Check Point
SOFTWARE TECHNOLOGIES LTD.

Check Point SandBlast AGENT

36%
компаний подверглись заражению программами-вымогателями в 2016 году

8 вымогательских кампаний по всему миру запускает сервис Cerber

каждый день

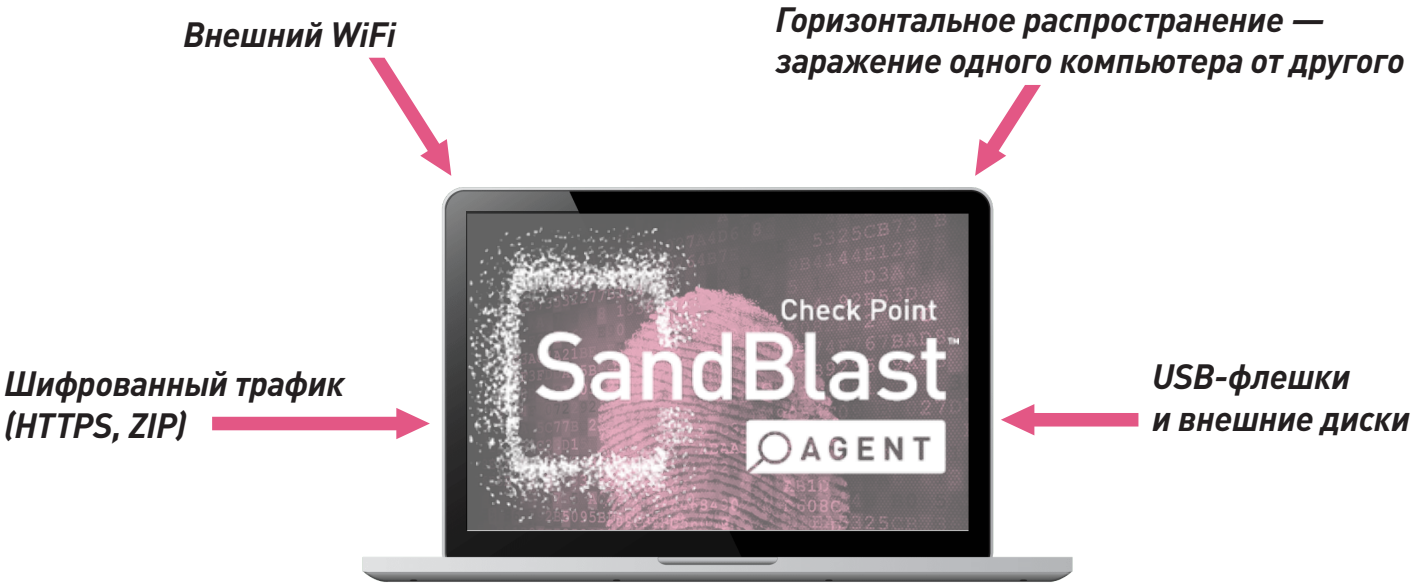
более
400 000
компьютеров в 160 странах мира подверглось атаке WannaCry

Petya заразил более 2000
компаний Украины, России, стран Европы и Южной Америки

РАСТЕТ КОЛИЧЕСТВО АТАК «НУЛЕВОГО ДНЯ», ОТ КОТОРЫХ ТРАДИЦИОННЫЕ АНТИВИРУСЫ ЗАЩИТИТЬ НЕ МОГУТ

За последние годы в сфере киберпреступности произошли серьезные изменения. Теперь злоумышленникам не требуется создавать свои собственные инструменты для атак. Средства взлома, доставки, шифрования, управления, сбора денег — все уже доступно для использования и регулярно обновляется создателями. Стоимость атак стала существенно ниже. Активное распространение биткойнов дало возможность анонимно и безопасно собирать с пользователей выкуп. Все это привело к взрывному росту количества заражений.
С помощью средств для модификации атаки злоумышленники легко преодолевают защиту на базе сигнатур. Традиционные антивирусы уже неэффективны, так как сигнатуры для новых угроз появляются с опозданием.

НЕКОТОРЫЕ ВЕКТОРЫ АТАК ТРЕБУЮТ ДОПОЛНИТЕЛЬНОЙ ЗАЩИТЫ



Основная причина массовости WannaCry и Petya — горизонтальное распространение

CHECK POINT SANDBLAST AGENT

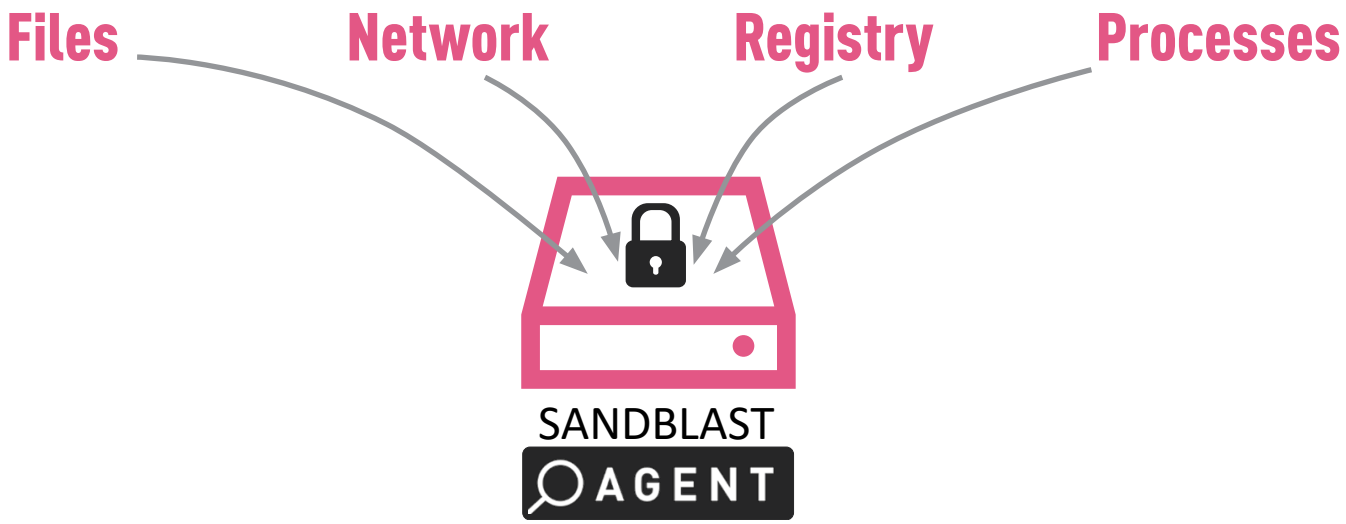
КОМПЛЕКСНЫЙ ПОДХОД К ЗАЩИТЕ РАБОЧИХ СТАНЦИЙ

1. PREVENTION (ПРЕДОТВРАЩЕНИЕ АТАКИ ДО ЕЕ НАЧАЛА)

- **Threat Emulation.** Все файлы, попадающие на рабочую станцию, будут проверены и при необходимости проэмулированы с помощью SandBlast (на локальном устройстве или в облаке).
- **Threat Extraction.** При скачивании из интернета все файлы, требующие эмуляции, будут мгновенно конвертированы в безопасные копии. При этом сохраняется внешний вид оригинального документа, который будет доступен для автоматического скачивания после окончания проверки.
  По статистике Check Point, только 10% пользователей захотят скачать оригинальный документ.
- **Anti-Phishing.** Предотвращает утечку конфиденциальных данных.

2. НАБЛЮДЕНИЕ И АНАЛИЗ

- **SandBlast Agent** постоянно **отслеживает поведение** рабочей станции, в том числе операции с файлами, реестром, процессы и сетевые соединения. Эта **информация сохраняется** локально в защищенной области диска. По умолчанию размер базы событий составляет 1Gb, что соответствует примерно одному месяцу работы.
- **Поведение** рабочей станции непрерывно **анализируется** на предмет подозрительной активности. В процессе мониторинга не создается существенной нагрузки на CPU или диск (в пределах 2-3%).



3. ОБНАРУЖЕНИЕ И ОСТАНОВКА АТАКИ

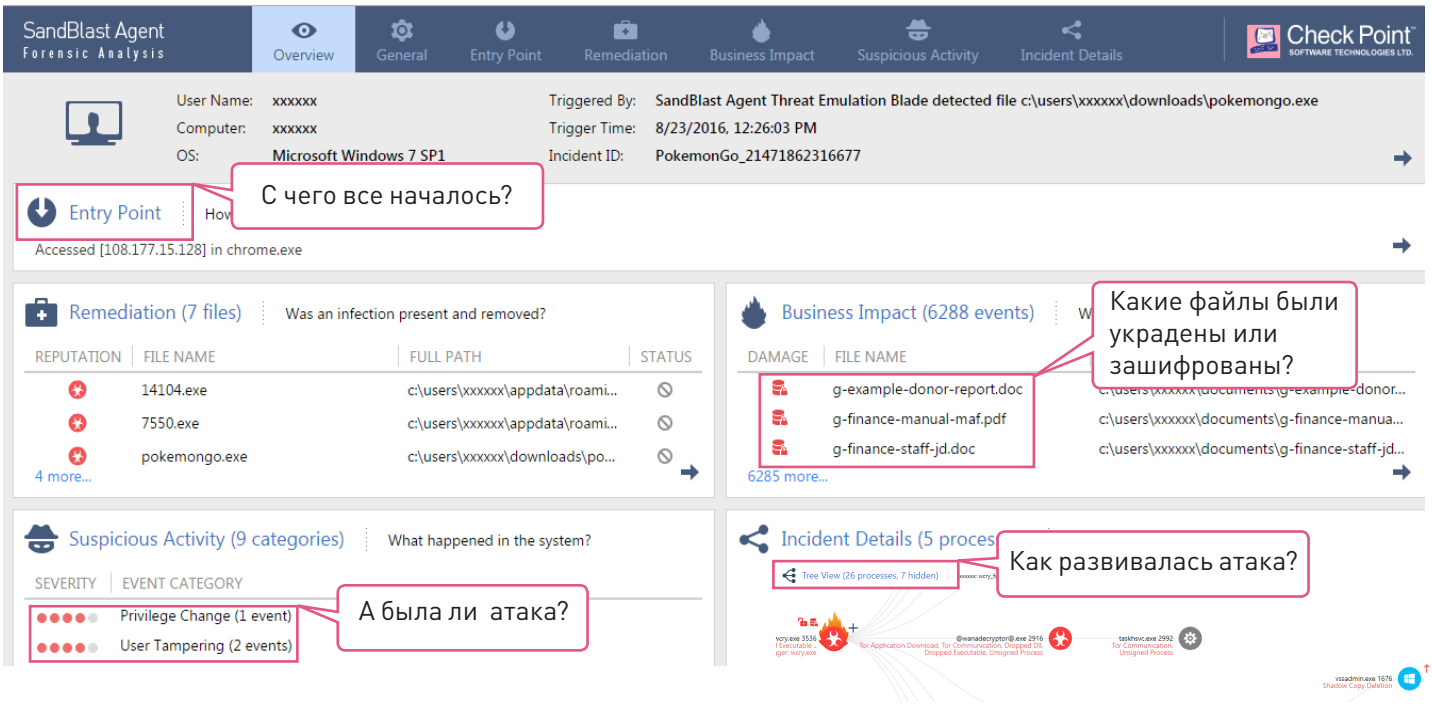
- **Движок поведенческого анализа** регулярно обновляет информацию об актуальных угрозах и способен обнаружить самую скрытную подозрительную активность;
- **Anti-Bot** отследит соединения с серверами контроля и управления;
- **Anti-Ransomware** обнаружит и остановит нелегальное шифрование;
- **Anti-Exploit** обнаружит взлом на начальном этапе, еще до того, как зловред попытается скрыть свою активность.

4. REMEDIATION (УСТРАНЕНИЕ ПОСЛЕДСТВИЙ)

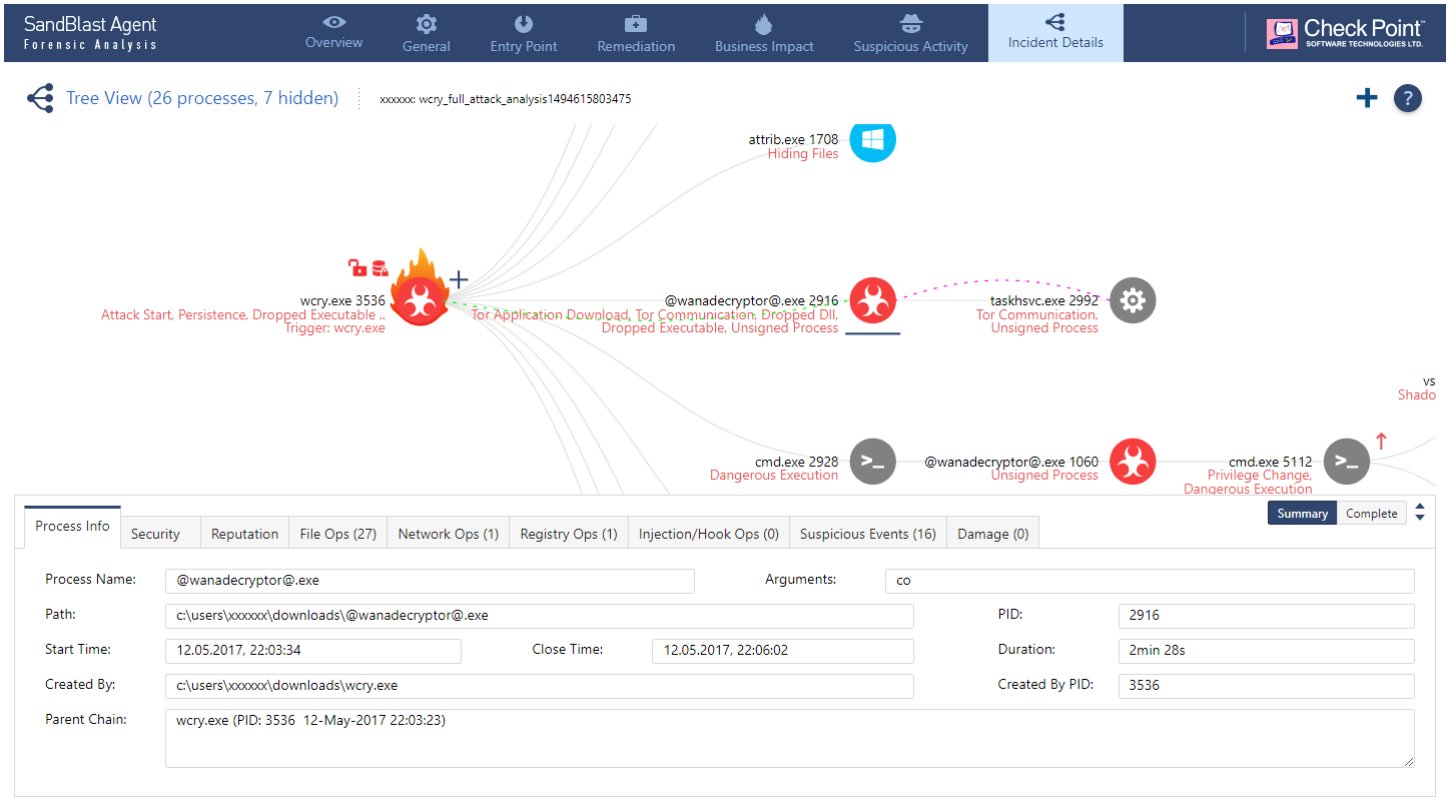
- После обнаружения угрозы SandBlast Agent остановит опасные процессы. Изменения, внесенные зловредом, будут отменены: реестр, файлы будут возвращены в первоначальное состояние.
- Зашифрованные файлы будут восстановлены. Модуль Anti-Ransomware определяет случаи подозрительной модификации (в том числе нелегальное шифрование). Для таких случаев делается кратковременная резервная копия этих файлов (бекап), которая используется для их восстановления при необходимости.

5. FORENSIC ANALYSIS (РАССЛЕДОВАНИЕ ИНЦИДЕНТА)

- После того, как атака остановлена и последствия устранены, SandBlast Agent проводит автоматическое расследование инцидента. Оно позволяет понять, с чего началась атака, какие были использованы бреши в безопасности, какой нанесен ущерб.



ХРОНИКА РАЗВИТИЯ ИНЦИДЕНТА



ПРОДУКТЫ ДЛЯ ЗАЩИТЫ РАБОЧИХ СТАНЦИЙ

	SandBlast Anti-Ransomware	SandBlast Agent	Endpoint Complete Protection Suite
Deployment	Endpoint Agent	Endpoint Agent	Endpoint Agent
Management	SmartCenter	SmartCenter	SmartCenter
Anti-Ransomware	✓	✓	✓
Incident analysis & Quarantine	✓	✓	✓
Forensics report		✓	✓
Browser Extension		✓	✓
Threat Emulation & Extraction		✓	✓
Zero Phishing		✓	✓
Anti-Bot		✓	✓
Anti-Virus			✓
Full Disk Encryption & Media Encryption			✓
Firewall & VPN			✓

PREVENTION 24X7
в том числе
в режиме офлайн

АНАЛИЗ ПОВЕДЕНИЯ

УСТРАНЕНИЕ ПОСЛЕДСТВИЙ

РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ

ИНТЕГРАЦИЯ
с SandBlast Network
и Smart Management

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