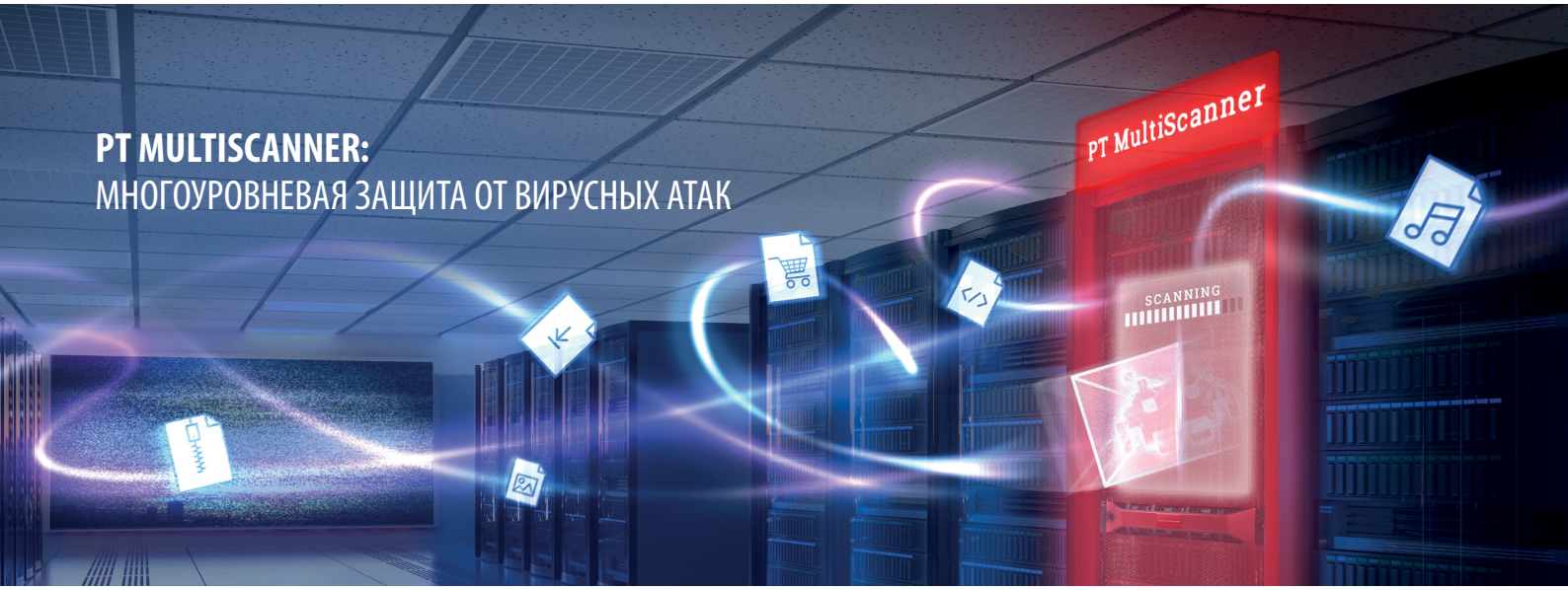


PT MULTISCANNER: МНОГОУРОВНЕВАЯ ЗАЩИТА ОТ ВИРУСНЫХ АТАК

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- **Предотвращение вирусных атак.** Выявление и блокировка распространения вредоносного ПО поверх различных компонентов инфраструктуры: почта, сетевой трафик, пользовательский веб-трафик, файловые хранилища, веб-порталы.
- **Локализация угроз.** Определение отправителей и участников распространения вредоносного ПО в инфраструктуре для последующего расследования и реагирования на угрозу.
- **Обнаружение длительных и целенаправленных атак.** PT MultiScanner реализует дополнительный уровень защиты, способный реагировать на сложные, многоступенчатые атаки. Возможности ретроспективного анализа позволяют выявлять факты реализации угроз нулевого дня и скрытое присутствия вредоносного ПО в инфраструктуре.
- **Единая система хранения.** Централизованное хранение и анализ всех передаваемых объектов из разных потоков трафика для удобства расследования атак.

Атаки с использованием вредоносного ПО по-прежнему остаются одними из самых популярных. Согласно исследованиям Positive Technologies, за второй квартал 2017 года в 38% совершаемых атак использовалось вредоносное ПО. Ежедневно появляется около 300 000 новых экземпляров вредоносного ПО, а развитие тренда «вредонос как услуга» (malware as a service) расширяет возможности злоумышленников по организации атак. Несмотря на развитие технологий выявления вредоносного ПО, существующие подходы не могут гарантировать достаточного уровня защиты. Среди причин можно выделить:

- сложность локализации распределенной атаки, ее последствий в прошлом и в настоящем;
- моновендорные схемы защиты от вредоносного ПО;
- отсутствие единой точки мониторинга всех передаваемых объектов в инфраструктуре.

Многопоточная система выявления вредоносного контента PT MultiScanner помогает преодолеть недостатки существующих подходов. Это современное средство контроля за распространением вредоносного ПО в инфраструктуре, которое позволяет значительно увеличить эффективность обнаружения и блокировки заражений по всей инфраструктуре как в реальном времени, так и в ретроспективе.

PT MultiScanner — серверное решение, которое разворачивается в инфраструктуре и предназначено для мониторинга и блокировки угроз в рамках защиты почтового трафика, веб-трафика, файловых хранилищ и веб-порталов. Система выявляет зараженные объекты в различных потоках данных компании и агрегирует однотипные элементы атаки в одну угрозу, благодаря чему можно эффективно выявлять массовые заражения и проводить расследования, в том числе за длительный период времени.

Интеграция PT MultiScanner с MaxPatrol SIEM позволяет работать с событиями и инцидентами в едином интерфейсе, в привязке к топологии сети, а также получать корреляции вердиктов PT MultiScanner с событиями от других систем.

Кроме этого, Positive Technologies Expert Security Center предлагает услуги по экспертной верификации и оценке опасности найденных объектов и по расследованию инцидентов.

ПРЕИМУЩЕСТВА

+ **Мультивендорный подход**
Для выявления вредоносов используются несколько антивирусных движков, статический анализ и черные списки, поставляемые Positive Technologies. Обновление базы знаний доступно онлайн и офлайн.

+ **«Умные» вердикты**
Вердикт по результатам анализа объекта формируется на основе базы знаний и собственной классификации вредоносного ПО Positive Technologies.

+ **Удобство использования**
Система предоставляет интуитивно понятный веб-интерфейс, а вся информация, необходимая для ежедневной работы специалиста по ИБ, визуализируется на дашбордах.

+ **Простота внедрения**
Быстрое развертывание (весь процесс занимает меньше часа) и поддержка стандартных интерфейсов взаимодействия (SPAN, MTA, ICAP, REST API) позволяют легко встроить PT MultiScanner в существующую инфраструктуру.

+ **Масштабируемость**
С ростом потока сканируемых объектов производительность легко регулируется наращиванием компонентов системы.

ВАРИАНТЫ ИСПОЛЬЗОВАНИЯ PT MULTISCANNER

+ **Контроль корпоративного трафика** (мониторинг)
Проверка файлов из захватываемого со SPAN-порта коммутатора сетевого трафика в режиме реального времени, обогащение событий в системах защиты (IPS/IDS, SIEM), оперативное реагирование и расследование инцидентов.

+ **Защита почты** (мониторинг и блокирование)
Онлайн-проверка почтовых сообщений, выявление вредоносных вложений и источников рассылки, проверка почтовых архивов (в том числе разделенных на части и защищенных паролем), защита против социальной инженерии с использованием вредоносного ПО.

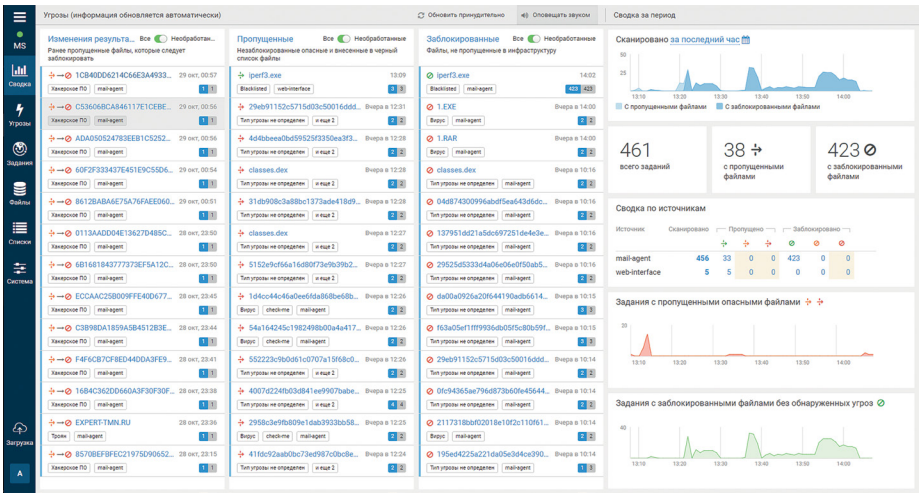
+ **Проверка пользовательского веб-трафика** (мониторинг и блокирование)
Повышение общего уровня защиты периметра за счет выявления вредоносного содержимого в файлах, загруженных из внешних подсетей (в том числе по HTTPS).

+ **Защита веб-порталов** (мониторинг и блокирование)
Активная защита веб-приложений от вредоносного контента, контроль утечек информации и выявление ботов, контроль контента, загружаемого пользователями.

+ **Контроль файловых хранилищ** (мониторинг и блокирование)
Выявление вредоносного содержимого, зараженных дистрибутивов и документов, своевременная блокировка распространения вредоносных файлов, ретроспективная проверка и отложенное выявление угроз в ранее загруженных объектах при обновлении баз знаний.

+ **Внутренний сервис**
Повышение уровня информационной безопасности за счет анализа файлов, загружаемых вручную, ведение базы знаний и учет статистики по загруженным объектам и вердиктам, уведомление пользователей об обнаруженном вредоносном содержимом в ранее загруженных файлах.

+ **Расследование инцидентов ИБ**
Поддержка процесса расследования инцидента и предоставление необходимых инструментов. Ретроспективное выявление атакованных узлов и анализ схемы распространения атаки.



О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.

POSITIVE TECHNOLOGIES

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays