Proteja a sua impressora. Proteja o seu negócio.

Comparando a Lexmark e a HP

O aumento no uso de dispositivos na rede das empresas continua a fazer da segurança um desafio e uma preocupação crescentes – incluindo as impressoras e multifuncionais, que podem ter as mesmas vulnerabilidades que qualquer outro dispositivo final na rede.

Os fabricantes de impressoras estão lidando com esses problemas de segurança com uma variedade de recursos, tecnologias e soluções que ajudam a minimizar os riscos.

Porém, no caso da segurança, nem todas as impressoras são iguais. Ao conectar uma nova impressora ou multifuncional à sua rede, é muito importante que você esteja ciente dos recursos de segurança que ela apresenta. E, embora tanto a HP quanto a Lexmark sustentem que as suas impressoras e multifuncionais oferecem medidas de segurança adequadas, uma análise detalhada revela algumas discrepâncias.

Declarações de segurança da Lexmark

"Gama completa de segurança" é o termo usado pela Lexmark ao descrever a sua abordagem abrangente para proteger um ambiente corporativo. Ela divide-se em sete pontos-chave para a segurança do produto:

- **Acesso seguro**
- **Rede**
- **Segurança do documento**
- **Gerenciamento remoto seguro**
- **Soluções de segurança**
- **Segurança do disco rígido**
- **Padrões e certificações**

Como a Lexmark diz entender a realidade multifacetada das ameaças à segurança, ela responde com uma "abordagem holística e sistemática que envolve o dispositivo, a frota de impressoras e toda a infraestrutura de rede". Essa é uma abordagem normal para a segurança ao comparar os seus recursos de segurança com uma de suas ofertas recentemente comercializadas.

Embora a Lexmark também afirme que a segurança "está integrada em cada produto, com recursos de segurança padrão adequados ao uso pretendido de cada dispositivo e opções disponíveis para atender a requisitos especiais", comparado a outras soluções de impressão, não há inovação ou diferenciação em relação aos padrões da indústria.

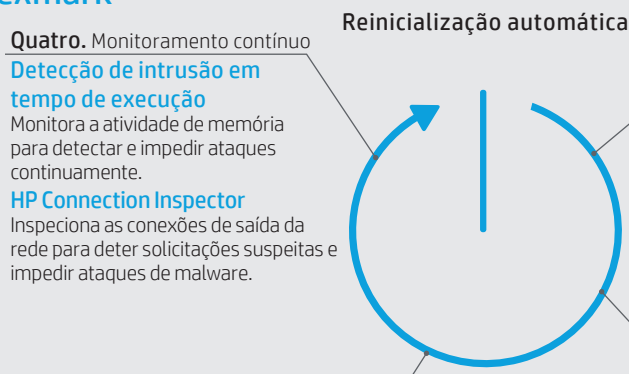
Segurança de impressão HP com autorreparação – HP versus Lexmark

Descobrindo as vantagens da HP ao comparar a Lexmark com as 4 principais etapas incluídas no ciclo de operação da multifuncional HP.

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.



Recursos de segurança – uma comparação lado a lado

	Lexmark	HP
 **Detecção de dispositivos/lista de permissões**	• Não declara uma revisão da memória em busca de ataques de injeção. • Só é possível detectar o firmware malicioso no dispositivo (também conhecido como lista de permissões). • Tecnologia de inicialização segura valida a integridade da BIOS na inicialização. • Firmware criptografado e assinado garante que apenas o firmware criado pelos sistemas da Lexmark possam ser instalados nos dispositivos (também conhecido como lista de permissões). • Ao detectar um firmware não original, os usuários receberão uma notificação. A verificação contínua garante que o firmware não tenha sido adulterado durante a operação. • Se o firmware estiver corrompido, os dispositivos deixam de imprimir e somente uma intervenção física pode corrigi-lo.	• Com o HP SureStart, a integridade do código da BIOS é validada. Se a BIOS estiver comprometida, a multifuncional HP se reinicia e carrega uma "cópia dourada" segura assinada digitalmente pela HP. A impressão não é interrompida. • Suporta a detecção de intrusões no dispositivo, que monitora continuamente a memória em busca de malware malicioso.
 **Proteção de documentos e dados**	• Protege os dados de impressão contra pessoas não autorizadas usando um Modelo de Remoção de Impressão Segura padronizado. • Indica que as informações digitalizadas estão protegidas contra usuários não autorizados, mas sem especificar como. • Pode solicitar que os clientes usem fornecedores de MPS terceirizados para executar tarefas de gerenciamento remotamente.	• Atende ao padrão líder da indústria para armazenamento de dados e é criptografado usando o mais alto nível de criptografia (AES-256). • Sua capacidade de sobrescrever atende aos padrões do Instituto Nacional de Padrões e Tecnologia (NIST) e do Departamento de Defesa dos Estados Unidos (DoD). • Oferece várias soluções de impressão "pull": baseada em nuvem, no local e híbrida, para ajudar as organizações a alcançar suas necessidades exclusivas de impressão confidencial e de redução de custos. • Ajuda os usuários a protegerem documentos confidenciais contra analisadores de pacotes de dados com criptografia completa que protege as informações mais valiosas da empresa – tanto em trânsito quanto estáticas. • Oferece proteção adicional com total segurança da inicialização ao encerramento com autorrecuperação para minimizar a interrupção dos negócios – apoiada por fortes soluções comerciais.
 **Software de segurança**	• A política de segurança do MarkVision Enterprise (MVE) da Lexmark é manual e específica do dispositivo. A configuração inicial pode ser árdua e, se o dispositivo for alterado e um novo modelo for colocado na rede, o processo manual poderá ter que ser repetido. • Vários dispositivos e seus recursos determinam configurações individuais de segurança em toda a empresa. • O MVE não possui tecnologia instantânea e uma política integrada baseada nos padrões NIST.	• A proteção de segurança instantânea avalia automaticamente a conformidade de dispositivos compatíveis com a HP. • A alteração do dispositivo não afeta os esforços de gerenciamento das políticas da empresa. • O HP JetAdvantage Security Manager –gerenciador de políticas de conformidade, o primeiro do setor, impulsionado pelas mesmas políticas, vencedor do Laboratório Internacional do Comprador (BLI) – pode configurar até 250 recursos de segurança. Em comparação, o Lexmark MVE configura apenas 115.

Opinião da HP sobre a análise BLI

Recentemente, a BLI conduziu uma análise dos recursos de segurança das ofertas de impressão, software e serviços pelos principais fabricantes de impressoras. Por meio desta análise, a BLI concluiu que vários fabricantes, incluindo a Lexmark e a HP, se destacaram por seus esforços de segurança em oito categorias. Cada um desses fabricantes recebeu o prêmio BLI Pacetter para segurança de impressão.

Jamie Bsales, diretor de análise de software da BLI na Keypoint Intelligence, diz: "A segurança do dispositivo da Lexmark é incomparável e inclui recursos avançados, como verificação da integridade do firmware na inicialização, verificação da integridade da BIOS, detecção de intrusões, relatórios e muito mais. Foi facilmente colocada entre os melhores dos 13 Fabricantes de Equipamentos Originais (OEMs) incluídos no nosso estudo".

No entanto, de acordo com a pesquisa da HP, acreditamos que a análise deve ser mais rigorosa e aplicada à importância dos recursos com base no seu impacto no nível de segurança, facilidade de implementação e manutenção. Um exame mais detalhado dos dados revela diferenças significativas entre o nível de segurança e os recursos oferecidos pela Lexmark e pela HP.

	Lexmark	HP
Verificação de integridade da BIOS	• O dispositivo será desligado se for detectada uma BIOS corrompida	• O dispositivo será desligado se for detectada uma BIOS corrompida • O dispositivo se autorrecuperará e reiniciará em bom estado sem intervenção da TI
Detecção de intrusão	• Os eventos de segurança podem ser enviados para um servidor remoto (por exemplo, sistema de detecção de intrusão)	• Os eventos de segurança podem ser enviados para um servidor remoto (por exemplo, sistema de detecção de intrusão) • Eventos de segurança são configurados para serem utilizados por uma ferramenta SIEM (Splunk, Arcsight, SIEMonster) • Os eventos de segurança são interrompidos em tempo real por uma tecnologia integrada no dispositivo que varre a memória de tempo de execução. Se um malware for detectado, o dispositivo limpa a memória e reinicia em bom estado
Cumprimento de políticas	• As configurações de segurança podem ser programadas com um horário	• As configurações de segurança podem ser programadas com um horário • A segurança instantânea garante que um dispositivo receba automaticamente as configurações necessárias quando é adicionado à rede • As políticas de referência são facilmente estabelecidas usando uma política integrada baseada nas melhores práticas do NIST

Ferramentas de avaliação

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

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

© Copyright 2018 HP Development Company, L.P. As informações aqui contidas estão sujeitas a alterações sem aviso prévio. As únicas garantias de produtos e serviços HP estão definidas nas declarações de garantia expressa que os acompanham. Nada aqui contido deve ser interpretado como constituindo garantia adicional. A HP não é responsável por omissões nem erros técnicos ou editoriais contidos neste documento.

4AA7-2062PTL, Rev 1, Julho 2018