Certifique-se de que a sua impressora e a sua rede estão seguras.

Comparação entre Ricoh e HP

As impressoras e os dispositivos multifuncionais de hoje têm as mesmas vulnerabilidades que outros terminais na rede. Eles contêm informações e dados potencialmente sensíveis, tornando-se os principais alvos para uma violação de segurança.

É por isso que é fundamental considerar como a sua tecnologia de impressão trata a questão da segurança para reduzir riscos e proteger os seus dispositivos, documentos, dados e negócios.

A Ricoh afirma que fornece uma variedade de recursos de segurança para minimizar os riscos. Dada a importância da segurança no local de trabalho, vale a pena verificar a forma como as medidas de segurança da Ricoh se comparam com as da HP.

Declarações de segurança da Ricoh

A Ricoh destaca três alegações para a segurança dos seus dispositivos:

- **Detección de intrusos**— Para a Ricoh, usuários individuais podem ser identificados pela copiadora multifuncional. As funções de autenticação de usuários da Ricoh são baseadas em códigos de usuário de até oito dígitos ou em combinações de nomes de usuário e senhas. As copiadoras multifuncionais Ricoh permitem a autenticação do usuário por meio de um sistema de autenticação existente.[1]
- **Detecção de dispositivo**— para evitar que o firmware autêntico seja substituído pelo firmware não autorizado, a Ricoh usa assinaturas eletrônicas para validar o firmware. Além disso, um Trusted Platform Module (TPM)–um módulo de segurança de hardware inviolável–valida a autenticidade do firmware da multifuncional e dos aplicativos instalados antes de permitir que a multifuncional funcione. Essas tecnologias garantem a segurança do dispositivo.
- **Proteção de documentos e dados**— para aumentar a segurança contra uso não autorizado, los arquivos PDF podem ser protegidos por criptografia e senha. Ao usar a função de impressão bloqueada, uma senha é especificada ao enviar o documento, e essa senha deve ser inserida na copiadora multifuncional antes que ele possa ser impresso. A função de guarda de cópia imprime/copia documentos com padrões invisíveis especiais integrados ao fundo. Agendas de endereços, informações de autenticação e documentos são criptografados ao serem armazenados na multifuncional.

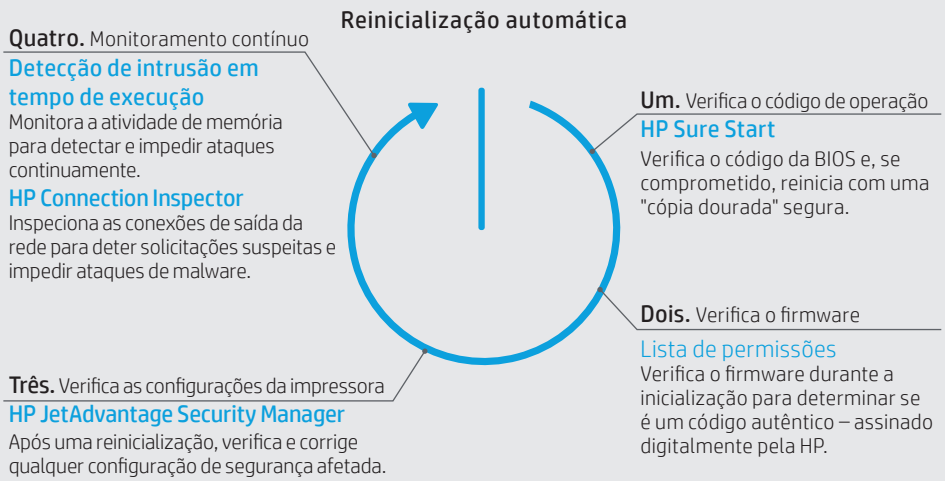
Apesar dessas alegações, a Ricoh ainda fica aquém das expectativas quando comparada com a oferta de segurança de ponta a ponta da HP com o HP Security Manager e os recursos de segurança integrados prontos para uso.

Segurança de impressão HP com autorreparação

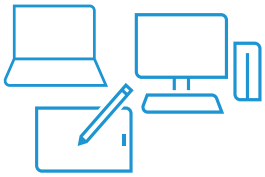
Como funciona?
Os recursos de segurança integrados abordam quatro etapas principais no ciclo de um dispositivo HP.

Somente dispositivos HP Enterprise podem ser reiniciados e reparados automaticamente se forem atacados.

O HP JetAdvantage Security Manager conclui o ciclo de teste.



Nova segurança integrada: HP Connection Inspector	**O mais recente diferenciador de segurança da HP impede que malwares se conectem com servidores.** • Monitora conexões de rede de saída (pacotes) • Aprende o que é normal, depois inspeciona e interrompe os pacotes suspeitos	• Aciona uma reinicialização para iniciar procedimentos de autorreparação sem necessidade de a TI intervir • Cria eventos de segurança que podem ser integrados a uma ferramenta SIEM como o Splunk • Nenhum concorrente oferece esses recursos

	Ricoh	HP
 Detecção de dispositivo/criação de lista branca	• As Soluções de Segurança da Ricoh são descritas como uma abordagem multicamada que ajuda a fechar a porta para aqueles que desejam explorar vulnerabilidades. • Concentra-se na segurança padrão do dispositivo legado, como segurança de portas, autenticação de usuários, protocolos de rede, sobrescrita de dados e criptografia. • Não faz nenhuma alegação quanto à varredura de memória para ataques injetados. • Não fornece o Secure Boot para proteger o código da BIOS em seus dispositivos.	• Supera a oferta da Ricoh Security com capacidades e proteções abrangentes, líderes do setor, incluindo BIOS autorrecuperável, integridade do código de firmware e Detecção de Intrusão. • Lidera a indústria com a Detecção de Intrusão do dispositivo que monitora continuamente a memória em busca de malwares mal–intencionados. • A Proposição de Valor FutureSmart da HP fornece proteção de investimento de dispositivo e tem fornecido Detecção de Intrusão e lista branca como atualização de firmware nos Dispositivos FutureSmart 3.7 desde 2012.
 Proteção de documentos e dados	• Considera que a educação do usuário final é importante para reduzir o risco de violação de dados; entretanto, não fornece o nível de tecnologia para salvaguardar quando esse tipo de ameaça está dentro de um firewall e se enraíza em dispositivos. • Concentra-se em requisitos de segurança de documentos de dados padrão que estão em pé de igualdade com a indústria, mas ficam aquém da segurança de impressão da HP. • Reconhece que o seu conjunto completo de recursos de segurança não fornece as proteções necessárias para eliminar completamente os riscos causados por erros humanos.	• Oferece soluções superiores de monitoramento e gerenciamento de segurança que ajudam a identificar vulnerabilidades e estabelecem uma abordagem unificada e baseada em políticas para proteção de dados, fortalecimento de conformidade e redução de risco, tudo isso economizando significativamente tempo e recursos. • Supera os requisitos de segurança da Ricoh na segurança de ponta a ponta, incluindo monitoramento e avaliação de segurança baseados em políticas, segurança Instant–On, integração SIEM no dispositivo, inclusão da lista de verificação do U.S. NIST e pesquisa por palavra-chave DLP.
 Software de segurança	• Não possui um processo de inicialização segura que protege a BIOS. • Oferece validação de firmware apenas para dispositivos com um chip TPM. • Não oferece proteção contra injeção de memória ou monitoramento para comportamento anômalo no tempo de execução do código. • Faltam soluções robustas e centradas na segurança que garantam a conformidade de segurança do dispositivo com políticas definidas. • Não fornece detecção e análise de ameaças em tempo real ou integração com ferramentas SIEM, como ArcSight ou Splunk, para fornecer informações sobre possíveis ataques. • A oferta da ferramenta de Gerenciamento de Frota não possui: 1. Uma política de segurança básica que se alinha com os padrões do NIST para aplicar a todos os dispositivos. 2. Um processo robusto de criação de políticas para ajustar as políticas de segurança às necessidades específicas do cliente. 3. Tecnologia Instant-On que garante que as políticas sejam atribuídas à medida que os dispositivos fiquem on-line. 4. Reparação automática de até 250 configurações de segurança que não estejam em conformidade com as políticas definidas.	• Oferece o Gerenciador de Segurança HP Jet Advantage, um gerenciador de conformidade inédito no setor, com base em políticas, premiado pelo BLI, que é vendido pela HP, e foi desenvolvido e mantido pela equipe da HP. • A solução pode avaliar, relatar e corrigir até 250 configurações, e é projetada para funcionar com 115 modelos de dispositivos HP. • Possui tecnologia Instant–On que avalia automaticamente a conformidade de dispositivos HP compatíveis.

Perguntas frequentes sobre segurança de impressão

P1: Minha empresa utiliza firewalls para proteger minha rede; por que precisamos de segurança em nossas impressoras?

R: Você usa proteção contra malware/vírus em seus PCs e laptops? Além disso, você precisa proteger dispositivos de outros dispositivos em sua rede. Se um PC for infectado com malware por meio de phishing por e-mail, não há muito que um firewall possa fazer para proteger os sistemas contra isso.

P2: Dada a complexidade da nossa rede e os dados disponíveis em nossos servidores e outros terminais, por que os hackers mirariam nas impressoras?

R1: Os hackers não necessariamente atacam os sistemas de forma direta, eles procuram o ponto mais fraco como uma leoa caçando a gazela mais lenta do rebanho. As impressoras muitas vezes são ignoradas nas políticas de segurança, portanto, elas podem ser a gazela lenta. Uma vez que eles estão na sua rede, eles podem acessar outros recursos, por isso é tão importante ter a segurança do dispositivo de impressão integrada de fábrica.

R2: As impressoras geralmente processam e até armazenam dados altamente sensíveis, podendo ser alvos importantes em uma violação de dados.

P3: O que acontece se um hacker tentar instalar malware na minha impressora?

R: As impressoras HP fornecem proteção contra a instalação de programas maliciosos, incluindo o malware. Nossa tecnologia de criação de lista branca garante que somente o código autêntico da HP seja instalado no sistema, incluindo o firmware (o sistema operacional de um dispositivo de impressão) e quaisquer outras soluções.

P4: Realmente precisamos de toda essa segurança para as nossas impressoras?

R1: As impressoras realmente devem ser tratadas como cidadãos iguais em sua rede. Elas são um alvo tão provável quanto qualquer outro terminal e lidam com informações altamente sensíveis com frequência.

R2: A segurança requer diligência constante– basta uma brecha na sua armadura para perpetrar uma violação de dados que poderia custar a uma empresa milhões de dólares para se recuperar.

P5: Qual é o diferencial-chave de segurança da HP em comparação com o da Ricoh?

R: Nossa capacidade de recuperação automática de potenciais riscos de segurança, seja no dispositivo individual com autorrecuperação ou na frota por meio do Gerenciador de Segurança HP Jet Advantage.

Ferramentas de avaliação

O quanto as suas impressoras estão seguras? Avalie a segurança do seu ambiente de impressão com estas úteis ferramentas on-line da HP:

- **Pesquisa da HP Secure Print Analysis—** autoavaliação on-line para determinar se você está seguindo as melhores práticas em segurança de impressão: hp.com/go/SPA
- **HP Quick Assess—** avaliação técnica gratuita das 13 principais configurações em até 20 impressoras HP (a consulta por telefone está disponível nos EUA): hp.com/go/quickassess

[1] Fonte: https://www.ricoh.com/security/products/mfp/function/

4AA7-1567PTL, Rev 1, Julho 2018