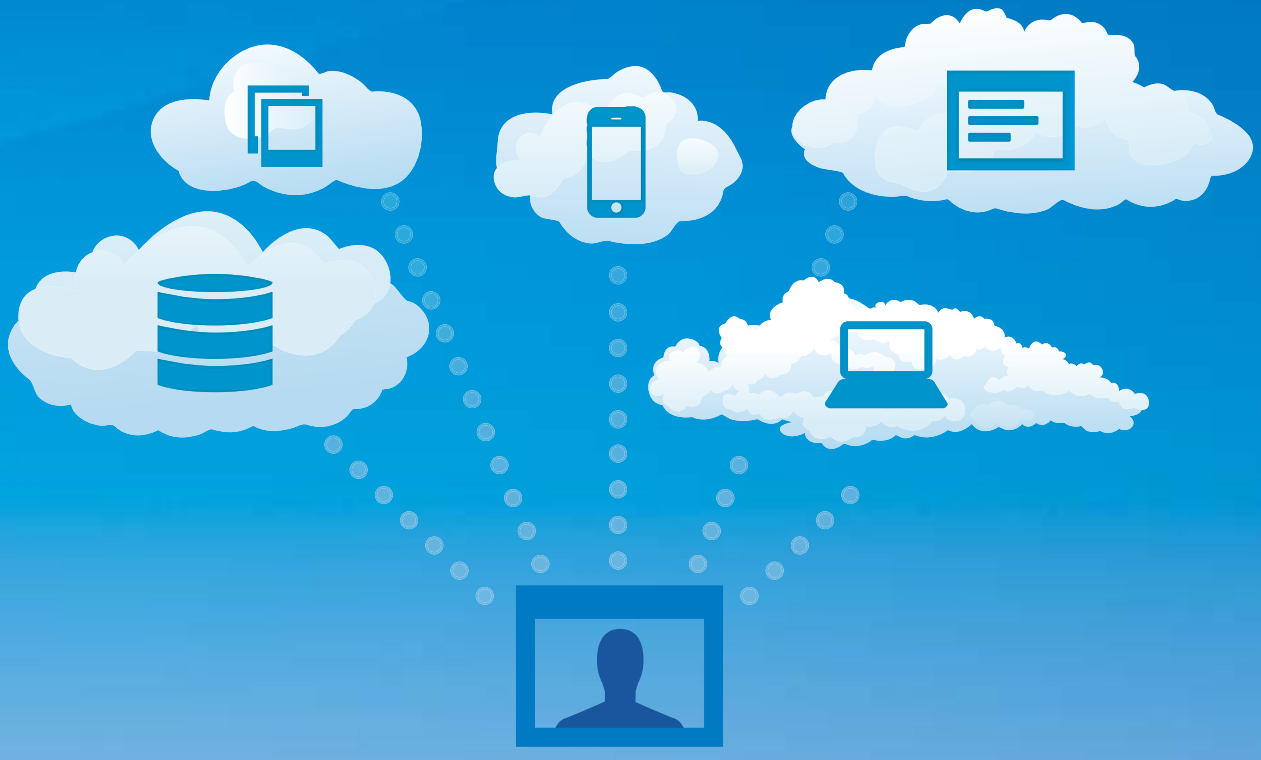
БЕЗОПАСНОСТЬ И СОБЛЮДЕНИЕ УСТАНОВЛЕННЫХ ТРЕБОВАНИЙ В ЭПОХУ ОБЛАЧНЫХ СРЕД



QUALYS®

Содержание

Введение

Мы вступили в эпоху повсеместного распространения технологий. Дома, в офисе или в дороге: большинство из нас постоянно поддерживает связь не только с другими людьми, но и работает с огромными массивами информации, используя различные технологии. Стало непросто разделять рабочее время и досуг, поскольку одни и те же устройства используются в обеих сферах жизни. Вместе с широкими возможностями эта неотвратимая тенденция несет в себе значительные риски для организаций, выбирающих культуру «всегда на связи» для своих заказчиков, торговых партнеров и сотрудников.

Услуги в сфере информационных технологий востребованы всегда и везде, а вся необходимая для этого информация может храниться где угодно. В компании Qualys мы придерживаемся мнения, что организациям, которые не хотят оказаться не у дел, просто необходимо вступить в «эпоху облачных сред», уходя от ограничений клиент-серверных приложений и даже веб-приложений первого поколения, окунуться в новый мир усовершенствованных коммуникаций, тесного сотрудничества и увеличенной производительности.

Безопасность и соблюдение установленных требований в эпоху облачных сред

Эпоху облачных сред можно описать по нескольким признакам:

Ориентированность на браузеры

Веб-браузер — это стандартный интерфейс для работы в сети Интернет, с корпоративными системами и хранилищами данных. Это свойство обеспечивает всесторонний доступ ко информации на различных устройствах, включая компьютеры и смартфоны, владельцами которых являются как компании, так и их сотрудники (концепция использования персональных устройств «BYOD»). В то же время у браузеров есть уязвимости, которые могут привести к заражению вредоносным ПО - несмотря на усилия разработчиков по устранению этих проблем - и стать наилегчайшим путём атаки для злоумышленников, стремящихся получить информацию, выкрасть учетные данные для доступа к бизнес приложениям или полностью контролировать устройства пользователей.

Веб-приложения: Новый периметр

Веб-приложения теперь представляют собой основную точку доступа к сетям и данным предприятий, тем самым, заменяя традиционный периметр. В настоящее время компаниям приходится тратить столько же времени и усилий для обнаружения, отслеживания и управления веб-приложениями, сколько они затрачивают в сетях с традиционным периметром. Важность этих приложений, количество и ценность их ключевых данных привлекают злоумышленников, которые стремятся воспользоваться уязвимыми местами и недостатками конфигурации приложений для получения ценной информации или снижения доступности приложений.

Независимость от места хранения данных

Облачные вычисления предоставляют возможность приложениям использовать данные из любого места и в любом месте. Данные могут храниться в многообразии различных внутренних и облачных хранилищ, требуя при этом безопасных коммуникаций между этими системами. И хотя многие разработчики приложений для облачных сред вложили немалые средства в обеспечение безопасности, облачные сервисы (по определению) предлагают компаниям ограниченные возможности видимости и доступа к основной архитектуре приложений, снижая возможности для определения потенциальных недостатков и подтверждения эффективности их стратегий безопасности.

Глобализация — это норма, а не исключение

Облачные среды разрушают региональные и территориальные границы. Данные перемещаются из одного места в другое, пользователи прозрачно перемещаются между различными пунктами, а администрирование систем может выполняться различными авторизованными третьими сторонами, не обязательно сотрудниками вашей организации. Это создает определенные юридические трудности, дополнительные требования к подлинности и доверию, а также усложняет процедуру отчетности и аттестации в рамках обеспечения соответствия принятым требованиям.

Смешанная инфраструктура

Крупные организации не могут мгновенно отключить свои внутренние системы, напротив, они, прилагают значительные усилия для повышения эффективности этих ресурсов посредством консолидации и виртуализации. С учетом того, что в обозримом будущем ИТ-инфраструктура останется гибридом традиционных физических центров обработки данных и облачных технологий, необходимо реализовывать контроль безопасности и регулярно составлять документацию по соответствию принятым стандартам независимо от того, находится ли технологический ресурс в ЦОД вашей компании или в облачной среде поставщика из другой страны.

Производительность, адаптивность и экономические преимущества облачных вычислений означают, что облачные среды будут продолжать развиваться, невзирая на все риски и сложности. Поэтому подробнее рассмотрим все проблемы, которые возникают у любой организации в эпоху облачных сред.

Возможные трудности, связанные с обеспечением безопасности и соблюдением установленных требований в эпоху облачных сред

Безопасность — это та битва, которую ваша компания не сможет выиграть, поэтому успех в этой борьбе часто измеряется отсутствием имени организации в заголовках новостей и отсутствием возбуждённых уголовных дел против высшего руководства компании. Переход к веб-ориентированной реальности и возрастающее использование облачных и гибрибных инфраструктур еще более усложняют работу специалистов по информационной безопасности.

Безопасность в масштабах облачной среды

По мнению альянса «Cloud Security Alliance», одной из основных характеристик облачной среды является «высокая адаптивность», означающая, что такая среда может развиваться настолько быстро, насколько это необходимо вашей компании. В прошлом новые устройства необходимо было приобрести, подготовить и установить, что давало компании время для организации их защиты. Введение в эксплуатацию нового экземпляра облачной среды занимает минуты, а это создает некоторые трудности как для видимости (знать в любой момент времени, какие устройства фактически находятся вне организации), так и для контроля (быть уверенным в том, что на новых ресурсах применяются надлежащие конфигурации и элементы управления).

Увеличение площади нападения

По мере того, как веб-приложения возникают в виде «нового периметра», компаниям нужно принять реальность, в которой количество периметров равно количеству веб-приложений. В сочетании с увеличившимся количеством внештатных исполнителей и коммерческих партнеров это приводит к резкому увеличению площади нападения. Такой быстрый рост количества целей, среди которых базы данных, настольные ПК, мобильные устройства, роутеры, серверы и коммутаторы, также способствует увеличению количества уязвимостей в системах безопасности, что теоретически предоставляет хакерам несанкционированный доступ к ИТ-системам. Теперь уже недостаточно создать надежный периметр сетевой защиты и пренебречь заботой о безопасности внутренних сетей и устройств.

Использование существующих методов обеспечения безопасности

В течение длительного времени организации разворачивали специальные продукты обеспечения безопасности, которые использовались для решения определенных задач в этой области. Однако, такой подход зачастую не предоставляет компании полную картину безопасности и соблюдения установленных требований. По мере того, как ИТ-инфраструктуры развиваются и включают в себя сочетание внутренней, облачной и гибридной сред, такие узкоспециализированные продукты, используемые локально, создают определенные трудности в предоставлении полной и точной информации об ИТ-активах и конфигурациях, тем самым не позволяя компаниям обеспечить эффективную защиту своих инфраструктур от угроз, которые несет с собой эпоха облачных сред.

Безопасность «тонких» устройств

Развитие смартфонов способствовало появлению более сложных и безопасных операционных систем для мобильных устройств, закрытых по умолчанию и предлагающих ядру операционной системы ограниченные возможности контроля. Вчерашние технологии защиты от вредоносного программного обеспечения на уровне ядра более не актуальны. Поскольку для этих устройств характерны случаи утечки данных и поражения вредоносными программами, компаниям необходимо рассмотреть различные способы обеспечения их безопасности.

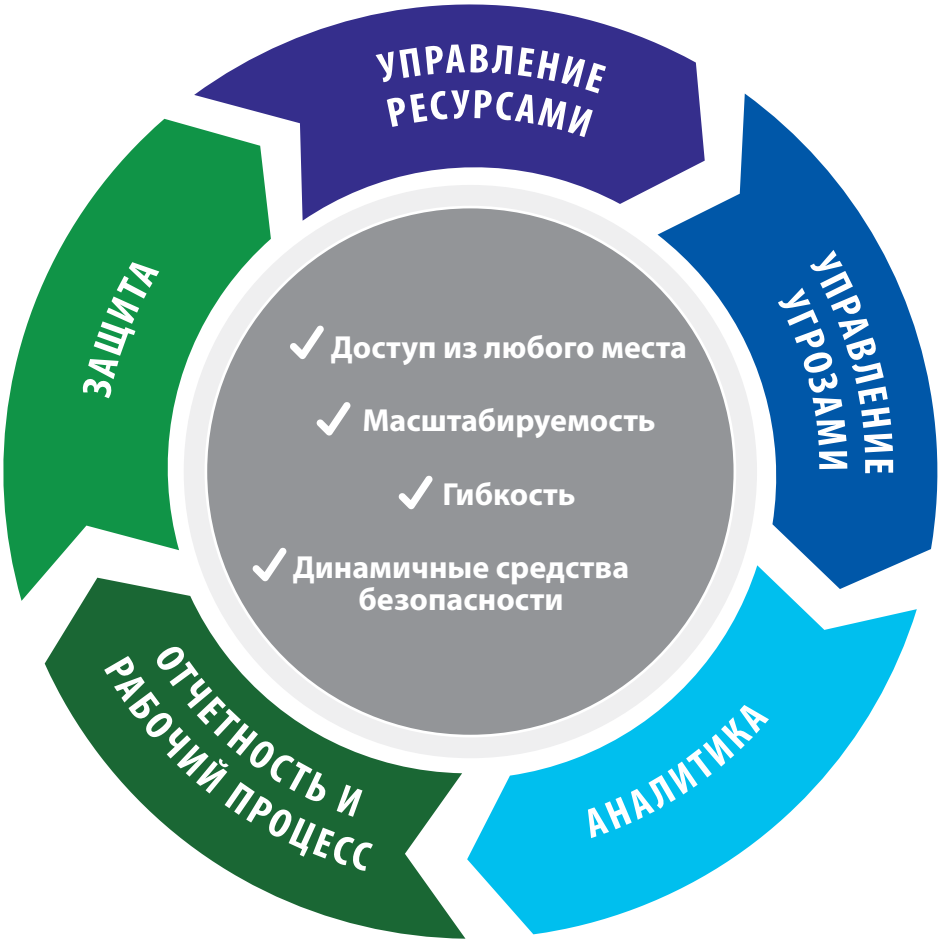
Приоритет мер по обеспечению безопасности

Постоянные ограничения в финансировании, ресурсах и квалифицированных кадрах усложняют для многих компаний задачу по обеспечению безопасности в эпоху облачных вычислений, так как успешная защита зависит от тщательного выбора предпринимаемых мер. Эпоха облачных вычислений затрудняет принятие решений, принуждая компании назначать приоритеты задачам по обеспечению безопасности, распределенным среди внутренних и внешних поставщиков услуг и персонала, что не всегда удается контролировать должным образом. Проблема усугубляется еще и характером действий злоумышленников, которые могут начать новую атаку, требующую незамедлительных действий, что делает неприменимым даже самый лучший план защиты.

Отчетность о соблюдении установленных требований

Плачевные последствия нарушений безопасности – все более ужесточающиеся требования регуляторов и стандартов безопасности. Принимая во внимание глобальный характер большинства предприятий эпохи облачных вычислений, ваша компания, скорее всего, должна соблюдать правила и политики различных государственных и местных органов власти, которые зачастую совпадают и постоянно меняются. Соблюдение стандартов различных регуляторов требует дорогостоящих и трудоемких мер, тогда как их несоблюдение будет иметь серьезные финансовые последствия и негативно отразится на репутации компании. В качестве примеров таких общепринятых стандартов можно привести «Международную конвергенцию измерения капитала и стандартов капитала: новые подходы» (Basel II), «Закон об ответственности и переносе данных о страховании здоровья граждан» (HIPAA), «Стандарты Североамериканской корпорации по обеспечению надежности электросистем» (NERC), «Стандарты безопасности данных в сфере платежных карт» (PCI DSS), и закон «Сарбейнза-Оксли» (SOX). По данным исследования, проведенного в 2011 году компанией Gartner, соответствие стандартам PCI DSS обходится компаниям среднем в 1,7 миллиона долларов, а ведь это только один стандарт.

Платформа безопасности облачной среды:
формирование основ для обеспечения безопасности и соблюдения установленных требований в эпоху облачных сред



Используемые сегодня локальные решения заказчиков не могут удовлетворить потребностям, связанным с безопасностью и соблюдением установленных требований в эпоху облачных вычислений, а значит, требуется новый подход.

Важные характеристики платформы облачной среды

Доступ из любого места

Ваши сотрудники, поставщики услуг и заказчики могут находиться где угодно, поэтому платформа обеспечения безопасности облачной среды должна быть доступна в любом месте и в любое время.

Гибкая масштабируемость

Функция обеспечения безопасности и соблюдения установленных требований в эпоху облачных вычислений должна быть такой же гибкой и масштабируемой, как и сама облачная среда. По мере роста ИТ-инфраструктуры вашей компании платформа, использующаяся для обеспечения безопасности, должна расширяться пропорционально.

Гибкость по требованию

Платформа обеспечения безопасности в эпоху облачных вычислений должна быть достаточно гибкой, чтобы предложить компании нужные услуги в нужное время и с оплатой только за используемые сервисы.

Динамичные средства безопасности

Противоборствуя постоянно изменяющимся, тщательно спланированным атакам, платформа обеспечения безопасности облачной среды должна обновляться динамически и использовать самую последнюю информацию об уязвимостях, конфигурациях и вредоносных программах, что позволит вашей компании быстрее реагировать на возникающие угрозы.

Платформа обеспечения безопасности облачной среды и соблюдения установленных требований должна выполнять следующие функции для удовлетворения потребностей современных компаний:

Управление ресурсами

Ваша организация не может защитить ресурсы, которые ей не известны. Более того, чтобы установить приоритеты, необходимо изучить ценность конкретного ресурса для вашей организации. Таким образом, платформа должна обладать функциональными возможностями для управления ресурсами.

Управление угрозами

Платформа должна обладать функцией обнаружения уязвимости, оценивать и контролировать конфигурации и определять риск, который та или иная атака представляет для организации. В разнородных ИТ-средах платформа должна обеспечивать единое представление о традиционных центрах обработки данных и о частных/ публичных облачных средах, о многочисленных устройствах и приложениях.

Аналитика

Ключевым фактором для определения приоритетных действий и противостояния современным атакам является получение практической информации из различных источников данных. Платформа должна обладать функцией анализа данных и обеспечивать четкую визуализацию информации, необходимой для принятия быстрых решений, для администраторов службы безопасности.

Отчетность и рабочий процесс

Принимая во внимание увеличивающееся количество нормативных требований в различных регионах и юрисдикциях, платформа должна обеспечивать общий комплект отчетов для всего предприятия, одновременно поддерживая все нормативы для предоставления отчетности и предлагая возможность поддерживать рабочие процессы между предприятиями, так как привлечение сторонних ресурсов для обеспечения функций безопасности становится все более распространенным явлением.

Защита

Если имеется возможность заблокировать атаку и свести к минимуму вероятность ложного срабатывания, платформа должна обеспечивать возможность либо предоставлять непосредственную защиту, либо интегрироваться с другими активными средствами безопасности, включая предотвращение вторжений и межсетевые экраны следующего поколения.

Платформа для обеспечения безопасности облачной среды не создается за одно мгновение. В действительности требуется около десяти лет, чтобы приобрести достаточное количество заказчиков, обеспечить присутствие в других странах, создать средства безопасности и получить необходимые профессиональные навыки на уровне мировых стандартов. А чтобы удовлетворить всем потребностям предприятий по обеспечению безопасности и соблюдению установленных требований в эпоху облачных вычислений, требуется уникальная компания, и эта компания — Qualys.

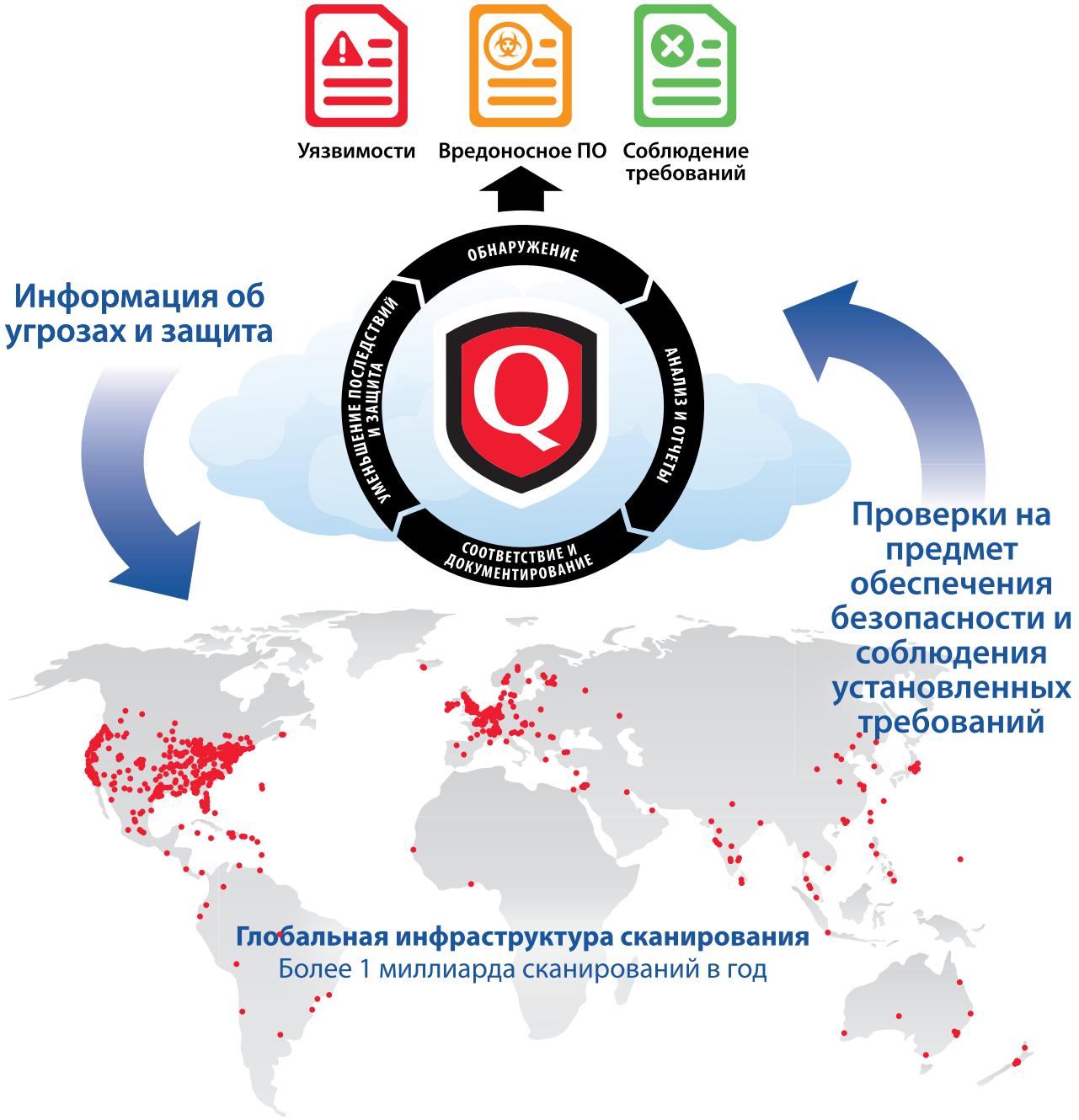
Обеспечение безопасности и соблюдение установленных требований в эпоху облачных сред

Компания Qualys была основана в 1999 году на пике развития технологий, когда безопасность в сети Интернет только начала появляться на повестке дня руководителей компаний. В декабре 2000 года компания стала одной из первых на рынке продуктов по управлению уязвимостями. Благодаря действенной комбинации высокоточных и удобных технологий сканирования, выполняемого через сеть Интернет, Qualys первой начала использовать бизнес-модель «Программное обеспечение как услуга», или SaaS, для решения проблем, связанных с обеспечением безопасности и соблюдением установленных требований для организаций всех размеров.

Основным решением Qualys является облачная платформа QualysGuard, предоставляющая интегрированный пакет решений для автоматизации жизненного цикла поиска ресурсов, оценки безопасности и соблюдения установленных требований для ИТ-инфраструктуры и ресурсов предприятий независимо от того, находятся ли они внутри предприятия, в ее сетевом периметре или в облачной среде. Реализованную в QualysGuard модель предоставления облачных услуг можно легко и быстро развернуть в глобальном масштабе, что обеспечивает более быстрое внедрение, более широкое применение и меньшую общую стоимость владения по сравнению с традиционными локальными программными продуктами для предприятий. QualysGuard предоставляет компаниям применимую на практике информацию о потенциальных уязвимостях и вредоносных программах в их ИТ-инфраструктуре и помогает обеспечить соответствие внутренним политикам и общепринятым стандартам.

Результаты говорят сами за себя. За последние 13 лет компания Qualys создала глобальную базу клиентов, в которую входят более 6 700 компаний, расположенных в более чем 100 странах, включая большинство компаний из списков «Forbes Global 100» и «Fortune 100». Ежегодно эти клиенты выполняют более миллиарда сканирований/аудитов IP-адресов.

Применимая на практике информация



Эпоха облачных вычислений обяжет компании всех размеров и форм проявить гибкость в вопросах защиты своих важных информационных ресурсов. QualysGuard предоставляет применимый на практике подход и позиционируется как стратегическая платформа компании по обеспечению безопасности информационных технологий и соблюдению установленных требований на многие годы.

Облачная платформа QUALYSGUARD®

Облачная платформа QualysGuard состоит из комплекта решений по обеспечению безопасности информационных систем и соблюдению установленных требований, которые используют общие и расширяемые службы и легко масштабируемую многопользовательскую инфраструктуру облачной среды.

Инфраструктура облачных сред QualysGuard

Инфраструктура QualysGuard включает в себя данные, аналитические возможности, программное и аппаратное обеспечение и средства для управления инфраструктурой, необходимые для создания платформы облачной среды. Ниже приведены некоторые ключевые аспекты:

Расширяемый объем услуг
Модульная и расширяемая инфраструктура QualysGuard использует технологии виртуализации и облачных сред, что позволяет нашим разработчикам динамически распределять при необходимости дополнительную емкость по всей платформе QualysGuard для дальнейшего расширения и масштабируемости наших решений.

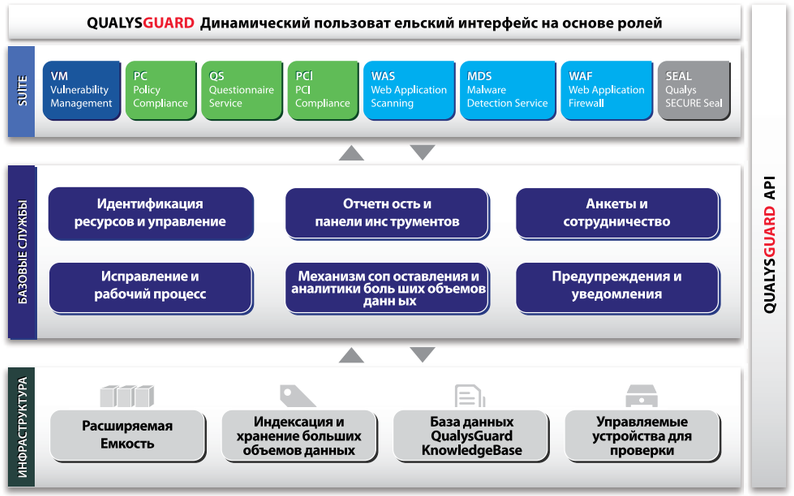
Индексирование и хранение больших объемов данных
Аналитический механизм QualysGuard, созданный на основе нашей модели безопасного хранения данных, осуществляет индексирование петабайтов данных и использует полученную информацию в режиме реального времени для выполнения команд или правил для динамического обновления свойств ИТ-ресурсов с целью использования в различных рабочих процессах для проверки, создания отчетов и исправления.

База знаний
Платформа QualysGuard опирается на наш обширный архив информационных данных, базу знаний «QualysGuard KnowledgeBase», в которой хранится информация обо всех известных уязвимостях и средствах контроля соответствия для большого количества устройств, технологических разработок и приложений, способствующую реализации нашей технологии обеспечения безопасности и соблюдения установленных требований. База знаний динамически пополняется данными об уязвимостях, контрольных проверках, подтвержденных исправлениях и подробными сведениями о содержимом.

Управляемые устройства
Qualys размещает и управляет тысячами физических устройств, распределенными по всему миру, которые используются для оценки внешних систем и веб-приложений наших заказчиков. Для доступа к внутренним ИТ-ресурсам организации разворачивают в пределах своих внутренних сетей физические устройства или загружаемые виртуальные образы. Устройства QualysGuard самостоятельно обновляются с максимальной прозрачностью, используя нашу запатентованную автоматическую технологию управления.

Базовые службы QualysGuard

Базовые службы платформы QualysGuard обеспечивают интегрированные рабочие процессы, управление, анализ и отчетность в режиме реального времени для всех наших решений для обеспечения безопасности информационных технологий и соблюдения установленных требований. Наши базовые службы включают:



Идентификация и управление ресурсами
Предоставляет вашей компании возможность быстро определять, группировать и управлять большим количеством ресурсов в пределах высоко динамичных ИТ-сред, автоматизируя процесс управления активами и иерархической организацией ИТ-ресурсов.

Отчетность и панели инструментов
Легко конфигурируемый механизм создания отчетности, который представляет вашей организации отчеты и информационные панели, исходя из ролей пользователей и привилегий доступа.

Анкеты и сотрудничество
Конфигурируемый механизм анкетирования обеспечивает вашей организации возможность легко зафиксировать существующие рабочие процессы для оценки элементов управления и сбора доказательств для подтверждения и документирования соблюдения установленных требований.

Исправление и рабочий процесс
Интегрированный механизм рабочих процессов позволяет вашей организации автоматически создавать заявки в службы технической поддержки для исправления и управлять исключениями из правил соответствия на основании предусмотренных политик, обеспечивая последующее рассмотрение, комментирование, отслеживание и выполнение.

После завершения проверки этот механизм автоматически распределяет задачи по исправлению среди ИТ администраторов, отслеживает исправление и закрывает открытые заявки после устранения уязвимостей и подтверждения исправления последующими проверками.

Механизм сопоставления и аналитики больших объемов данных
Механизм аналитики выполняет индексирование, поиск и сопоставление петабайтов данных об обеспечении безопасности и соответствии установленным требованиям с данными о других инцидентах, а также с данными, предоставленными средствами обеспечения безопасности третьих сторон. Встроенные рабочие процессы позволяют вашей компании быстро оценить риск и получить доступ к информации для исправления, анализа инцидента и судебных разбирательств.

Предупреждения и уведомления
Механизм предупреждений создает и рассылает сообщения по электронной почте для предупреждения сотрудников о новых уязвимостях, случаях проникновения вредоносных программ, завершении проверок, открытых заявках и обновлениях систем.

QualysGuard Cloud Suite

Платформа QualysGuard позволяет вашей организации использовать только те решения, которые вам необходимы, когда они вам необходимы, а также платить только за то, чем вы действительно пользуетесь. Ваша организация может оформить подписку на одно или несколько решений по обеспечению безопасности и соблюдению установленных требований и со временем расширить рамки использования.

Управление уязвимостями
Служба управления уязвимостями «QualysGuard Vulnerability Management» (VM) является передовым решением отмеченный множеством наград, которое автоматизирует проверки сети и управление уязвимостями во всей организации, включая сетевое обнаружение и топологию сети, управление ресурсами, отчет об уязвимостях и контроль исправления. Основываясь на нашей обширной базе знаний, содержащей информацию об известных уязвимостях, QualysGuard VM обеспечивает экономически эффективное средство для устранения слабых мест в системе защиты без значительного потребления ресурсов.

Соответствие политикам
Служба обеспечения соответствия политикам «QualysGuard Policy Compliance» (PC) позволяет компаниям анализировать и собирать информацию о конфигурациях и контроле доступа, предоставляемую сетевыми устройствами и веб-приложениями, и автоматически сопоставляет эту информацию с внутренними политиками и общепринятыми стандартами для документального подтверждения соблюдения установленных требований. QualysGuard PC является полностью автоматизированным инструментом, который позволяет сократить расходы, связанные с соблюдением установленных требований, без необходимости использования программных агентов.

Сервис Опросников
Сервис Опросников в QualysGuard - это облачное решение, которое позволяет централизовать и автоматизировать запуск, отслеживание, оценку и одобрение риск-проверок и проверок на соответствие требованиям. Этот сервис уменьшает количество ресурсов (материальных и нематериальных) для сбора информации от различных заинтересованных сторон, помогая организациям направить и расширить их программы по оценке поставщиков с точки зрения рисков, информационной безопасности и соответствия требованиям .

Соответствие стандарту PCI DSS
Служба обеспечения соответствия стандартам «QualysGuard PCI Compliance» (PCI) может предоставить компаниям, которые хранят данные владельцев платежных карт, экономически эффективное и высокоавтоматизированное решение для проверки и документального подтверждения соответствия стандартам PCI DSS. С помощью QualysGuard PCI торговые компании могут заполнять ежегодную «Анкету самооценки» (SAQ), а также выполнять проверки на наличие уязвимостей для ежеквартальных аудитов по требованию стандарта PCI DSS и обеспечения безопасности веб-приложений.

Проверка защищенности веб-приложений
Служба проверки веб-приложений «QualysGuard Web Application Scanning» (WAS) использует возможности масштабируемости облачной платформы для выполнения поиска, внесения в списки и проверки как отдельных, так и всех веб-приложений компаний. Служба QualysGuard WAS выполняет проверку и осуществляет анализ индивидуальных веб-приложений и определяет уязвимости, представляющие опасность для баз данных или способные помочь обойти средства управления доступом к приложениям.

Выявление вредоносного ПО
Служба выявления вредоносных программ «QualysGuard Malware Detection Service» (MDS) предоставляет компаниям возможность проверять, выявлять и удалять вредоносное программное обеспечение со своих веб-сайтов. QualysGuard MDS использует поведенческий и статический анализ для поиска вредоносных программ и мониторинга веб-сайтов на постоянной основе.

Межсетевой экран для веб-приложений
Межсетевой экран для веб-приложений «QualysGuard Web Application Firewall» (WAF) обеспечивает защиту веб-приложений промышленного уровня без дополнительных затрат, площадей и сложностей, связанных с использованием аппаратных межсетевых экранов для веб-приложений. Он защищает веб-приложения от векторов атак, дополняя стандартные конфигурации веб-приложений и виртуальные исправления. QualysGuard WAF также повышает эффективность веб-сайтов, уменьшая время загрузки страниц и оптимизируя пропускную способность с помощью нашей глобальной сети веб-кэшей.

Qualys SECURE Seal
Печать «Qualys SECURE Seal» предоставляет компаниям возможность продемонстрировать онлайн-клиентам использование проактивной программы обеспечения безопасности. Печать безопасности подразумевает проверку на наличие вредоносных программ, уязвимостей сети и веб-приложений и подтверждает безопасность сертификатов SSL. Компании, демонстрирующие отсутствие серьезных нарушений безопасности, могут разместить на своих веб-сайтах печать «Qualys SECURE Seal».

Почему именно Qualys?

Основная цель компании Qualys — изменение способов защиты и обеспечения безопасности ИТ-инфраструктур и приложений организаций. Qualys — это лучший выбор по обеспечению безопасности и соблюдению установленных требований для вашей компании!

Проверенный бренд в области безопасности облачных сред

Компания Qualys стояла у истоков разработки продуктов для безопасности облачных сред, представив первое решение по управлению уязвимостями как сервис в 2000 году и сохраняя репутацию проверенного и объективного поставщика надежных и точных продуктов для оценки уязвимостей и обеспечения соответствия установленным требованиям.

Масштабируемая и расширяемая платформа для обеспечения безопасности облачных сред

Легко масштабируемая архитектура и модульные решения для обеспечения безопасности и соответствия установленным требованиям позволяют компаниям всех размеров, действующих в самых различных отраслях, использовать функциональные возможности для обеспечения безопасности своих ИТ-инфраструктур. Облачная платформа QualysGuard подходит как небольшим фирмам, так и крупным глобальным компаниям, которые используют миллионы подключенных к сети устройств и приложений.

Опыт инноваций в области продуктов для обеспечения безопасности облачных сред и соблюдения установленных требований

Вот уже более 12 лет компания Qualys предлагает инновационные решения для обеспечения безопасности облачных сред и соблюдения установленных требований, с помощью которых наши клиенты могут более эффективно и с меньшими расходами защитить свои ИТ-среды. Qualys инвестировал большие средства в разработку облачной платформы QualysGuard и полностью готов к решению проблем, возникающих в постоянно меняющейся среде обеспечения безопасности информационных технологий и соблюдения установленных требований.

Платите только за то, чем вы пользуетесь, и когда вы этим пользуетесь

Платформа QualysGuard позволяет клиентам без каких-либо проблем протестировать одно или несколько наших решений, используя любой веб-браузер. Такая модель предлагает нашим клиентам возможность оформить подписку только на необходимые им решения; при этом они могут легко расширить рамки своей подписки, когда это потребуется.

Для получения доступа к бесплатной пробной версии «QualysGuard Cloud Suite» посетите веб-сайт по адресу http://www.qualys.com/trial

50+ из списка Forbes Global 100

пользуется облачной платформой QualysGuard для обеспечения безопасности и соответствия требованиям

- **8** из 10 ведущих компаний **программного обеспечения**
- **8** из 10 ведущих компаний **области биотехнологий**
- **8** из 10 ведущих компаний **технологического направления**
- **8** из 10 ведущих компаний **розничной торговли**
- **7** из 10 ведущих компаний **области здравоохранения**
- **7** из 10 ведущих **банков**
- **7** из 10 ведущих компаний **медиа-корпораций**
- **7** из 10 ведущих компаний **продуктовой отрасли**
- **6** из 10 ведущих **автопроизводителей**
- **6** из 10 ведущих компаний **химической ромышленности**
- **6** из 10 ведущих компаний **телекоммуникационных услуг**
- **6** из 10 ведущих **конгломератов**

QUALYS®
CONTINUOUS SECURITY

QUALYS®

Qualys, Inc. (NASDAQ: QLYS)

Headquarters
1600 Bridge Parkway
Redwood City, CA 94065 USA
T: 1 (800) 745 4355, info@qualys.com

Qualys – это глобальная компания с представительствами по всему миру. Чтобы найти представительство в своем регионе, посетите веб-сайт **http://www.qualys.com**