Segurança na era do trabalho híbrido

Um guia e uma lista de verificação para implementar uma segurança abrangente.

xerox™

A maneira como as empresas atuam e o fluxo das informações mudaram

À medida que evoluímos para novas maneiras de trabalhar, dispositivos, documentos e dados permanecem sendo a força vital de cada empresa. Após a confusão para manter as empresas funcionando, o trabalho flexível tornou-se o novo normal. Você já fez o suficiente para permanecer protegido onde quer que o trabalho seja feito?

Os dados de que dependemos para impulsionar os negócios também colocam nossas organizações em risco considerável. Uma violação de qualquer tipo pode ser devastadora, causando caos e falta de confiança, fazendo cair os preços das ações e até mesmo levando ao recebimento de ações disciplinares e altas multas dos reguladores.

Criamos este e-book para ajudar a sua empresa a fazer as melhores escolhas para garantir a segurança de documentos e dados de negócios protegendo a infraestrutura de impressão que os armazena. Ele foi projetado para auxiliar todas as pessoas e organizações, independentemente da função ou do tamanho, na compreensão dos procedimentos e das políticas necessárias para garantir a segurança ideal da infraestrutura de TI. Isso inclui ativos externos, além do firewall corporativo.

Consulte a lista de verificação neste e-book com frequência e compartilhe-a com os colegas. Quando todos estão bem-informados e em sintonia, você pode ter mais confiança nas suas decisões de segurança e na saúde cibernética de sua organização.

Sua estratégia de segurança atende às demandas dessa nova era de trabalho híbrido? Você pode comprovar a conformidade sem sombra de dúvidas? Poucas empresas são tão seguras quanto pensam.

ÍNDICE

A ameaça é real

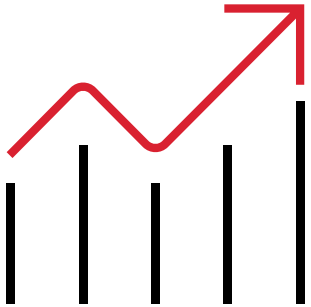
Ninguém pode ignorar a segurança da sua infraestrutura de TI atualmente. E a ameaça não desaparecerá amanhã. Agora, mais do que nunca, os possíveis pontos de entrada estão em expansão devido ao novo local de trabalho flexível.

Não importa se você adotou práticas de trabalho flexíveis ou trabalha com clientes que trabalham assim. a necessidade de segurança de documentos, dispositivos e conteúdos nunca foi tão abrangente.

- A propriedade intelectual precisa ser protegida dos concorrentes
- As informações financeiras e pessoais dos clientes precisam estar protegidas dos hackers
- Registros de funcionários e informações de identificação pessoal criam preocupações com recursos humanos
- Regulamentos e exigências do setor adicionam mais complexidade

Há muito tempo organizações maiores são alvos, mas os empresários de pequeno e médio porte estão se tornando cada vez mais vulneráveis à medida que os hackers direcionam mais esforços para eles. E todos estão sob pressão para atender às políticas e mandados de segurança internos e externos e comprovar a conformidade com parceiros, fornecedores e clientes leais.

Isso significa que todos, independentemente do cargo, departamento e linha de negócios, desempenham um papel importante e devem priorizar a segurança e a conformidade.



As violações de segurança cresceram para **61%** das organizações no ano passado, aumentando para **70%** nos EUA e **66%** em serviços comerciais e profissionais.

Fonte: Quocirca – The Print Security Landscape, 2023 (EUA e UE)

Os custos estão aumentando

As violações de segurança estão ficando mais caras em todo o mundo, tanto em custos financeiros quanto em consequências indiretas. Essas consequências incluem o tempo, o esforço e os recursos gastos na notificação das vítimas e na investigação do incidente, juntamente com o impacto negativo na reputação da organização.

Nenhuma empresa, nenhum setor e nenhum departamento estão seguros. Os cibercriminosos estão lançando ataques contra pessoas, famílias, empresas, governos, polícia, hospitais, escolas, bancos, redes elétricas, serviços públicos, data centers, servidores, redes, PCs, laptops, tablets e smartphones.

Atingindo o nível mais alto de todos os tempos, a média do custo de uma violação de dados foi de US$ 4,35 milhões em 2022.

Os cinco principais países e regiões com o maior custo médio de uma violação de dados foram os Estados Unidos, com USD 9,44 milhões; o Oriente Médio, com USD 7,46 milhões; o Canadá, com USD 5,64 milhões; o Reino Unido, com USD 5,05 milhões; e a Alemanha, com USD 4,85 milhões.[1] A estimativa é que os custos globais com o crime cibernético cresçam 15% por ano nos próximos três anos, chegando a US$ 10,5 trilhões anualmente até 2025.[2]

A frequência dos ataques de ransomware a governos, empresas, consumidores e dispositivos continuará aumentando nos próximos cinco anos, chegando a ocorrer a cada dois segundos até 2031.[2]

Mas, quanto mais rápida uma violação de dados puder ser identificada e contida, menor será o custo.

1. Cost of a Data Breach Report 2022 – Ponemon Institute, patrocinado, analisado e publicado pela IBM Security® (WW)
2. Top 10 Cybersecurity Predictions And Statistics For 2023 – Cybercrime Ventures (WW)

US$ 935 mil

é o custo médio estimado de uma violação de dados.

Fonte: Quocirca – The Print Security Landscape, 2023 (EUA e UE)

Os pontos de entrada são numerosos e estão em expansão

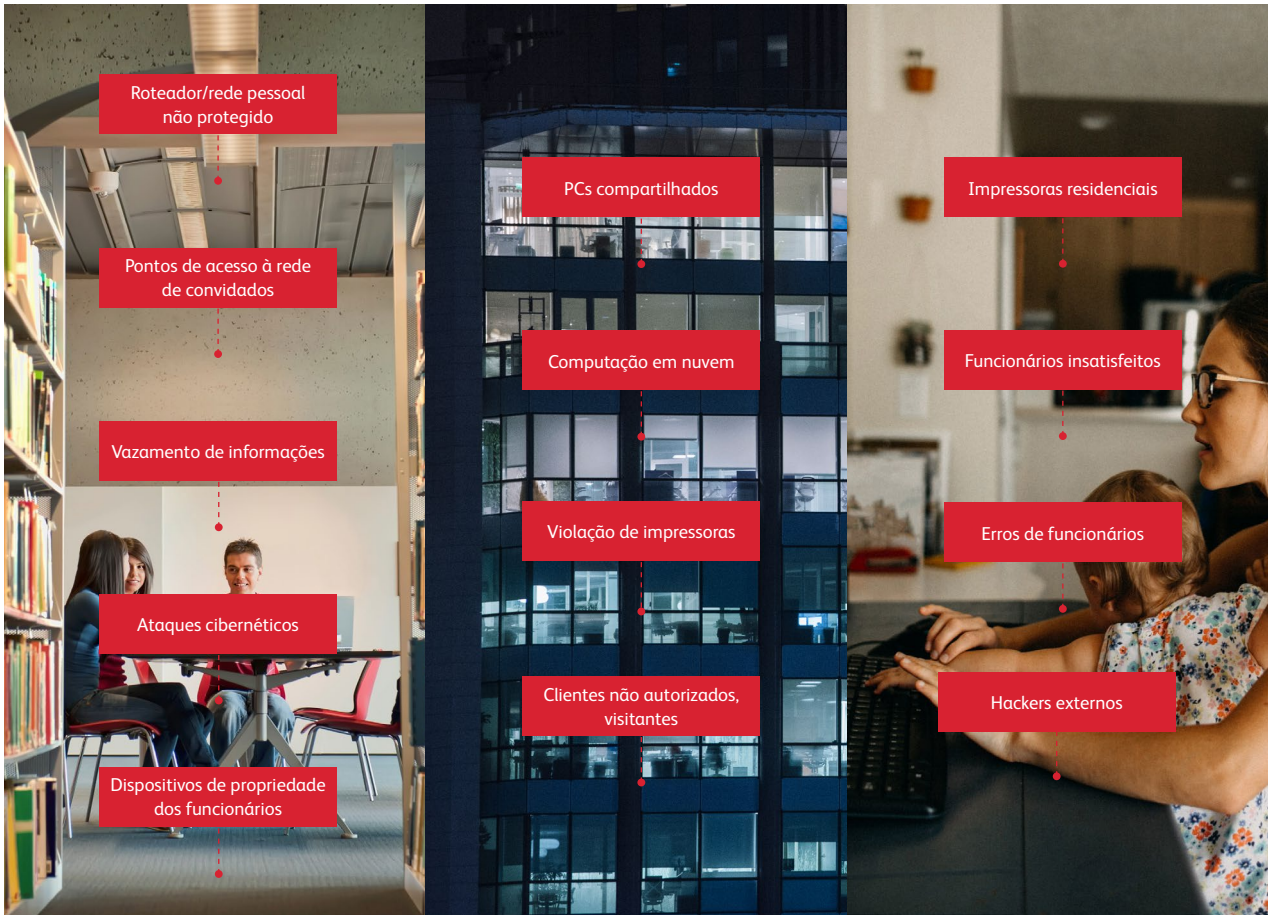
Ameaças surgem de todos os aspectos na sua infraestrutura de TI e daqueles que interagem com ela, interna e externamente. Agora você também precisa considerar funcionários ou clientes que trabalham em casas menos seguras ou locais remotos, até mesmo usando ativos não controlados pelas políticas de TI.

Em média, **25%** das forças de trabalho são totalmente remotas, **33%** são híbridas e **42%** estão totalmente no escritório.

Fonte: Quocirca – The Print Security Landscape, 2023 (EUA e UE)

Mais de **7%** dos dispositivos desktop Windows estão executando versões sem suporte.

Participação de mercado de versão desktop Windows no mundo todo – fevereiro de 2023



Violações de impressoras acontecem

Para hackers que procuram uma maneira de entrar em uma rede corporativa ou pessoal, implementações de IoT inseguras, como impressoras, fornecem o ponto de entrada perfeito. Seguir algumas etapas simples pode ajudar a reduzir o risco e deter os invasores em seus ataques.

O QUE FAZER? ALOCAR OU FAZER PARCERIA COM OS RECURSOS APROPRIADOS NECESSÁRIOS PARA UMA ESTRATÉGIA E IMPLEMENTAÇÃO DE SEGURANÇA ABRANGENTES.

Garantir que seus dispositivos de impressão sejam tão seguros quanto você espera requer uma estratégia abrangente, que cruze várias camadas — dados, documentos, pessoas, dispositivos, regras e regulamentos gerais que regem seus negócios.

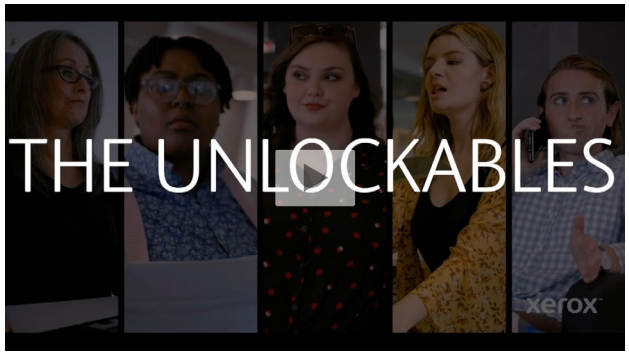
As organizações, grandes e pequenas, devem ter políticas e procedimentos de segurança em vigor para malware e ataques, vazamentos de dados e computação em nuvem, bem como políticas de funcionários. No entanto, muitas organizações ainda não têm essas políticas e procedimentos para sua infraestrutura de impressão.

As violações de dados relacionadas à impressão permanecem predominantes, com **61%** dos entrevistados relatando pelo menos uma perda de dados nos últimos **12** meses, aumentando para **67%** entre as organizações de médio mercado.

Fonte: Quocirca – The Print Security Landscape, 2023 (EUA e UE)

O fator humano

Quando ocorrem violações de segurança ou dados, é natural olhar para a TI. No entanto, erros ou ações do usuário que se enquadram fora das diretrizes de comportamento recomendadas pela TI causam muito mais problemas. Suas maiores ameaças cibernéticas não são agentes maliciosos. São seus funcionários: eles cometem erros de forma não intencional. Eles usam atalhos não aprovados. Eles se esforçam para fazer mais com menos. Como resultado, podem tomar decisões que colocam seu negócio em risco.



Clique aqui para assistir ao vídeo.

O QUE FAZER?

Primeiro faça uma análise para descobrir como seus usuários estão trabalhando com documentos e dispositivos. Em segundo lugar, procure implementar um ambiente de trabalho com segurança Zero Trust.

A análise dos usuários pode responder a perguntas como estas:

- Quem está imprimindo fora do horário comercial, quando poucos funcionários estão trabalhando?
- Uma pessoa importante se demitiu. O que ela imprimiu recentemente?
- Um funcionário digitalizou ou enviou conteúdo por e-mail para um local não autorizado, como uma nuvem pública?

Implementar o Zero Trust:

- Ajuda a reduzir o fator humano
- Ativa a autenticação, de modo que somente usuários autorizados possam acessar o que está disponível apenas para eles
- Leva a mudanças conscientes no comportamento

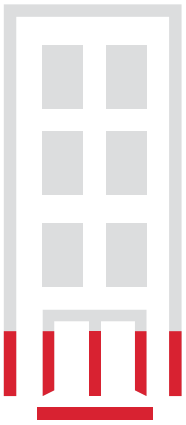
A análise do usuário e a implementação da segurança Zero Trust podem guiá-lo para mais serviços e soluções que impulsionam a sustentabilidade, a produtividade e a conformidade.

> **95%** das violações de segurança cibernética são causadas por erro humano.
>
> Fonte: The Global Risks Report 2022 – Fórum Econômico Mundial

Em uma pesquisa recente, metade dos entrevistados dizem que incluem a impressão como parte de sua estratégia de Zero Trust, e outros 39 % planejam fazer isso nos próximos 12 meses.[1]

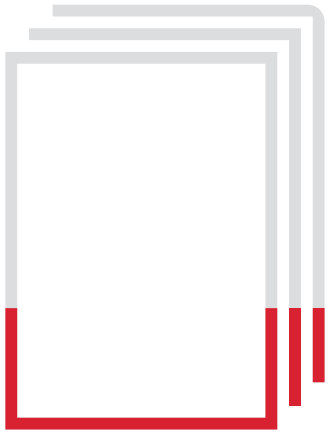
1. Estudo de tendências de segurança Zero Trust de 2022 da Quocirca. (EUA e Reino Unido)

As medidas de segurança estão atrasadas



19%

dos entrevistados estão completamente confiantes de que sua infraestrutura de impressão está segura.



Em média,

27%

dos incidentes de segurança de TI estavam relacionados a documentos em papel.

Para

34%

dos entrevistados, o principal desafio é evitar que documentos confidenciais e sensíveis sejam impressos.

Fonte: Quocirca – The Print Security Landscape, 2023 (EUA e UE)

As preocupações de segurança estão em crescimento, mas as medidas de segurança ficam para trás. Onde está sua empresa? Você está preocupado com a segurança de sua infraestrutura de TI e dos documentos, dispositivos, conteúdo e dados que ela armazena? O que você não está fazendo, mas poderia ou deveria?

Indo além do gerenciamento de impressão

A Internet das Coisas (IoT) não é mais composta apenas de computadores e telefones. As informações não estão mais contidas em ambientes controlados e confiáveis. A nuvem mudou a maneira como as empresas operam, essencialmente permitindo o acesso a dados, aplicativos, plataformas e serviços em qualquer lugar, a qualquer hora.

À medida que seu local de trabalho vai além do escritório físico e se torna mais conectado, o número de dispositivos inteligentes e IoT em seus locais de trabalho aumentará, e a necessidade de ir além dos Serviços de Impressão Gerenciada tradicionais também aumentará.

Uma abordagem baseada em dados para a segurança que usa análises para identificar oportunidades para economia de custos e produtividade é essencial para otimizar a maneira como os funcionários e a tecnologia trabalham juntos, resultando em locais de trabalho mais produtivos e eficientes e maior segurança e conformidade.

AQUI ESTÃO SEIS ELEMENTOS PRINCIPAIS A SEREM CONSIDERADOS AO ESCOLHER UM PARCEIRO PARA AJUDAR VOCÊ A ELIMINAR LACUNAS DE SEGURANÇA:

1. Ele pode aplicar a solução aos dispositivos certos no momento certo e criar políticas fáceis de aplicar e cumprir?
2. Ele entende seus requisitos de rede? Ele pode recomendar soluções que se ajustem corretamente e utilizem dados para dar suporte a manutenção contínua e serviços e suporte proativos?
3. Ele está focado na inspeção e no monitoramento consistentes de todos os dispositivos e processos de documentos para garantir a conformidade automaticamente em toda a linha?
4. Ele pode fazer correções no parque de impressão, na impressora e nos níveis de configuração para que os problemas fora de conformidade possam ser identificados e resolvidos rapidamente?
5. Ele fornece relatórios contínuos em tempo real para mostrar a conformidade e/ou destacar áreas que precisam ser abordadas?
6. Ele pode fazer isso independentemente do local de trabalho?

As empresas investirão **US$ 15 trilhões** em IoT até 2025.*

*Fonte: vXchnge (WW)

Uma abordagem de segurança Zero Trust abrangente

A proteção total de endpoints em um mundo móvel, orientado por nuvem e IoT requer uma abordagem multicamada e vigilância constante, mas não é possível monitorar todos os endpoints manualmente. Apesar dos novos desafios que a atualidade traz, a maioria das estratégias de segurança não leva em conta o fato de que os documentos, os dados e o conteúdo que impulsionam os negócios atuais vivem em qualquer lugar e estão disponíveis 24 horas por dia, 7 dias por semana.

É essencial que o seu provedor de serviços adote uma abordagem abrangente e multicamada para a segurança, com inteligência proativa que proteja dispositivos, documentos, dados e conteúdo. Ao mesmo tempo, complemente a implementação do Zero Trust oferecendo soluções que se alinhem perfeitamente.

Dispositivos seguros
Certifique-se de que suas impressoras tenham proteção integrada e máxima segurança assim que estiverem conectadas à rede.

Gerenciamento seguro do parque de impressão
Defina as normas de configuração de segurança e valide automaticamente a conformidade.

Gerenciamento de impressão
Controle o acesso aos documentos e forneça informações úteis.

Dados e conteúdo seguros
Blinde a segurança contra divulgação não autorizada de dados e conteúdo (no dispositivo ou na nuvem).

68 %

das organizações sofreram um ou mais ataques a endpoints.

Fonte: Ponemon Institute, estudo do estado do risco de segurança de endpoints, 2020

Próximos passos: Identificar lacunas, ganhar confiança

Qual o seu grau de certeza de que seus dispositivos, documentos e dados estão seguros e quais áreas de segurança você considerou e implementou ao fazer isso? É importante que você esteja informado sobre discussões e decisões de segurança em sua organização e ciente das lacunas existentes para saber se está indo na direção certa para o seu negócio.

O QUE VEM DEPOIS?

1. Entenda as políticas de segurança de sua empresa para dispositivos, documentos e dados.
2. Identifique e envolva os principais interessados e avalie seu nível de risco.
3. Isole as vulnerabilidades do dispositivo ou do processo e os pontos fracos e tome medidas para garantir que sejam solucionados.
4. Use a lista de verificação a seguir para discutir necessidades e lacunas com sua equipe.

Os Serviços de Impressão Gerenciada da Xerox® são uma forma simplificada e segura de acelerar a transformação digital e melhorar o modo como as pessoas e a tecnologia trabalham em conjunto.

Fornecemos monitoramento e conformidade de segurança interativa a partir de um painel visual e intuitivo e tecnologias de segurança da impressora integradas com as plataformas líderes de mercado Trellix[3] DXL e Cisco® pxGrid, permitindo uma resposta instantânea e automática a ameaças.

Além disso, somos o primeiro fornecedor de impressão a receber autorização de segurança do FedRAMP para serviços de impressão gerenciada baseados em nuvem, um elemento dos Serviços de Impressão Gerenciada da Xerox®. Somos posicionados como líderes no IDC Security Marketscape, bem como nos relatórios Print Security Landscape da Quocirca, graças ao nosso foco em segurança, capacitação de TI e usuários finais. Juntos, podemos criar um ambiente mais seguro.

Saiba mais em **www.xerox.com/pt-br/sobre-nos/security-solutions**

3. Trellix, anteriormente conhecida como McAfee® Enterprise Business.

Uma lista de verificação abrangente: Dispositivos, documentos e dados

Quer você mesmo esteja procurando implementá-lo ou optar por trabalhar com parceiros confiáveis, este é o seu guia de trabalho para uma abordagem abrangente de segurança Zero Trust.

Qualificações e práticas recomendadas de segurança para parceiros

Elementos a considerar para garantir segurança abrangente de dispositivos, documentos e dados.

ANÁLISE E RELATÓRIOS DE SEGURANÇA

- ☐ O parceiro trabalha com você para avaliar as necessidades de segurança e identificar onde suas informações residem, como são transferidas e suas maiores áreas de risco?
- ☐ O parceiro fornece um plano/estratégia de segurança abrangente que engloba dispositivos, documentos e dados?
- ☐ O parceiro ajuda você a definir políticas de segurança, validar a conformidade, controlar o acesso e bloquear a divulgação não autorizada de documentos e dados confidenciais?
- ☐ O parceiro tem diretrizes claras para estratégias que apoiem suas iniciativas de segurança Zero Trust?
- ☐ O parceiro tem tecnologias robustas que podem ser usadas para garantir a qualidade e a precisão dos dados?
- ☐ O parceiro se reúne com você proativamente para tratar de segurança e outros problemas?
- ☐ Os relatórios fornecidos pelo parceiro de segurança trazem informações sobre a implementação de políticas de segurança e dispositivos em risco?

RECOMENDAÇÕES PARA DISPOSITIVOS, COLOCAÇÃO E OTIMIZAÇÃO

- ☐ O parceiro de segurança ajudará você a selecionar os melhores dispositivos para fins de segurança? As impressoras mais seguras têm várias camadas de recursos de segurança e são capazes de se integrar a programas de gerenciamento de segurança centralizados, como o Trellix[3] ePolicy Orchestrator e Cisco ISE.
- ☐ O parceiro pode usar análises para entender na íntegra os dispositivos que você tem hoje e identificar áreas de redução ou otimização?

COMPROMISSO COM A INOVAÇÃO EM SEGURANÇA

- ☐ O parceiro trabalha com fornecedores que investem em pesquisa, desenvolvimento e engenharia de segurança? A Xerox, por exemplo, dedica uma porcentagem da receita à segurança e outros projetos críticos de pesquisa, desenvolvimento e engenharia.
- ☐ O provedor de serviços de segurança utiliza pessoas, processos e tecnologia para atender aos mais altos padrões de conformidade de segurança?

PROGRAMA DE CONFORMIDADE DE SEGURANÇA

- ☐ Esses fornecedores ganham acreditações, passam por auditorias rigorosas e recebem inúmeras certificações por suas ofertas de hardware e software?

SOFTWARE DE SEGURANÇA DE MPS

- ☐ O parceiro trabalha com fornecedores de serviços de impressão gerenciada cujo back-office é certificado pela ISO 27001 como uma instalação segura?
- ☐ O software do parceiro pode questionar a impressora ou a frota de impressoras multifuncionais quanto aos níveis de firmware de dispositivos e determinar se estão alinhados às suas políticas de segurança?
- ☐ As configurações de segurança podem ser facilmente definidas e monitoradas e qualquer dispositivo fora de conformidade é corrigido sem esforço manual adicional?
- ☐ Você pode visualizar documentos confidenciais que são impressos, copiados ou digitalizados que não são aprovados e receber uma notificação sobre esse comportamento?
- ☐ O parceiro pode fornecer relatórios contínuos em tempo real por meio de um painel interativo para mostrar a conformidade e/ou destacar áreas que precisam ser abordadas?
- ☐ Os dados confidenciais são protegidos por meio de acesso a usuários e grupos, proteção por senha, criptografia de conteúdo e retenção e disposição automatizadas?

3. Trellix, anteriormente conhecida como McAfee® Enterprise Business.

TECNOLOGIA BASEADA EM PADRÕES

A segurança de dispositivos de endpoint pode afetar sua capacidade de atender às demandas regulatórias e do setor.

- ☐ Os produtos que os parceiros fornecem são projetados para dar suporte a padrões e regulamentos como HIPAA, Sarbanes-Oxley, a Lei Gramm-Leach-Bliley, FDA 21 CFR Parte 11 e GDPR?
- ☐ O parceiro trabalha com fornecedores que procuram a validação de segurança de dispositivos por terceiros, participando do programa International Common Criteria for Information Technology and Security Evaluation para certificação (ISO/IEC 15408)?
- ☐ Esses fornecedores enviam todo o dispositivo, não apenas um kit de segurança, para avaliação? Isso é importante para empresas de alta segurança, como agências governamentais que compram MFPs com unidades de armazenamento, garantindo que proteção extra seja integrada ao dispositivo.

Suporte ao Zero Trust

AUTENTICAÇÃO DA REDE

A segurança melhora quando os administradores limitam o acesso aos usuários com base em sua função/seu cargo.

- ☐ Usuários autorizados devem fazer login com uma senha ou um cartão de identificação para acesso seguro às funções do dispositivo?
- ☐ Essas sessões de autenticação e autorização podem ser auditadas?
- ☐ O logon único (SSO) e a autenticação multifator (MFA) foram implementados para maior segurança?

ACESSO ÀS INFORMAÇÕES

- ☐ O uso de conteúdo confidencial pode ser sinalizado e monitorado?
- ☐ Uma notificação desse acesso não autorizado pode ser enviada?
- ☐ Você pode limitar e rastrear quem tem acesso a informações confidenciais?
- ☐ Há controles em vigor para gerenciar essas informações em dispositivos de saída?

POLÍTICA DE SEGURANÇA DOS DISPOSITIVOS

Considere o acesso aos ativos de rede, não apenas às informações.

- ☐ Você criou uma política de segurança para acesso e impressão em ativos de rede?
- ☐ Quando os dados são movidos de e para dispositivos multifuncionais, eles são protegidos com criptografia de ponta?

DIRETRIZES PARA FUNCIONÁRIOS

- ☐ Existem medidas em vigor para garantir que os funcionários compreendam e cumpram as diretrizes de segurança?
- ☐ As atividades dos funcionários que quebram essas diretrizes de segurança são rastreadas?
- ☐ Você tem uma política e processo de aprovação de firmware de dispositivos antes da implantação?
- ☐ Existe um processo para determinar a credibilidade das atualizações de software e validar assinaturas digitais?

Fatores importantes de segurança do dispositivo

VULNERABILIDADE DOS DISPOSITIVOS

- ☐ Os dispositivos incluem um firewall de rede para impedir o acesso externo não autorizado a seus sistemas por meio de uma conexão de rede?
- ☐ Existem possíveis vulnerabilidades que podem expor seus dispositivos a um ataque?

- ☐ Há controles em vigor para proteger a integridade do firmware de dispositivos, como assinatura digital, criptografia e verificação?
- ☐ Os dispositivos possuem proteção integrada contra malware?
- ☐ Você tem uma maneira consistente de garantir que os dispositivos cumpram as políticas para ativos de rede?
- ☐ Você tem um processo para que ocorram apenas os comportamentos esperados do dispositivo?
- ☐ O gerenciamento automatizado de certificados está disponível?
- ☐ Você é capaz de proteger a comunicação entre seus dispositivos e sua rede ou seus dispositivos de funcionários?

GARANTIA DE CORREÇÃO

- ☐ O que acontecerá se um dispositivo ficar fora de conformidade com a política de segurança? Você recebe um alerta quando isso acontece?
- ☐ Existem etapas específicas para levá-lo de volta à conformidade?
- ☐ Você tem uma política de correção?
- ☐ Você tem uma maneira de verificar se a política está em vigor?
- ☐ Se um ativo de rede sair da conformidade, você pode capturar dados para relatórios?
- ☐ Existe uma trilha de auditoria?
- ☐ Os dispositivos têm a capacidade de transferir o log de auditoria para um servidor SIEM ou de registro de auditoria?

Fatores de vulnerabilidade de informações com base em documentos

SEPARAÇÃO DE FAX/REDE

- ☐ Conexões de fax desprotegidas criam uma possível backdoor para sua rede. Existe uma separação completa entre linhas telefônicas e conexões de fax de rede?

SOBRESCRIÇÃO DE IMAGEM

- ☐ Os dispositivos podem ser configurados para substituir automaticamente os arquivos armazenados nas unidades de armazenamento?
- ☐ Você tem uma política documentada para purgar ou destruir unidades de armazenamento de máquinas removidas do serviço?

Segurança em todo o ciclo de vida do dispositivo

PROGRAMA DE PATCH DE SEGURANÇA E COMUNICAÇÕES

- ☐ Você tem um fornecedor de soluções de segurança que oferece um programa ativo de patch de segurança? Isso significa que ele monitora novas vulnerabilidades nos dispositivos, assim como os desenvolvedores de software de SO rastreiam novos vírus que têm o software como alvo.
- ☐ O provedor de soluções de segurança publica boletins de segurança quando correções de vulnerabilidades em produtos/software são lançadas?
- ☐ Você pode se inscrever em feeds RSS e receber alertas imediatos quando novos boletins e patches são publicados?
- ☐ O fornecedor tem um programa de detecção de problemas para ajudar a descobrir possíveis vulnerabilidades?

REMOÇÃO DA UNIDADE DE ARMAZENAMENTO

- ☐ Você tem um parceiro de serviços de impressão gerenciada que faz recomendações da maneira mais eficaz para eliminar os dados das unidades de armazenamento?
- ☐ Sua metodologia para purgar/destruir unidades de armazenamento de máquinas removidas do serviço está em conformidade com o NIST SP 800-88r1?
- ☐ As trocas e as devoluções que serão remanufaturadas vão ser substituídas ou reformatadas?

Se você não tiver marcado todos os itens desta lista, talvez precise de um parceiro para ajudar você a chegar lá. Saiba mais sobre as melhores e mais abrangentes soluções de segurança da categoria que fornecemos em **www.xerox.com/pt-br/sobre-nos/security-solutions**

Para agendar uma avaliação completa do local de trabalho, acesse **www.xerox.com/pt-br/servicos-empresariais/digital-evaluation-form**

Sobre a Xerox

Em uma era de trabalho híbrido, não estamos apenas pensando no futuro; nós o estamos construindo. A Xerox Corporation é uma líder de tecnologia focada na interseção entre o físico e o digital. Usamos automação e personalização de última geração para redefinir a produtividade, impulsionar o crescimento e tornar o mundo mais seguro. Todos os dias, nossas tecnologias inovadoras e soluções de trabalho inteligentes desenvolvidas pela Xerox® ajudam as pessoas a se comunicar e trabalhar melhor. Descubra mais em **www.xerox.com.br** e siga-nos no Twitter **@Xerox**.