Documento técnico

Cumpra os requisitos de conformidade relativos à segurança da rede e dos dados

Recomendações para a aplicação de controlos de segurança ao parque de impressão

Índice

Clique aqui para ver a versão mais recente deste documento

O incumprimento dos requisitos de conformidade pode prejudicar a sua empresa

Além de multas avultadas e processos judiciais, uma falha de segurança pode gerar perda de receitas e provocar danos à sua reputação. Ao criar o seu plano de segurança, lembre-se de que a sua rede é tão segura como o seu elo mais fraco. Os dispositivos de impressão e de processamento de imagens apresentam muitas das vulnerabilidades de segurança dos computadores. É essencial implementar dispositivos e soluções que o ajudem a cumprir os requisitos de conformidade e a proteger as suas informações empresariais das ameaças de segurança.

Quais são os riscos?

A não conformidade regulamentar e legal acarreta custos elevados para as organizações mundiais, que incluem multas, perda de negócios, danos à reputação e processos judiciais coletivos.

Os terminais não protegidos ou indevidamente protegidos facilitam a prática do cibercrime. As organizações inquiridas pela Ponemon num estudo recente sofreram, em 2016, uma média de 2 ataques por semana, o que representa um aumento de 23% em relação ao ano anterior, resultando num prejuízo médio anual de 9,5 milhões de dólares destinado ao combate do cibercrime.[1] Só no último ano, mais de 4 mil milhões de registos de dados foram comprometidos em todo o mundo, o que representa um aumento de 400% em relação aos dois anos anteriores.[2]

Apesar de muitos departamentos de TI aplicarem medidas rigorosas de segurança aos computadores e à rede, os dispositivos de impressão e de processamento de imagens são muitas vezes negligenciados. No entanto, as impressoras podem permitir o acesso não autorizado à sua rede, pelo que protegê-las é igualmente importante. Do total das violações de dados significativas comunicadas pelos gestores de TI, 26% envolveram impressoras.[3]

Para ajudar a combater esta ameaça crescente, organismos governamentais de todo o mundo estão a implementar novos regulamentos de segurança que exigem que as empresas protejam melhor as informações dos seus clientes. O novo Regulamento Geral sobre a Proteção de Dados (GDPR) da UE, por exemplo, é um regulamento-chave que entra em vigor em 2018. O GDPR aumenta os requisitos em matéria de proteção de dados exigidos às empresas. Por isso, deverá certificar-se de que todos os dispositivos na sua rede, desde computadores a impressoras, estão devidamente protegidos. O novo regulamento não afeta apenas os países da UE – as empresas mundiais devem igualmente cumpri-lo caso recolham e utilizem dados de residentes na UE. As organizações terão de monitorizar e avaliar todos os dispositivos por forma a detetar e notificar falhas de segurança no prazo de 72 horas após terem tido conhecimento do ocorrido. Se as auditorias de conformidade detetarem que as falhas não foram monitorizadas ou notificadas, as empresas ficarão sujeitas a multas que ascendem a 20 milhões de euros ou a 4% do volume de negócios anual da empresa.

Utilize controlos de segurança de base para melhorar a conformidade

É difícil manter-se a par dos requisitos de conformidade e dos regulamentos do setor. Felizmente, o Center for Internet Security (CIS) criou um conjunto de controlos de segurança de base para simplificar as recomendações em termos de cibersegurança. Os Critical Security Controls (Controlos Críticos de Segurança) do CIS consistem em 20 ações específicas que ajudam a impedir ataques informáticos. (Para saber mais informações, consulte https://www.cisecurity.org/critical-controls.cfm.) Os Controlos estão alinhados com muitos outros regulamentos do setor, como o PCI-DSS (Payment Card Industry Data Security Standard), ISO 27001, recomendações do US-CERT (The United States Computer Emergency Readiness Team), HIPAA (Health Insurance Portability and Accountability Act), FFIEC (Federal Financial Institutions Examination Council) e NIST (National Institute of Standards and Technology). A finalidade dos Controlos não é substituir os outros quadros regulamentares, embora sejam utilizados frequentemente pelas empresas para facilitar a respetiva aplicação.

Os Critical Security Controls do CIS dão prioridade a um pequeno número de ações que apresentam resultados significativos. Abordam os padrões de ataques mais frequentes, indicados nos principais relatórios de ameaças. A sua criação contou com a participação de um grande número de especialistas do setor, incluindo especialistas em análise forense e organizações de resposta a incidentes. Além disso, os Controlos são constantemente atualizados com base na evolução das ameaças e ataques.

Utilize os Critical Security Controls do CIS para organizar o seu plano de segurança e cumprir os requisitos de conformidade. O presente documento técnico apresenta sugestões de ações para cada um dos 20 Controlos por forma a ajudar a proteger os seus dispositivos de impressão, dados e documentos, no âmbito do seu plano de segurança mais abrangente. Os Controlos 4, 6, 8, 12, 13 e 15 abordam especificamente a proteção de dados e atividades de monitorização relacionadas com os novos requisitos do GDPR.

Critical Security Controls do CIS e ações recomendadas

CSC 1: Inventário de dispositivos autorizados e não autorizados

Controlo – Efetue, de forma ativa, a gestão (inventário, monitorização e correção) de todos os dispositivos de hardware na rede, para que apenas seja concedido acesso aos dispositivos autorizados e sejam detetados os dispositivos não autorizados e não geridos, bem como impedido o respetivo acesso.

Recomendação – Certifique-se de que todos os dispositivos de impressão na sua rede estão identificados e são geridos de forma ativa a fim de garantir a conformidade com a política de segurança. Uma ferramenta eficaz de gestão de segurança de impressão permite detetar e tornar visíveis todos os dispositivos ligados à rede e aos computadores.

CSC 2: Inventário de software autorizado e não autorizado

Controlo – Efetue, de forma ativa, a gestão (inventário, monitorização e correção) de todo o software na rede, para que apenas o software autorizado seja instalado e executado e seja detetado o software não autorizado e não gerido, bem como impedida a respetiva instalação ou execução.

Recomendação – Certifique-se de que todo o firmware e soluções carregados nos dispositivos de impressão e de processamento de imagens estão atualizados e assinados e de que a respetiva autenticidade se encontra validada. Escolha dispositivos de impressão com proteção do BIOS e firmware incorporados para assegurar que apenas é carregado código autêntico. As soluções de gestão de parques de impressão permitem implementar atualizações pró-ativas de firmware em todo o parque. O software (baseado em servidor e baseado em cliente) deverá estar assinado, e a respetiva autenticidade deverá estar validada.

CSC 3: Configurações de segurança para hardware e software em dispositivos móveis, computadores portáteis, estações de trabalho e servidores

Controlo – Estabeleça, implemente e efetua, de forma ativa, a gestão (monitorização, notificação e correção) das configurações de segurança de computadores portáteis, servidores e estações de trabalho através de uma gestão rigorosa das configurações e do processo de controlo de alterações por forma a impedir que os atacantes explorem definições e serviços vulneráveis.

Recomendação – À semelhança dos outros terminais da rede, as impressoras devem estar configuradas de forma segura. Deverá criar e implementar uma política de segurança em todos os seus dispositivos de impressão e remediar, de forma ativa, quaisquer desvios em relação à política. As listas de verificação de segurança (como o NIST) ou os serviços de consultoria em matéria de segurança podem ajudá-lo a criar e implementar uma política de segurança de impressão abrangente. Uma ferramenta eficaz de gestão de segurança de impressão permite automatizar a criação de políticas, a implementação, a avaliação e a remediação de definições dos dispositivos em todo o parque de impressão. As impressoras multifunções (MFP) de nível empresarial (Enterprise) têm mais de 250 definições de segurança, pelo que a automatização deste processo permite uma poupança de tempo significativa.

CSC 4: Avaliação e remediação contínua de vulnerabilidades

Controlo – Recolha dados, avalie-os e adote medidas, de forma contínua, ao tirar partido das novas informações obtidas para identificar e corrigir vulnerabilidades, bem como para minimizar as oportunidades de os atacantes executarem ataques.

Recomendação – As soluções SIEM (Security Information and Event Management), como o ArcSight, Splunk ou SIEMonster, permitem monitorizar a atividade na sua rede e notificar os administradores no momento de ocorrência dos incidentes. A monitorização dos dispositivos de impressão é tão importante como a monitorização dos computadores – certifique-se de que as suas impressoras enviam mensagens do syslog para a sua ferramenta SIEM.

Escolha dispositivos de impressão com funcionalidades que permitam detetar ataques em tempo real e recuperar automaticamente, maximizando o tempo de atividade e minimizando as intervenções dos profissionais de TI.

Para reduzir a vulnerabilidade, utilize uma ferramenta de gestão da segurança do parque que permita identificar as novas impressoras e implementar automaticamente as definições da política de segurança empresarial assim que os dispositivos forem ligados à rede. Agende avaliações/remediações regulares para manter todo o parque de impressão em conformidade com a política.

CSC 5: Utilização controlada de privilégios administrativos

Controlo – Monitorize, controle, previna e corrija a utilização, a atribuição e a configuração de privilégios administrativos em computadores, redes e aplicações.

Recomendação – Escolha dispositivos e soluções de impressão que permitam autenticar os utilizadores e controlar o acesso à funcionalidade com base na função da pessoa, por forma a que apenas os funcionários de TI e outro pessoal autorizado possam instalar e configurar as definições dos dispositivos. Utilize software de gestão de segurança do parque para implementar as palavras-passe de administrador em todo o parque.

CSC 6: Manutenção, monitorização e análise de registos de auditoria

Controlo – Recolha, efetua a gestão e analise registos de auditoria de eventos que permitam ajudar a detetar e compreender um ataque e recuperar do mesmo.

Recomendação – Os dispositivos de impressão deverão permitir gerar mensagens de incidentes do syslog, para que a sua equipa de segurança possa analisar regularmente os registos de auditoria por forma a detetar e resolver os problemas. Escolha dispositivos que permitam enviar este tipo de mensagens para as soluções de gestão de segurança do parque e para as ferramentas SIEM com vista à monitorização em tempo real e à geração de relatórios para efeitos de auditoria ou outros requisitos de conformidade.

CSC 7: Proteções do e-mail e do browser

Controlo – Reduza o risco de ataques e as oportunidades de os atacantes manipularem o comportamento humano através da respetiva interação com browsers e sistemas de e-mail.

Recomendação – As impressoras multifunções estão frequentemente ligadas à internet, por exemplo, para enviarem digitalizações através de e-mail. Certifique-se de que as digitalizações enviadas por e-mail são encriptadas de modo a proteger os dados sensíveis. Implemente dispositivos e soluções que permitam autenticar os utilizadores e controlar o acesso aos recursos no dispositivo (como servidores web ou funcionalidade de e-mail) com base na função da pessoa. Crie uma lista de "Websites fidedignos" para as suas impressoras multifunções e efetue a gestão adequada da mesma por forma a assegurar que o dispositivo acede apenas a websites fidedignos. Integre vários métodos de autenticação (como PIN/PIC, LDAP ou autenticação Kerberos) com Active Directory para simplificar a gestão e aumentar a segurança. Os dispositivos de impressão ligados à rede deverão ter proteção incorporada contra malware e vírus, e o firmware das impressoras deverá ser atualizado regularmente com as proteções mais recentes.

CSC 8: Defesas contra malware

Controlo – Controle a instalação, a propagação e a execução de códigos maliciosos em vários pontos da empresa, ao mesmo tempo que otimiza a utilização da automatização para permitir a rápida atualização das defesas, a recolha de dados e a execução de ações de correção.

Recomendação – Escolha dispositivos de impressão que permitam carregar apenas código verificado e assinado e que tenham funcionalidades antimalware que permitam a monitorização ativa da memória do dispositivo e o reinício em caso de ataque. As ferramentas de gestão de segurança de impressão permitem avaliar e remediar automaticamente as definições dos dispositivos em todo o parque. Deverá igualmente certificar-se de que todas soluções de software de impressão estão assinadas e de que a respetiva autenticidade é validada.

CSC 9: Limitação e controlo de portas de rede, protocolos e serviços

Controlo – Efetue a gestão (monitorização, controlo e correção) da utilização operacional de portas, protocolos e serviços em dispositivos ligados à rede, por forma a minimizar as vulnerabilidades que os atacantes possam explorar.

Recomendação – Se não estiverem já desativados por defeito, desative todas as portas não utilizadas e protocolos não seguros (como o FTP ou Telnet) que os atacantes poderão utilizar para aceder ao dispositivo. Poupe tempo precioso aos profissionais de TI e reduza os riscos ao implementar uma ferramenta de gestão de segurança de impressão para manter automaticamente as definições dos dispositivos em conformidade em todo o parque. Utilize palavras-passe de administrador, autenticação e controlos de acesso com base nas funções para limitar o acesso às funcionalidades e definições do dispositivo.

CSC 10: Capacidade de recuperação de dados

Controlo – Faça cópias de segurança das informações importantes através de uma metodologia comprovada que permite recuperar dados com rapidez.

Recomendação – Este Controlo não se aplica atualmente a impressoras.

CSC 11: Configurações de segurança para dispositivos de rede como firewalls, routers e comutadores

Controlo – Estabeleça, implemente e efetua, de forma ativa, a gestão (monitorização, notificação e correção) das configurações de segurança dos dispositivos de infraestrutura de rede através de uma gestão rigorosa das configurações e do processo de controlo de alterações de modo a impedir que os atacantes explorem definições e serviços vulneráveis.

Recomendação – As impressoras fazem parte da rede e, tal como outros terminais, deverão ser configuradas de forma segura. As ferramentas de gestão de segurança de impressão permitem automatizar a implementação, a avaliação e a remediação das definições dos dispositivos em todo o parque, de modo a manter a rede segura e poupar tempo precioso aos profissionais de TI.

CSC 12: Defesa de perímetros

Controlo – Detete, previna e corrija o fluxo de informação que é transferido entre redes de diferentes níveis de confiança, com ênfase nos dados que apresentam riscos para a segurança.

Recomendação – Utilize a encriptação para proteger os dados em trânsito (trabalhos de impressão ou digitalização em trânsito da impressora ou para a impressora) e os dados inativos no disco rígido do dispositivo. Escolha dispositivos e soluções de impressão que permitam autenticar os utilizadores e controlar o acesso à utilização com base na função da pessoa, por forma a que, por exemplo, apenas os utilizadores autorizados possam enviar trabalhos de digitalização por e-mail ou enviar ficheiros para destinos na nuvem. Configure os websites fidedignos na lista de Websites fidedignos" para impedir o acesso a websites maliciosos. As soluções de impressão móvel segura permitem aos utilizadores imprimir facilmente a partir dos respetivos dispositivos móveis, mantendo ao mesmo tempo a rede protegida.

CSC 13: Proteção de dados

Controlo – Impeça a "exfiltração" de dados, mitigue os efeitos de dados exfiltrados e garanta a privacidade e a integridade das informações sensíveis.

Recomendação – Utilize a encriptação para proteger os dados em trânsito (trabalhos de impressão ou digitalização em trânsito da impressora ou para a impressora) e os dados inativos no disco rígido do dispositivo. Implemente soluções de impressão *pull-print* para evitar que documentos sensíveis sejam esquecidos em tabuleiros de saída. Certifique-se de que os dados armazenados em discos rígidos são apagados de forma segura antes de devolver dispositivos alugados ou de os reciclar no fim de vida.

CSC 14: Acesso controlado com base no princípio da necessidade de informação

Controlo – Monitorize, controle, previna, corrija e proteja o acesso a componentes críticos (por exemplo, informações, recursos e sistemas) de acordo com a definição formal das pessoas, computadores e aplicações que têm o direito de aceder a estes componentes críticos com base numa classificação aprovada.

Recomendação – Escolha dispositivos e soluções de impressão que permitam autenticar os utilizadores e controlar o acesso às funcionalidades com base na função da pessoa. Integre vários métodos de autenticação (como PIN/PIC, LDAP ou autenticação Kerberos) com Active Directory para simplificar a gestão e aumentar a segurança. As soluções de impressão *pull-print* ajudam a impedir que documentos sensíveis caiam nas mãos erradas.

CSC 15: Controlo do acesso sem fios

Controlo – Monitorize, controle, previna e corrija a utilização segura de redes locais sem fios (WLAN), pontos de acesso e sistemas cliente sem fios.

Recomendação – Uma ferramenta eficaz de gestão de segurança de impressão permite automatizar a implementação, a avaliação e a remediação das definições dos dispositivos, incluindo definições sem fios, em todo o parque. Utilize as soluções de controlo de acesso para restringir o acesso a funcionalidades do dispositivo, como a digitalização para e-mail, com base na função do utilizador. As soluções de impressão móvel segura permitem aos utilizadores imprimir facilmente a partir dos respetivos dispositivos móveis, mantendo ao mesmo tempo a rede protegida. Por exemplo, os dispositivos que suportam impressão sem fios ponto a ponto permitem aos utilizadores de dispositivos móveis imprimir diretamente através de um sinal sem fios dedicado da própria impressora – sem aceder à rede ou ao serviço sem fios da empresa.

CSC 16: Monitorização e controlo de contas

Controlo – Efetue, de forma ativa, a gestão do ciclo de vida das contas do sistema e das aplicações (criação, utilização, dormência e eliminação) para minimizar as oportunidades de os atacantes tirarem partido destas.

Recomendação – Escolha dispositivos e soluções de impressão que permitam autenticar os utilizadores e controlar o acesso às funcionalidades com base na função da pessoa. Integre a autenticação com Active Directory para uma gestão centralizada e segurança reforçada. Reveja regularmente as contas de utilizadores, desative as que não forem necessárias, e utilize soluções de monitorização para monitorizar a utilização das contas. Encripte os nomes de utilizador e as credenciais de autenticação das contas, quer se trate de dados em trânsito ou de dados inativos armazenados no dispositivo. Os consultores de segurança podem ajudá-lo a elaborar um plano de segurança de impressão abrangente por forma a minimizar os riscos e, em alguns casos, podem ajudá-lo a gerir a segurança, inclusive a monitorização e o controlo das contas.

CSC 17: Avaliação das competências de segurança e formação adequada para preencher lacunas

Controlo – Identifique os conhecimentos, as competências e as capacidades específicas necessárias para melhorar a segurança da empresa; desenvolva e execute um plano integrado para avaliar, identificar e corrigir lacunas através de políticas, planeamento organizacional, formação e programas de sensibilização para todas as funções existentes na organização.

Recomendação – Os consultores de segurança de impressão têm conhecimentos especializados para o ajudar a avaliar os riscos de segurança, desenvolver uma política e um plano de segurança abrangentes e implementar recomendações relativas a tecnologias e processos. Alguns serviços de segurança poderão inclusive gerir a segurança e a conformidade da impressão por si.

CSC 18: Segurança do software de aplicação

Controlo – Efetue a gestão do ciclo de vida de segurança de todo o software desenvolvido internamente e adquirido externamente por forma a prevenir, detetar e corrigir debilidades de segurança.

Recomendação – Adira às práticas recomendadas de desenvolvimento destinadas a todas as soluções de impressão desenvolvidas. Escolha soluções de software assinadas e validadas como autênticas.

CSC 19: Resposta a incidentes e gestão de incidentes

Controlo – Proteja as informações da organização, bem como a respetiva reputação, ao desenvolver e implementar uma infraestrutura de resposta a incidentes (por exemplo, planos, funções definidas, formação, comunicações e supervisão da gestão).

Recomendação – Certifique-se de que o seu ambiente de impressão está incluído no seu plano de respostas a incidentes.

CSC 20: Testes de intrusão e exercícios de Red Team

Controlo – Teste a solidez global das defesas da organização (tecnologia, processos e pessoas) ao simular os objetivos e as ações de um atacante.

Recomendação – Inclua o seu ambiente de impressão nos testes de intrusão. Avalie regularmente as vulnerabilidades do ambiente de impressão e atualize o plano de segurança por forma a resolver as vulnerabilidades detetadas.

Dê o próximo passo

A implementação das recomendações apresentadas no presente documento técnico pode ajudá-lo a reforçar a segurança de impressão e a cumprir os requisitos de conformidade. Precisa de ajuda? Os serviços de gestão e de aconselhamento em matéria de segurança de impressão podem ajudá-lo a desenvolver um plano e a implementar processos e tecnologias com vista a melhorar a segurança dos seus dispositivos de impressão, dados e documentos.

Anexo A: Funcionalidades, soluções e serviços de segurança de impressão da HP

As funcionalidades de segurança incorporadas nos dispositivos HP, juntamente com soluções de software líderes do setor, podem ajudá-lo a cumprir os requisitos regulamentares e legais em matéria de segurança e a proteger as informações da sua empresa das ameaças de segurança.

As funcionalidades de segurança incorporadas nas impressoras e multifunções HP Enterprise oferecem proteção contra malware e permitem detetar e recuperar imediatamente de um ataque. A segurança de impressão da HP é a única solução a oferecer deteção em tempo real, monitorização automatizada e validação de software incorporada, para impedir as ameaças no momento em que ocorrem.[4] (Facilita o cumprimento dos CSC 2, 4, 6 e 8.) hp.com/go/PrintersThatProtect

As soluções **HP Access Control** disponibilizam uma série de funcionalidades de autenticação e controlo do acesso baseado nas funções dos utilizadores por forma a reduzir potenciais falhas de segurança, além de permitir a monitorização de trabalhos, bem como a gestão e a análise de dados contabilísticos associados à impressão. (Facilita o cumprimento dos CSC 5, 7, 10, 12, 13, 14, 15 e 16.) hp.com/go/hpac

A **encriptação** e as **HP JetAdvantage Workflow Solutions** protegem os dados armazenados nos dispositivos HP Enterprise e os dados em trânsito de ou para os dispositivos de impressão ou nuvem. (Facilita o cumprimento dos CSC 12 e 13.) hp.com/go/upd, hp.com/go/documentmanagement

As **HP Pull Printing Solutions** protegem os documentos confidenciais ao armazenar os trabalhos de impressão num servidor seguro, na nuvem, ou no seu computador. Os utilizadores autenticam-se na localização de impressão escolhida para aceder aos respetivos trabalhos e imprimi-los. (Facilita o cumprimento dos CSC 10, 13 e 14.) hp.com/go/hpac, hp.com/go/JetAdvantageSecurePrint

A **HP JetAdvantage Connect** permite aos utilizadores móveis imprimir facilmente a partir dos respetivos smartphones e tablets, mantendo a segurança e o controlo administrativo necessários. (Facilita o cumprimento dos CSC 12 e 15.) hp.com/go/JetAdvantageConnect

Os dados de eventos das impressoras HP podem ser enviados para as ferramentas SIEM, como o ArcSight, Splunk ou SIEMonster. A sua equipa de segurança pode visualizar facilmente os terminais da impressora como parte do ecossistema das TI mais abrangente e executar as ações de correção necessárias. (Facilita o cumprimento dos CSC 4 e 6.)

O **HP JetAdvantage Security Manager** é a única ferramenta de conformidade da segurança de impressão baseada em políticas existente no setor.[5] Ajuda-o a definir uma política de segurança para todo o parque, a automatizar a remediação das definições dos dispositivos e a instalar e renovar certificados exclusivos, ao mesmo tempo que apresenta os relatórios necessários para comprovar a conformidade. A funcionalidade Instant-On da solução configura automaticamente os novos dispositivos assim que são adicionados à rede ou após um reinício. (Facilita o cumprimento dos CSC 1, 2, 3, 4, 5, 6, 8, 9, 11 e 15.) hp.com/go/securitymanager

Os **HP Secure Managed Print Services** oferecem a segurança de impressão mais sólida e abrangente do setor.[6] A segurança de impressão pode ser algo difícil de conseguir. Deixe a HP encarregar-se da gestão da sua segurança de impressão, desde a proteção dos dispositivos a soluções de segurança avançadas que cumprem os requisitos relativos a pessoas, processos e conformidade. (Facilita o cumprimento dos CSC 2, 3, 12, 16, 17, 18 e 19.) hp.com/go/SecureMPS

Os **HP Print Security Professional Services** disponibilizam especialistas em segurança para o ajudar a avaliar o seu ambiente de impressão, a definir de forma pró-ativa políticas de segurança e a manter o seu plano de segurança atualizado. Podemos inclusive gerir a segurança e a conformidade da impressão por si. (Facilita o cumprimento dos CSC 2, 3, 12, 16, 17 e 19.) hp.com/go/SecureMPS

Notas

[1] Estudo "Cost of Cyber Crime Study & the Risk of Business Innovation", elaborado pela Ponemon e patrocinado pela HPE (2016).

[2] Relatório "2016 Year End Data Breach Quick View" elaborado pela Risk Based Security (janeiro de 2017).

[3] 26,2% dos inquiridos sofreram uma violação à segurança das TI significativa que necessitou de remediação, e mais de 26,1% destes incidentes envolveram impressoras. Estudo "IT and Print Security Survey 2015" elaborado pela IDC (setembro de 2015) – (documento n.º US40612015).

[4] A afirmação é aplicada a dispositivos do segmento HP Enterprise lançados no mercado no início de 2015 e é baseada na análise da HP referente a funcionalidades de segurança incorporadas de impressoras concorrentes do mesmo segmento publicadas em 2016. Apenas a HP oferece uma combinação de funcionalidades de segurança para a verificação da integridade até ao BIOS com capacidades de autorrecuperação. Poderá ser necessária uma atualização de pacotes de serviços do HP FutureSmart para ativar as funcionalidades de segurança. Para consultar uma lista de produtos compatíveis, aceda a hp.com/go/PrintersThatProtect. Para saber mais informações, aceda a hp.com/go/printersecurityclaims.

[5] O HP JetAdvantage Security Manager deve ser adquirido sem separado. Para saber mais informações, aceda a hp.com/go/securitymanager. A afirmação é baseada num estudo interno da HP relativamente às ofertas dos concorrentes "Device Security Comparison" (janeiro 2015) e num relatório da Buyers Laboratory LLC "Solutions Report on HP JetAdvantage Security Manager 2.1" (fevereiro de 2015).

[6] Inclui capacidades de segurança para dispositivos, dados e documentos disponibilizadas por fornecedores líderes de serviços de impressão geridos. A afirmação é baseada na análise da HP de informações disponíveis publicamente durante o período de 2015-2016 relativamente a serviços de segurança, software de gestão e de segurança, e funcionalidades de segurança incorporadas em impressoras concorrentes do mesmo segmento. Para saber mais informações, aceda a hp.com/go/MPSsecurityclaims ou a hp.com/go/mps.

Subscrever atualizações
hp.com/go/getupdated

Partilhar com colegas

4AA6-8821PTE, junho de 2017, Rev. 1