positive technologies

MaxPatrol 8

Система контроля защищенности и соответствия стандартам

ПРЕИМУЩЕСТВА MAXPATROL 8

ОБШИРНАЯ БАЗА ЗНАНИЙ

Более 87 000 уязвимостей способна выявлять MaxPatrol 8. Эксперты Positive Technologies исследуют новые угрозы и регулярно передают данные о способах их выявления в единую базу

ВЫСОКИЙ УРОВЕНЬ ЭКСПЕРТИЗЫ

Более 500 признанных экспертов по информационной безопасности работают над продуктом

ПОДДЕРЖКА БОЛЬШОГО КОЛИЧЕСТВА СИСТЕМ

Более 1000 разнообразных систем, в том числе российских

ВСЕСТОРОННЯЯ ПРОВЕРКА СООТВЕТСТВИЯ СТАНДАРТАМ

MaxPatrol 8 содержит более 300 стандартов безопасности и дает возможность добавлять политики ИБ

ЗАКАЖИТЕ ПИЛОТНОЕ ВНЕДРЕНИЕ

Система MaxPatrol 8 предназначена для контроля защищенности информационных систем и их соответствия стандартам безопасности. В основе MaxPatrol 8 лежат механизмы тестирования на проникновение, системных проверок и контроля соответствия стандартам. Это позволяет получать объективную оценку состояния защищенности IT-инфраструктуры в целом, а также отдельных подразделений, узлов и приложений, что необходимо для своевременного обнаружения уязвимостей и предотвращения атак с их использованием.

PENTEST	AUDIT	COMPLIANCE
Режим тестирования на проникновение реализует проверки, типичные для сканера сетевого уровня: инвентаризационные, «баннерные» проверки, фаззинг, подбор учетных записей. Также в MaxPatrol 8 есть специализированные проверки для анализа защищенности веб-приложений и СУБД.	Режим системного сканирования позволяет провести инвентаризацию аппаратного и программного обеспечения, сбор конфигурационных параметров ОС, служб, СУБД, прикладных систем и средств защиты информации, выявить уязвимости, ошибки конфигурации и контролировать обновления.	Режим контроля соответствия стандартам позволяет проверять выполнение требований российских регулирующих органов, международных и отраслевых стандартов, корпоративных регламентов.

Охватывает все информационные ресурсы компании

Поддерживает и позволяет контролировать параметры более чем 1000 систем: сетевые и системные инфраструктуры, серверы, беспроводные сети и IP-телефонию, базы данных, ERP-системы, приложения, в том числе веб-приложения, АСУ ТП.

Выявляет уязвимости с максимальной точностью

Выявляет уязвимости, ошибки конфигурации компонентов информационных систем, проверяет соответствие их параметров 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) и более чем 180 техническим стандартам безопасности. Также позволяет настроить собственные политики для контроля выполнения корпоративных правил безопасности.

MaxPatrol 8 —
стандарт анализа защищенности в России

Более 10 лет на рынке продуктов информационной безопасности

ГОСУДАРСТВЕННАЯ СЕРТИФИКАЦИЯ

MaxPatrol 8 имеет сертификаты ФСТЭК России и Минобороны России, поддерживает выявление уязвимостей, включенных в банк данных угроз безопасности ФСТЭК, и позволяет выполнить требования по защите:

- критической информационной инфраструктуры (приказы ФСТЭК № 239 и 235)
- персональных данных (приказ ФСТЭК № 21)
- информации в ГИС, в АСУ ТП и в информационных системах общего пользования (приказы ФСТЭК № 19, 31 и 489)

Автоматизирует процессы ИБ и контролирует их эффективность

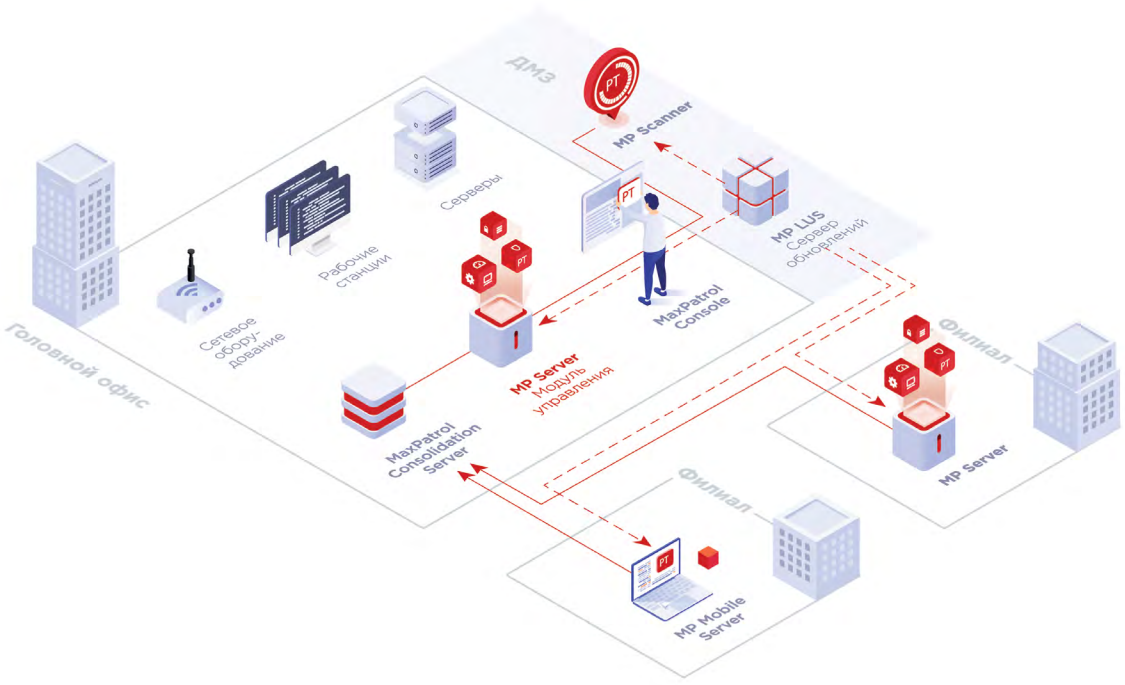
MaxPatrol 8 автоматизирует процессы инвентаризации ресурсов, управления уязвимостями, контроля соответствия политикам безопасности и контроля изменений, что позволяет снизить затраты на аудит и контроль защищенности, подготовку IT-проектов и проектов по ИБ. Можно оценивать эффективность подразделений ИТ и ИБ с помощью расширяемого набора метрик безопасности и KPI — отслеживать состояние системы, динамику прохождения проверок, проводить сравнение подразделений.

MaxPatrol 8 наиболее эффективен:

- как инструмент контроля безопасности и соответствия стандартам для специалистов центра управления ИБ компании (security operations center, SOC)
- для проверки работы отделов ИТ и ИБ, а также качества услуг, оказываемых штатными сотрудниками и сторонними подрядчиками
- для предоставления корпоративным клиентам услуг по обеспечению безопасности информационных систем на условиях аутсорсинга
- для проведения тестов на проникновение и проверок уровня безопасности внешними и внутренними аудиторами, регулирующими органами.

Архитектура MaxPatrol 8

Архитектура продукта обеспечивает гибкое масштабирование и позволяет внедрять систему в компаниях любого размера. MaxPatrol 8 можно адаптировать к своей инфраструктуре — выбрать количество серверов, сканеров, режимы сканирования.



ptsecurity.com
pr@ptsecurity.com

vk.com/ptsecurity,
t.me/Positive_Technologies,
twitter.com/ptsecurity,
vk.com/phdays