



Семейства Harmony & CloudGuard в 2023 году

CPX Afterparty Partners

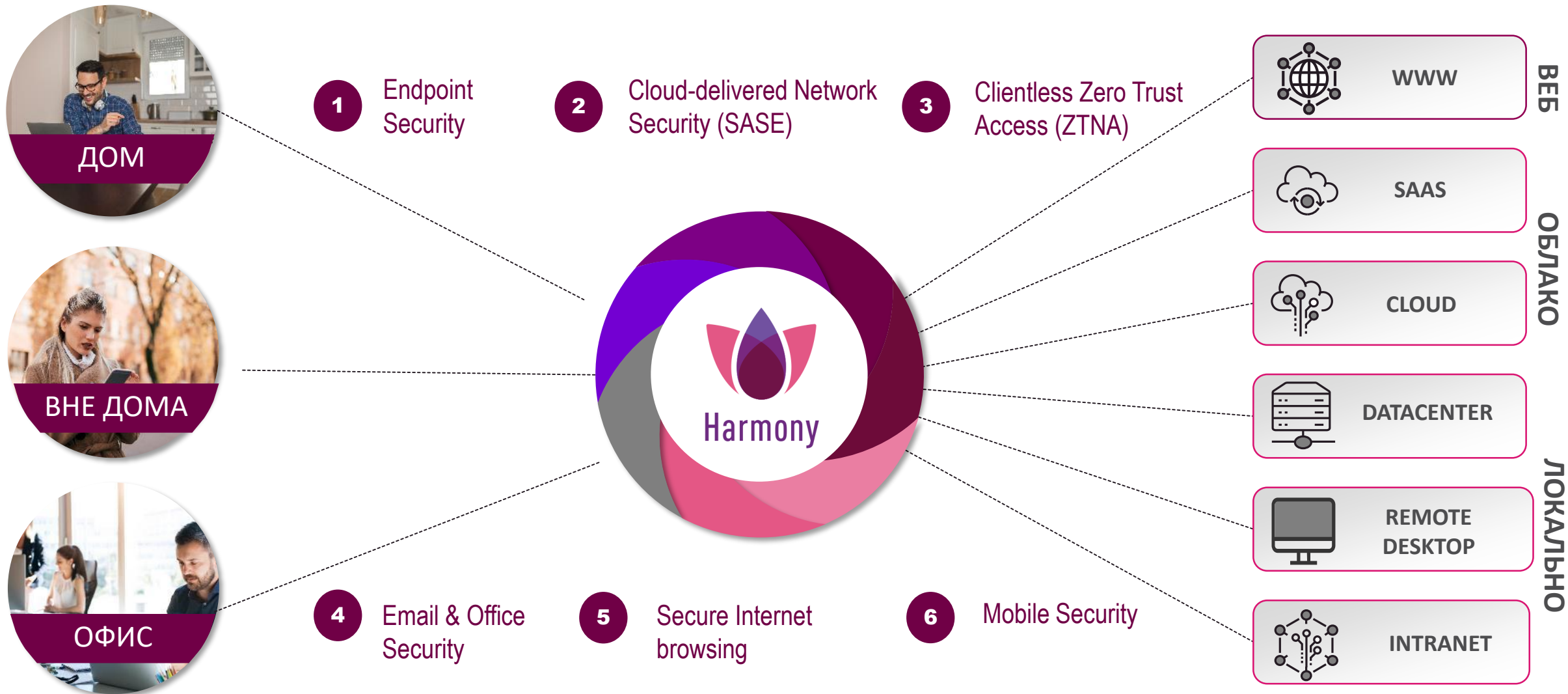


Турков Никита | Инженер Безопасности

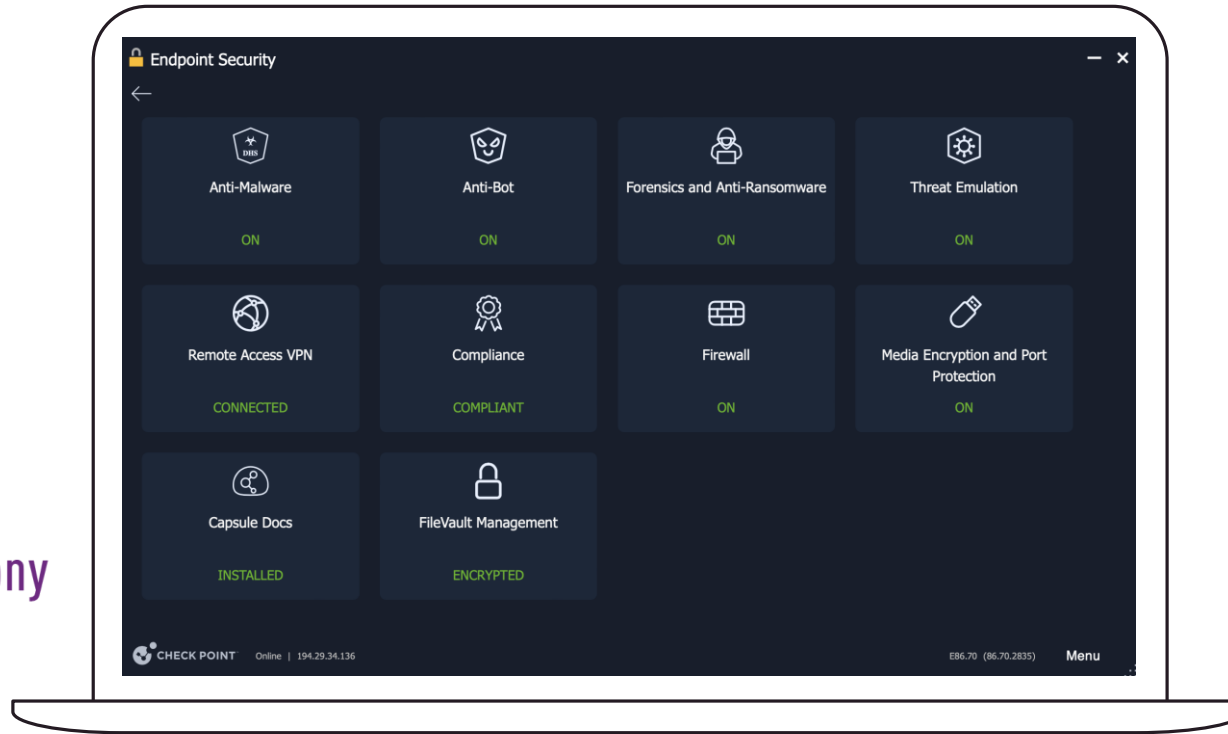
nikitat@checkpoint.com

YOU DESERVE THE BEST SECURITY

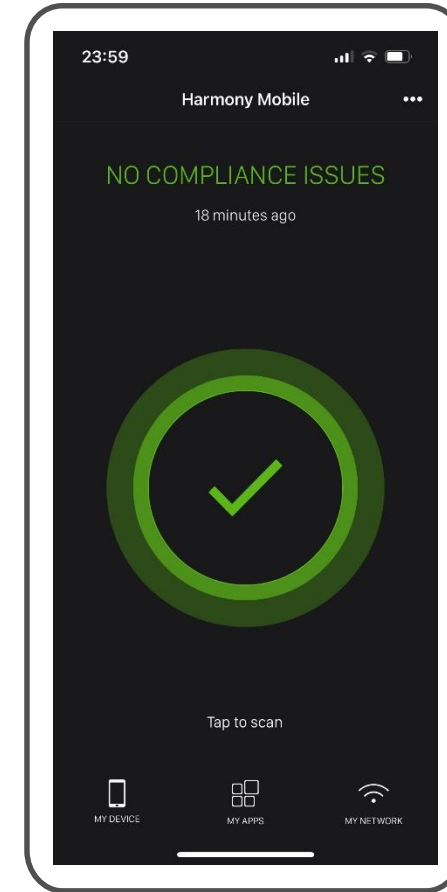
Защита пользователей и их устройств



Агенты для защиты от атак 0-дня и других угроз



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



iOS, Android



Автономная работа и отчеты для инцидентов

The screenshot displays the SandBlast Forensics interface for an incident. The top navigation bar includes tabs for OVERVIEW, GENERAL, ENTRY POINT, REMEDIATION, BUSINESS IMPACT, SUSPICIOUS ACTIVITY, and INCIDENT DETAILS. The overview section shows key details: CLEANED status, Maze malware family, HIGH severity, Endpoint Anti-Ransomware triggered by, trigger c:\windows\system32\wbem\wmic.exe, protection name ransomware.win.shdwdel, and remote user Administrator. The BUSINESS IMPACT section shows 84 Data Ransom. The REMEDIATION section shows 100% completion for terminated processes, quarantined/deleted files, and restored files. A modal window titled 'Check Point Anti Ransomware' displays 'FILE RESTORATION SUCCEEDED' with 148 out of 149 files restored to their original locations.

SandBlast Forensics AGENT

Check Point SOFTWARE TECHNOLOGIES LTD.

OVERVIEW GENERAL ENTRY POINT REMEDIATION BUSINESS IMPACT SUSPICIOUS ACTIVITY INCIDENT DETAILS

CLEANED status

Maze malware family

HIGH severity

Endpoint Anti-Ransomware triggered by

c:\windows\system32\wbem\wmic.exe trigger

ransomware.win.shdwdel protection name

Administrator remote user

ATTACK STATS What sort of connections and processes were involved?

BUSINESS IMPACT What was the potential damage done?

84 Data Ransom

REMEDIATION Were all incident created elements removed?

100% 2/2 terminated processes

100% 1059/1059 quarantined/deleted files

100% 72/72 restored files

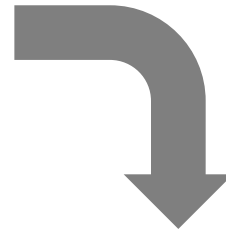
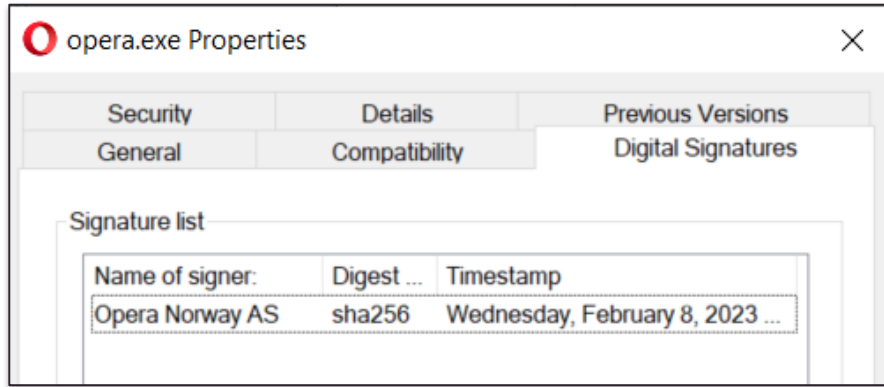
Check Point Anti Ransomware

FILE RESTORATION SUCCEEDED

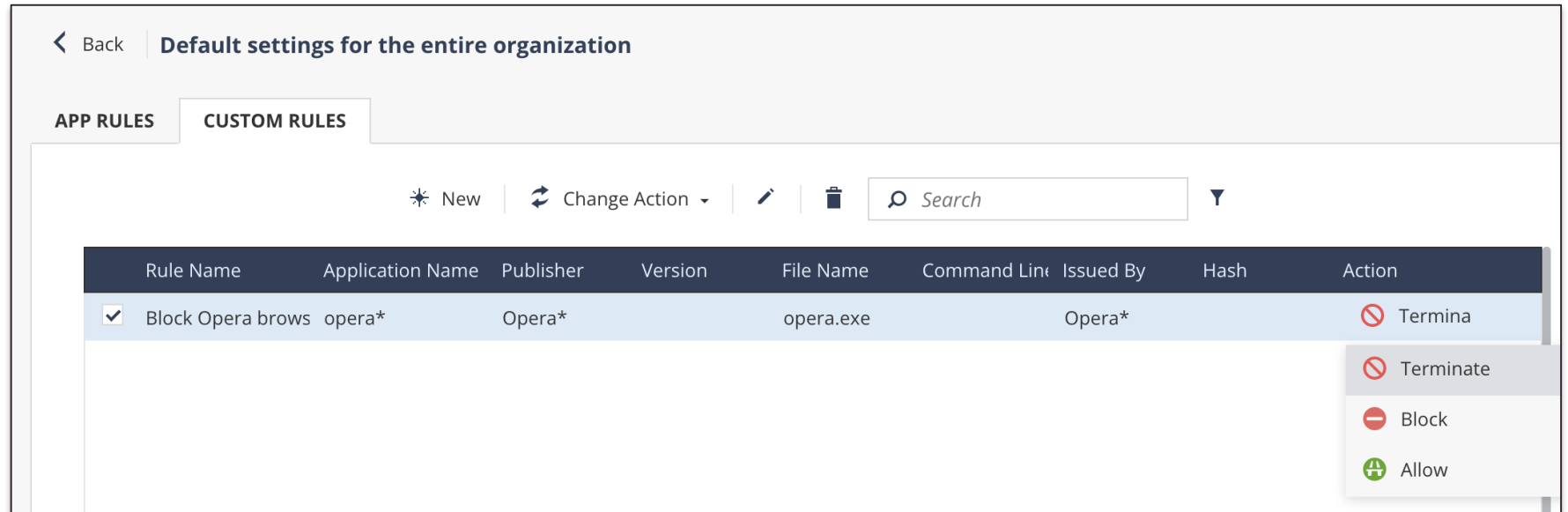
148 out of 149 files were restored
Files restored to: Original file location

CLOSE

Новое: Application Control с Wildcard



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



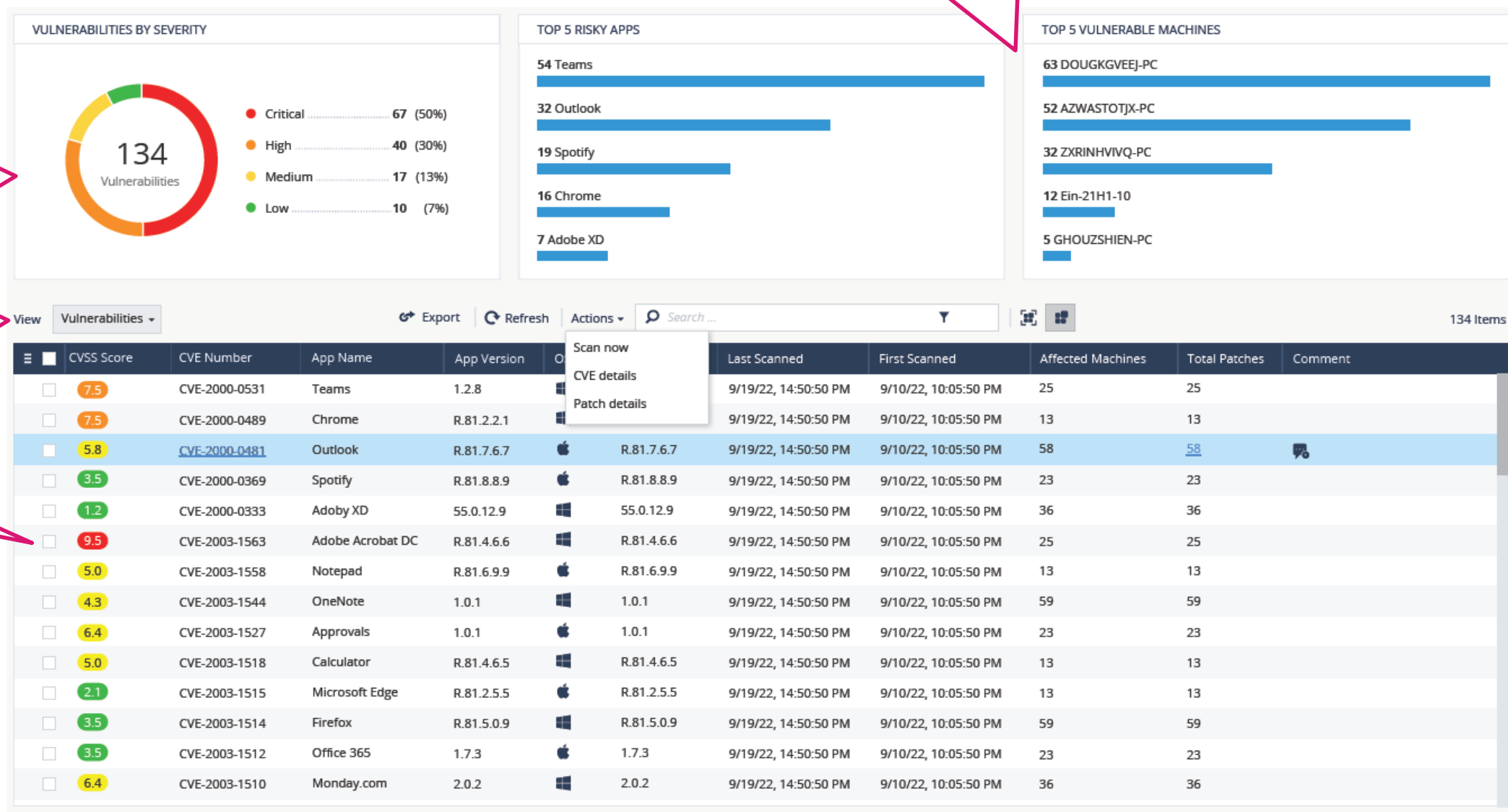
Новое: Posture Management

Фокус на наиболее уязвимые хосты в компании

Фокус на наиболее опасные уязвимости

Просмотр всех уязвимостей внутри организации

Сортировка по CVSS



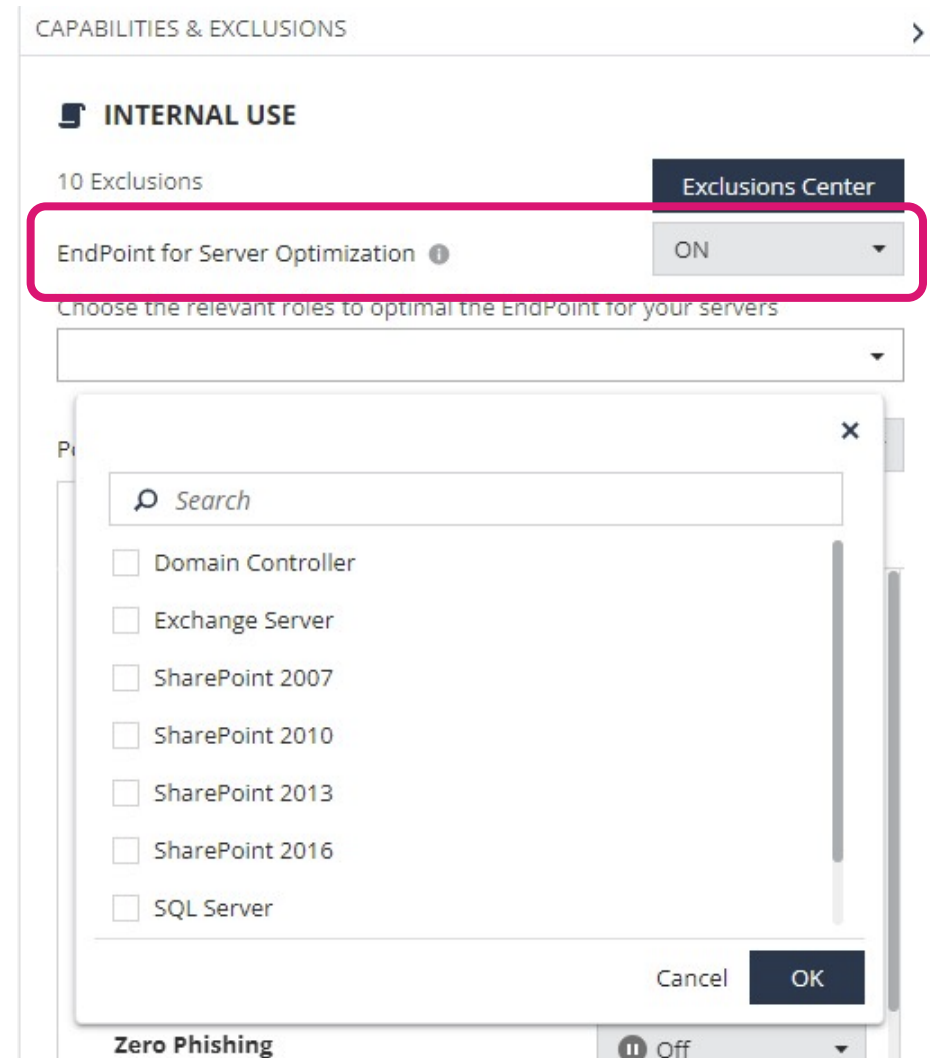
Новое: оптимизация работы для серверных ОС

NEP 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.

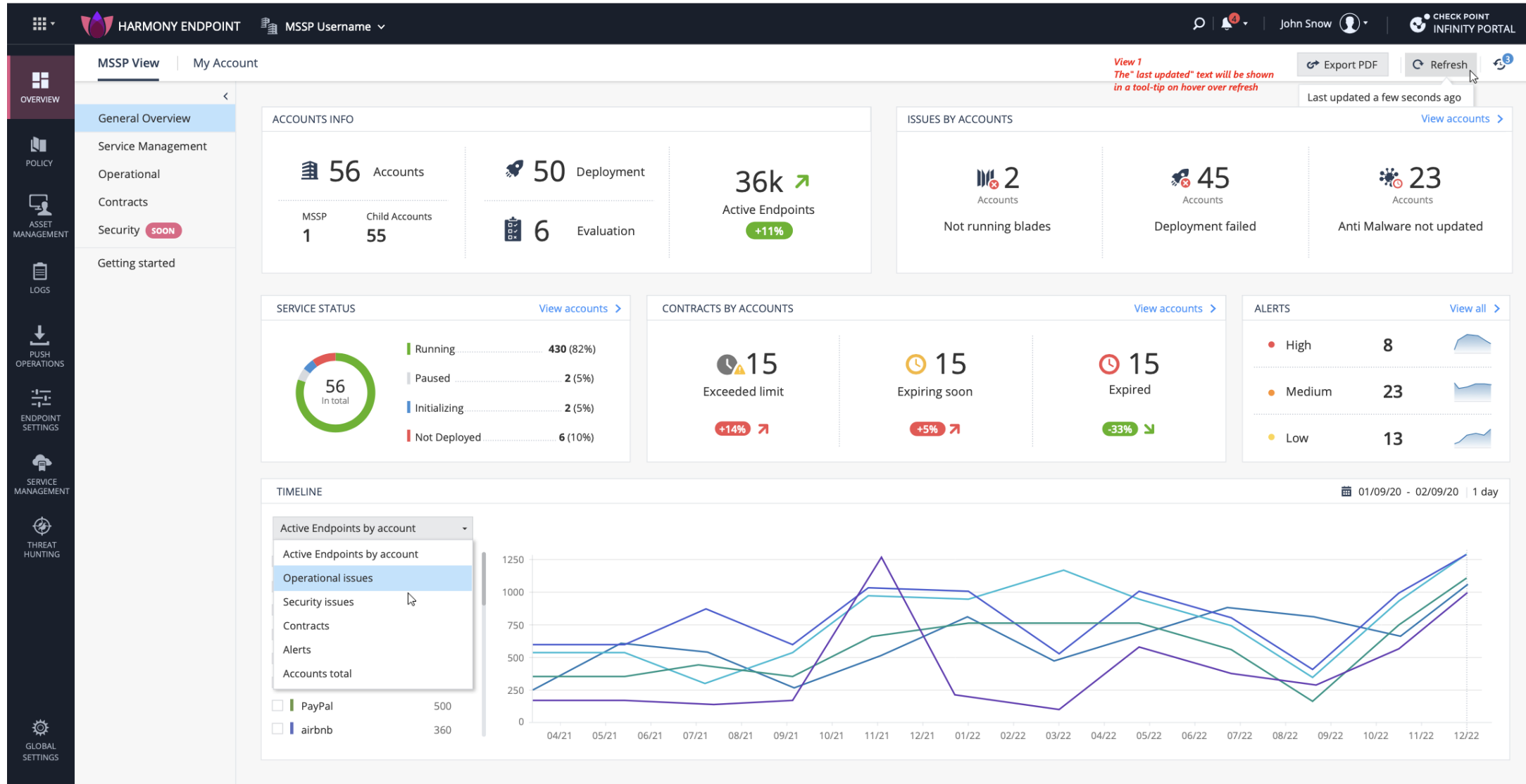


Feature type	Feature	Data Protection	Prevent	Basic	Advanced	Complete
Management	On-Premise Management Console	+	+	+	+	+
	Cloud Management Console	+	+	+	+	+
Threat Intelligence	Threat Cloud		+	+	+	+
	IOC Management		+	+	+	+
Access Control	Firewall	+	+	+	+	+
	Application Control	+	+	+	+	+
	Endpoint Compliance	+	+	+	+	+
	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-NAR-EP-PREVENT**

**Уже доступен в
каталоге!**

Harmony Endpoint MSSP в Infinity Portal (EA)



Q1

2023

Q2

2023

Q3

2023

Q4

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



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



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



Best Security

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



EDR & XDR

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



EDR & XDR

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



EDR & XDR

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



EDR & XDR

- TBD



Posture Management

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



Posture Management

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



Posture Management

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

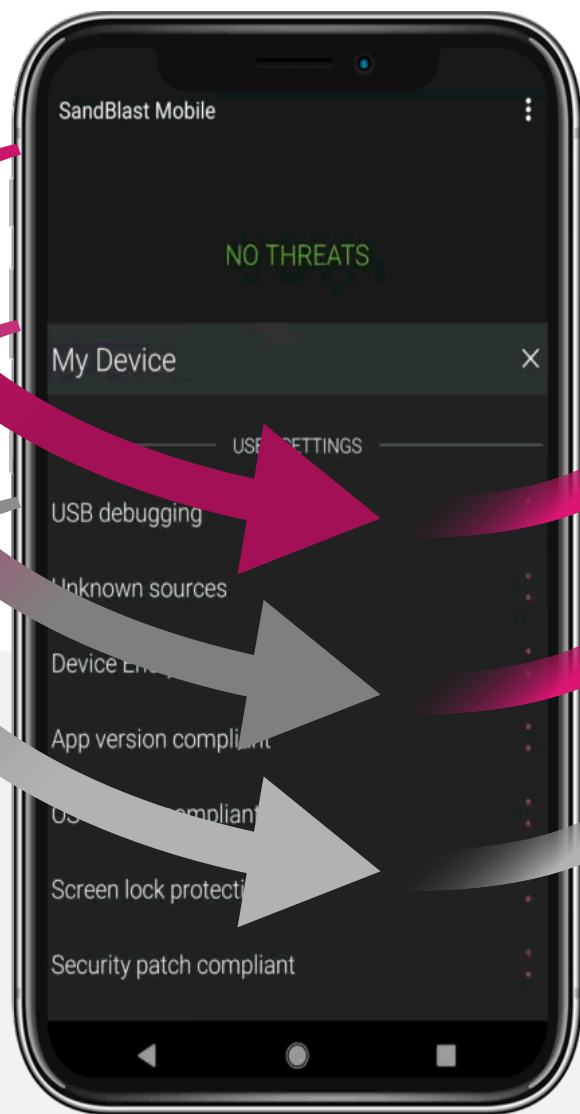


Posture Management

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

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

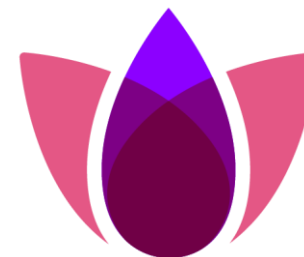
Мобильные устройства требуют защиты



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

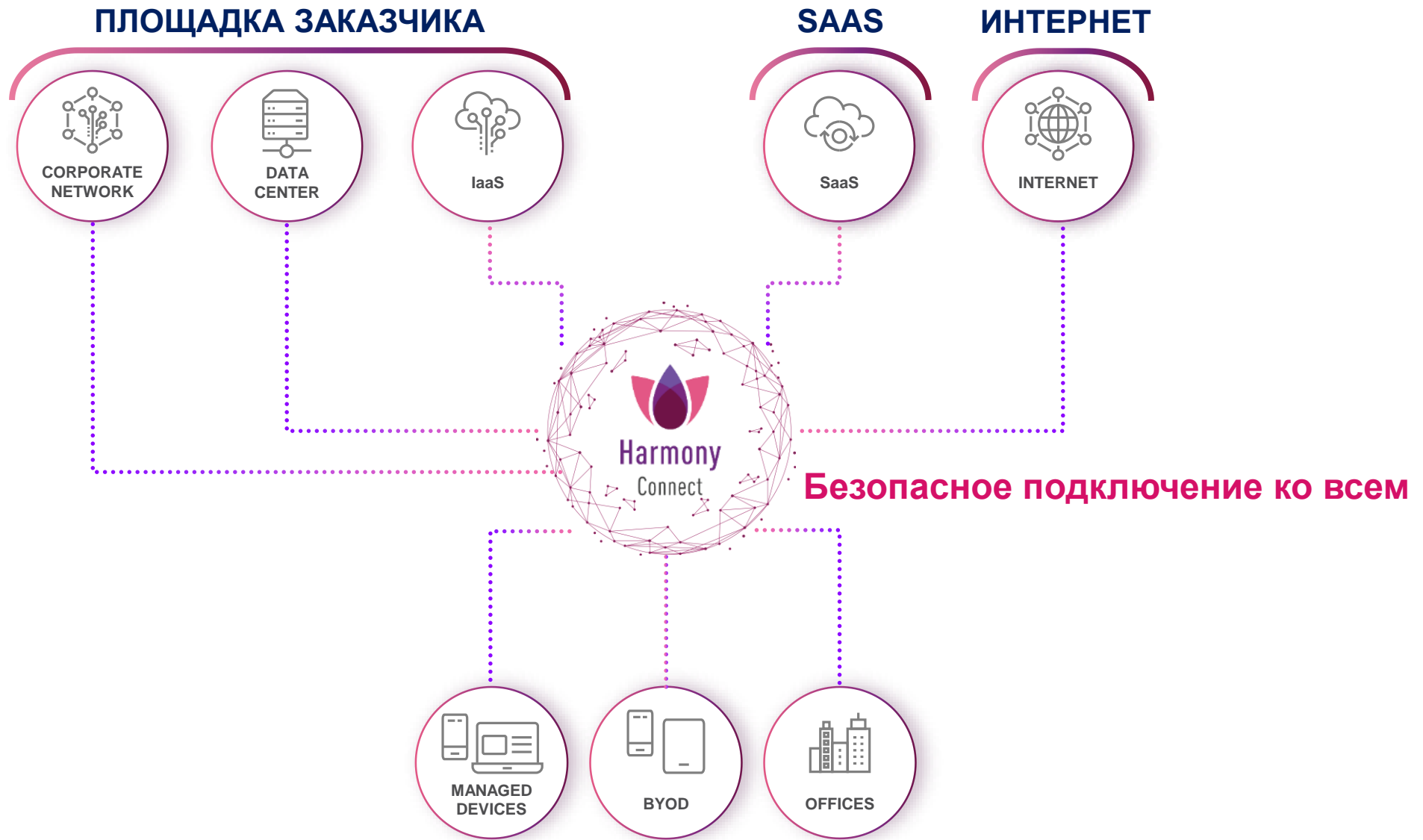
Файл начинает загружаться

Файл отправляется на эмуляцию

Детали отчета доступны пользователю



Шлюз для пользователей вне периметра



Harmony Connect's Global PoPs

sk177806

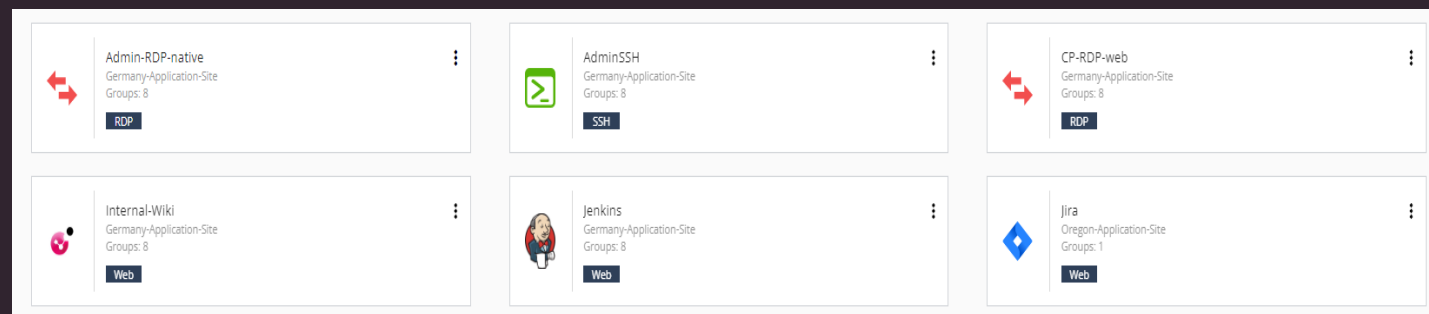
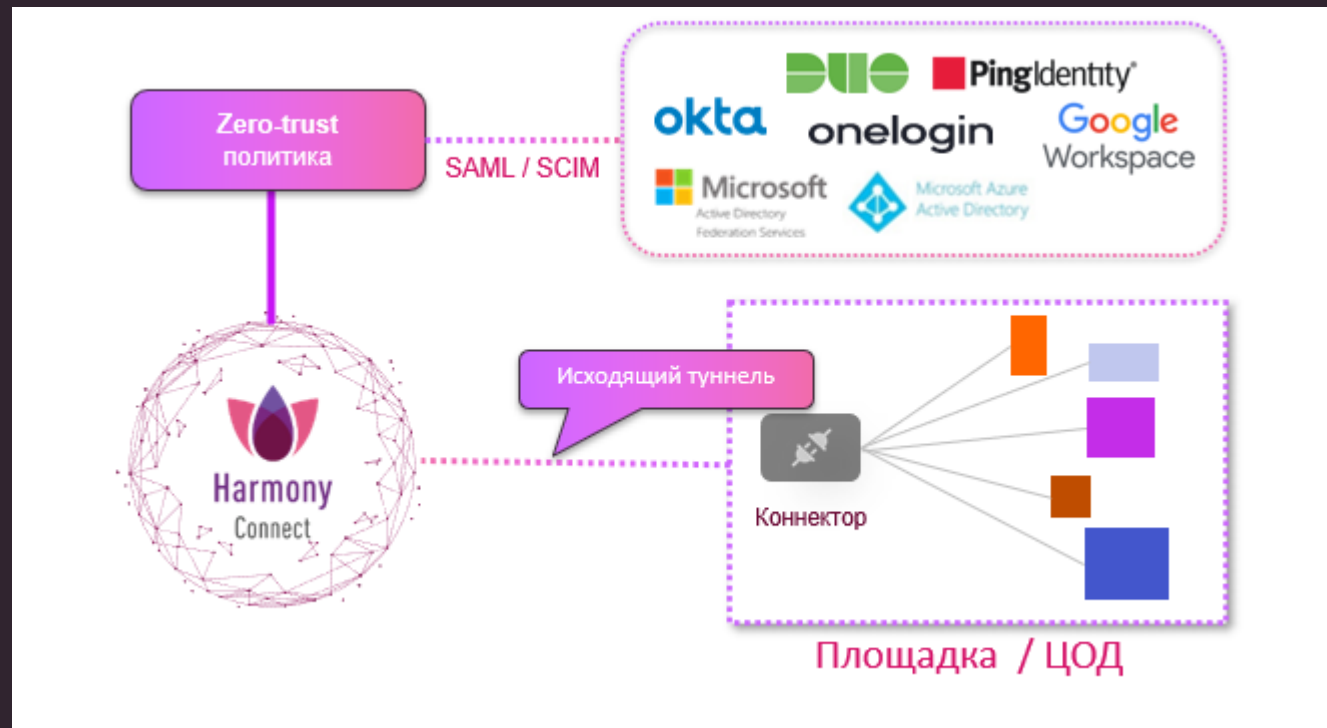


- Australia-East
- Bahrain
- Brazil
- Canada-Central
- France
- Germany
- Hong Kong
- India-Central
- Ireland
- Italy
- Japan-East
- Japan-West
- Singapore
- South Africa
- South Korea-North
- Sweden
- UK-East
- US North-West
- US North-West
- US South-East
- US South-West
- Australia-Central
- Australia-South
- Canada-North East
- China-North
- China-North West
- India-North
- India-South
- Indonesia
- Netherlands
- Norway
- South Korea-South
- Switzerland
- UAE
- UK-West
- US-Central
- US-South

- Austria
- Israel
- Spain

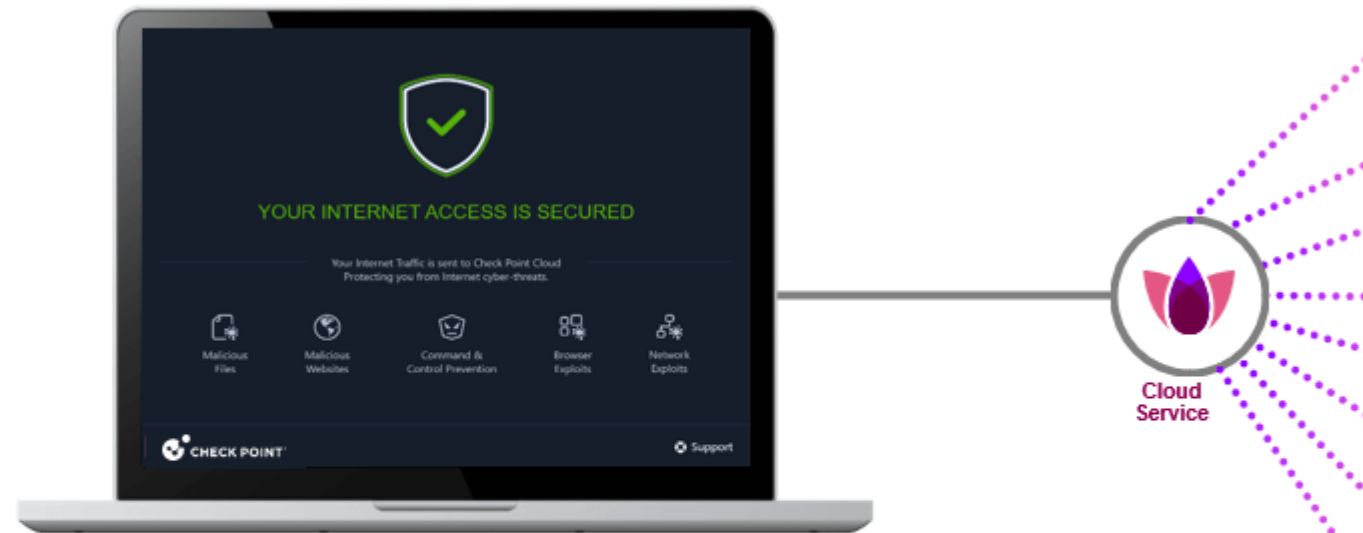
 Existing  Newly Launched  Coming Soon

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

The screenshot shows the 'Trust Profile' configuration window for a 'Standard Managed Device'. The 'Device posture' section is active, displaying various security checks for Windows OS. The 'WINDOWS' tab is selected, and the 'Allow Windows OS' toggle is turned on. The following checks are enabled:

- Windows is up-to-date
- Windows OS minimum version: 10
- Antivirus is active and up-to-date
- Full disk encryption is active
- Compliant according to Check Point Harmony Endpoint
- Installed Windows patches (with a 'Configure' button)
- Check file(s) (with 'Required files (2)' and 'Banned files (0)' buttons)
- Check registry items (with 'Required registry (3)' and 'Banned registry (1)' buttons)
- Check Running processes (with 'Required processes (4)' and 'Banned processes (2)' buttons)

At the bottom of the window, there are 'CANCEL' and 'SAVE' buttons.

Фаза 1

Проверка устройства на compliance-правила, валидация.

Фаза 2

Zero Trust политика, профили доверия внутри правил.

Horizon XDR/MDR



Last 7 Days | Priority: Critical High Medium Low

Gateway 1.5M Events 1 Log servers	Endpoint 374M Events 512 Endpoints	Email 235M Events 212 E-mails
---	--	---

XDR/XPR Prevention Status

523 Automatic	64 Manual	0 In Progress	0 User action required
---------------	-----------	---------------	------------------------

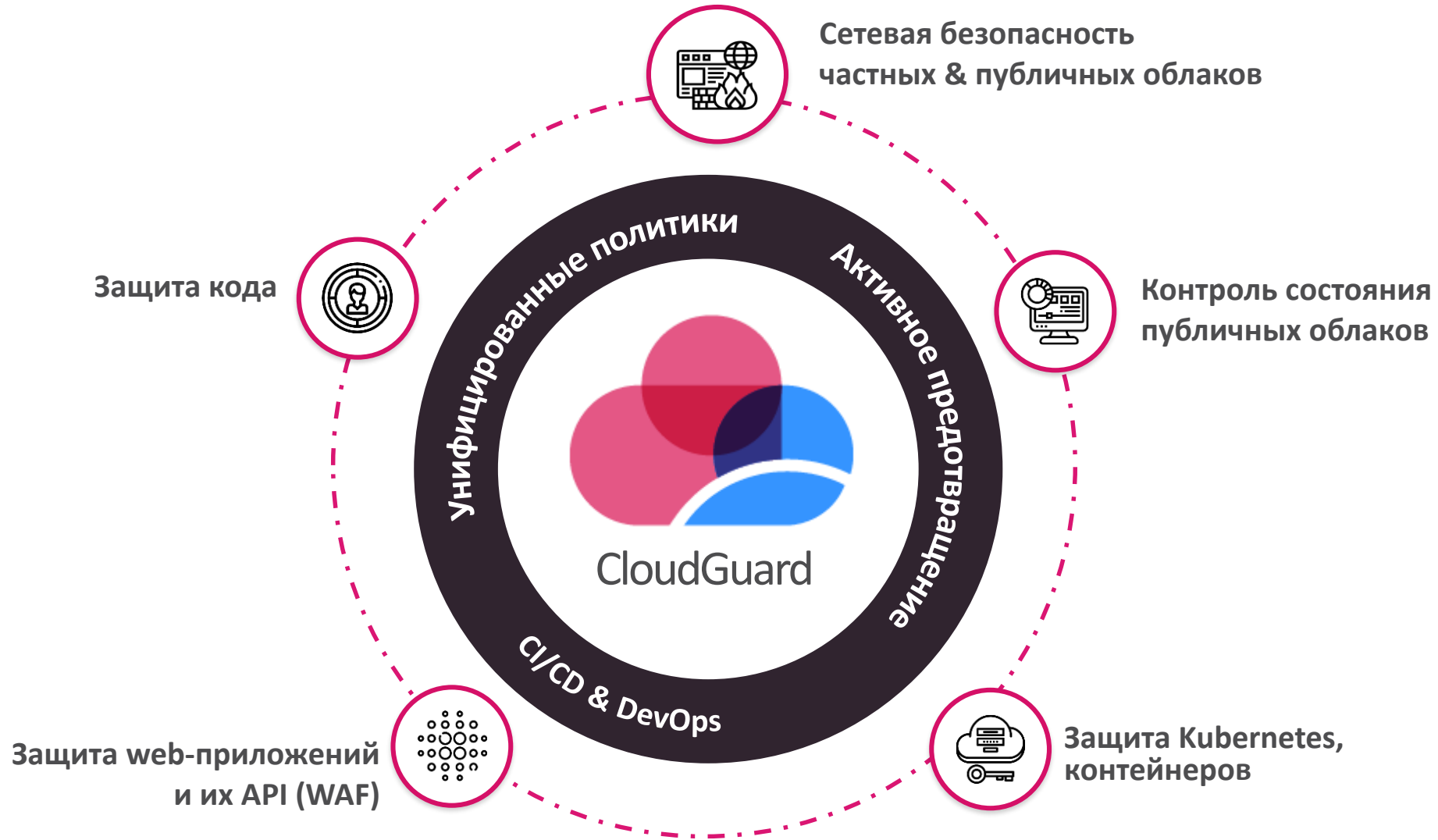
Prevention by sources

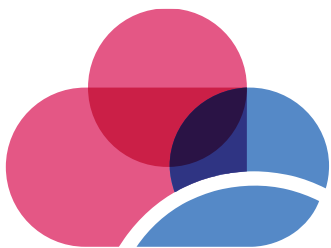
723k Total Gateway	157k Total Email	251k Total Endpoint
-----------------------	---------------------	------------------------

Time span: Last Month | Sort by: Priority | 1 selected of 4 [Select all](#)

Critical Mar 4, 2023 17:46 (ID 834) Possible threat classified as "Exploit" reaching stage "Command and Control" Unassigned * New	2 Insights 1 Assets 2 Indicators And Artifacts First Mar 4, 2023 16:12 172.32.177.233 Last Mar 4, 2023 16:15 183.111.204.30 183.111.204.170
High Mar 4, 2023 14:56 (ID 824) Abnormal behavior of type "XDR.Behavioral.Lateral_Movement.Remote_Co..." Unassigned * New	12 Insights 4 Assets 6 Indicators And Artifacts First Mar 4, 2023 13:25 DESKTOP7-KA... SRV-CONF-34 http://20.104... 20.104.136.45 Last Mar 4, 2023 14:58 katyn Administrator 20.104.136.229 +3 more...
Low Feb 15, 2023 19:09 (ID 160) Possible threat classified as "XDR.Behavioral.C&C" reaching stage "Discovery" Aaron Bontrager In progress	13 Insights 1 Assets 0 Indicators And Artifacts First Feb 15, 2023 11:15 192.168.1.10 Last Feb 16, 2023 00:25
Low Feb 15, 2023 15:09 (ID 159) Abnormal behavior from application(s) "VNC", used for "Remote Administration", is... Adi Gal * New	1 Insights 1 Assets 0 Indicators And Artifacts First Feb 15, 2023 14:56 192.168.30.10 Last Feb 15, 2023 14:56

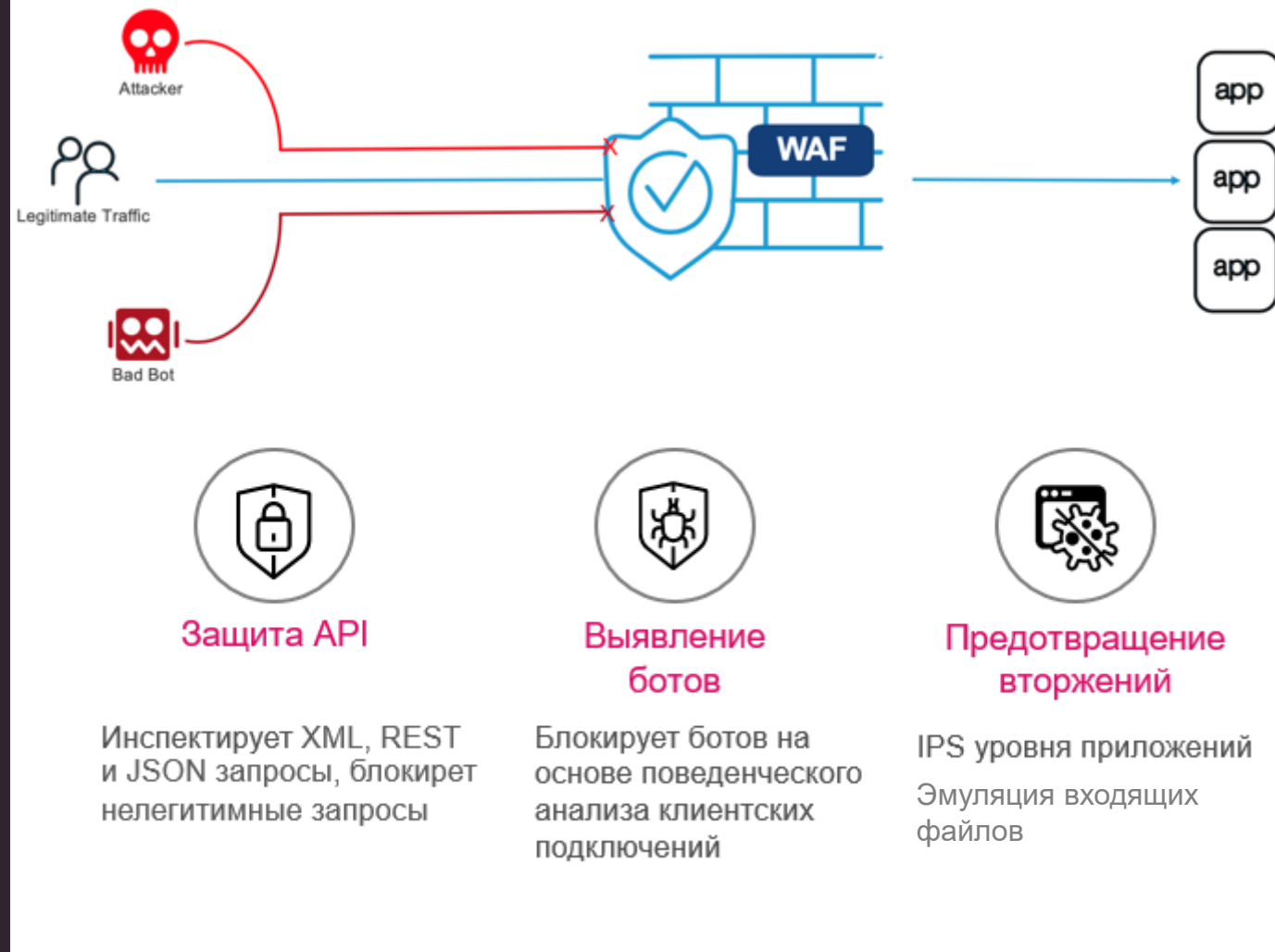
Для разработчиков и облаков





CloudGuard

Безопасность веб-приложения Appsec



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

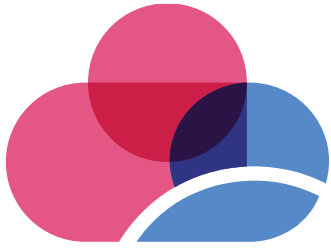
AppSec

ML, AI, Emulation +
ThreatCloud

Динамический анализ

Низкий уровень FP/FN

Полностью
автоматизированный
процесс защиты



CloudGuard

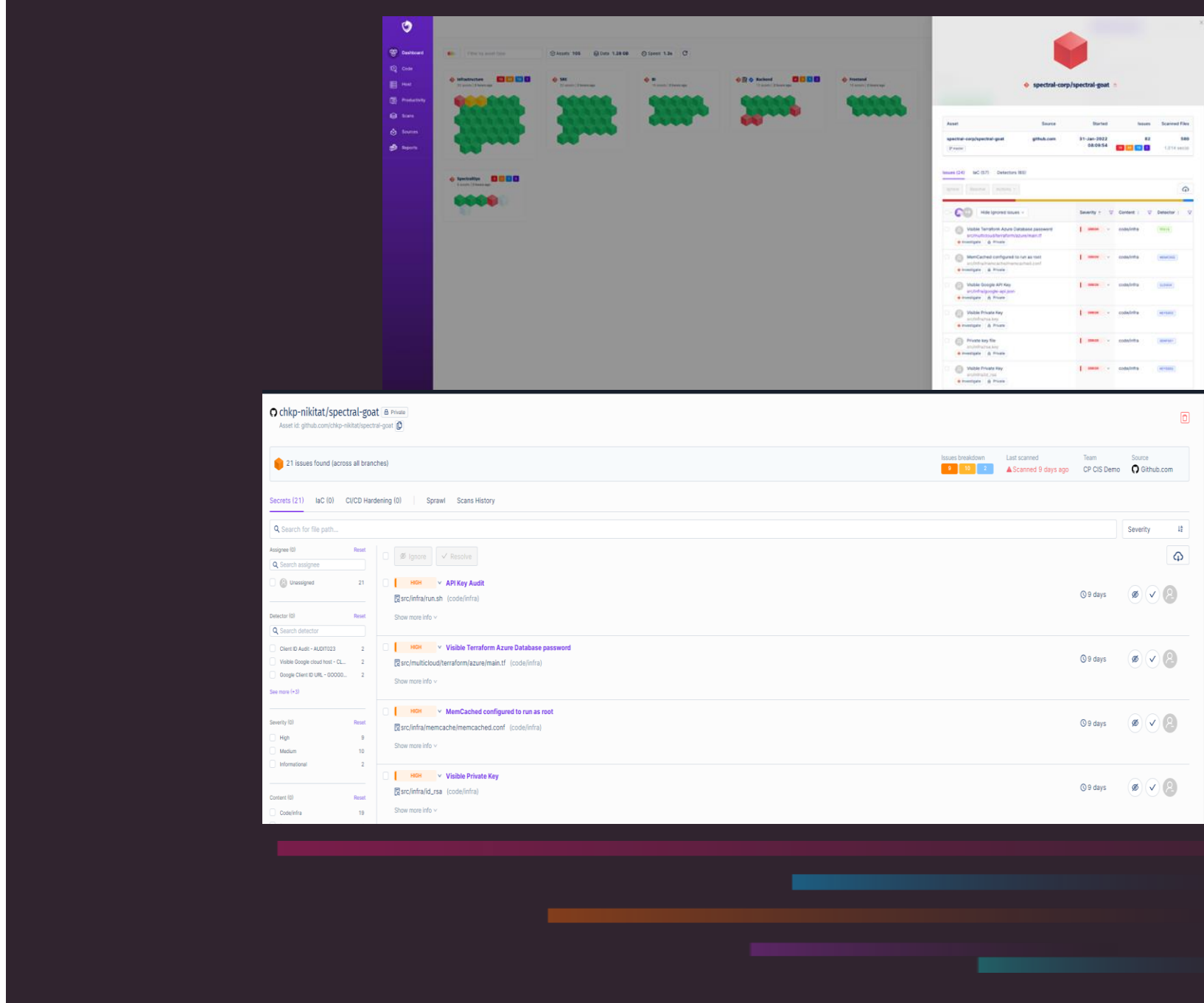
Безопасность кода Spectral

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!

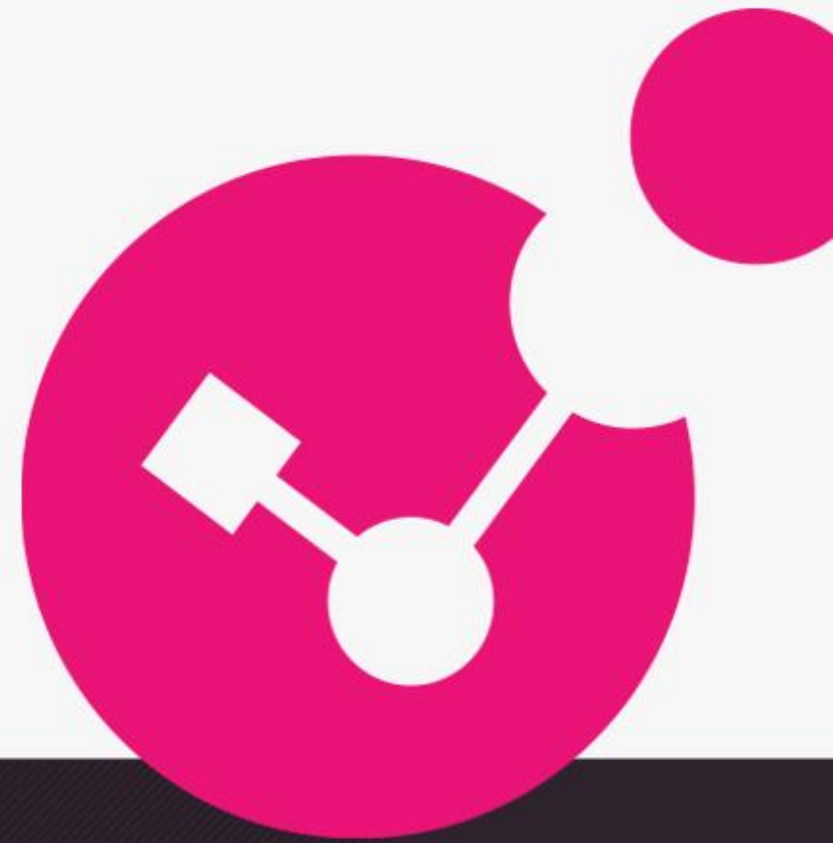


СПАСИБО!

nikitat@checkpoint.com

Турков Никита | Инженер Безопасности

13 апреля 2023 года



YOU DESERVE THE BEST SECURITY