

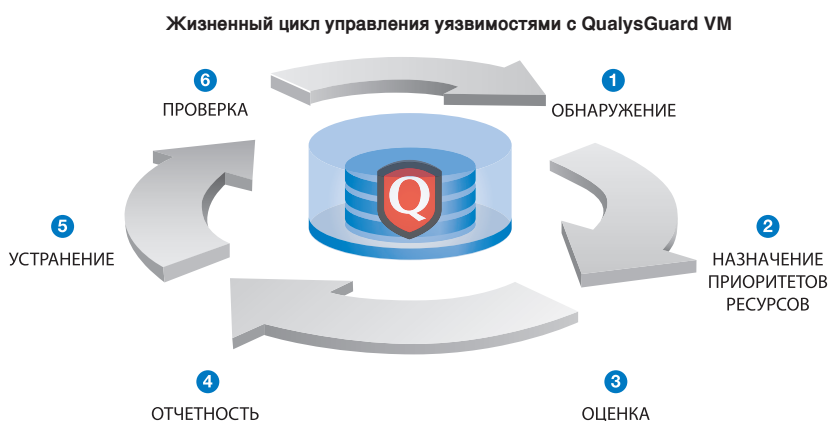
ИСПОЛЬЗУЙТЕ РЕШЕНИЕ ДЛЯ УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ И РИСК-МЕНЕДЖМЕНТА, ПРЕДОСТАВЛЯЕМОЕ «ПО ТРЕБОВАНИЮ»

QualysGuard[®] Vulnerability Management (VM) автоматизирует на предприятии процесс сетевого аудита и управления уязвимостями, который включает в себя: обнаружение сетевых ресурсов, построение наглядной карты сети, назначение приоритетов для ресурсов, предоставление отчетов по оценке уязвимостей и отслеживание процесса их устранения в соответствии с теми рисками, которые они несут для бизнеса. С помощью QualysGuard VM менеджеры безопасности смогут провести аудит, повысить защищенность сети и обеспечить ее соответствие, как внутренним политикам безопасности, так и внешними нормативными требованиями. Поскольку решение основано на технологии SaaS («ПО как сервис») и предоставляется как услуга, то нет необходимости разворачивать и внедрять какую-либо дополнительную инфраструктуру и соответственно нести затраты на ее сопровождение.

QualysGuard Vulnerability Management для крупных предприятий с распределенной инфраструктурой

QualysGuard VM позволяет предприятиям эффективно управлять уязвимостями своей сети и контролировать ее безопасность благодаря централизованным отчетам. Решение обеспечивает полный процесс их устранения, с применением апробированных средств, и встроенной системы заявок.

QualysGuard предоставляет обширные отчеты об уязвимостях, которые включают: оценку уровня их критичности, оценку времени, необходимого для их устранения, степени их воздействия на бизнес, а также анализ тенденций в области проблем безопасности.



Преимущества управления уязвимостями с QualysGuard VM:

- Снижение риска благодаря автоматизации процесса выявления уязвимостей и определение приоритетов в отношении их устранения, исходя из степени бизнес риска
- Проведение аудита без каких-либо агентов. Материалы аудиторской проверки достоверны и защищены от изменений. Качество аудита соответствует внешнему независимому аудиту
- SaaS технология, предоставляемая «по требованию», обеспечивает значительные экономические преимущества, поскольку не требует значительных капиталовложений, привлечения дополнительных кадровых ресурсов, а также развертывания и управления инфраструктурой
- Уникальная масштабируемость делает решение идеальным для крупных, структурно распределенных организаций
- Возможность быстро идентифицировать, визуализировать и организовать сетевые ресурсы по бизнес-подразделениям и группам ресурсов

Qualys располагает тысячами клиентов по всему миру, включая более 35 компаний из списка Fortune Global 100 и крупнейшим в мире внедрением с применением 223 аппаратных сканеров которые распределены в 53 странах и сканируют более 700 000 систем на базе одной из компаний, входящей в список Fortune Global 50.

“ QualysGuard значительно облегчает нашу работу по аудиту нашей сети. Раньше нам приходилось кропотливо собирать результаты и анализировать их вручную, чтобы подготовить весомые отчеты, в результате чего они все равно были противоречивы. ”

Крис Лалонд, Старший Менеджер по Информационной Безопасности, eBay

“ QualysGuard позволяет нам проводить аудит систем безопасности по мере необходимости, оперативно выявлять уязвимости, как только информация о них добавляется в базу данных QualysGuard, и проактивно работать для их устранения. Это помогает нам обезопасить все точки входа в нашу сеть, обеспечить соблюдение политик безопасности нашей компании и облегчает выполнение федеральных требований. ”

Пол Симмондс, Директор по глобальной информационной безопасности
ICI



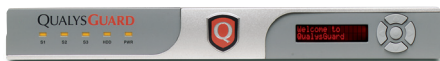
- Второй год подряд решение QualysGuard признано лучшим решением года в области аудита и управления уязвимостями

Централизованное управление уязвимостями

- Автоматическая централизованная отчетность по результатам распределенных сканирований
- Единое администрирование как внутреннего, так и внешнего сканирования
- Приборная панель для руководителей
- Интерактивный портал для поиска информации о ресурсах сети
- Авторизованный доступ пользователей из любого месторасположения
- Экспорт отчетов в форматы HTML, MHT, PDF, CSV и XML

Автоматизация

- Осуществляемые по заданному графику сканирования и исследования сети
- Автоматическое непрерывное обновление базы знаний по уязвимостям
- Автоматическое создание, назначение и контроль заявок на устранение уязвимостей



Аппаратные Сканеры QualysGuard представляют собой удобную в использовании инфраструктуру сканирования распределенных сетей, которую можно развернуть за несколько минут.

Достоверность

- Обширная база знаний по уязвимостям включает в себя тысячи уникальных проверок
- Апробированная независимая сертификация безопасности сети и аудиторские материалы, защищенные от изменений
- Механизм сканирования на основе логических выводов не использующий активных мер взлома
- Возможность сканировать как используя аутентификацию, так и без нее
- Внутреннее и внешнее сканирование позволяет получить полную картину уязвимостей сети
- Возможность настройки сканирования для специализированного аудита
- Уникальные отпечатки для более 2 000 операционных систем, приложений и протоколов

Отчетность

- Настраиваемые отчеты по бизнес-подразделениям для руководителей и менеджеров
- Автоматическое предоставление дифференцированных отчетов и отчетов по тенденциям
- Отчет по устранению уязвимостей включает в себя: отражение тенденций выполнения заявок по группам ресурсов, пользователям и уязвимостям

- Отчеты по контрольным показателям для всех заинтересованных сторон предприятия
- Автоматическое создание и распространение отчетов
- Множество различных вариантов распространения отчетов, включая предоставление в виде зашифрованного PDF файла

Масштабируемость / Гибкость развертывания

- Технология SaaS, предоставляемая «по требованию», дает пользователям возможность осуществлять сканирование в любой точке мира без дополнительной инфраструктуры
- Быстрое сканирование путем балансирования загрузки аппаратных сканеров
- Бизнес-подразделения и группы ресурсов определяются пользователем на основе бизнес-процессов
- Непрерывное шифрование данных об уязвимостях
- Управление доступом пользователей по иерархическому принципу позволяет делегировать полномочия в соответствии с организационной структурой
- Управление процессом устранения уязвимостей на основе существующей политики с автоматическим созданием заявок для уполномоченных лиц

Совместимость

- Расширяемая библиотека XML API (интерфейс прикладного программирования)
- Готовая интеграция с ведущими SIM решениями
- Интеграция с системами Helpdesk
- Интеграция с системами управления обновлениями для автоматической установки патчей
- Поддержка CVSS - отраслевого стандарта для оценки уязвимостей (Common Vulnerability Scoring System)
- Поддержка отраслевого стандарта для настройки собственных типов проверок на уязвимости, используя OVAL (Open Vulnerability Assessment Language)

Поддержка/Обновление

- «Живая» поддержка в режиме 24x7x365
- Непрерывное обновления сигнатур и улучшения функциональности производятся автоматически и прозрачно для пользователя
- Постоянные web-курсы для пользователей
- Технические обучающие семинары и сертификация.

Ценообразование

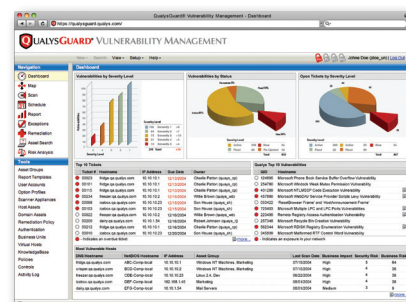
- Годовая подписка: неограниченное количество сканирований заранее определенного количества IP устройств: идеальное решение для регулярных оценок безопасности сетевых ресурсов.

- По числу сканирований: гибкое использование. QualysGuard Enterprise для ежеквартального или периодического сканирования

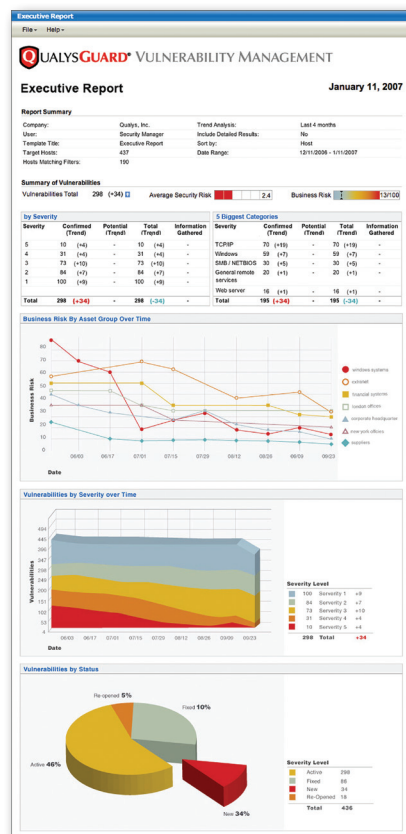
QualysGuard Vulnerability Management также доступен, как часть системы QualysGuard Security & Compliance Suite, состоящей из:

- QualysGuard Vulnerability Management
- QualysGuard Policy Compliance
- QualysGuard PCI Compliance
- QualysGuard Web Application Scanning

Более подробная информация: www.qualys.com



Настраиваемая панель управления для каждого пользователя



Отчет о тенденциях бизнес рисков