positive technologies

# PT Sandbox

Сетевая песочница для выявления сложных целевых атак с применением вредоносного ПО

**В каждой второй кибератаке злоумышленники применяют вредоносное ПО под видом обычных файлов и ссылок и развивают его так, чтобы обходить антивирусы, межсетевые экраны, IDS, IPS, почтовые и веб-шлюзы. По данным Positive Technologies, в 70% компаний замечена активность вредоносов, которую пропустили базовые средства защиты.**

## Где PT Sandbox выявляет угрозы

- Электронная почта.
- Файловые хранилища.
- Веб-трафик пользователей.
- Внутренний трафик организации.
- Порталы ручной проверки файлов.
- Корпоративные системы, включая системы документооборота.

## Знания PT Expert Security Center

**PT ESC — экспертный центр безопасности Positive Technologies.** Специалисты PT ESC расследуют инциденты в крупных компаниях и постоянно отслеживают активность хакерских группировок, действующих на территории России и стран СНГ. Знания об угрозах, получаемые в ходе этих исследований, оперативно поставляются в PT Sandbox.

## Решение

PT Sandbox — риск-ориентированная сетевая песочница, которая выявляет сложные киберугрозы, даже если злоумышленник тщательно скрывается. Она защищает от целевых и массовых атак с применением вредоносного ПО и угроз нулевого дня, обнаруживает как распространенные вредоносы (шифровальщики, вымогатели, шпионское ПО, утилиты для удаленного управления, загрузчики), так и сложный инструментарий хакерских группировок (руткиты, буткиты).

Каждый объект анализируется в PT Sandbox с помощью технологий машинного обучения, статическим и динамическим методом с помощью уникальных правил PT Expert Security Center (PT ESC), а также проверяется несколькими антивирусными движками.

Экспертные знания PT ESC о новейших угрозах доставляются в продукт за 2,5 часа. Это позволяет защитить компанию от кибератаки в случае, если преступник эксплуатирует уязвимость нулевого дня, патч для которой еще не выпущен.

## Преимущества

**Адаптация защиты к особенностям бизнеса**
Ключевая особенность PT Sandbox — возможность адаптировать защиту от угроз к особенностям ИТ-инфраструктуры и бизнес-процессов компании. Для этого предусмотрены следующие механизмы:

- **Поддержка виртуальных сред для анализа** (как с Windows различных версий, так и с российскими операционными системами — Astra Linux и «РЕД ОС»). Продукт полностью покрывает связанные с вредоносным ПО тактики и техники атакующих по матрице MITRE ATT&CK для этих типов ОС.
- **Гибкая кастомизация виртуальных сред.** В них можно добавить специфическое ПО (и его версии), которое действительно используется в компании и может стать точкой входа для злоумышленников.
- **Выявление угроз как в корпоративном, так и в технологическом сегменте.** Промышленная версия PT Sandbox позволяет анализировать объекты в промышленной виртуальной среде и выявляет специфическое вредоносное ПО, нацеленное на компоненты АСУ ТП.
- **Наличие приманок, провоцирующих вредоносное ПО на активные действия и помогающих выявить нарушителя.** В файлах-приманках содержатся поддельные учетные записи, файлы конфигурации или другие ценные данные. Процессы-приманки имитируют работу банковского ПО, софта разработчиков, активность пользователей. PT Sandbox выявляет попытки похитить подобные сведения или внедриться в процессы. Основной набор приманок для Windows и Linux доступен «из коробки», но по запросу эксперты PT ESC могут создать уникальные ловушки, имитирующие работу критически важных для клиента систем.

## Дополнительно

### Высокая производительность

Гибкое управление обработкой файлов и ссылок и неограниченные возможности горизонтального масштабирования системы обеспечивают высокую производительность под любой нагрузкой.

### Режимы мониторинга и блокировки

PT Sandbox позволяет отслеживать угрозы или блокировать их в автоматическом режиме.

### Легкая интеграция

Поддержка множества вариантов интеграции «из коробки» и гибкий API позволяют использовать PT Sandbox в любой конфигурации информационных систем.

### Поддержка экосистемы Positive Technologies

PT Sandbox бесшовно интегрируется с MaxPatrol SIEM, PT Application Firewall, PT ISIM, PT Network Attack Discovery и PT XDR.

### Возможность работы on-premise

Конфиденциальные файлы при проверке не покидают периметра компании.

### Выполнение требований регуляторов

PT Sandbox внесен в реестр российского ПО и сертифицирован ФСТЭК. Позволяет выполнять требования приказов ФСТЭК России от 25.12.2017 № 239, от 18.02.2013 № 21 и от 11.02.2013 № 17.

### Выявление угроз, которые не были обнаружены ранее

PT Sandbox проводит регулярный ретроспективный анализ уже проверенных ранее файлов после обновления базы знаний. Это позволяет максимально быстро обнаруживать скрытые в инфраструктуре угрозы и реагировать на атаки до того, как злоумышленник достиг цели.

### Обнаружение угроз не только в файлах, но и в трафике

Помимо самих файлов PT Sandbox проверяет трафик, который генерируется в процессе анализа их поведения, а также выявляет вредоносную активность, скрытую под TLS. Это существенно повышает эффективность детектирования атак — даже в шифрованном трафике.

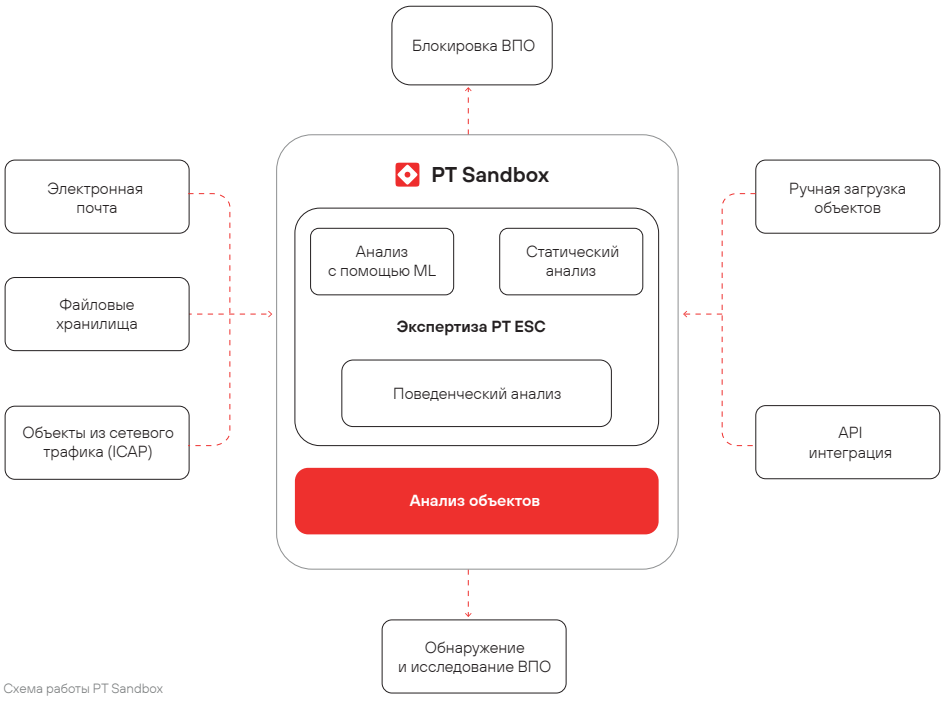


Схема работы PT Sandbox

## Протестируйте PT Sandbox

Хотите оценить эффективность PT Sandbox в вашей инфраструктуре? Оставьте заявку на демонстрацию возможностей продукта или пилотный проект.

## Остались вопросы?

Задайте их экспертам по продукту в чате PT Sandbox в Telegram.

**ptsecurity.com**
pr@ptsecurity.com



PT-SANDBOX_A4.0009.004.APR.24.2023