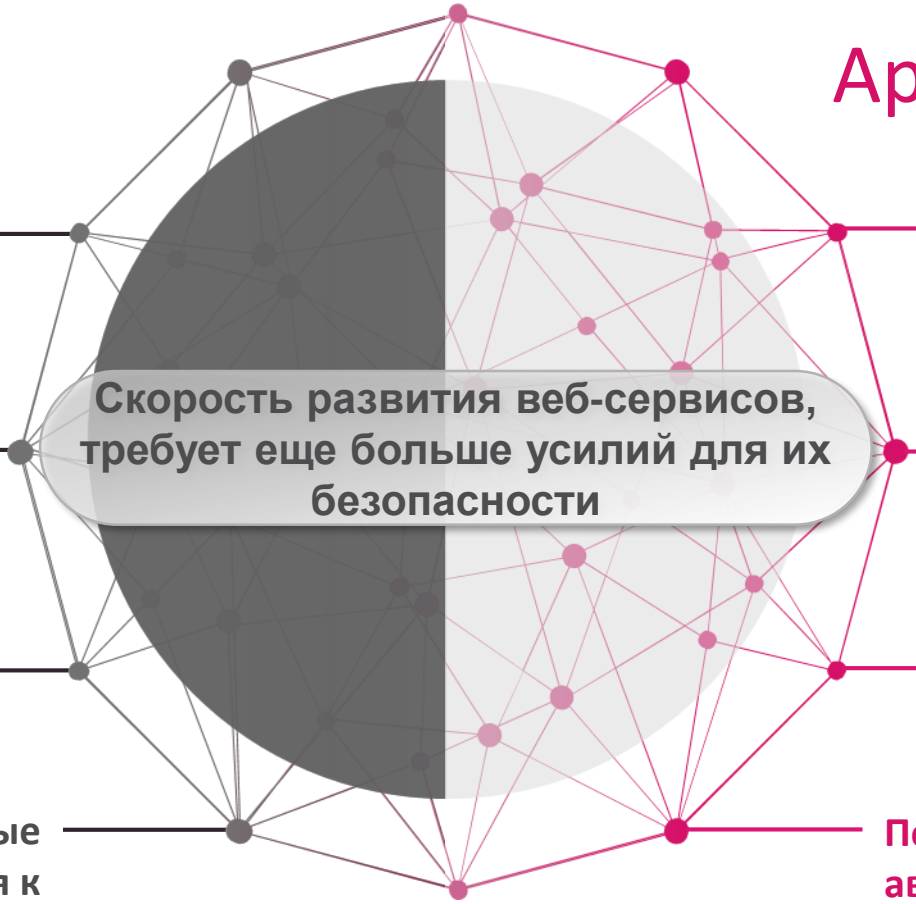
Блокирует ботов на основе поведенческого анализа клиентских подключений

Предотвращение вторжений

IPS уровня приложений

Эмуляция входящих файлов

WAF могут быть разными



Legacy WAF

20 лет технологии защиты

Сигнатурный анализ

Высокий уровень FP

Повышенные требования к администратору

Скорость развития веб-сервисов, требует еще больше усилий для их безопасности

AppSec

ML, AI, Emulation + ThreatCloud

Динамический анализ

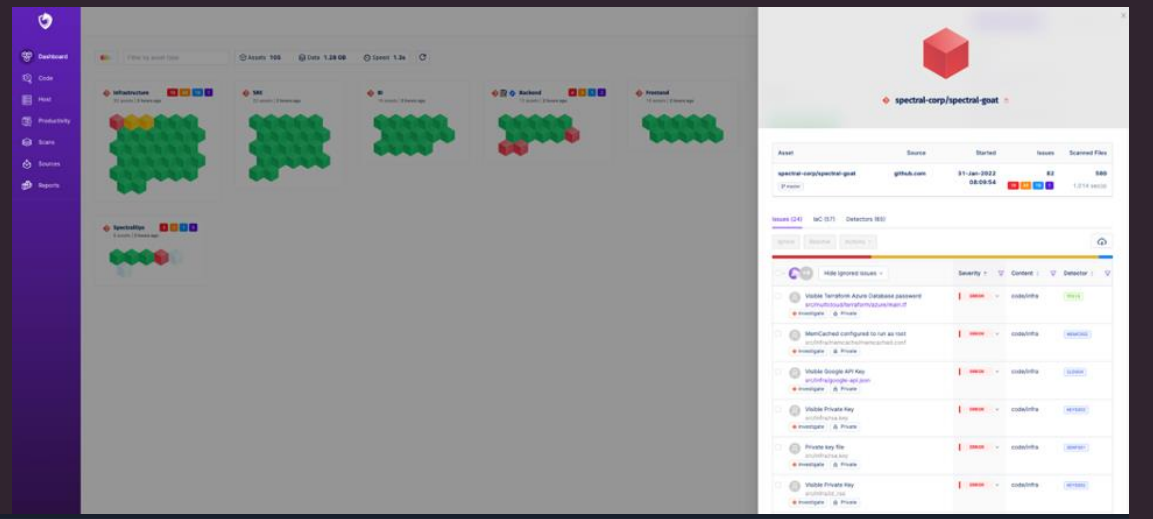
Низкий уровень FP/FN

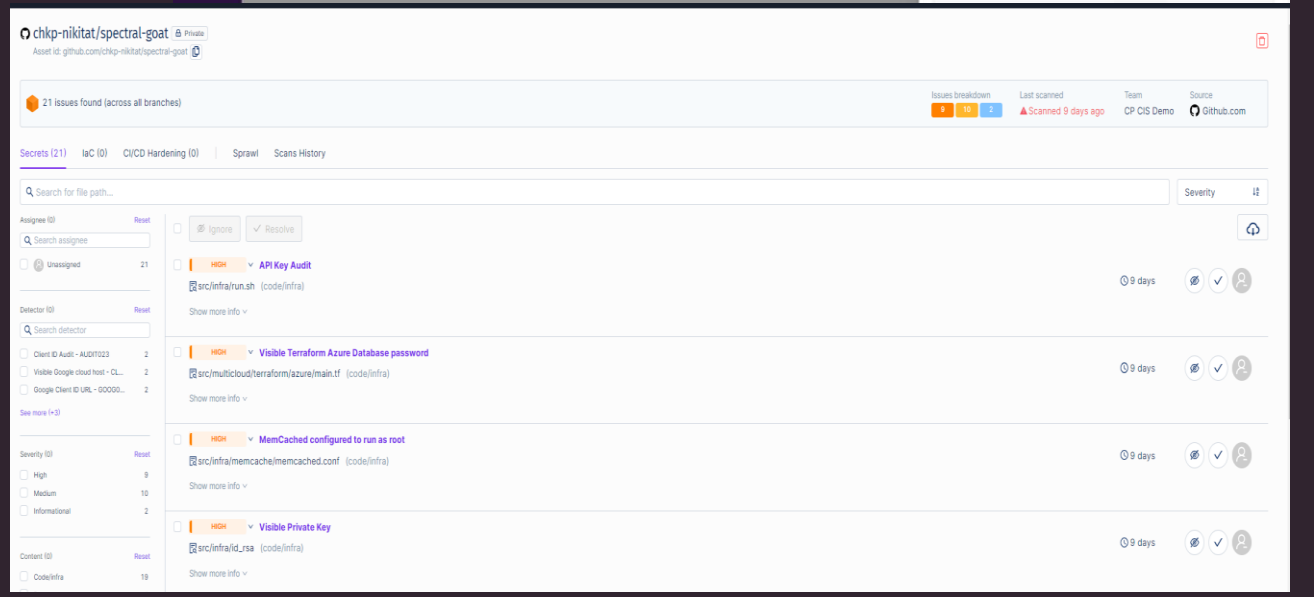
Полностью автоматизированный процесс защиты

CloudGuard

Безопасность кода Spectral

- Интегрируется локально, в публичный репозиторий или CI/CD
- Постоянно сканирует ваш код – анализирует утечки, ошибки в конфигурации, уязвимости
- Оптимизирует процесс разработки и содержит низкий уровень FP
- Анализ событий с подробной информацией для разработчика в GUI.





ИТОГО

telegram

youtube

- Пилот любого продукта
- Помощь в проекте
- Демо-стенд для Вас!

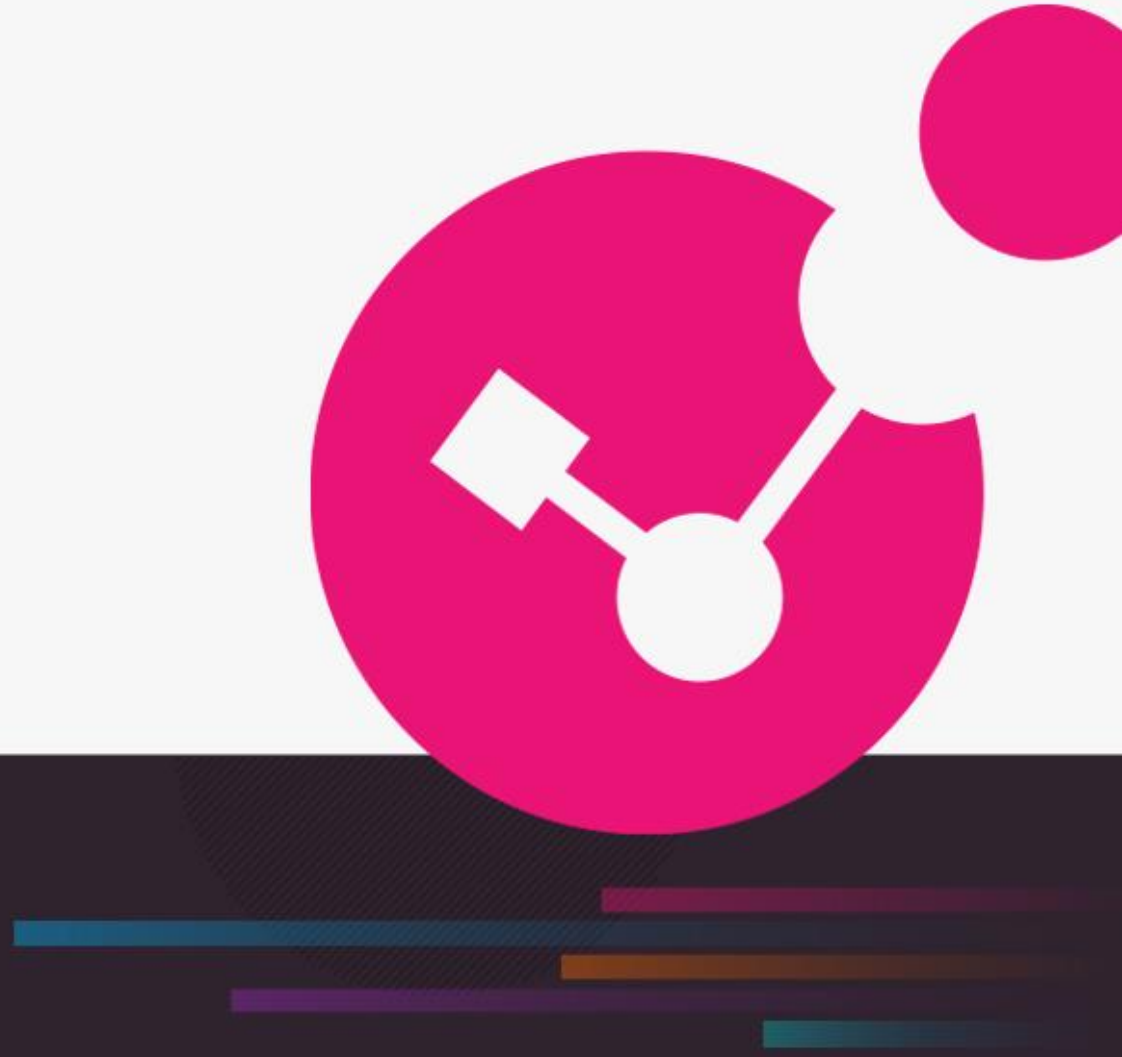
CHECK POINT™

СПАСИБО!

nikitat@checkpoint.com

Турков Никита | Инженер Безопасности

13 апреля 2023 года



YOU DESERVE THE BEST SECURITY