

HARMONY ENDPOINT: СОВРЕМЕННАЯ ЗАЩИТА РАБОЧИХ СТАНЦИЙ


70%

успешных атак начинаются с рабочих станций


\$1 млн

может достигать ущерб от атак на компании малого и среднего бизнеса. 63% подобных атак успешны


#1

Harmony Endpoint показал наивысший уровень защиты, опередив решения других вендоров (NSS Labs AEP 2020)


100%
защита

Из тысяч заказчиков, использующих Harmony Endpoint, никто не пострадал от широко распространенных и таргетированных атак*

* по состоянию на апрель 2022

Для защиты от таргетированных атак и шифровальщиков антивируса не достаточно

В современном очень динамичном мире сотрудникам приходится много работать в мобильном режиме. Они решают массу рабочих задач вне офиса, причем не менее эффективно. Корпоративные пользователи читают почту в транспорте, а также получают доступ к файлам и ресурсам из дома или через точку доступа в кафе. Такой режим требует обеспечения надежной защиты пользовательских устройств от киберугроз.

Обычный антивирус может заблокировать только часть атак, сигнатуры для которых уже существуют. Используя доступные инструменты для модификации атак «на лету», хакеры могут легко обходить традиционную защиту, что приводит к стремительным масштабным взломам со значительным ущербом. Предотвращение атак, в том числе пока неизвестных, на уровне рабочей станции становится важнейшим требованием к системе безопасности организаций.

Социальную инженерию, фишинг, атаки через внешний Wi-Fi, зашифрованный трафик, вредоносное ПО с флеш-карт, горизонтальное распространение угроз, бестелесные атаки можно остановить только на рабочей станции – с помощью продвинутых технологий.

Полная защита рабочей станции

Уменьшить площадь атаки

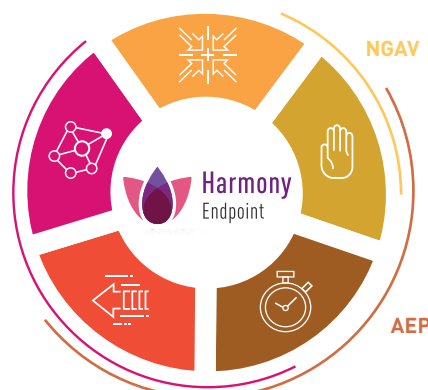
Firewall, Application Control, Port Protection, VPN

Расследовать и составить отчет

Хроника атаки: последовательность событий, тип атаки, точка входа, индикаторы, текущее состояние, ущерб, MITRE ATT&CK

Заблокировать угрозу и устранить последствия

Anti-Bot, FW, Anti-Ransomware, Forensic Remediation, карантин

EDR


Предотвратить атаку

Anti-Virus, Threat Extraction, Threat Emulation, Zero Phishing, FW, Anti-Exploit, NGAV

Обнаружить по поведению

Behavioral Guard, Anti-Ransomware, Anti-Evasion, Threat Hunting, Anti-Fileless, Anti-Bot, Machine Learning

HARMONY ENDPOINT – комплекс уникальных технологий

Полноценная защита в Harmony Endpoint стала возможной благодаря использованию целого ряда уникальных технологий, работающих на разных стадиях атаки. Шифрование данных, VPN, локальный межсетевой экран и Application Control часто позволяют вообще избежать атаки. В случае, если атака все-таки состоялась, технологии Zero-Phishing и URL Filtering ограничат доступ к вредоносным сайтам, Anti-Virus защитит от известных угроз, а Threat Extraction (мгновенная конвертация файлов в безопасную форму) и Threat Emulation (динамический анализ) заблокируют неизвест-

ные. Набор технологий поведенческого анализа, таких как Anti-Evasion, Anti-Exploit, Anti-Bot, Anti-Ransomware и другие, позволяют отследить и остановить опасную активность. HEP постоянно анализирует поведение системы (операции с файлами и процессами, изменения реестра и сетевые соединения), и сохраняет информацию о событиях локально на жесткий диск. В случае инцидента эта информация позволяет не только понять всю схему атаки и отследить ее вплоть до ее возникновения, но и вернуть систему в изначальное состояние, в том числе восстановить поврежденные файлы.

FORENSIC ANALYSIS – автоматическое расследование инцидента

Требуется ли немедленные действия?

Где слабое звено? Точка проникновения.

Полная картина развития атаки.

Какой нанесен ущерб?

Реальная ли это атака или ложная?

Пакеты поставки

Функционал/Конфигурация HEP	Basic	Advanced	Complete
Централизованное развертывание и управление*	✓	✓	✓
Access Control, Port Protection, VPN	✓	✓	✓
Антивирус следующего поколения (NGAV)**	✓	✓	✓
Firewall, Application Control, Port Protection, VPN	✓	✓	✓
Zero-Phishing, URL Filtering	✓	✓	✓
Endpoint Detect and Response (Forensic Analysis), Threat Hunting	✓	✓	✓
Threat Emulation and Extraction		✓	✓
Защита данных (Full Disk Encryption and Media Encryption)			✓

* Все пакеты управляются с помощью платформы управления SmartEndpoint, развернутой локально или в облаке

** Все пакеты HEP могут как интегрироваться с существующим Антивирусом, так и полностью его заменить за счет встроенного антивирусного движка



Представительство в России и СНГ

Check Point Software Technologies (Russia) OOO
 109544, Москва, бульвар Энтузиастов, 2, Деловой центр «Голден Гейт»
 Тел./факс: +7 495 967 7444 • www.checkpoint.com/ru • Эл. почта: Russia@checkpoint.com