



Defenda sua rede com a impressão mais segura do mundo¹

94%

das empresas de serviços financeiros dizem que a segurança da copiadora/impressora é importante ou muito importante²



61%

das organizações relataram pelo menos uma única violação de dados relacionada à impressão no ano passado³



43%

das empresas ignoram as impressoras em suas práticas de segurança de terminais⁴





Apenas 18% das empresas monitoram as impressoras contra ameaças.⁴ E a sua?

“Comprovando seu investimento em longo prazo em segurança da impressão, a HP possui o mais amplo e profundo portfólio de serviços e soluções de segurança do mercado.”

– Quocirca, janeiro de 2017⁵

Reconheça os riscos ocultos

A TI recebe tarefas continuamente para proteção de informações confidenciais, incluindo identidades de funcionários e dados de clientes, em vários dispositivos e ambientes. Embora muitos departamentos de TI apliquem rigorosamente medidas de segurança a computadores individuais e à rede, dispositivos de impressão e imagem com frequência são negligenciados e deixados expostos. Quando há dispositivos desprotegidos, toda a rede pode estar exposta a um ataque de cibersegurança.

Compreenda os custos potenciais

Até mesmo uma única violação da segurança tem o potencial de ser onerosa. Se informações privadas forem colocadas em risco devido à impressão e imagem inseguras, as ramificações poderiam incluir roubo de identidade, furto de informações sobre a concorrência, comprometimento da imagem ou reputação da marca e litígio. Além disso, a não conformidade regulamentar e jurídica pode resultar em multas pesadas.

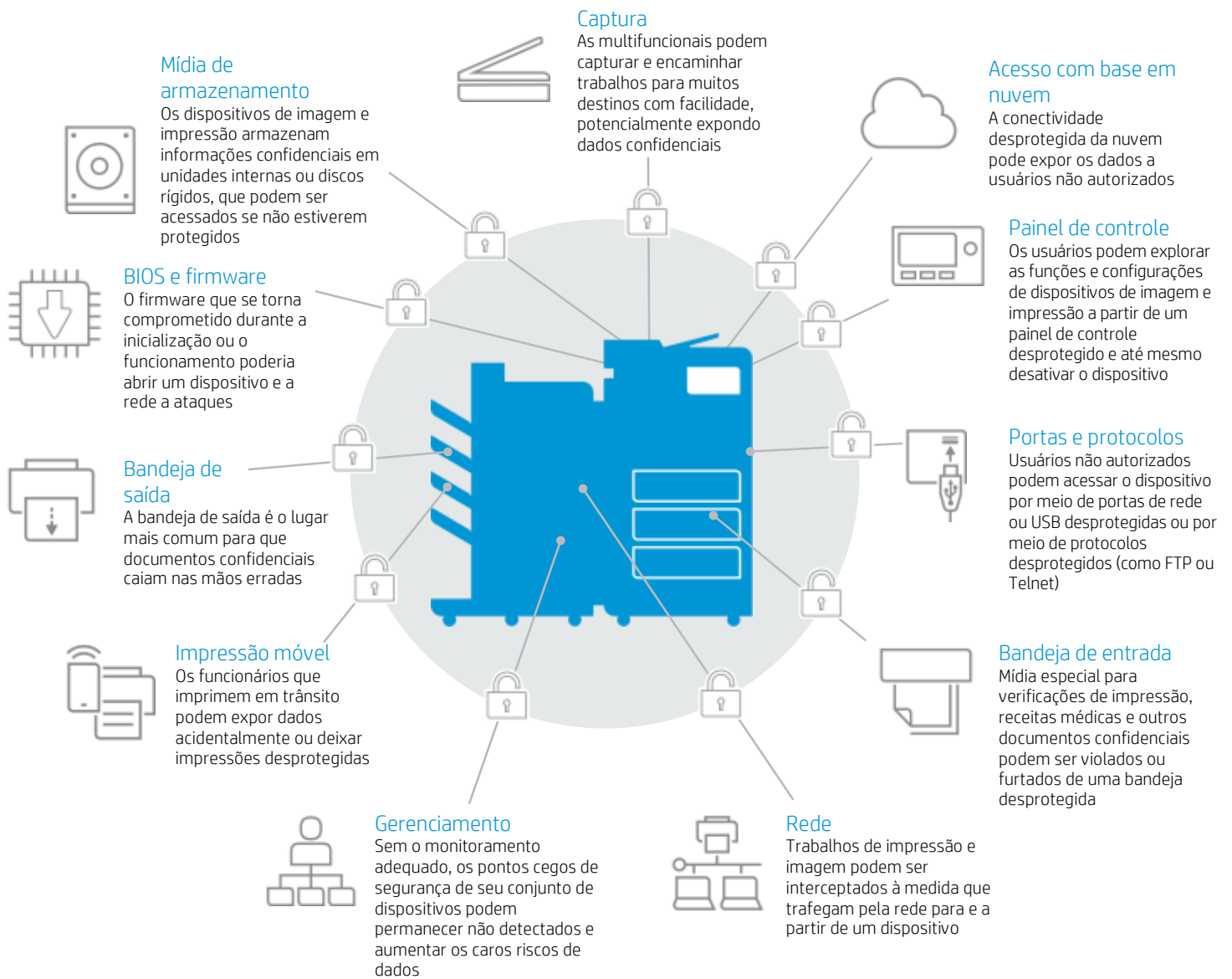
A HP pode ajudar

Defenda sua rede com a impressão mais segura do mundo.¹ As impressoras HP estão sempre alertas, detectando e interrompendo ameaças continuamente enquanto se adaptam às novas. A HP pode ajudar você a automatizar dispositivos, dados e proteções de documentos com um amplo portfólio de soluções. Nossos especialistas em segurança da impressão podem ajudar você a desenvolver e implantar uma estratégia completa de segurança de imagem e impressão.

Defenda seus dispositivos, dados e documentos

Brechas críticas podem ocorrer em vários pontos em seu ambiente de imagem e impressão. Uma vez que você compreenda essas vulnerabilidades, poderá reduzir os riscos mais facilmente.

Pontos de vulnerabilidade de imagem e impressão





Proteja o dispositivo



Saiba mais

Serviços HP Custom Recycling
hp.com/go/businessrecycling

HP Secure Managed Print Services
hp.com/go/securemp

As impressoras da HP são desenvolvidas para funcionar em conjunto com soluções de gerenciamento e monitoramento da segurança para ajudar a reduzir riscos, aumentar a conformidade e proteger sua rede de ponta a ponta. (Nem todos os recursos e soluções estão disponíveis em todos os dispositivos da HP.⁶)

Práticas de segurança fundamentais

Armazenamento criptografado com apagamento seguro

Quaisquer informações confidenciais armazenadas na unidade interna ou no disco rígido são potencialmente vulneráveis a furto. Muitos dispositivos da HP vêm com criptografia integrada para proteger os dados. Quando os dados armazenados não forem mais necessários, use recursos do dispositivo integrados para sobrescrever dados e remover informações confidenciais com segurança.

Descarte seguro

Os *serviços HP Custom Recycling* podem assegurar que os dados sejam eliminados dos discos rígidos antes da reciclagem de produtos antigos de maneira responsável.

Acesso seguro para reparo da impressora

Conhecer as práticas de segurança dos fornecedores de manutenção de impressoras ajudará a proteger dados sigilosos. Escolha *HP Secure Managed Print Services (MPS)* ou parceiros HP para obter assistência especializada.

Desativação de portas e protocolos não utilizados

Reduza a superfície de ataque por meio da configuração de dispositivos adequada. Desative portas físicas e protocolos desprotegidos (como FTP ou Telnet) para impedir o uso ou o acesso não autorizado.

Controle de acesso do administrador para o dispositivo

Defina senhas de administrador para que apenas a equipe de TI ou outros funcionários autorizados possam definir as configurações do dispositivo.

Listas de permissões do código de firmware

Consulte a página seguinte para obter informações sobre como as listas de permissões podem proteger seu conjunto de dispositivos contra malware.

Práticas de segurança avançadas



Saiba mais

Recursos de segurança da impressão integrados:

- HP Sure Start (integridade do BIOS)
- Listas de permissões do código de firmware
- Detecção de invasão em tempo de execução
- HP Connection Inspector

hp.com/go/PrintersThatProtect

HP JetAdvantage Security Manager:

hp.com/go/securitymanager

Common Criteria Certification

As impressoras empresariais da HP possuem certificado de conformidade com padrões de segurança reconhecidos internacionalmente, como Common Criteria Certification (CCC) e FIPS 140. Assegure-se de que as atualizações de firmware dos dispositivos tenham assinatura de código para confirmar a autenticidade e a integridade do código e para manter a conformidade.

Recursos de segurança da impressão detectam e interrompem ataques automaticamente

As impressoras empresariais da HP incluem recursos de segurança que ajudam a protegê-las para que não se tornem um ponto de entrada para ataques em sua rede. Somente a segurança da impressão HP oferece detecção em tempo real, monitoramento automatizado e validação de software integrada para interromper as ameaças no momento que se iniciam.⁷

As impressoras empresariais da HP, da Pro⁸ à Enterprise⁷, estão sempre alertas, detectando e interrompendo ameaças continuamente durante todas as fases da operação:

- **Durante a inicialização.** O código de inicialização (para dispositivos Pro) ou BIOS (para dispositivos Enterprise) é um conjunto de instruções usado para carregar componentes críticos de hardware e iniciar o firmware. A integridade do código é validada em todos os ciclos de inicialização — ajudando a proteger seu dispositivo contra ataques.
- **Ao carregar firmware.** *Listas de permissões* verificam automaticamente o firmware na inicialização para determinar se o código é autêntico e correto — assinado digitalmente pela HP. Caso seja detectada uma anomalia, o dispositivo reinicializa para um estado offline seguro e notifica a TI.
- **Durante o tempo de execução.** Os recursos integrados da HP ajudam a proteger a memória dos dispositivos enquanto estão em operação e conectados à rede — exatamente quando a maioria dos ataques ocorre. No caso de um ataque, o dispositivo é desligado.

Dispositivos HP Enterprise podem fazer autorreparo

Além de serem capazes de detectar e interromper ameaças, as impressoras HP Enterprise fazem o autorreparo automaticamente contra ataques, assim a TI não precisa intervir.⁷ Esses recursos acionam uma reinicialização automaticamente no caso de um ataque ou anomalia. Os administradores podem ser notificados por meio de ferramentas de gerenciamento de eventos e informações de segurança (SIEM) como ArcSight, Splunk e SIEMonster.

- O *HP Sure Start* é o único BIOS de autorreparo do setor.⁷ Se o BIOS estiver comprometido, o HP Sure Start reinicia com uma “versão oficial” segura do BIOS.
- A *detecção de invasão em tempo de execução* monitora operações complexas de memória e firmware, interrompe a invasão automaticamente e reinicia no caso de um ataque.
- O *HP Connection Inspector* avalia conexões de rede de saída para determinar o que é normal, interromper solicitações suspeitas e frustrar malware ao acionar automaticamente uma reinicialização.

Com a proteção do investimento do firmware HP FutureSmart atualizável, você pode adicionar listas de permissões, detecção de invasão em tempo de execução e o HP Connection Inspector a muitas impressoras HP Enterprise existentes.⁷

O HP JetAdvantage Security Manager completa o ciclo de verificação

Após ocorrer uma reinicialização — ou em qualquer momento que um novo dispositivo é adicionado à rede — o *HP JetAdvantage Security Manager* automaticamente avalia e, se necessário, faz a remediação de configurações de segurança do dispositivo para estar em conformidade com as políticas pré-estabelecidas da empresa.⁹ Não há necessidade de intervenção da TI.

Como funciona?

Os recursos de segurança integrados abordam quatro etapas principais no ciclo de um dispositivo da HP.

Em caso de ataque, os dispositivos HP Enterprise podem reiniciar e fazer autorreparo.

O HP JetAdvantage Security Manager completa o ciclo de verificação.

Quatro. Monitoramento contínuo

Protege as operações e interrompe ataques enquanto o dispositivo está em funcionamento.

Inspeciona conexões de rede de saída para interromper solicitações suspeitas (somente Enterprise).

Três. Verificação de configurações

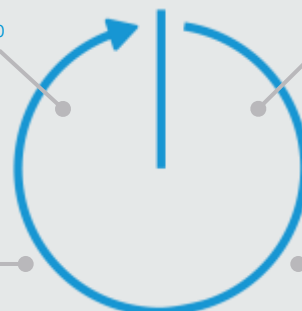
Após uma reinicialização, o HP JetAdvantage Security Manager verifica e corrige quaisquer configurações de segurança do dispositivo afetado.

Um. Verificação do código de BIOS/inicialização

Impede a execução de código mal-intencionado durante a inicialização ao permitir que apenas códigos autênticos com assinatura HP sejam carregados.

Dois. Verificação do firmware

Permite que apenas firmware legítimo e autêntico — digitalmente assinado pela HP — seja carregado.





Proteja os dados



Saiba mais

HP Web Jetadmin
hp.com/go/wja

HP Universal Print Driver com impressão
criptografada segura
hp.com/go/upd

Soluções de fluxo de trabalho HP JetAdvantage
hp.com/go/documentmanagement

HP Access Control
hp.com/go/hpac

Armazenados ou em trânsito, seus dados requerem proteção constante. Aqui estão algumas etapas essenciais para ajudar a garantir utilização e entradas seguras.⁶

Práticas de segurança fundamentais

Padrões de rede IPsec ou 802.1x

Use padrões de rede criptografados para proteger os dados que se deslocam pela rede entre o dispositivo e as ferramentas de gerenciamento como *HP Web Jetadmin* ou o *Servidor da web incorporado da HP*.

Criptografe dados em trânsito

Proteja os trabalhos de impressão que se deslocam para o dispositivo com criptografia como Internet Print Protocol sobre TLS (IPPS). Ou o *HP Universal Print Driver Secure Encrypted Print*, que fornece criptografia e descriptografia AES256 verdadeiramente simétricas de trabalhos de impressão, do cliente para a página, com base em uma senha definida pelo usuário e utilizando bibliotecas de criptografia Microsoft® em conformidade com o padrão FIPS 140.

Na digitalização, as *soluções de fluxo de trabalho HP JetAdvantage* podem ajudar a proteger as informações confidenciais enquanto aumentam a eficiência. Por exemplo, o HP Capture and Route se integra perfeitamente com o HP Access Control para maior segurança, com a conveniência de uma única autenticação e a capacidade de monitorar conteúdos para governança de informações.¹⁰

Criptografe dados inativos

Proteja informações confidenciais de negócios armazenadas no disco rígido com criptografia integrada. Para fornecer um nível extra de segurança, o acessório HP Trusted Platform Module (TPM) opcional pode ser adicionado facilmente ao dispositivo, reforçando a proteção de credenciais e dados criptografados ao selar automaticamente as chaves de criptografia dos dispositivos para o TPM. Ele fornece uma identidade segura dos dispositivos ao gerar e proteger chaves privadas de certificados.

Proteção de firewall

Impeça que malware e vírus entrem na rede ao limitar o acesso da impressora a dispositivos de computação na rede.

Autenticação nativa de usuários

Reduza custos e os riscos de segurança ao requerer que os usuários façam login com PIN/PIC, LDAP ou autenticação Kerberos. Você também pode integrá-los com o Active Directory.

Controles de acesso com base em função

O *HP Access Control Rights Management* ajuda a reduzir custos e os riscos de segurança por meio de restrições de recursos de impressão. Os controles de acesso com base em função permitem que você ofereça diferentes recursos a diferentes usuários ou até mesmo departamentos inteiros, dependendo de suas necessidades. Por exemplo, você pode limitar quem pode enviar e receber fax, digitalizar para e-mail ou digitalizar para fax.

Práticas de segurança avançadas



Saiba mais

HP Access Control
hp.com/go/hpac

HP JetAdvantage Connect
hp.com/go/JetAdvantageConnect

HP Capture and Route
hp.com/go/hpcr

Autenticação e rastreamento avançados

Implante autenticação avançada (como senhas, cartões de proximidade, Smart Cards ou biometria) e soluções de rastreamento para controle e segurança adicionais.

- O *HP Access Control Secure Authentication* restaura o controle, reforça a segurança e reduz os custos. Obtenha uma variedade de controles e opções avançadas, incluindo toque para autenticação com dispositivos móveis habilitados para NFC.--
- O *HP Access Control Job Accounting* ajuda você a controlar e reunir dados com precisão, analisar os resultados e, então, criar e enviar relatórios. Aplique dados extraídos para alocar custos de impressão, motivar funcionários a imprimir com mais inteligência e fornecer à TI as informações necessárias para aprimorar previsões em todo o conjunto de dispositivos.

Dispositivos móveis incluídos no acesso à rede

Use seus dispositivos móveis como parte de sua política geral de segurança da impressão para controle de acesso à impressora. A HP oferece soluções com base em servidor que fornecem recolhimento de impressão seguro, bem como recursos avançados de gerenciamento e elaboração de relatórios.

- O *HP JetAdvantage Connect* fornece impressão móvel intuitiva e confiável, projetada para as empresas. Ajude a economizar tempo e dinheiro aproveitando as ferramentas e políticas de rede de TI existentes para gerenciar a impressão móvel.¹¹ Os usuários podem imprimir com segurança a partir de uma variedade de smartphones e tablets — onde e quando precisarem — com facilidade de impressão semelhante a de PCs.
- O *HP Access Control* inclui recursos para gerenciar a impressão móvel. Ele utiliza a infraestrutura de e-mails existente, permitindo que os usuários móveis enviem um trabalho de impressão por e-mail para sua fila de impressão e, em seguida, retirem-no de qualquer impressora ou multifuncional habilitada para a solução. Proteja dispositivos de impressão de rede com recursos de autenticação seguros, incluindo o Mobile Release.

Impeça vazamentos de dados antes que ocorram

As soluções da HP oferecem recursos para ajudar a proteger contra a perda de dados. Com o *HP Capture and Route Data Loss Prevention*, você pode evitar que as informações confidenciais sejam digitalizadas ou enviadas por fax. O *HP Access Control Print Data Loss Prevention* permite que você impeça que documentos sigilosos sejam impressos. Controle seus dados mais importantes para desencorajar e impedir violações, sem desacelerar os fluxos de trabalho. Obtenha alertas de segurança inteligentes com base no termos de sua escolha.

Aplique certificados digitais às impressoras

Aumente a segurança de seu ambiente de impressão ao aplicar certificados digitais a impressoras e multifuncionais em rede. Economize tempo ao usar o HP JetAdvantage Security Manager para instalar e renovar certificados automaticamente.⁹



Proteja o documento

Integre soluções inteligentes de hardware e software com seu plano de segurança de TI maior para proteger as informações confidenciais em seus documentos impressos.⁶



Saiba mais

HP JetAdvantage Secure Print
hp.com/go/JetAdvantageSecurePrint

HP JetAdvantage Private Print
hp.com/go/JetAdvantagePrivatePrint

HP Access Control
hp.com/go/hpac

Proteção a documentos da HP e da TROY
hp.com/go/HPandTROY

Práticas de segurança fundamentais

Controle o acesso a formulários pré-impressos

Equipe suas impressoras e multifuncionais com bloqueio de bandejas de entrada para ajudar a impedir furto de papel especial usado para impressão de cheques, receitas médicas ou outros documentos confidenciais.

Use o recolhimento de impressão ou a impressão por PIN opcional para proteger documentos sigilosos

Os usuários podem fazer a adesão para impressão por PIN ou recolhimento de impressão, reduzindo tanto a dependência de impressoras pessoais quanto os riscos de trabalhos de impressão caírem nas mãos erradas. Essas medidas de segurança também reduzem impressões não retiradas, o que pode cortar os custos e o desperdício.

Para a impressão por PIN, quando os usuários enviam trabalhos de impressão confidenciais, atribuem um PIN que deve ser inserido no dispositivo para liberar o trabalho.

O recolhimento de impressão armazena trabalhos de impressão na nuvem ou no PC do usuário. Os usuários fazem a autenticação em seu local de impressão escolhido para recolher seus trabalhos. A HP oferece duas soluções de recolhimento de impressão com base na nuvem:

- O *HP JetAdvantage Secure Print* é uma solução acessível desenvolvida para PMEs que armazena os trabalhos de impressão na nuvem ou na área de trabalho do usuário. É fácil de configurar e usar, permite que os usuários liberem trabalhos a partir de um dispositivo móvel e suporta dispositivos de vários fornecedores.¹²
- O *HP JetAdvantage Private Print* é a solução gratuita da HP com base na nuvem que oferece as vantagens do recolhimento da impressão, sem a complexidade. É simples de configurar e não precisa de servidor, instalação ou manutenção.¹³

Práticas de segurança avançadas

Exija o recolhimento de impressão para qualquer trabalho de impressão

O *HP Access Control Secure Pull Printing* ajuda a proteger as informações confidenciais, aumentar a eficiência e a segurança dos dispositivos. Essa robusta solução baseada em servidor oferece várias formas de autenticação, incluindo liberação por crachá, bem como segurança de nível corporativo e recursos de gerenciamento.

Use MICR, marcas d'água ou outros recursos para impedir cópias ou modificação

As soluções para impedimento de falsificação da HP e da TROY incluem o uso de toner de segurança que mancha o papel caso seja sujeito à adulteração química, adicionando marcas d'água de dados variáveis às páginas impressas e incorporando códigos que podem ser lidos por máquinas que controlam e fazem a auditoria de documentos individuais. As multifuncionais podem integrar recursos antifraude — incluindo assinaturas personalizadas, logotipos de empresas e fontes de segurança — a documentos confidenciais impressos como receitas médicas, certidões de nascimento ou transcrições.



Monitore e gerencie seu ambiente de impressão



Saiba mais

HP JetAdvantage Security Manager
hp.com/go/securitymanager

Soluções de monitoramento e gerenciamento da segurança podem ajudar você a identificar vulnerabilidades e estabelecer uma abordagem unificada com base em políticas para proteção de dados, redução de riscos e manutenção da conformidade.⁶ Previna brechas na proteção e ajude a evitar multas onerosas.

Práticas de segurança fundamentais

Atualize os dispositivos com o firmware/SO mais recente

Use o HP Web Jetadmin¹⁴ para fazer atualizações de firmware em todo o conjunto de dispositivos, garantindo que os dispositivos estejam atualizados com os mais recentes recursos de segurança e proteção do dispositivo.

Revise logs de eventos de segurança da impressão

Os dispositivos da HP enviam eventos/notificações da impressora para um servidor syslog para que a TI possa corrigir problemas caso necessário.

Avalie e faça a remediação de configurações do dispositivo

Gerencie as configurações de segurança básicas da impressora em todo o conjunto de dispositivos com o *HP Print Manageability Integration Kit (MIK)*, um plug-in para Microsoft® System Center Configuration Manager (SCCM). O Microsoft® SCCM é uma solução de gerenciamento amplamente utilizada para planejar, implantar, configurar e monitorar pontos de extremidade remotamente. O HP Print MIK pode detectar, avaliar e remediar as 15 principais configurações de segurança e informar os resultados.

Para um gerenciamento da segurança abrangente em todo o conjunto de dispositivos, escolha o *HP JetAdvantage Security Manager*.⁹ Essa solução ajuda você a reduzir custos e recursos para estabelecer uma política de segurança em todo o conjunto de dispositivos, automatizar a remediação de configurações do dispositivo e instalar e renovar certificados exclusivos enquanto obtém os relatórios de que você precisa para provar a conformidade.



Saiba mais

HP JetAdvantage Security Manager
hp.com/go/securitymanager

Práticas de segurança avançadas

Implante o software SIEM para detectar e documentar ameaças

Os dados de eventos de dispositivos HP FutureSmart podem ser enviados para ferramentas de detecção de incidentes como ArcSight, Splunk e SIEMonster para monitoramento em tempo real. A segurança da TI pode visualizar facilmente os pontos de extremidade das impressoras como parte do ecossistema mais amplo de TI para detectar e solucionar alertas de segurança de impressoras.

Faça a configuração automática de novos dispositivos de impressão quando são adicionados à rede

O recurso de segurança Instant-on incluído com o HP JetAdvantage Security Manager configura novos dispositivos automaticamente quando são adicionados à rede ou após uma reinicialização.

Elaboração de relatórios de auditoria da conformidade da segurança do conjunto de dispositivos de impressão

Use o HP JetAdvantage Security Manager para criar relatórios de prova de conformidade que demonstram a aplicação de políticas de segurança para impressoras e proteção dos dados do cliente.

A violação de conformidade pode prejudicar seus negócios

Pontos de extremidade protegidos ou com pouca proteção criam mais oportunidades para o cibercrime. Para ajudar a combater a crescente ameaça, órgãos governamentais de todo o mundo estão implementando rigorosas normas de segurança que requerem que as organizações protejam melhor as informações do cliente.

As organizações que não estiverem em conformidade podem enfrentar custos pesados, incluindo multas, perda de

negócios, danos à reputação e ações coletivas.

É essencial implantar dispositivos e soluções — como impressoras HP Enterprise e o HP JetAdvantage Security Manager — que possam ajudá-lo a cumprir os requisitos de conformidade e proteger suas informações empresariais contra ameaças de segurança.



Obtenha a ajuda de que você precisa

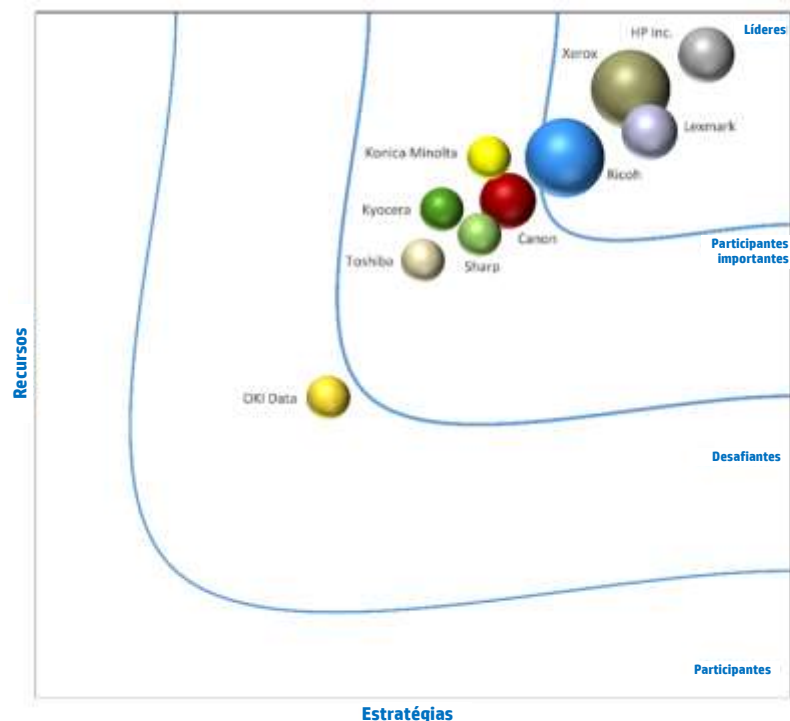
Você não tem que oferecer proteção sozinho. Uma equipe de consultores de suporte pode mostrar a você como aumentar a segurança de seus dados, dispositivos e documentos.

Colabore com especialistas em segurança da impressão para avaliar suas vulnerabilidades de segurança da impressão atuais. Podemos ajudá-lo a criar uma política de segurança da impressão abrangente baseada nas necessidades dos negócios e em práticas recomendadas e criar um plano para alcançar maior segurança em seu ambiente exclusivo.

Reconhecida como líder do setor

A HP foi denominada líder do setor no primeiro relatório da IDC MarketScape, Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment (Avaliação de fornecedores de cópias impressas para serviços e soluções mundiais de segurança de 2017). (Encontre o relatório [aqui](#).) De acordo com o relatório, “a abordagem de segurança da HP Inc. leva em consideração toda a infraestrutura de impressão e documentos, começando com o bloqueio de dispositivos e ampliando para todos os aspectos do uso de dispositivos e da proteção de conteúdos”. A imagem mostrada aqui é da Avaliação de fornecedores de 2017 da IDC.¹⁵

O modelo de análise de fornecedores IDC MarketScape é projetado para fornecer uma visão geral da adequação competitiva dos fornecedores de ICT em um determinado mercado. A metodologia de pesquisa utiliza uma rigorosa metodologia de pontuação com base em ambos os critérios qualitativos e quantitativos que resulta em uma única ilustração gráfica da posição de cada fornecedor dentro de um determinado setor. A pontuação de Recursos mede a execução de negócios, lançamento no mercado e produtos do fornecedor no curto prazo. A pontuação de Estratégias mede o alinhamento das estratégias do fornecedor com os requisitos do cliente em um período de 3 a 5 anos. A participação no mercado do fornecedor é representada pelo tamanho dos ícones.¹⁵



Primeiros passos

Entre em contato com seu representante de vendas para obter mais informações sobre recursos, soluções e serviços de segurança da HP que podem colocá-lo no caminho para uma maior proteção e tranquilidade.

Saiba mais

hp.com/go/printersecurity

¹ A afirmação “digitalização mais segura” tem base em análise feita pela HP e publicada em 2017 de recursos de segurança de impressoras concorrentes da categoria. Apenas a HP oferece uma combinação de recursos de segurança que podem monitorar para detectar e impedir um ataque automaticamente e em seguida autovalidar a integridade de software em uma reinicialização. Para obter uma lista de impressoras, acesse: hp.com/go/PrintersThatProtect. Para obter mais informações: hp.com/go/printersecurityclaims.

² InfoTrends, “Designing Hardware & Solutions” (Desenvolvendo hardware e soluções), Brendan Morse, outubro de 2016.

³ Quocirca, “Managed Print Services Landscape, 2016” (Cenários de serviços de impressão gerenciada, 2016), quocirca.com/content/managed-print-services-landscape-2016, julho de 2016.

⁴ Pesquisa feita pela Spiceworks com 309 tomadores de decisões de TI na América do Norte, EMEA e APAC, em nome da HP, em novembro de 2016.

⁵ Quocirca, “Print security: An imperative in the IoT era” (Segurança da impressão: um imperativo na era de IoT), quocirca.com/content/print-security-imperative-iot-era, janeiro de 2017.

⁶ As soluções podem não ser suportadas em todos os dispositivos da HP; as soluções podem exigir aquisições adicionais.

⁷ Os recursos de segurança integrados mais avançados da HP estão disponíveis em dispositivos HP Enterprise com firmware FutureSmart 4.5 ou posterior e estão baseados em análise feita pela HP de recursos de segurança integrados de impressoras equivalentes da concorrência publicados em 2017. Apenas a HP oferece uma combinação de recursos de segurança para verificação de integridade no nível do BIOS com recursos de autorreparo. Para obter uma lista de produtos compatíveis, acesse hp.com/go/PrintersThatProtect. Para obter mais informações, acesse hp.com/go/printersecurityclaims.

⁸ Determinados dispositivos HP LaserJet Pro e PageWide Pro incluem recursos integrados que podem detectar e interromper um ataque. Para obter mais informações, visite hp.com/go/PrintersThatProtect.

⁹ O HP JetAdvantage Security Manager deve ser adquirido separadamente. Para saber mais, acesse hp.com/go/securitymanager.

¹⁰ Uma senha adicional é obrigatória quando você envia informações para um repositório final protegido por senha.

¹¹ O HP JetAdvantage Connect funciona com os principais dispositivos móveis. Um plug-in único deve ser instalado para dispositivos com sistemas operacionais Android™, Google Chrome™ e Microsoft®. Para obter detalhes e uma lista de sistemas operacionais suportados, acesse hp.com/go/JetAdvantageConnect.

¹² HP JetAdvantage Secure Print: O recolhimento de impressão funciona com qualquer impressora ou multifuncional conectada à rede. A autenticação no dispositivo está disponível para muitos dispositivos HP LaserJet, PageWide e OfficeJet Pro e para alguns dispositivos de outros fabricantes. Alguns dispositivos podem requerer uma atualização de firmware. Conexão de Internet necessária para armazenamento em nuvem e recuperação de trabalhos de impressão. A liberação de trabalhos de impressão a partir de um dispositivo móvel requer uma conexão de rede e código QR. Para obter mais informações e uma lista de impressoras e multifuncionais suportadas, acesse hp.com/go/JetAdvantageSecurePrint.

¹³ O HP JetAdvantage Private Print está disponível sem nenhum custo e requer que a impressora esteja conectada à Internet com os serviços da web habilitados. Não disponível em todos os países. Saiba mais em hp.com/go/JetAdvantagePrivatePrint.

¹⁴ O HP Web Jetadmin está disponível para download gratuito em hp.com/go/webjetadmin.

¹⁵ Com base na análise da IDC de fornecedores de cópia impressa e na opinião relacionada à liderança da HP: “A HP possui uma vantagem com esses fortes recursos e serviços de TI... e facilitando uma estratégia de segurança abrangente e integrada em toda a infraestrutura de TI.” FONTE: [IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment \(Avaliação de fornecedores de cópias impressas para serviços e soluções mundiais de segurança de 2017\)](#) (Cópias impressas para serviços e soluções mundiais de segurança de 2017), por Allison Correia e Robert Palmer, outubro de 2017, Documento da IDC nº US41988517.

Inscreva-se para obter atualizações

hp.com/go/getupdated



Compartilhe com colegas

© Copyright 2014-2018 HP Development Company, L.P. As informações aqui contidas estão sujeitas a alterações sem aviso. As únicas garantias para produtos e serviços HP estão definidas nas declarações de garantia expressa que acompanham tais produtos e serviços. Nenhuma parte deste documento deve ser interpretada como garantia adicional. A HP não se responsabiliza por omissões, erros técnicos ou erros editoriais contidos neste documento.

Android e Google Chrome são marcas comerciais registradas da Google Inc. Microsoft é marca do grupo de empresas Microsoft registrada nos Estados Unidos.

4AA3-1295PTL, maio de 2018, Rev. 11

