Check Point
SOFTWARE TECHNOLOGIES LTD.

Check Point SandBlast NETWORK

SandBlast

PROTECTION FROM 0-DAY THREATS

ЗАЩИТА ОТ УГРОЗ «НУЛЕВОГО ДНЯ» СТАЛА НЕОБХОДИМОЙ

971

Неизвестный зловред атакует организации **каждый час**

52%

Компаний скачали хотя бы один файл с неизвестным ранее зловредом

36%

Компаний подверглись заражению программами-вымогателями в 2016 году

более **300 000**

Компьютеров в 150 странах мира подверглось атаке WannaCry в мае 2017 года

За последние годы информационные атаки стали намного сложнее: теперь они состоят из нескольких этапов и включают разнообразные модули. В то же время стоимость реализации атаки снизилась, так как злоумышленники используют готовую инфраструктуру, а также целый арсенал инструментов для обхода традиционных средств защиты.

Теперь практически каждая атака становится атакой «нулевого дня». Особенно если речь идет о целенаправленных (таргетированных) атаках.

КАК ЗАЩИТИТЬСЯ ОТ ТОГО, О ЧЕМ МЫ ЕЩЕ НЕ ЗНАЕМ?

Одним из самых эффективных способов обнаружения новых угроз является эмуляция: открытие (или запуск) подозрительного файла в изолированной среде и наблюдение за его поведением. Это трудоёмкий процесс, который проводится либо на отдельном устройстве, либо в облаке.

ОБНАРУЖИТЬ МАЛО, НУЖНО ПРЕДОТВРАТИТЬ

Решения для защиты от угроз различаются по принципам работы. Некоторые устаревшие решения работают в режиме ***Detection***, то есть позволяют только обнаруживать атаку (honey pots, сенсоры и детекторы, анализаторы сетевой активности и другие). Технологии Check Point реализуют намного более эффективный режим ***Prevention***, при котором **угроза блокируется** еще до того, как может нанести вред организации.

Detection

Устаревший подход

- Требует постоянного (круглосуточного) контроля со стороны ИТ-сотрудников
- При обнаружении угрозы приходится сразу работать с последствиями
- Требуется высокая квалификация

VS

Prevention

Комплексный подход Check Point

- Угрозы отслеживаются и блокируются автоматически до попадания в сеть
- Создаются регулярные отчеты об инцидентах

CHECK POINT SANDBLAST

Check Point SandBlast позволяет защитить организацию от угроз «нулевого дня» в режиме Prevention. Решение устойчиво к способам обхода детектирования, используемым злоумышленниками, что подтверждается высочайшим уровнем обнаружения. При этом SandBlast не тормозит бизнес-процессы и мгновенно доставляет безопасное содержимое.

В основе SandBlast лежит целый ряд сложных технологий анализа и обработки трафика, в том числе Threat Emulation и Threat Extraction, которые поднимают защиту на новый уровень.

Threat Emulation — эмуляция всех подозрительных файлов с возможностью блокировки доступа к ним до окончания проверки. Используя машинное обучение, многостадийный анализ и исследование поведения, SandBlast обеспечивает не только высочайший уровень обнаружения, но и быструю эмуляцию и непревзойденную производительность.

Вердикт выносится не более чем через 4 минуты. Детектирование 100% попыток уклонения от обнаружения, согласно тестам NSS Labs

Threat Extraction позволяет мгновенно предоставить пользователю безопасную копию подозрительного документа, пока производится анализ и эмуляция. Оригинал будет автоматически доступен пользователю в случае признания его безопасным.

Сокращение площади атаки в 10 раз благодаря технологии Threat Extraction*

* Согласно статистике Check Point, только 10% пользователей будут скачивать оригинал документа

- Эмуляция может осуществляться как на локальном устройстве, так и в облаке. Возможна и гибридная схема.
- Инфраструктура информационной безопасности Check Point — это полноценная защита от любых известных и неизвестных угроз, а также от таргетированных атак.
- Устройство SandBlast может интегрироваться в готовую инфраструктуру: поддерживаются ICAP, MTA, SPAN-port, Inline-режим

R80

R80 SECURITY MANAGEMENT — НЕПРЕВЗОЙДЕННЫЙ УРОВЕНЬ УДОБСТВА НАСТРОЙКИ, УПРАВЛЕНИЯ И ВИДИМОСТИ УГРОЗ

Все решения Check Point работают как единое целое и управляются с одной платформы. Информация об угрозах поступает от разных источников (блейдов) и консолидируется в удобные отчеты. Настраивать и применять политики можно с единой консоли. Рутинные задачи автоматизированы, поэтому персонал может работать более эффективно и быстрее реагировать на инциденты.

GARTNER

Консоль управления Check Point остается де-факто **золотым стандартом**, с которым сравнивают остальных

95% успешных атак можно было предотвратить, если бы существующие решения для защиты были настроены правильно

УСТРОЙСТВА SANDBLAST

Производительность				
	TE100X	TE250X	TE1000X	TE2000X / TE2000X HPP
Рекомендуется, файлов в месяц	100 тыс	250 тыс	1 млн	1.5 млн / 2 млн
Рекомендуется, пользователей	До 1,000	До 3,000	До 10,000	До 20,000
Производительность	150 Mbps	700 Mbps	2 Gbps	4 Gbps
Количество виртуальных машин	4	8	28	40 / 56

PREVENTION
Любой трафик, любой уровень

КАЧЕСТВО ДЕТЕКТИРОВАНИЯ
Отслеживание исполнения кода на уровне CPU

НИЗКАЯ СТОИМОСТЬ ЭКСПЛУАТАЦИИ

ПОЛНАЯ ИНТЕГРАЦИЯ

КОНТАКТЫ
Check Point Software Technologies
Россия и СНГ
russia@checkpoint.com