



Безопасность принтеров HP DesignJet

С каждым днем угрозы безопасности становятся все более изощренными. Каждое устройство в сети компании является точкой уязвимости. Это касается и сетевых принтеров, а, следовательно, и широкоформатных принтеров.



Целевые клиенты

Организации всех размеров, из разных регионов мира и разных отраслей, которым требуется обеспечить безопасность своих общих сред печати и обработки изображений.

Контактные лица

- Руководитель службы информационной безопасности или директор по ИТ-безопасности
- Директор по ИТ
- Менеджеры по безопасности/соблюдению нормативов
- ИТ-руководители и другие ответственные лица

Характеристики идеального клиента

- Повышают требования к безопасности из-за роста угроз и необходимости соблюдения нормативов
- Не могут мириться с рисками, связанными с тем, что сеть организации подвержена утечке данных
- Вынуждены платить высокие штрафы из-за несоблюдения нормативов, связанных с обработкой данных заказчиков
- Используют строго конфиденциальные данные в своих ежедневных бизнес-операциях

Ситуация на рынке

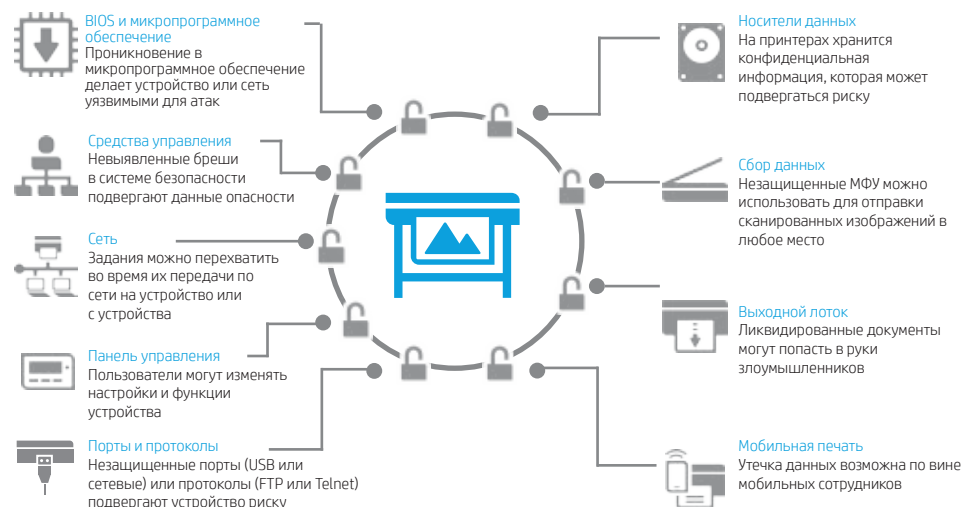
В условиях все более сложных и настойчивых атак со стороны киберпреступников сетевые брандмауэры уже не являются достаточной мерой для обеспечения безопасности. Организациям необходимо защитить свои конечные устройства за пределами брандмауэра, в том числе и сетевые принтеры.

Стоимость устранения последствий одной утечки, связанной с действиями злоумышленников, случайным неправомерным доступом к данным внутри компании или нарушением нормативных либо законодательных требований, может быть очень высока. Ежегодные потери составляют около 4 миллионов долларов США⁴. Сюда входят штрафы, потеря бизнеса, подрыв репутации и коллективные иски.

Требования к соблюдению нормативов становятся все более сложными. И организациям нужны устройства и решения, которые помогут успешно соблюдать эти требования.

Проблемы безопасности у клиентов

И хотя многие ИТ-отделы внедряют новые инструменты для обеспечения безопасности отдельных компьютеров и всей сети предприятия, устройства печати и обработки изображений часто упускаются из виду остаются незащищенными.



Потребности клиентов в сфере безопасности

Вашим клиентам нужны простые решения для защиты устройств, данных и документов. Им также необходимо поддержать своих ИТ-специалистов и сэкономить их время за счет оптимизированных средств управления безопасностью печати и отчетности о соблюдении нормативных требований.

Безопасность устройств

- Защита BIOS и микропрограммного обеспечения от атак и вредоносного ПО
- Защита обновлений микропрограммного обеспечения
- Настройки и пароли безопасности на устройствах

Безопасность данных

- Шифрование данных, передаваемых на принтер и с принтера, а также данных, хранящихся на принтере
- Поддержка цифровых сертификатов, подписанных CA (PKI)
- Безопасные процессы очистки и утилизации жестких дисков
- Проверка подлинности учетных данных пользователей и управление доступом
- Решения безопасной мобильной печати

Безопасность документов

- Решения безопасной печати по PIN-коду

Мониторинг безопасности парка устройств и соблюдение нормативов

- Контроль над безопасностью парка устройств с помощью множества функций конфигурации и мониторинга
- Расширенные возможности отчетов, помогающие соблюдать нормативы

Ценное предложение для клиентов

- Минимизация рисков разорительных кибератак
- Защита конфиденциальных данных и документов
- Экономия времени за счет автоматизации управления безопасностью в масштабе парка устройств
- Обеспечение соблюдения отраслевых нормативов и получение простого доступа к данным для отчетности о нормативном соответствии

Ценное предложение для партнеров

- Возможность роста в результате того, что клиенты активно вкладывают средства в безопасность печати
- Ведение аргументированных переговоров и продажа высоких объемов продукции, повышающая прибыль организации; обсуждение решений безопасности смещает акцент со стоимости на получаемые преимущества

Уточняющие вопросы

Вопросы заказчику:

- Имеется ли у вас стратегии в сфере безопасности для устройств печати и обработки изображений?
- Имеете ли вы дело с конфиденциальной информацией, такой как личные данные сотрудников или сведения о заказчиках?
- Шифруете ли вы задания печати?
- Защищены ли ваши принтеры от вредоносного ПО и вирусов?
- Как часто вы применяете обновления для микропрограммы принтеров?

- Применяете ли вы в принтерах административные пароли, и может ли кто угодно менять настройки ваших устройств?
- Сколько времени тратят ИТ-специалисты на конфигурирование ваших принтеров?

Предлагаемые HP решения безопасности для принтеров HP DesignJet

Функции безопасности, встроенные в принтеры HP DesignJet, помогут компаниям защитить устройства, данные и документы. К тому же, они помогут вашим заказчикам в управлении безопасностью и соблюдением нормативов для парка устройств.

Защищенные и безопасные принтеры

- **Пакеты микропрограммного обеспечения с подписью HP** — пакеты микропрограмм имеют цифровую подпись группы HP Code Signing. Каждая новая устанавливаемая микропрограмма проходит проверку.
- **UEFI Secure Boot** — проверяет целостность операционной системы во время запуска
- **Шифрование жестких дисков** — процессы шифрования и дешифровки в HP соответствуют стандарту AES (256 бит)
- **Безопасное удаление файлов и очистка дисков** — эти процедуры гарантируют, что важные данные, хранящиеся в системах, будут удалены без возможности последующего восстановления.
- **Блокировка доступа к панели управления** — доступ к панелям управления принтеров блокируется, поэтому неавторизованные пользователи не могут зайти в систему принтера и изменить его настройки.

Программное обеспечение безопасности




Кроме самих устройств, компания HP предлагает решения для обнаружения, защиты, мониторинга и управления парком устройств, а также длительной защиты данных и документов.

- **HP JetAdvantage Security Manager** — единственный в отрасли инструмент обеспечения соответствия требованиям безопасности печати, который автоматизирует управление безопасностью парком устройств⁶. — Поддерживает создание политик безопасности печати и их развертывание в масштабе парка устройств — Отчеты на основе оценки рисков помогают ИТ-специалистам быстро проверять состояние парка устройств и обеспечивать соблюдение нормативов — Автоматизированное применение и обновление уникальных сертификатов, подписанных CA
- **HP Web Jetadmin** — повышение производительности и сокращение эксплуатационных затрат благодаря удостоенному наград ведущему отраслевому решению для управления печатью. Простая в использовании программа HP Web Jetadmin оснащена простым веб-интерфейсом для установки, настройки, управления и устранения неисправностей устройств печати HP и других производителей, подключенных к сети и ПК⁷.

Услуги по обеспечению безопасности

- **Специальные услуги HP по утилизации** — гарантируют удаление всех данных с жестких дисков перед ответственной утилизацией старых продуктов по окончании их срока службы. Подробнее см. на веб-сайте hp.com/go/businessrecycling.

Решения безопасности для HP DesignJet и аналогичные решения для устройств конкурентов

		HP DesignJet (1)	Canon (2)	Epson (3)	Ricoh (4)
УСТРОЙСТВО 	Функции безопасного управления сетью с помощью протокола SNMP v3	✓	✓	⊘	✓
	Безопасное удаление файлов	✓	⊘ (6)	⊘	✓
	Безопасная очистка дисков	✓	✓ (5)	✓	✓
ДАННЫЕ 	Поддержка стандарта 802.1x	✓	⊘ (6)	✓	✓
	Шифрование жестких дисков	✓	⊘	✓	✓
	Протокол IPSEC (Internet Protocol Security)	✓	⊘ (6)	✓	✓
ДОКУМЕНТ 	Печать по ПИН-коду	✓	⊘	⊘	✓

(1) В сравнении участвовали следующие модели: HP DesignJet T930, T1530, T2530 MFP, T3500 MFP
(2) В сравнении участвовали следующие модели: Canon iPF785, iPF770, iPF850, iPF770L36, M40 Scanner
(3) В сравнении участвовали следующие модели: Epson SC-T5200/D, SC-T5200F MFP
(4) В сравнении участвовали следующие модели: Ricoh MP CW2201SP
(5) Для моделей с жестким диском
(6) M40 Scanner: Да

Как одержать победу

Предприятиям жизненно необходимо очень серьезно относиться к безопасности печати. HP предлагает лучшие в отрасли продукты и решения, помогающие защищать устройства, данные и документы.

¹ «Insecurity of Network-Connected Printers», Ponemon Institute, октябрь 2015 г.

² «Why enterprise security priorities don't address the most serious threats», Help Net Security, июль 2015 г.

³ 26,2% респондентов рассказали о значительных сбоях в безопасности ИТ, которые потребовали серьезной работы по устранению, причем в более 26,1% этих инцидентов были задействованы процессы печати. Отчет IDC «IT and Print Security Survey 2015», документ № US40612015, сентябрь 2015 г.

⁴ Ponemon Institute, отчет «Cost of Data Breach Study Global Analysis», 2016 г.

⁵ Quocirca, «Managed Print Services Landscapes for 2014 and 2015».

⁶ На основе внутреннего исследования конкурирующих предложений компаний HP (Device Security Comparison, январь 2015 г.) и отчета по решению HP JetAdvantage Security Manager 2.1, подготовленного Buyers Laboratory LLC в феврале 2015 г. Решение HP JetAdvantage Security Manager приобретается отдельно. Дополнительные сведения см. на сайте hp.com/go/securitymanager.

⁷ Программу HP Web Jetadmin можно бесплатно загрузить по адресу hp.com/go/wja

Отправить коллегам

© HP Development Company, L.P., 2017. Приведенная в этом документе информация может быть изменена без уведомления. Гарантийные обязательства для продуктов и услуг HP приведены только в условиях гарантии, прилагаемых к каждому продукту и услуге. Никакие содержащиеся здесь сведения не могут рассматриваться как дополнительные гарантийные обязательства. HP не несет ответственности за технические, редакторские и другие ошибки в данном документе.

Android и Google Chrome являются товарными знаками корпорации Google Inc. Microsoft является зарегистрированными в США товарными знаками группы компаний Microsoft.

Конфиденциальная информация HP, 2017 г. Настоящий документ содержит конфиденциальную и/или охраняемую законом информацию. Данная информация предназначена только для внутреннего использования компанией HP и торговым партнером.

Если вы не входите в число лиц, указанных на обложке этого документа, то вам строго запрещено читать, передавать или распространять этот документ или иными способами использовать его содержимое.

