McAfee Vulnerability Manager

Непрерывный и высокоэффективный мониторинг активов в режиме реального времени

Основные отличительные качества

- Непревзойденная масштабируемость, точность и гибкость.
- Оценка новых устройств в режиме реального времени сразу после их появления в сети; полный перечень программных и аппаратных активов; сопоставление пользователей и активов; а также автоматическое составление топологии сети.
- Сочетает в себе функции активного и пассивного обнаружения устройств и мониторинга сети, позволяющие находить виртуальные, мобильные и скрытые устройства.
- Сканирование активов и составление базы заслуживающих доверия активов производится по результатам глубокого аудита устройств.
- Динамическое тегирование систем позволяет полностью автоматизировать процесс оценки уязвимостей.
- Постоянное обновление информации об угрозах и уязвимостях благодаря использованию технологии McAfee Global Threat Intelligence™.
- Защита привилегированных учетных записей обеспечивается с помощью встроенных технологий Cyber-Ark.
- Сканирует как сети IPv4, так и IPv6.
- Абсолютно гибкая система отчетности: достаточно один раз выполнить сканирование активов, чтобы в любое время иметь возможность составлять по≈ним отчеты.
- Автоматизированные рабочие процессы управления рисками могут включать в себя приложения McAfee, самостоятельно разработанные приложения и приложения сторонних поставщиков.

Обеспечьте безопасность своей компании с помощью самого гибкого, надежного и масштабируемого из имеющихся в отрасли решений! К вашим услугам — простая в использовании комплексная система управления уязвимостями в режиме реального времени. Благодаря функции управления активами (McAfee Asset Manager) решение McAfee® Vulnerability Manager обеспечивает непревзойденный уровень масштабируемости и быстродействия, активно или пассивно охватывая всё, что находится в вашей сети. Если у устройства или актива есть IP-адрес и он использует вашу сеть, то McAfee Vulnerability Manager автоматически в реальном времени обнаруживает его и получает к нему доступ, определяя степень нормативно-правового соответствия всех активов в вашей сети.

Решение McAfee Vulnerability Manager задает стандарты работы на рынке, поскольку учитывает характерные условия вашего предприятия и анализирует все типы конфигураций сетей и активов. Решение выполняет как непрерывное пассивное сканирование активов, так и активное сканирование выбранных вами активов по требованию, что дает вам возможность обнаруживать активы, проводить их оценку, снижать их уровень риска, а также составлять отчеты по всем своим активам. У вас есть возможность выявлять скрывающиеся в вашей сети устройства, а также смартфоны, планшетные компьютеры и ноутбуки, появляющиеся и вновь исчезающие в промежутках между запланированными проверками. Вы будете удивлены, узнав о количестве устройств, которые вы не замечаете и не сканируете и которые угрожают нормативно-правовому соответствию вашей организации. Тысячи организаций используют McAfee Vulnerability Manager для быстрого поиска и присвоения приоритетов уязвимостям. При этом масштаб развертывания варьируется от нескольких сотен узлов до одного узла, непрерывно сканирующего более 4 миллионов IP-адресов.

Простота внедрения

Компания McAfee позволяет без труда установить надежную систему сканирования. Решение McAfee Vulnerability Manager легко устанавливается на физическом и виртуальном оборудовании пользователя. Альтернативно могут использоваться аппаратные устройства с настроенными параметрами безопасности. Свое первое сканирование вы можете начать уже через несколько минут после установки продукта.

Точно также вы с легкостью сможете загрузить данные инвентаризации ваших активов и управлять ими. Модуль McAfee Asset Manager позволяет автоматически обновлять базу активов при появлении в сети новых устройств, сообщая вам в реальном времени о находящихся в сети устройствах. Кроме того, решение McAfee Vulnerability Manager напрямую интегрируется с корпоративными инструментами управления активами, включая LDAP, Microsoft Active Directory и управляющую платформу McAfee® ePolicy Orchestrator® (McAfee ePO™), что дает вам возможность иметь один центральный репозиторий данных об активах.

Сбор информации по всем активам

Использование модуля McAfee Asset Manager позволяет собирать более точные сведения за счет функций постоянного пассивного обнаружения и мониторинга. После быстрого развертывания на порте SPAN система начинает мониторинг трафика, обнаруживая и проверяя на соответствие стандартам все ресурсы вашей сети, включая незаконные устройства, забытые хост-системы VMware и мобильные устройства. В ходе мониторинга система ведет учет устройств, их действий и сеансов связи. Эти детали помогают оценивать и снижать риск. Собранная информация об устройствах автоматически поступает в систему управления McAfee Vulnerability Manager для немедленной оценки. McAfee Asset Manager может также выполнить инвентаризацию всего программного и аппаратного обеспечения на каждом обнаруженном активе.

Сканирование в соответствии с вашими требованиями

McAfee Vulnerability Manager имеет ряд функций, с помощью которых вы можете оценивать и документировать соответствие своих систем отраслевым нормам. Для ускорения процесса определения политик выполните сканирование эталонной системы (gold standard), что позволит вам создать базовый вариант политики. Кроме того, вы можете использовать наши предустановленные шаблоны соответствия политиками или же можете загрузить их извне с помощью нашего протокола Security Content Automation Protocol (SCAP).

Решение McAfee Vulnerability Manager сканирует все активы в сети, включая даже сложные активы, размещенные в промежуточных средах и в средах объектов критической инфраструктуры. Так, например, если у вас есть сети без внешнего подключения, то для обнаружения и сканирования таких активов можно использовать сканер, установленный на ноутбуке или на виртуальной системе. После этого вы можете либо оставить результаты сканирования в изолированной среде, либо при необходимости свести их в централизованную систему.

Поддержка функций сканирования

- Поддерживает функцию сканирования более 450 версий операционных систем, включая версии Microsoft Windows, UNIX, Cisco, Android, Linux, Apple Macintosh, Apple iOS и VMware.
- Обеспечивает глубину сканирования веб-приложений (OWASP Top 10 и CWE Top 25).
- Осуществляет поиск уязвимостей и вредоносных программ в продуктах AOL, Apple, Microsoft (Office, IIS, Exchange), Blue Coat, CA, Cisco, Citrix, Facebook, Google, HP, IBM (Lotus Notes и WebSphere), Novell, Oracle, Real Networks, RIM (BlackBerry Enterprise Server), SAP, Oracle Java, Symantec и VMware.
- Выполняет сканирование баз данных основных поставщиков, среди которых СУБД: DB2, MySQL, Oracle, Microsoft SQL Server и Sybase.

Стандарты и сертификаты

- Включает шаблоны для ASCI 33, BASEL II, BILL 198 (CSOX), BSI IT (GR), COBIT, FDCC, FISMA, GLBA, HIPAA, ISO 27002, JSOX, MITS, PCI, SOX, NIST SP 800-68, SANS Top 20, SCAP, OVAL и др.
- Поддерживает следующие стандарты, включая сертифицированные для стран СНГ стандарты аудита: COBIT, CPE, CVE, CVSS, DISA STIG, FDCC/SCAP, ISO17799/ISO 27002/FINRA, ITIL, NIST-SP800, NSA, OVAL и SANS Top 20.
- Сертифицирован на соответствие стандарту Common Criteria.
- Сертифицирован на соответствие стандарту шифрования FIPS-140-2.

Технические характеристики

Посетите страницу www.mcafee.com/ru, где приведены технические характеристики и требования к аппаратному и программному обеспечению.

Большинство операционных систем предоставляют конфиденциальную информацию о своей конфигурации лишь после введения учетных данных, однако иногда сотрудникам отделов ИТ-безопасности бывает сложно получить доступ к учетным данным. В McAfee Vulnerability Manager встроен разработанный компанией Cyber-Ark комплект Privileged Identity Management, дающий возможность максимально просто, безопасно и без ущерба для производительности использовать учетные данные в процессе обнаружения и сканирования активов.

Определение риска за считанные минуты

При обнаружении в вашей сети новой системы McAfee Asset Manager передает в McAfee Vulnerability Manager подробную информацию об этой системе для проведения целенаправленного сканирования. Спустя несколько минут вы получаете информацию о состоянии данной системы и о том риске, который она представляет для вашей среды.

Тегирование активов для повышения эффективности

Использование политик тегирования позволяет автоматически распределять новые устройства по группам сканирования в зависимости от характеристик и уровня риска этих устройств. В зависимости от заданных вами политик сканирование распределенных таким образом новых систем может проводиться либо сразу, либо в ходе очередного сканирования.

Обнаружение уязвимостей и вредоносных программ

В отличие от других устройства, которые лишь фиксируют «лежащие на поверхности» открытые порты и конфигурации, решение McAfee Vulnerability Manager углубляется в детали. Оно выполняет оценку на уровне систем и приложений, которые включают данные о заголовках баз данных, настройках политик, разделах реестра, правах доступа к файлам и дискам, а также о работающих сервисах. Решение тестирует более 450 версий операционных систем, обнаруживая широчайший диапазон уязвимостей. Проверки также вылавливают вредоносное содержимое, включая трояны, вирусы и другие вредоносные программы.

Вы можете расширять набор стандартных проверок и обновлений, необходимых для обнаружения угроз «нулевого дня», путем создания собственных сценариев и правил тестирования программ собственного производства и устаревших программ. Решение McAfee Vulnerability Manager также выполняет оценку содержимого от сторонних производителей, написанного в соответствии со стандартами XCCDF, OVAL и другими стандартами SCAP.

Особое внимание к веб-приложениям

McAfee Vulnerability Manager позволяет администраторам управлять веб-приложениями таким же образом, как они управляют традиционными сетевыми активами. Активы веб-приложений могут быть объединены в группы, наделены собственным уровнем важности, иметь своих владельцев и права. McAfee Vulnerability Manager имеет ряд полностью автоматизированных функций для проведения глубокого сканирования веб-приложений на наличие всех веб-уязвимостей.

Постоянные обновления

Миллионы датчиков, установленных по всему миру, отправляют сведения о самых последних изменениях картины угроз для анализа, который выполняется силами сотен исследователей McAfee Labs. Собранная в режиме реального времени с помощью технологии McAfee Global Threat Intelligence информация о рисках и угрозах поступает прямо в систему управления McAfee Vulnerability Manager, что помогает защитить вас от новейших угроз.

Неограниченные возможности управления, масштабирования и интеграции

Компания McAfee позволяет вам создавать гибкие схемы сканирования, отчетности и управления, тем самым обеспечивая предпочтительный для вас порядок работы. Вы можете ограничиться мониторингом только тех активов, которые находятся вблизи от сканера, или из единой консоли контролировать работу сотен удаленных сканеров. Наша многоуровневая архитектура может быть расширена, чтобы удовлетворить потребностей предприятий любого размера.

Используя открытый интерфейс программирования приложений (API), решение McAfee Vulnerability Manager может интегрироваться с большинством приложений.

Реагирование на основе анализа риска

Возможность получить единое представление о всех уязвимостях, позволяет принимать конкретные меры противодействия, а также сокращать расходы, связанные с установкой пакетов исправлений и проведением аудитов. Так, например, в каждый «вторник исправлений» (Patch Tuesday) вы можете быстро определить, какие из ваших компьютеров могут быть затронуты уязвимостью, только что обнаруженной в Microsoft Windows или продуктах Adobe. За несколько минут, без необходимости повторного поиска уязвимостей, McAfee Vulnerability Manager представит в наглядном виде и оценит степень потенциального риска новых угроз на основе имеющихся данных конфигурации и показателей уровня риска.

С помощью этой информации, вы можете выбрать активы, основываясь на их критической важности и, щелкнув правой кнопкой мыши, запустить мгновенное целевое сканирование.

Соответствие нормам дает уверенность в безопасности

Убедительные доказательства (ожидаемые и фактические результаты сканирования и данные о непроверенных системах и сбоях при сканировании) обеспечивают документированное подтверждение того, что конкретные системы «не являются уязвимыми». Именно это требование все чаще предъявляется при аудите. Благодаря сочетанию средств активного и пассивного мониторинга активов, тестирования систем на проникновение и сканирования с аутентификацией и без аутентификации, решение McAfee Vulnerability Manager дает вам возможность с большой точностью выявлять уязвимости и случаи нарушения политик. Еще никогда раньше комплексное управление уязвимостями не было настолько простым.

McAfee
An Intel Company

ООО «МакАфи Рус»
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
Бизнес центр «Башни на набережной»
4ый этаж, офис 405 – 409
Телефон: +7 (495) 967 76 20
Факс: +7 (495) 967 76 00
www.McAfee.ru

53000ds_mvm-mam_1012_fnl_ETMG