

Брошюра

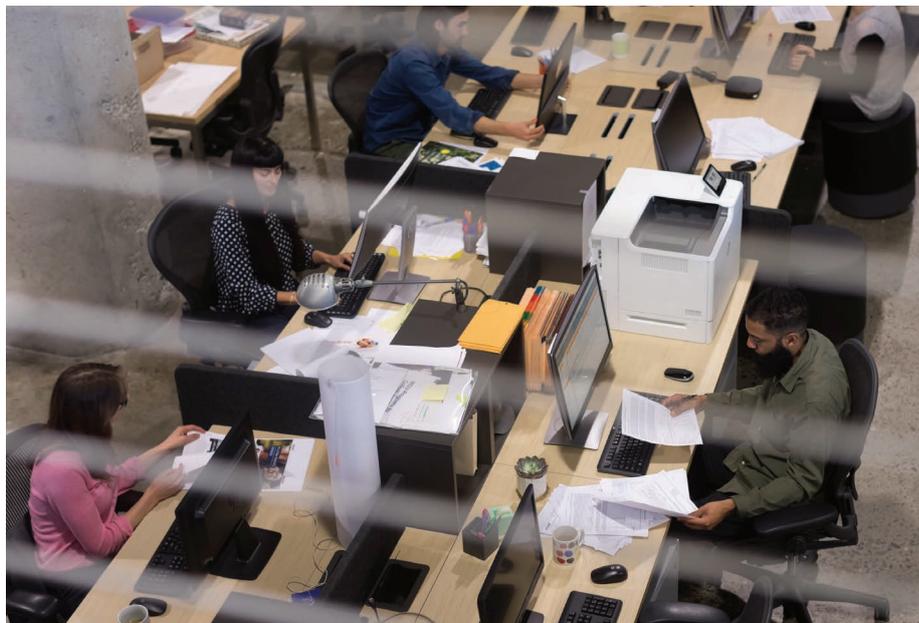
Защита всего парка устройств с помощью простого решения безопасности при печати на основе политик

Обеспечьте безопасное развитие бизнеса с помощью решения HP JetAdvantage Security Manager



11,7 млн долларов

Средний материальный ущерб от утечки данных¹



Ваше предприятие сталкивается с проблемами безопасности ежедневно

В вашей компании постоянно создаются конфиденциальные данные, которые являются очень важными для бизнеса. При этом в ней, наверняка, используются разные методы защиты, включая проверку подлинности, шифрование и мониторинг, чтобы обеспечить безопасность данных в сети, на персональных компьютерах и серверах. Однако является ли ваша среда печати и обработки изображений такой же защищенной, как и другие компоненты инфраструктуры?

Риски нарушения безопасности и связанные с ними расходы могут быть очень высоки, независимо от того, идет ли речь о распечатанных документах, оставленных без присмотра в принтере, обработке секретных данных, передаваемых с компьютера на устройства, или конфиденциальной информации, хранящейся на жестких дисках устройства. Чтобы обезопасить ваш бизнес, требуется решение, которое поможет упростить и укрепить защиту среды печати и обработки изображений, сэкономит время и деньги вашего предприятия, которые можно потратить более эффективно.



Первое в отрасли решение, обеспечивающее управление безопасностью

Чтобы помочь вам защитить ресурсы, компания HP разработала решение HP JetAdvantage Security Manager. Оно воплощает рациональный подход к обеспечению безопасности устройств HP для печати и обработки изображений на основе соблюдения политик. Решение HP Security Manager поможет повысить безопасность парка устройств печати и обработки изображений HP, предотвращая утечку данных и обеспечивая защиту ваших устройств и информации, необходимой для работы компании.

Решение HP Security Manager предлагает простой, интуитивный процесс для обеспечения безопасности всего парка устройств. Обеспечьте эффективное развертывание и мониторинг устройств на базе единой политики безопасности и защитите новые устройства HP сразу после их добавления в сеть с помощью технологии HP Instant-on Security.² Обеспечьте соблюдение нормативных требований на основе политик безопасности с помощью автоматизированных средств мониторинга HP Security Manager и отчетов на основе оценки рисков. Автоматическое развертывание и обновление сертификатов идентификации поможет укрепить информационную безопасность и одновременно значительно сократить административные расходы.

Защита парка устройств с помощью решения HP Security Manager

Решение HP Security Manager предлагает упрощенный подход к защите всего парка устройств HP, который гарантирует строгое выполнение нормативных требований и снижение рисков.

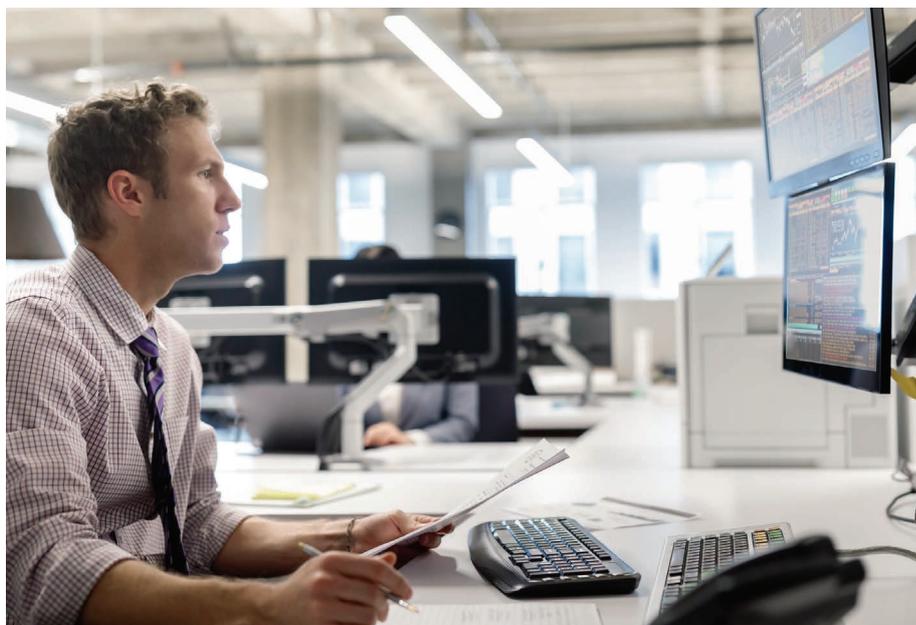


Обеспечьте безопасность всего парка устройств благодаря простому созданию политик

Простой в использовании редактор политик HP помогает создать всестороннюю политику для вашей среды с помощью интуитивно понятной системы правил. Внесение изменений в политики безопасности в точном соответствии с нуждами компании, нормативными требованиями и отраслевыми стандартами не вызывает проблем.

Шаблон стандартной политики HP Security Manager

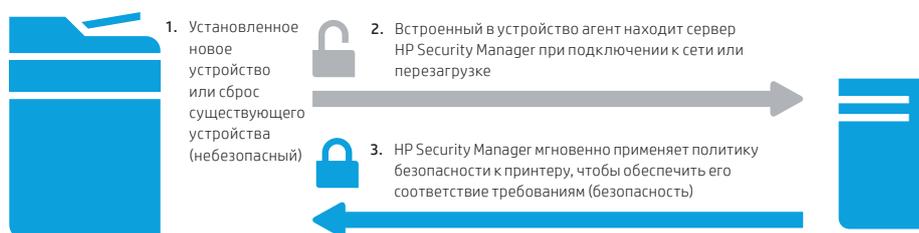
Простота разработки политики безопасности для среды печати с использованием шаблона стандартной политики HP Security Manager. Шаблон обеспечивает базовые настройки для защиты общей корпоративной среды печати, однако легко адаптируется в соответствии с индивидуальными требованиями к политике безопасности. В шаблоне наряду с настройками, рекомендованными Национальным институтом стандартов и технологий США, и контрольным списком, составленным на основе лучших методик HP, используются настройки безопасности с учетом требований клиентов. Так создается безопасная и эффективная среда печати.³



Разные способы применения политики для новых устройств

Добавлять устройства HP в HP Security Manager легко.

- **Автоматическое обнаружение:** разрешите Security Manager обнаруживать ваши устройства HP с помощью функции автоматического обнаружения. Настройте мониторинг определенного количества сетевых сегментов или диапазон IP-адресов. Затем выберите в списке устройства, которыми вы хотите управлять.
- **Файл .txt или .xml:** добавьте существующий список устройств, импортировав файл .txt или .xml с IP-адресами устройств или именами хостов, включая файлы .xml, экспортированные из HP Web Jetadmin.⁴
- **Технология Instant-On Security:** используйте функцию HP Instant-on Security для автоматического добавления устройства HP в Security Manager сразу после его подключения к сети (или после холодного сброса) без обращения к ИТ-специалисту. Благодаря уникальным возможностям технологии HP Instant-on Security, используемой в HP Security Manager, устройства тут же настраиваются в соответствии с конкретной корпоративной политикой безопасности, что помогает экономить время и сводить к минимуму возможные риски.²



HP Instant-on Security

Максимальная эффективность инвестиций благодаря проактивному подходу

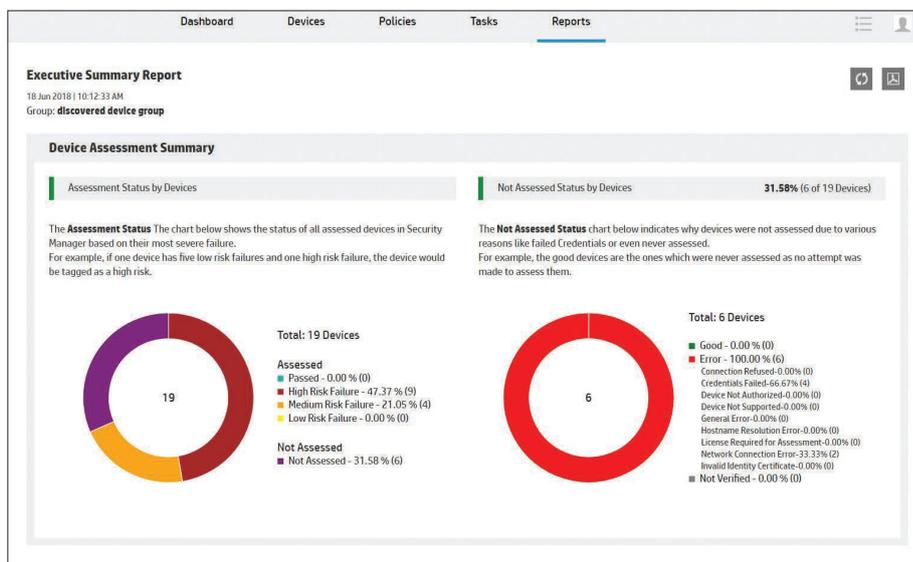
HP Security Manager помогает обеспечивать соблюдение требований благодаря непрерывным оценкам и автоматизированному устранению недостатков в работе устройств. Вы устанавливаете периодичность оценки состояния (и при необходимости восстановления) устройств. Она может выполняться ежедневно, каждую неделю или каждый месяц — по необходимости.

- **Оценка:** во время плановой оценки HP Security Manager запускается в фоновом режиме и выполняет проверку соответствия настроек безопасности вашего парка устройств требованиям конкретной политики. В процессе оценки несоответствующие функции идентифицируются и включаются в отчеты.
- **Устранение недостатков:** HP Security Manager автоматически применяет правильные настройки безопасности ко всем несоответствующим функциям, выявленным в ходе оценки. Удовлетворяющая требованиям настройка снова оценивается, чтобы подтвердить ее успешное применение.

Снижение рисков благодаря подробным отчетам по безопасности парка устройств

Обеспечьте защиту информации с помощью встроенных инструментов создания отчетов. Пользователи могут создавать сводные отчеты по всем уровням риска для парка устройств, а также анализировать конкретные риски, связанные с отдельным устройством или настройкой безопасности. Можно также включить отправку сообщения электронной почты высокого уровня важности с отчетом после каждой автоматически запланированной оценки и устранения недостатков.

HP Security Manager также может провести оценку рисков и выявить наименее защищенные устройства. На менее защищенных устройствах может быть развернута не самая последняя версия микропрограммы устройства, микропрограмма Jetdirect, она может не поддерживать функции Sure Start, Run Time Intrusion Detection или Whitelisting.



Простая, интуитивная оценка риска



Защитите свой парк устройств благодаря универсальному управлению сертификатами

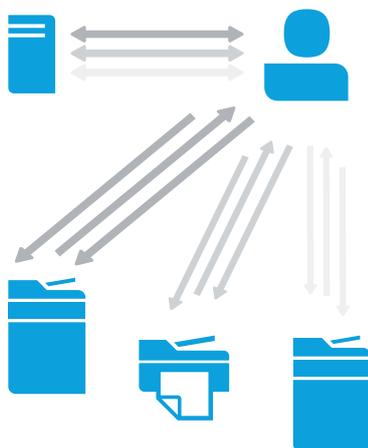
Сертификаты выполняют важную функцию защиты потока информации, поступающей на устройства и передаваемой из него. Они используются для удостоверения подлинности и шифрования данных, обеспечивая безопасную связь между надежными объектами. Ручная установка уникальных сертификатов — это сложный и нередко сопряженный с ошибками процесс, который занимает много времени — до 15 минут на каждое устройство. Это вынуждает многих клиентов или полностью отказываться от использования сертификатов, или применять их надлежащим образом.

Последние инновации HP Security Manager позволяют оптимизировать этот процесс за счет развертывания уникальных сертификатов соответствия в масштабе парка устройств, непрерывного мониторинга с целью подтверждения их правомерности и автоматически выполняемой замены недействительных или сертификатов с истекшим сроком.

HP Security Manager позволяет эффективно применять и обновлять сертификаты идентификации и соответствия устройств, что способствует повышению безопасности инфраструктуры, приложений и каналов связи устройств.

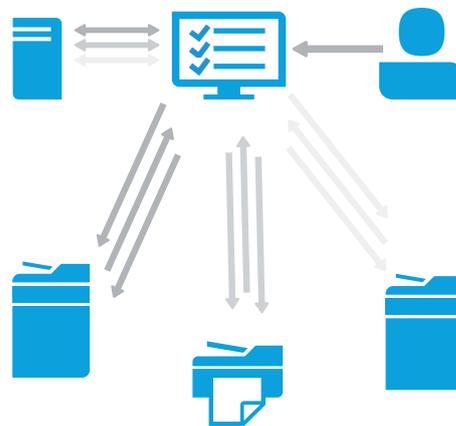
До

Процесс выполнялся вручную на каждом устройстве, это требовало много времени, часто возникали ошибки



После

Простая, эффективная, однократная настройка для всего парка устройств благодаря решению HP Security Manager



Какие преимущества обеспечиваются этим простым в использовании решением?

HP Security Manager — универсальное решение по обеспечению безопасности, которое можно использовать в разных средах и деловых условиях.

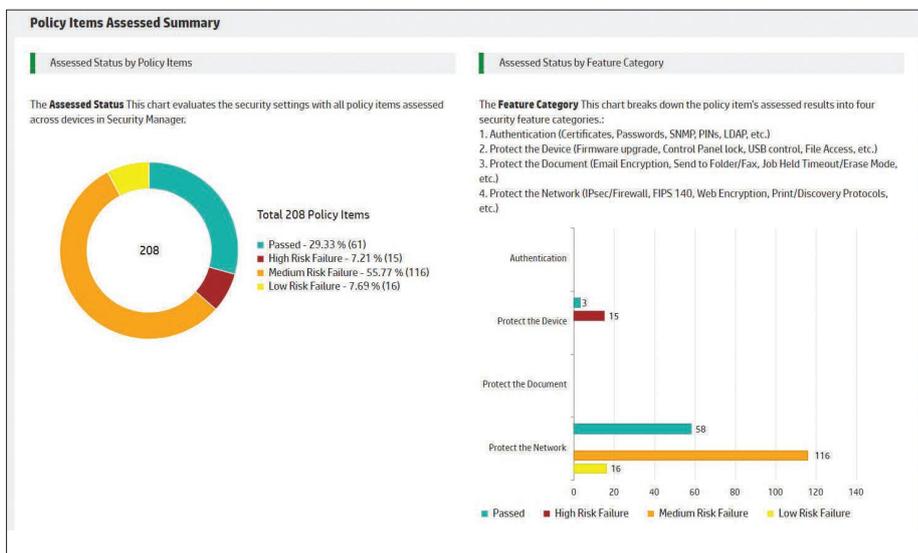
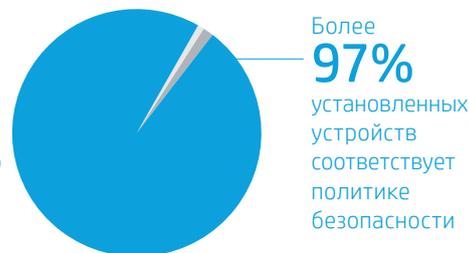
Например, для фирм, оказывающих финансовые услуги, обеспечение защиты информации клиента является залогом успешной работы. Кроме того, она является необходимой в соответствии с отраслевыми требованиями. Однако учитывая, что парк печатных устройств часто включает более тысячи единиц, обеспечение безопасности требует значительных усилий по администрированию.

Благодаря решению HP Security Manager фирмы, оказывающие финансовые услуги, могут экономить средства и время, планируя ежедневные процедуры оценок и устранения неполадок в работе парка устройств печати и обработки изображений HP. Это поможет обеспечить соответствие всего парка устройств требованиям политики безопасности компании, а также освободить ИТ-специалистов, чтобы они могли сосредоточить свои усилия на других операциях. Администраторы также могут распечатывать или сохранять встроенные отчеты на уровне парка оборудования, отдельного устройства или функций, которые подтверждают соответствие требованиям политики и безопасность клиентской информации.

До использования HP Security Manager



После использования HP Security Manager





Технические характеристики

Поддерживаемые сетевые операционные системы	HP Security Manager поддерживает следующие 32- и 64-разрядные ОС: Microsoft® Windows® 7 SP1, 8, 8.1, 10; Microsoft Windows Server® 2008 R2 (только 64-разрядная версия), 2012, 2012 R2, 2016
Поддерживаемые базы данных	Microsoft SQL Server Express 2012, Microsoft SQL Server 2012 (Enterprise), Microsoft SQL Server Express 2014 (в комплекте), Microsoft SQL Server 2014 (Enterprise)
Проверенные браузеры	Internet Explorer 11 и более поздние версии, Google Chrome™ v60.0 и более поздние версии
Версии .NET	Требуется NET 3.5 и 4.6.2
Поддерживается устройствами	Сведения о совместимости устройств см. на сайте hp.com/go/securitymanager
Системные требования	<p>Требования к серверу: двухъядерный процессор 2,33 ГГц или более мощный, не менее 4 Гбайт ОЗУ (32-разрядные системы), не менее 8 Гбайт ОЗУ (64-разрядные системы)</p> <p>Требования к клиенту: ПК с процессором с частотой 1,8 ГГц, не менее 3 Гбайт ОЗУ 32-разрядные системы), не менее 4 Гбайт ОЗУ (64-разрядные системы)</p> <p>Требования к устройствам хранения данных: не менее 4 Гбайт свободного места на жестком диске. Требуемое пространство для базы данных отличается для HP Security Manager и зависит от следующих факторов: количество оцениваемых устройств, масштаб оценки политики, число политик, используемых для оценки, будущие оценки, а также рекомендации, полученные после оценки. Настоятельно рекомендуется при управлении более чем 1000 устройств использовать полную версию SQL.</p>
Производительность	Компания HP протестировала до 10 000 устройств на сервере (возможны большие значения) и вышла на показатель оценки 1500 устройств в час с использованием Стандартной политики HP Security Manager. ⁵
Поддерживаемые языки	Английский и упрощенный китайский

Источники подробной информации

Для получения дополнительных сведений о том, как сделать HP JetAdvantage Security Manager неотъемлемой частью общей стратегии безопасности ИТ вашей компании или получить бесплатную пробную версию, посетите веб-сайт hp.com/go/securitymanager, обратитесь к представителю HP или обратитесь к партнеру со статусом HP Document Solutions Specialist.

Дополнительная информация

hp.com/go/securitymanager

- ¹ Исследование «2017 Cost of Cyber Crime», проведенное Ponemon по заказу HPE в 2017 г. https://www.accenture.com/t20170926T072837Z_w_us-en/acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf
- ² Доступно не для всех моделей устройств и версий микропрограмм.
- ³ Данный инструмент предназначен только для общего сравнения. В основе данной информации лежат внутренние спецификации, характеристики, опубликованные производителем, а также собственные данные и алгоритмы. Компания Hewlett-Packard Company не гарантирует точность информации. Пользователи могут настраивать политики безопасности, используемые при анализе. Это повлияет на результаты. Фактические результаты могут несколько отличаться.
- ⁴ ПО HP Web Jetadmin можно загрузить бесплатно на веб-сайте hp.com/go/webjetadmin.
- ⁵ Производительность зависит от размера политики (количества правил) и от того, прошли ли печатающие устройства процедуру восстановления и находятся ли в стабильном состоянии.

Подписаться на информационные бюллетени HP
hp.com/go/getupdated



Поделиться с коллегами

© Hewlett-Packard Development Company, L.P., 2012–2018 Информация в настоящем документе может быть изменена без предварительного уведомления. В отношении продуктов и услуг HP юридически обоснованными являются только те гарантии, которые установлены явным образом в гарантийных обязательствах, прилагаемых к таким продуктам и услугам. Никакие содержащиеся здесь сведения не могут рассматриваться как дополнительные условия гарантии. Компания HP не несет ответственности за содержащиеся в настоящем документе технические или редакторские ошибки или упущения.

Google Chrome — товарный знак корпорации Google. Microsoft, Windows, Windows Server и SQL Server — товарные знаки группы компаний Microsoft, зарегистрированные в США.

