POSITIVE TECHNOLOGIES

XSpider или MaxPatrol 8 — что выбрать?

В документе представлено сравнение XSpider и MaxPatrol 8, описаны их назначение и возможные сценария использования

	XSpider	MaxPatrol 8
О продуктах		
Продукт	Сетевой сканер уязвимостей	Система контроля защищенности и соответствия стандартам
Технологии	+ Анализ защищенности	+ Расширенный анализ защищенности + Оценка соответствия стандартам
Основные задачи	+ Проверять сеть компании на наличие уязвимостей + Получать данные о составе сети + Автоматизировать процесс выявления уязвимостей	Выстроить в компании процессы vulnerability & compliance management: + Проверять инфраструктуру компании на наличие уязвимостей + Проводить инвентаризацию активов + Проводить глубокую проверку: выявить уязвимости операционных систем, приложений, баз данных, определить ошибки конфигураций + Отслеживать изменения в состоянии защищенности + Автоматизировать контроль защищенности в организации + Контролировать соответствие политикам безопасности различной степени сложности + Проверять системы на соответствие требованиям регуляторов

	XSpider	MaxPatrol 8
Для кого		
Размер компании	+ Предназначен для небольших предприятий	+ Для организаций любого масштаба + Подходит для компаний с филиальной структурой
Количество проверяемых сетевых узлов	До 10 000	Нет ограничений по количеству узлов
Лицензирование	XSpider лицензируется по проверяемым узлам. При расширении инфраструктуры необходимо докупать лицензии	MaxPatrol 8 лицензируется по количеству серверов. Можно вертикально и горизонтально масштабировать, докупать различные модули, подключать дополнительные сканеры
Отрасли	Государственный сектор, медицина, образование, промышленность, ТЭК, финансовые организации, телеком-операторы, ретейл и другие отрасли	
Для каких потребностей		
Выявление уязвимостей	+ Сканирует сеть на наличие уязвимостей + Тестирует на проникновение + Проверяет веб-приложения + Проверяет парольную политику + Идентифицирует уязвимости из БДУ ФСТЭК, CVE, OWASP Top 10, а также собственной базы данных Positive Technologies	+ Сканирует сеть на наличие уязвимостей + Тестирует на проникновение + Анализирует защищенность + Проверяет веб-приложения + Проверяет парольную политику + Выявляет уязвимости внутри ОС и приложений, через сканирование с учетной записью + Выявляет ошибки конфигурации + Сканирует базы данных + Идентифицирует уязвимости из БДУ ФСТЭК, CVE, OWASP Top 10, а также собственной базы данных Positive Technologies
Инвентаризация IT-инфраструктуры	+ Проводит инвентаризацию сети: обнаруживает узлы сети, открытые порты, идентифицирует серверные приложения + Видит сетевые изменения в IT-инфраструктуре	+ Проводит инвентаризацию информационных активов: идентифицирует аппаратные платформы и установленное ПО, собирает конфигурационные параметры ОС, служб, СУБД, прикладных систем и средств защиты информации + Видит сетевые изменения и изменения внутри информационных активов + Собирает и обрабатывает сведения о состоянии защищенности инфраструктуры

	XSpider	MaxPatrol 8
Отчетность	+ Формирует отчеты о выявленных уязвимостях с рекомендациями по устранению	+ Формирует отчеты о выявленных уязвимостях с рекомендациями по устранению + Все отчеты хранятся в одном месте + Поддерживаются разнообразные шаблоны отчетов: ▪ *отчет об инвентаризации,* ▪ *отчет об уязвимостях,* ▪ *отчет о соответствии стандартам,* ▪ *дифференциальный отчет,* ▪ *аналитический отчет.* + Есть возможность формировать отчет под себя, в том числе создавать собственные шаблоны
Оценка соответствия стандартам		+ Проверяет на соответствие техническим стандартам безопасности CIS, SAP, VMware и собственным стандартам Positive Technologies + Есть возможность создавать пользовательские стандарты + Есть встроенная поддержка высокоуровневых стандартов — PCI DSS, ISO/IEC 27001, приказов ФСТЭК
Дополнительные возможности		+ Разграничивает права доступа к системе + Наличие мобильного сервера, оптимизированного для работы с территориально удаленной сетью + Может интегрироваться с другими системами

Ответы на часто задаваемые вопросы

У меня несколько филиалов и нужно выявлять только сетевые уязвимости.

Что выбрать?

Если у вас мало филиалов и нет необходимости в централизованном сборе результатов сканирования, то подойдет XSpider.

В случае покупки XSpider необходимо обеспечить сетевую связность филиалов для сканирования удаленных площадок, чтобы система смогла подключиться к сканируемым узлам по локальной сети. Также можно купить несколько копий XSpider и сканировать узлы локально в каждом филиале, но тогда пользователь не сможет централизованно выгрузить результаты сканирования, придется выгружать отчеты по отдельности.

Если у вас растущая инфраструктура и вам важно собирать данные в одном месте, то подойдет MaxPatrol 8.

Вы можете купить только модуль Pentest MaxPatrol 8, в этом случае также необходимо обеспечить сетевую связанность филиалов. Или приобрести MaxPatrol 8 со следующими компонентами: MP Server и несколько дополнительных MP Scanner в режиме Pentest. В таком случае пользователь сможет просканировать узлы и собрать сведения о них в одном месте, не прибегая к сторонним системам.

У нас очень ограниченный бюджет и мы хотим выстроить процесс управления уязвимостями.

Что выбрать?

Для того чтобы построить процесс управления уязвимостями, необходимо выявлять уязвимости, ошибки конфигурации и проверять соответствие стандартам безопасности. Для решения такой задачи обычного сетевого сканера недостаточно, поэтому XSpider не подойдет. Рекомендуем MaxPatrol 8.

Если нужно выстроить процесс управления уязвимостями, но бюджет ограничен, то можно сделать это в несколько этапов. Сначала купить модуль Pentest MaxPatrol 8 и с его помощью выявить и устранить все сетевые уязвимости. Далее докупить модуль Audit и выявить уязвимости ОС, приложений, баз данных и ошибки конфигурации. И в последнюю очередь приобрести модуль Compliance, чтобы выявлять несоответствие стандартам безопасности и политикам компании.

У нас маленькая организация, но регулятор требует использовать сертифицированное решение.

Что выбрать?

Оба решения имеют сертификаты ФСТЭК России и могут применяться в составе автоматизированных систем для защиты:

- персональных данных (закон № 152-ФЗ, приказ ФСТЭК № 21);
- государственных информационных систем (приказ ФСТЭК № 17);
- информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах (приказ ФСТЭК № 31).

Если организация небольшая, то подойдет XSpider.

Если также требуются отчеты о соответствии инфраструктуры компании высокоуровневым стандартам (ISO/IEC 27001, PCI DSS, приказ ФСТЭК № 239), то подойдет MaxPatrol 8.

Отличия XSpider и модуля Pentest MaxPatrol 8

В основе модуля Pentest системы MaxPatrol 8 и XSpider лежат одни и те же технологии, поэтому, если вы выбираете между двумя модулями сетевого сканирования, то нужно ориентироваться на отличия полноценных систем:

Масштабирование. XSpider лицензируется по количеству сканируемых IP-адресов. При этом пользователь не может изменять это количество в течение срока действия лицензии. MaxPatrol 8 лицензируется по количеству серверов и модулей, не ограничивая число сканируемых IP-адресов. MaxPatrol 8 легко масштабируется, есть возможность подключать дополнительные сканеры, увеличивая мощность. Архитектура MaxPatrol 8 позволяет покрыть любую инфраструктуру с любым количеством узлов.

Модульность. MaxPatrol 8 — модульное решение. Например, вы можете приобрести только модуль Pentest. Спустя какое-то время вы можете дополнить MaxPatrol 8 другими модулями: добавить модули Audit и Compliance. Таким образом MaxPatrol 8 позволяет полностью выстроить процесс управления уязвимостями и контроля за соблюдением политик ИБ. В случае покупки XSpider пользователь получает только сетевой сканер без возможности расширения его функций.

Управление. XSpider не имеет ролевой модели, им можно управлять только из одной учетной записи. Ролевая модель MaxPatrol 8 позволяет назначать разным пользователям определенные права для работы с системой. Например, только на выпуск отчетов, на проведение только аудита или только пентеста.

Вывод

Перед выбором системы важно определить круг задач, которые наиболее важны для вашей компании, и дальнейший вектор развития инфраструктуры. На основе этой информации можно сделать выбор в пользу XSpider, модуля Pentest или полноценной системы MaxPatrol 8.

Если у вас остались вопросы — пишите по адресу sales@ptsecurity.com.