

The logo consists of the letters 'PT' in a white, bold, sans-serif font, centered within a solid red square. The background of the entire page is a 3D architectural rendering of a grid of cubes. The cubes in the foreground are a vibrant red, while those receding into the background transition through shades of grey and white, creating a strong sense of depth and perspective.

PT

POSITIVE

TECHNOLOGIES

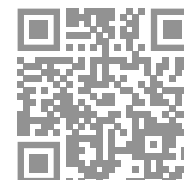
КАТАЛОГ
ПРОДУКТОВ



ПОЗИТИВНЫЙ ПОДХОД К КИБЕРБЕЗОПАСНОСТИ

ptsecurity.com

Узнайте, как защитить ваш бизнес
от современных киберугроз





ПРОДУКТЫ

ptsecurity.com

На странице каждого продукта вы можете узнать о сложности его внедрения и использования.

СЛОЖНОСТЬ ВНЕДРЕНИЯ



НИЗКАЯ
Можно внедрить самостоятельно



СРЕДНЯЯ
Может внедрить партнер



ВЫСОКАЯ
Может внедрить Positive Technologies

СЛОЖНОСТЬ ИСПОЛЬЗОВАНИЯ



НАЧАЛЬНЫЙ УРОВЕНЬ



СРЕДНИЙ УРОВЕНЬ



ЭКСПЕРТНЫЙ УРОВЕНЬ

Positive Technologies более 18 лет создает инновационные решения в сфере кибербезопасности.

Продукты и сервисы компании позволяют выявить, верифицировать и компенсировать реальные бизнес-риски, которые могут быть реализованы через IT-инфраструктуру предприятий различных отраслей. Наша технологическая база основана на многолетнем исследовательском опыте и экспертизе ведущих отечественных и зарубежных специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяет более 2000 компаний в 30 странах мира. В числе наших клиентов 80% участников рейтинга «Эксперт 400» в России и более двухсот зарубежных компаний.

Данный каталог содержит полный перечень наших продуктов, комплексных решений и экспертных сервисов, которые помогут выстроить надежную защиту вашей компании от кибератак.

Заказать бесплатный пилот продукта или решения, а также запросить консультацию по услугам вы можете, отправив заявку на sales@ptsecurity.com.

MAXPATROL SIEM

Система выявления инцидентов с уникальным подходом к обеспечению прозрачности IT-инфраструктуры и глубокой экспертизой в выявлении угроз

**ЗАДАЧИ,
КОТОРЫЕ
ВЫ МОЖЕТЕ
РЕШИТЬ**

- ✓ Выявление сложных угроз и атак, составление комплексной картины происходящего в IT-инфраструктуре
- ✓ Снижение трудозатрат экспертов ИБ на мониторинг состояния инфраструктуры и написание правил



**Выявляет
даже самые
новые угрозы**

Знания экспертов РТ регулярно передаются в базу РТ Knowledge Base в виде пакетов экспертизы. Пользователи MP SIEM получают пакеты из РТ KB, что помогает детектировать актуальные техники и тактики атак до наступления последствий и снижает потребность в специалистах ИБ.

**Дает детальную
информацию
об инфраструктуре**

Уникальная технология детальной инвентаризации дает MP SIEM подробную информацию о каждом активе и уязвимых местах, показывая оператору ИБ, что происходит в инфраструктуре. Из коробки доступна поддержка 300+ различных систем, включая большой спектр российского ПО.

**Работает
в сетях
любого
масштаба**

Среди 150+ внедрений MaxPatrol SIEM присутствуют: серверы с нагрузкой до 60 000 событий в секунду; иерархические инсталляции по всей территории РФ (до 15 подчиненных серверов); геораспределенные кластеры; сложные системы отчетности и мониторинга источников событий.

PT SANDBOX

Передовая песочница
с возможностью кастомизации
виртуальных сред

**ЗАДАЧИ,
КОТОРЫЕ
ВЫ МОЖЕТЕ
РЕШИТЬ**

- ✓ Выявление угроз, связанных с вредоносным ПО, в почте, файловых хранилищах, пользовательском веб-трафике и на веб-порталах
- ✓ Обеспечение защиты от целевых и массовых атак с использованием современного вредоносного ПО



**Защищает
именно вашу
инфраструктуру**

Продукт позволяет гибко настраивать виртуальные среды в соответствии с реальными рабочими станциями. Это обеспечивает высокое качество детекта даже в случае, если вредоносное ПО заточено специально под инфраструктуру компании.

**Обнаруживает
угрозы не только
в файлах,
но и в трафике**

PT Sandbox проверяет на наличие угроз весь трафик, который генерируется в процессе анализа подозрительного файла, а также расшифровывает TLS-трафик, выявляя в нем вредоносную активность.

**Выявляет
массовые атаки
и атаки,
не обнаруженные
ранее**

Продукт осуществляет пре-филтеринг файлов с помощью семи антивирусов, обеспечивая защиту от массовых угроз, а также проводит автоматический ретроспективный анализ после обновления базы знаний, выявляя атаки, которые не были замечены ранее.

PT MULTISCANNER

Многоуровневая система
защиты от вирусных угроз

**ЗАДАЧИ,
КОТОРЫЕ
ВЫ МОЖЕТЕ
РЕШИТЬ**

- ✓ Обеспечение мультивендорной антивирусной защиты IT-инфраструктуры
- ✓ Быстрая локализация вирусных угроз: централизованное отслеживание этапов и участников распространения вредоносного ПО



Защищает от массовых угроз

Продукт осуществляет проверку файлов с помощью нескольких антивирусов и по репутационным спискам, пополняемым экспертами PT ESC в ходе расследований инцидентов. Это позволяет защититься как от массовых угроз, так и от атак хакерских группировок.

Следит за всеми потоками данных

Продукт анализирует на наличие угроз файлы, которые попадают в корпоративную сеть в сетевом и почтовом трафике, загружаются в веб-приложения и файловые хранилища компании.

Выявляет атаки, не замеченные в прошлом

Благодаря автоматическому ретроспективному анализу PT MultiScanner находит вредоносное ПО, которое не было обнаружено ранее. Повторная проверка файлов запускается после обновлений баз данных продукта.

PT NETWORK ATTACK DISCOVERY

Система анализа сетевого трафика (NTA)
для выявления атак и их расследования

**ЗАДАЧИ,
КОТОРЫЕ
ВЫ МОЖЕТЕ
РЕШИТЬ**



- ✓ Обеспечение прозрачности происходящего в сети и получение подробной картины активности в инфраструктуре
- ✓ Повышение эффективности работы SOC, упрощение реагирования на инциденты и расследования атак
- ✓ Выявление сложных атак в трафике по большому количеству признаков



**Видит опасную
активность
во внешнем
и внутреннем
трафике**

PT NAD определяет более 50 протоколов, разбирает до уровня L7 включительно 30 наиболее распространенных из них и позволяет получить полную картину активности как на периметре, так и внутри инфраструктуры.

**Использует
передовые
технологии
выявления угроз**

Для выявления атак на ранних стадиях продукт использует технологии машинного обучения, глубокую аналитику, собственные правила детектирования угроз, индикаторы компрометации и ретроспективный анализ.

**Выявляет
присутствие угроз
по множеству
признаков**

Продукт обнаруживает вредоносное ПО в зашифрованном трафике, горизонтальное перемещение злоумышленника, скрытые каналы (туннелирование), коммуникацию с автоматически сгенерированными доменами, эксплуатацию уязвимостей и хакерский инструментарий.

PT APPLICATION FIREWALL

Мощный инструмент защиты веб-приложений от современных угроз

**ЗАДАЧИ,
КОТОРЫЕ
ВЫ МОЖЕТЕ
РЕШИТЬ**

- ✓ Обеспечение непрерывности бизнес-процессов и соответствия стандартам
- ✓ Обеспечение всесторонней и непрерывной защиты веб-приложений, в том числе постоянно обновляемых, а также защиты пользователей и инфраструктуры



**С высокой
точностью
определяет
веб-угрозы**

Комбинация позитивной и негативной моделей безопасности, анализ поведения пользователей и машинное обучение позволяют свести число ложных срабатываний к минимуму и мгновенно выявлять угрозы, в том числе попытки DDoS-и автоматизированных атак и атаки нулевого дня.

**Позволяет
гибко
настраивать
защиту**

Предустановленные шаблоны политик безопасности можно адаптировать к специфике приложений. Гибкость и высокий уровень автоматизации позволяют надежно защищать приложения любого типа (даже при непрерывном их обновлении) с высоким уровнем отказоустойчивости.

**Автоматически
приоритизирует
угрозы**

Уникальный для WAF механизм корреляции выстраивает цепочки атак, позволяет выявлять АРТ и автоматически приоритизировать обнаруженные угрозы по уровню риска. Это помогает мгновенно видеть серьезные угрозы и принимать меры противодействия.

PT APPLICATION INSPECTOR

Универсальный инструмент для анализа кода, выявляющий ошибки и уязвимости в веб-приложениях

**ЗАДАЧИ,
КОТОРЫЕ
ВЫ МОЖЕТЕ
РЕШИТЬ**

- ✓ Обеспечение безопасности веб-приложения на всех этапах его создания
- ✓ Выстраивание в компании эффективного процесса безопасной разработки
- ✓ Снижение стоимости исправления уязвимостей в ПО благодаря раннему выявлению



**С высокой
точностью выявляет
и автоматически
подтверждает
уязвимости**

Продукт выявляет уязвимости с минимумом ложных срабатываний благодаря комбинации статического, динамического и интерактивного методов анализа. Каждую уязвимость PT AI проверяет и подтверждает с помощью автоматически генерируемых запросов — безопасных эксплойтов.

**Позволяет
защищать уже
работающие
приложения**

Для защиты уже работающих приложений в PT AI существует механизм virtual patching — результаты анализа автоматически выгружаются в межсетевой экран уровня веб-приложений PT Application Firewall, который блокирует атаки на приложение на время исправления кода.

**Гибко и быстро
встраивается
в процессы
организации**

Продукт поддерживает процесс безопасной разработки (SSDL), интегрируется с основными средами разработки, системами контроля версий и отслеживания ошибок и может быть встроен в процессы непрерывной интеграции и непрерывной поставки.

PT ISIM

Программно-аппаратный комплекс,
обеспечивающий непрерывный
мониторинг защищенности сети АСУ ТП

**ЗАДАЧИ,
КОТОРЫЕ
ВЫ МОЖЕТЕ
РЕШИТЬ**

✓ Обеспечение контроля над векторами атак и соблюдением политик ИБ, специфических для конкретного промышленного объекта

✓ Выявление кибератак и неавторизованных действий персонала на ранних стадиях



**Непрерывно
инвентаризирует
и профилирует сеть**

Не оказывая влияния на технологический процесс, PT ISIM непрерывно инвентаризирует элементы сети АСУ ТП, контролирует ее целостность и оповещает о критически важных изменениях, которые могут являться признаком нарушения ИБ и требовать немедленного реагирования.

**С высокой
точностью
детектирует
угрозы
и аномалии**

PT ISIM использует собственную базу данных индикаторов промышленных угроз (PT ISTI) и благодаря комбинации сигнатурных методов обнаружения атак и механизма поведенческого анализа позволяет эффективно выявлять кибератаки на ранней стадии.

**Позволяет
соответствовать
требованиям**

PT ISIM обеспечивает реализацию широкого перечня мер защиты АСУ ТП в соответствии с 187-ФЗ, требованиями приказов ФСТЭК № 31, 239, 196, отраслевых стандартов и является ключевым звеном для системы ГосСОПКА.

MAXPATROL 8

Универсальное средство
автоматизированного анализа
защищенности и контроля
соответствия стандартам

**ЗАДАЧИ,
КОТОРЫЕ
ВЫ МОЖЕТЕ
РЕШИТЬ**

✓ Регулярный и комплексный
контроль состояния защищен-
ности всей IT-инфраструктуры

✓ Построение процесса управ-
ления уязвимостями на KPI,
прозрачных для руководства



**Охватывает все
информационные
ресурсы компании**

Поддерживает и позволяет контролировать параметры 1000+ платформ и приложений: сетевую и системную инфраструктуры, серверы, беспроводные сети и сети IP-телефонии, базы данных, приложения, системы ERP, веб-приложения, АСУ ТП.

**Выявляет
уязвимости
с максимальной
точностью**

Выявляет уязвимости, ошибки конфигурации компонентов информационных систем, проверяет соответствие настроек информационных систем требованиям ИБ. Использует методы черного и белого ящика для анализа защищенности узлов, проверяет актуальность уязвимостей, обеспечивая низкое число ложных срабатываний.

**Упрощает анализ
соответствия
стандартам
и политикам ИБ**

Содержит встроенные политики безопасности, позволяющие оценить соответствие инфраструктуры основным стандартам (ISO 27001/27002, PCI DSS и CIS). Также позволяет настроить специальные политики для контроля выполнения собственных корпоративных правил безопасности.



Построение распределенных систем кибербезопасности

Решение для обеспечения кибербезопасности компаний с иерархической структурой: крупных холдингов, корпораций с сетью филиалов, федеральных органов власти

Предполагает создание центра кибербезопасности на базе головного офиса и центров мониторинга в крупных филиалах, а также размещение сенсоров на нижних уровнях инфраструктуры.

Состав решения

MaxPatrol SIEM	PT Network Attack Discovery
PT MultiScanner	ПТ Ведомственный центр
MaxPatrol 8	Сенсоры

Преимущества



Повышает защищенность на всех уровнях инфраструктуры.



Централизует мониторинг средств защиты информации в компании.



Позволяет выстроить процессный подход к работе с инцидентами ИБ.



Позволяет выполнить требования регулирующих органов.

Построение SOC

Решение для любых компаний, планирующих построить собственный security operation center

Предполагает последовательные шаги: аудит периметра, защиту периметра, защиту внутренней инфраструктуры, введение продвинутых методов защиты и обучение специалистов SOC.

Состав решения

- MaxPatrol SIEM
- PT Network Attack Discovery
- MaxPatrol 8
- PT MultiScanner
- PT ISIM
- PT Application Inspector
- PT Application Firewall
- Услуги экспертного центра PT ESC

Преимущества



Позволяет выявлять атаки, своевременно реагировать и минимизировать потери.



Позволяет развивать внутреннюю экспертизу в области ИБ.



Устраняет наличие «полочного» ПО (shelfware).



Повышает трудозатраты злоумышленников на вход.

Раннее выявление целевых атак

Решение для крупных компаний, холдингов и корпораций с сетью филиалов, выстраивающих защиту от целевых атак (APT)

Помогает максимально быстро обнаружить скрытое присутствие злоумышленника в инфраструктуре и воссоздать полную картину атаки для эффективного расследования.

Состав решения

- PT Network Attack Discovery
- PT Sandbox
- Услуги экспертного центра PT ESC

Преимущества



Выявляет присутствие атакующего на периметре и в инфраструктуре.



Автоматически обнаруживает не выявленные ранее факты взлома инфраструктуры.



Использует уникальные технологии обнаружения атак в трафике.



Применяет передовой динамический анализ для выявления опасных файлов.

Защита приложений от веб-угроз


Решение для среднего и крупного бизнеса, которому требуется защита корпоративных веб-приложений на всех стадиях жизненного цикла

Позволяет внедрить в компании процесс безопасной разработки и эффективно создавать безопасные приложения, а также защитить от кибератак уже работающие приложения.

Состав решения

- PT Application Firewall
- PT Application Inspector
- Экспертная поддержка специалистов PT

Преимущества

-  Надежно защищает уязвимые приложения на время исправлений кода.
-  Снижает стоимость исправлений уязвимостей благодаря раннему выявлению.
-  Позволяет повысить эффективность бизнес-процессов компании.

Обеспечение безопасности объектов КИИ


Решение для субъектов КИИ, планирующих построить систему безопасности объекта КИИ в соответствии с требованиями закона № 187-ФЗ

Обеспечивает выполнение требований и автоматизирует взаимодействие с ГосСОПКА. Может быть использовано в том числе для распределенных инфраструктур.

Состав решения

- MaxPatrol SIEM
- PT Network Attack Discovery
- MaxPatrol 8
- PT MultiScanner
- PT ISIM
- PT Application Inspector
- PT Application Firewall
- Услуги экспертного центра PT ESC
- PT Ведомственный центр

Преимущества

-  Позволяет выявлять атаки на ранней стадии и в ретроспективе.
-  Позволяет эффективно расследовать возникающие инциденты ИБ.
-  Позволяет непрерывно взаимодействовать с ГосСОПКА.
-  Позволяет соответствовать требованиям регулирующих органов.

Создание центра ГосСОПКА и взаимодействие с НКЦКИ

Решение для организаций, планирующих поэтапное создание центра ГосСОПКА

Помогает постепенно развивать внутреннюю экспертизу ИБ, выстраивать процессы в подразделениях ИБ и успешно отражать как типовые атаки, так и новые их виды.

Состав решения

MaxPatrol SIEM	PT Network Attack Discovery	
MaxPatrol 8	PT MultiScanner	PT ISIM
PT Application Inspector	PT Application Firewall	
Услуги экспертного центра PT ESC		
ПТ Ведомственный центр		

Защита КИИ и взаимодействие с центром ГосСОПКА

Решение для компаний до 250 узлов и территориальных подразделений крупных компаний, позволяющее реализовать функций безопасности значимых объектов КИИ и построить взаимодействие с главным центром ГосСОПКА

Обеспечивает простой и удобный процесс информирования НКЦКИ в требуемом формате.

Состав решения

MaxPatrol SIEM	PT Network Attack Discovery
MaxPatrol 8	PT MultiScanner
ПТ Ведомственный центр	Оборудование

Преимущества

- 


Продукты имеют сертификаты соответствия ФСТЭК России.
- 


Все продукты включены в единый реестр российского программного обеспечения.
- 

Все продукты входят в единую экосистему Positive Technologies.

Преимущества

- 

Позволяет соответствовать требованиям ФСТЭК России и ФСБ России.
- 

Обеспечивает надежную всестороннюю киберзащиту компании.
- 

Автоматизирует реагирование на инциденты и взаимодействие с НКЦКИ (через ПТ ВЦ).
- 

Централизованное управление всеми продуктами и единая техподдержка.

Построение SOC в небольших компаниях



Решение для компаний до 500 узлов,
планирующих поэтапно построить собственный
мини-SOC (security operation center)



Обеспечивает реализацию
внутри компании основных задач
SOC и выполнение требований
законодательства.

Состав решения

MaxPatrol SIEM	PT Network Attack Discovery
MaxPatrol 8	PT MultiScanner
ПТ Ведомственный центр	Оборудование

Преимущества

-  Позволяет соответствовать требова-
ниям ФСТЭК России и ФСБ России.
-  Обеспечивает надежную всесторон-
нюю киберзащиту компании.

-  Автоматизирует реагирование на инциденты
и взаимодействие с НКЦКИ (через ПТ ВЦ).
-  Централизованное управление всеми
продуктами и единая техподдержка.





Услуги по анализу защищенности

Услуги по оценке уровня защищенности направлены на глубокий анализ различных аспектов корпоративной информационной безопасности или всей системы управления ИБ в компании в целом. Они позволяют своевременно выявить слабые места в защите и принять необходимые меры для их устранения.

>> Тестирование на проникновение

Поможет оценить риск и возможности проникновения злоумышленника в сеть компании.

>> Анализ защищенности беспроводных сетей

Поможет повысить безопасность корпоративной Wi-Fi инфраструктуры.

>> Анализ конфигураций сетевого оборудования

Поможет оценить и повысить безопасность настроек устройств сети.

>> Оценка осведомленности пользователей

Поможет повысить готовность персонала к кибератакам.

>> Анализ защищенности веб-приложений

Поможет существенно снизить риск успешной кибератаки как на внешний, так и внутренний периметр компании.

>> Анализ защищенности ERP-систем

Поможет оценить риски ИБ, связанные с критически значимыми системами управления бизнесом.

>> Анализ защищенности мобильных приложений

Поможет повысить защищенность данных ваших клиентов и предотвратить мошенничество.

Услуги мониторинга и реагирования на инциденты ИБ

Positive Technologies Expert Security Center — экспертное подразделение, оказывающее услуги по реагированию, расследованию инцидентов и мониторингу защищенности корпоративных систем на базе продуктов Positive Technologies. В основе услуг PT ESC — более 16 лет опыта в анализе защищенности, расследовании инцидентов и деятельности крупнейших APT-группировок, а также мониторинга безопасности крупных компаний.

»» **Мониторинг периметра**

Помогает непрерывно выявлять проблемы, возникающие на сетевом периметре компании.

»» **Поиск следов компрометации**

Позволяет выявить следы подготовки к хакерской атаке и признаки компрометации инфраструктуры.

»» **Реагирование и расследование**

Поможет существенно снизить риск успешной кибератаки как на внешний, так и внутренний периметр компании.

Услуги для непрерывного повышения защищенности бизнеса от киберугроз

Набор уникальных услуг по повышению защищенности бизнеса от киберугроз поможет вам непрерывно оценивать уязвимость компании перед действиями реальных злоумышленников и оперативно принимать меры по защите от кибератак и устранению последствий.

Сочетание сервисов моделирования сложных атак и услуг по выявлению угроз позволяет эффективно выстроить процессы обеспечения защиты ваших бизнес-процессов и свести к минимуму возможный финансовый и репутационный ущерб от кибератак.

»» **Эмуляция APT-атаки**

Поможет оценить и повысить устойчивость вашего бизнеса перед реальной атакой.

»» **Pentest 365**

Обеспечит непрерывное выявление актуальных векторов кибератак на вашу компанию.

»» **Red Team vs Blue Team**

Поможет в обнаружении угроз и совершенствовании стратегии реагирования на них.



ptsecurity.com