POSITIVE TECHNOLOGIES

Система оценки защищенности и соответствия стандартам

MaxPatrol

Краткое описание продукта

MAXPATROL: КЛЮЧЕВЫЕ ОСОБЕННОСТИ

MaxPatrol 8 — система оценки защищенности, которая выполняет сканирование в режиме Аудит (проверку на уязвимости конфигурации систем и на наличие уязвимостей), проверку на соответствие стандартам (Compliance) и тестирование на проникновение методом черного ящика, а также выпускает отчеты различного типа по результатам сканирования. Продукт может использоваться для проверки на соответствие стандарту PCI DSS, ISO, GDPR. MaxPatrol позволяет проводить тестирование на проникновение, оценку приложений, инвентаризацию сетей и проверку сетевого периметра.

Межплатформенная совместимость:

- сетевое оборудование Cisco, Juniper, Check Point, Arbor, Huawei, Nortel, Alcatel и др.;
- беспроводные VOIP-устройства и телекоммуникационное оборудование;
- операционные системы Windows, Linux, IBMAIX, HP-UX и Oracle Solaris;
- базы данных, включая Microsoft SQL, Oracle, IBMDB2, PostgreSQL, MySQL, Sybase и SAP Hana;
- настольные приложения: веб-браузеры, офисные приложения, службы мгновенных сообщений;
- инфраструктурные приложения, включая Active Directory, Microsoft Exchange, IBM Lotus, Microsoft IIS, Apache, IBM WebSphere, Apache Tomcat;
- платформы терминалов и виртуализации: VMware vSphere/ESXi, Microsoft Hyper-V, Citrix XenApp и др.;
- системы безопасности: personal IPS, firewalls, антивирусы и др.;
- критически значимые производственные системы: ERP, banking & billing systems, в том числе SAP R/3 и SAP NetWeaver.

Безопасность веб-приложений — оценка веб-приложений, написанных на AJAX, JSON, Flash и Java.

Анализ безопасности систем ERP — с использованием различных руководств, таких как SAP Security Guides, ISACA (ITAF).

Аудит политики паролей — проверка методами черного и белого ящика:

- для систем удаленного доступа и VPN (RDP, VNC, Telnet, SSH, RCP и т. п.);
- систем совместного использования файлов и каталогов;
- протоколов приложений: SAP, Oracle, SQL, Web, Email и т. п.;
- настольных приложений, например IM и браузеров.

Обнаружение вредоносного ПО — технология обнаружения небезопасного кода, вредоносного ПО и троянов во всех системах без использования агентов.

Автономная проверка целостности системы — встроенные базы для компонентов каждой системы позволяют обнаруживать инциденты или нежелательные изменения.

Гибкая система отчетности — поддерживает автоматизированные процессы, в том числе инвентаризацию, управление изменениями, контроль соответствия стандартам и производительности ИТ.

Интерфейс для интеграции на базе XML — позволяет создать единую инфраструктуру информационной безопасности, реализующую управление ресурсами, связь со службой поддержки, управление рисками, управление исправлениями, SIM/SIEM, IPS- и WAF-тестирование на проникновение, NAC/NAP.

Портал отчетности на базе QlikView — наглядно отображает уровень защищенности по отдельным регионам (например, по субъектам федерации), что особенно полезно при распределенной установке с большим количеством узлов. Это позволяет получить более развернутую и подробную аналитическую картину, дополняя возможности модуля отчетности MaxPatrol 8.

MAXPATROL В ЦИФРАХ

100 000+	уязвимостей. Это число растет ежедневно по мере того, как наш исследовательский центр обнаруживает и вносит в базу новые уязвимости.
10 000+	параметров конфигурации, которые система MaxPatrol способна обнаружить в более чем 100 платформах и приложениях
1 000+	систем, с которыми может работать MaxPatrol.
1 000+	готовых политик, предоставляемых с каждым внедрением MaxPatrol. Политики безопасности полностью соответствуют основным стандартам и нормам систем ИТ и ИБ.
1 000+	компаний, уже использующих MaxPatrol для обеспечения безопасности своих информационных систем.

MAXPATROL: ПРЕИМУЩЕСТВА ДЛЯ БИЗНЕСА

- **Единый инструмент для согласованности результатов.** С помощью MaxPatrol вы сможете комплексно контролировать состояние защищенности всей IT-инфраструктуры и оперативно реагировать на все значимые инциденты.
- **Автоматизация для эффективности.** MaxPatrol не требует установки программ-агентов на удаленных системах и предоставления повышенных привилегий, а также не вмешивается в работу информационной системы. Преимущество MaxPatrol — самое низкое число ложных срабатываний в отрасли.
- **Разноуровневая система отчетности для целостного понимания.** Получайте отчетность, позволяющую составить полное представление о реальной защищенности всех сегментов IT-инфраструктуры компании.
- **Гибкая настройка для формализации процессов.** Установите встроенные в MaxPatrol политики безопасности, чтобы оценить соответствие вашей системы основным стандартам (ISO 27001/27002, PCI DSS и CIS). Настройте специальные политики для контроля выполнения собственных корпоративных правил безопасности.
- **Гибкость и масштабируемость для нестандартных проектов.** Воспользуйтесь возможностью масштабирования системы MaxPatrol и разнообразием вариантов ее комплектации, чтобы получить оптимальное программное решение.
- **Поддержка экспертов для уверенности.** Наша команда разработчиков регулярно обновляет базу знаний MaxPatrol 8 по мере обнаружения новых угроз и уязвимостей и выхода новых требований. В вашем распоряжении — компетенции экспертов Positive Technologies, активно сотрудничающих с мировыми IT-вендорами — Oracle, HP, IBM, Microsoft и др.
- **Преимущества российской разработки для удобства работы.** Продукт имеет русскоязычный интерфейс, реализована возможность работы модулей системы по узким каналам связи, учтены требования российского законодательства в области информационной безопасности. MaxPatrol имеет сертификаты ФСТЭК России и Минобороны России, поддерживает выявление уязвимостей, включенных в банк данных угроз безопасности ФСТЭК, и может применяться для контроля защищенности информации в любых государственных информационных системах и информационных системах персональных данных.

MAXPATROL В ДЕЙСТВИИ

Сегодня крупнейшие коммерческие компании и государственные структуры, международные банки и телекоммуникационные холдинги используют MaxPatrol для поддержания высокого уровня безопасности своих операционных систем, баз данных, ERP-систем и веб-приложений.

MaxPatrol — масштабируемая система, с помощью которой можно контролировать уровень защищенности как небольших, так и крупных предприятий, распределенных по всей стране, через единую консоль управления. Один из крупнейших на сегодняшний день проектов по внедрению MaxPatrol охватил системы восьми подразделений заказчика, находящиеся в 26 странах. Сохраненная копия трафика позволяет в любой момент провести ретроспективный анализ и расследование инцидента.

MaxPatrol наиболее эффективен:

- для управления контролем безопасности и соответствия стандартам в составе общего центра управления информационной безопасностью компании (security operations center, SOC);
- проверки работы отделов ИТ и ИБ, а также качества услуг, оказываемых как штатными сотрудниками, так и сторонними компаниями;
- предоставления услуг по обеспечению безопасности информационных систем для корпоративных клиентов на условиях аутсорсинга;
- проведения тестирования на проникновение и проверок безопасности для внешних и внутренних аудиторов и регуляторов.

Подробную информацию о системе MaxPatrol и примеры внедрения смотрите на сайте ptsecurity.com

УВЕЛИЧИВАЙТЕ ЭФФЕКТИВНОСТЬ. УПРАВЛЯЙТЕ РИСКАМИ. СОКРАЩАЙТЕ ЗАТРАТЫ

Система MaxPatrol обеспечивает комплексную оценку защищенности и соответствия стандартам информационной безопасности всей вашей IT-инфраструктуры

В современном высокотехнологичном мире на первый план выходит проблема защищенности корпоративных информационных систем. Каждый новый инцидент подтверждает: когда конфиденциальная информация уязвима, потенциальный ущерб деятельности и репутации компании достигает колоссальных размеров. Защита компании от внешних угроз — сложная и затратная задача, особенно когда возникает необходимость соответствовать растущему количеству правовых стандартов и требований регуляторов, разрабатываемых для предотвращения подобных угроз. Однако незащищенная система обойдется еще дороже.

В попытках найти компромисс многие компании решают эту задачу по частям, выбирая разные инструменты для каждой системы, отдела или региона. В результате им приходится увеличивать бюджет и нанимать большое количество высокооплачиваемых специалистов, которые вручную тестируют и настраивают все системы. Снизить временные и денежные затраты позволит система MaxPatrol — комплексное программное решение, разработанное компанией Positive Technologies. MaxPatrol автоматизирует процесс поиска уязвимостей и контроля соответствия техническим стандартам в IT-инфраструктуре любого масштаба.

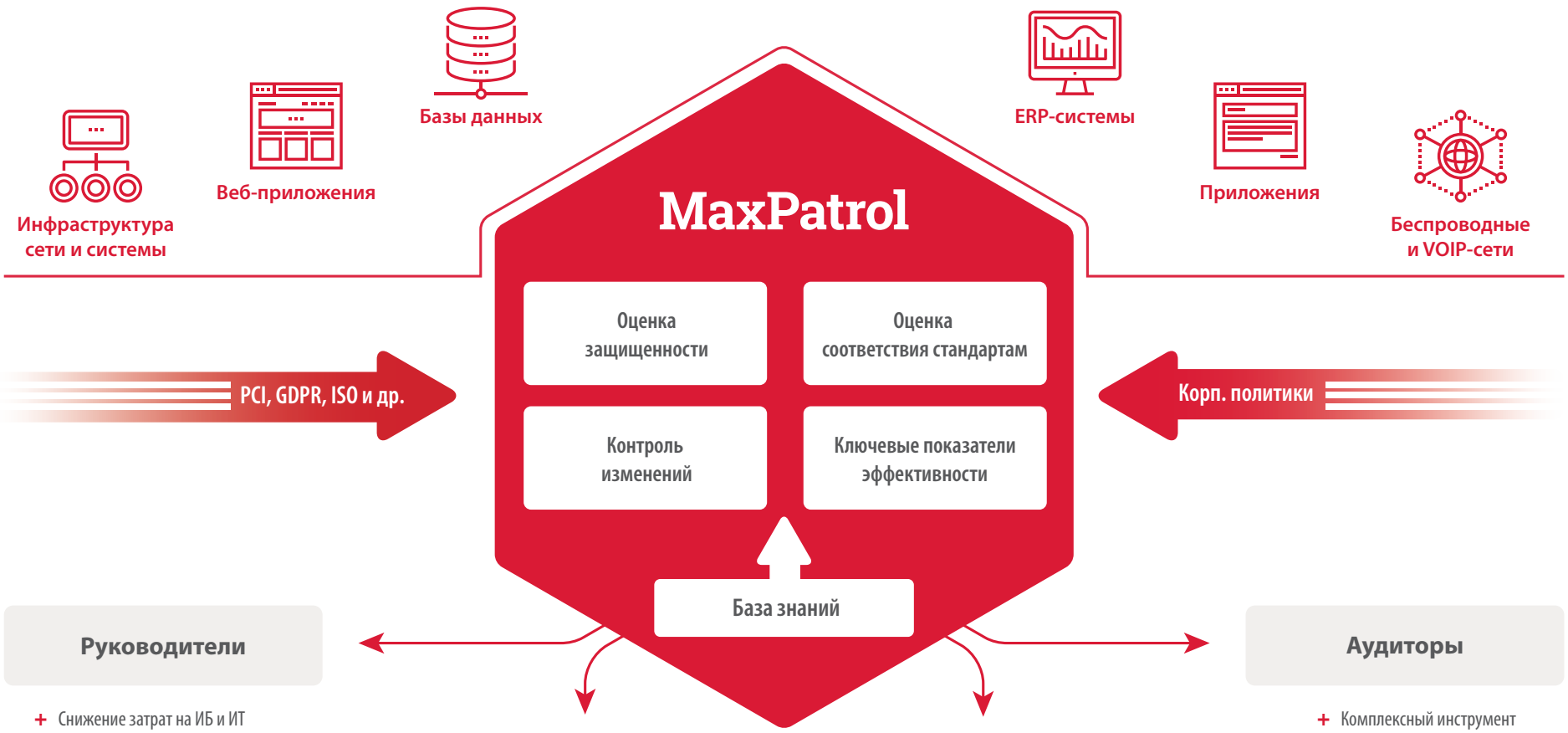
ЗАДАЧ МНОГО — РЕШЕНИЕ ОДНО

Используя систему контроля защищенности и соответствия стандартам MaxPatrol, вы получаете единое автоматизированное решение, которое позволит оценивать уровень защищенности информационных ресурсов всей организации.

MaxPatrol объединяет все необходимые механизмы оценки уровня безопасности: тестирование на проникновение (PenTest), системные проверки (Audit) и контроль соответствия стандартам (Compliance).

MaxPatrol позволяет централизованно управлять всеми элементами IT-инфраструктуры, не затрачивая дополнительные ресурсы на выполнение каждой отдельной задачи. С его помощью вы сможете получить целостную картину процессов ИБ в организации и контролировать параметры более 1000 платформ и приложений: сетевую и системную инфраструктуры, серверы, беспроводные сети и сети IP-телефонии, базы данных, приложения, системы ERP и веб-приложения. При этом MaxPatrol решает задачи безопасности информационных систем на всех структурных уровнях организации: от специалистов IT-отделов до первых лиц компании.

Автоматизация всех процессов в системе MaxPatrol, от сканирования до формирования отчетов, даст возможность повысить точность получаемой информации, экономить ресурсы и свести к минимуму влияние человеческого фактора.



Руководители

- Снижение затрат на ИБ и ИТ
- Высокоуровневая отчетность для бизнес-подразделений, KPI
- Соответствие стандартам организации
- Данные о текущем уровне защищенности

Специалисты по ИБ

- Выявление уязвимостей
- Управление соответствием стандартам
- Контроль соответствия политикам
- Контроль устранения уязвимостей

Специалисты по ИТ

- Простота внедрения
- Инвентаризация ресурсов ИТ
- Рекомендации по устранению уязвимостей
- Отчетность по обновлениям

Аудиторы

- Комплексный инструмент для оценки защищенности
- Поддержка основных международных стандартов
- Настраиваемая система отчетности

Страница MaxPatrol

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

pt@ptsecurity.com ptsecurity.com

MP_PB_A3.RUS.0003.08.AUG.21.2018