Xerox e Segurança de Informações

Seus Dados, Seu Negócio:
Parceria para Proteger
O Que é Mais Importante

Índice

Visão Geral

As informações são o principal ativo de cada organização e a segurança é essencial para o escritório - para documentos e para quaisquer dispositivos, incluindo impressoras e impressoras multifuncionais conectadas à rede. E, no século XXI, a rede é o hub de basicamente toda uma atividade de negócio.

Quase todos os negócios, e cada pessoa neles, estão conectados à Internet. Seu negócio - e cada organização com a qual você colabora - faz parte de um sistema global de redes e servidores de computadores interconectados. Há incontáveis usuários realizando tarefas simultaneamente, acessando e compartilhando informações, comprando e vendendo produtos e serviços, comunicando-se por e-mail, enviando mensagens instantâneas, usando Skype™, Twitter e muitos outros serviços.

A ameaça à segurança é bastante real e os interesses crescem a taxas exponenciais. Uma violação na segurança dos documentos de uma organização pode resultar em uma aquisição ou uso não autorizado de informações sensíveis ou proprietárias. Isso pode levar a uma divulgação nociva e a uma propriedade intelectual e segredos comerciais roubados ou comprometidos. E, para muitas organizações, essas violações de segurança podem terminar em multas e litígios muito dispendiosos, desde uma centena de milhares a milhões de dólares.

As crescentes ameaças atuais à segurança surgem em várias formas e em diferentes graus de severidade. A proliferação explosiva de dispositivos em rede significa um número ainda maior de pontos possivelmente vulneráveis de entrada para invasores. E a ameaça "hacker" é constante, com programas rodando 24 horas por dia, sete dias na semana que buscam e exploram automaticamente atalhos de segurança de rede.

As ameaças à segurança variam de mensagens tipo spam relativamente inofensivas a ameaças persistentes que podem destruir toda uma rede.

Com essa constante atividade de Internet, você deve ter certeza de que as informações confidenciais de sua empresa estejam seguras. Mas as exigências mudam e mudam diariamente.

As impressoras e as impressoras multifuncionais, ou MFPs, em rede que podem imprimir, copiar, digitalizar para destinos de rede, enviar anexos de e-mail e lidar com transmissões de recebimento e envio de fax são particularmente vulneráveis.

Para aqueles na Segurança de Informações, é crítico para a segurança de rede de uma organização ter certeza de que infrações de segurança não possam ocorrer por meio de impressoras e MFPs conectadas à rede - ou aos dispositivos em si. Depois de tudo, os ataques podem originar-se de formas inesperadas:

- A linha telefônica ligada a uma MFP poderia ser utilizada para acessar à rede.
- O servidor Web utilizado para gerenciar as MFPs e as impressoras pode estar vulnerável ao ataque.
- Dados eletrônicos desprotegidos podem ser inadequadamente acessados quando em repouso no disco rígido ou em movimento para/do dispositivo.
- Os e-mails maliciosos podem ser enviados de uma MFP sem trilha de auditoria.

As impressoras e as impressoras multifuncionais são sofisticadas, com plataformas múltiplas de TI de sub-sistema, e medidas de segurança significativas devem abranger cada elemento da plataforma.

As impressoras e MFPs modernas são bastante diferentes dos PCs e servidores.

- As impressoras e MFPs são dispositivos compartilhados com usuários múltiplos e administradores múltiplos.
- As impressoras e MFPs são dispositivos integrados:
  - Podem ser um sistema operacional real dentro do sistema.
  - O sistema operacional pode ter uma interface externa direta.
  - O sistema operacional pode ser proprietário.
  - O sistema operacional pode ser Microsoft® Windows®.

Visão Geral

- As impressoras e MFPs tem o que segue, todos eles tipicamente associados a nós computacionais mais avançados:
  - Pilhas de protocolo de rede
  - Funções de autenticação e autorização
  - Criptografia
  - Gerenciamento de dispositivos
  - Servidores de Internet

A heterogeneidade das implementações de uma impressora e uma MFP representa um desafio.

- Muito mais diversas que os PCs tradicionais
- Alto grau de diversidade no que se refere aos sistemas operacionais subjacentes entre os diferentes fabricantes e até mesmo dentro de linhas de produto exclusivas do fabricante

Os controles tradicionais do PC e do servidor não são otimizados para impressoras e MFPs.

- Abordagem de antivírus
  - Pode não estar disponível para o tipo de sistema operacional utilizado na impressora e na MFP
  - Geralmente se perde a guerra contra os vírus de uma forma ou de outra
  - Complexidade de gerenciamento de atualizações de arquivos de dados em um ambiente distribuído
- Reparação de impressoras e MFPs
  - O controle da versão de software de impressoras e MFPs é inconsistente
  - O gerenciamento de configuração gera uma despesa operacional
- Informações de Segurança e Gerenciamento de Eventos (SIEM)
  - Os alertas e a conscientização provenientes de impressoras e MFPs são diferentes
  - A reparação de impressoras e MFPs não é padronizada

Essa é uma situação muito diferente das impressoras e copiadoras antigas.

Qualquer pessoa pode lançar ataques contra uma rede e os ativos de informações de uma empresa caso o acesso físico e eletrônico de uma impressora e de uma MFP não seja bem controlado e protegido. Esses ataques podem ser tão simples quanto alguém pegar documentos deixados na bandeja de saída da impressora e da MFP ou vírus maliciosos eliminando documentos sensíveis da rede.

Todo o sistema de uma impressora e de uma MFP, juntamente com um software de gerenciamento de dispositivos na rede, deve ser avaliado e certificado de forma que a Segurança de Informações e todos os colaboradores de uma organização tenham certeza de que seus documentos e a rede estejam seguros e protegidos contra predadores de informações - ou até mesmo de violações internas de segurança.

A esse respeito, nem todas as impressoras e MFPs são iguais. Portanto, uma abordagem abrangente, baseada em uma segurança fundamental, funcional, avançada e útil, é essencial para a proteção dos ativos de informações dos negócios atuais.

Felizmente, a Xerox tem as capacidades de segurança para ajudar. Nos últimos 20 anos, a Xerox tem sido a líder no fornecimento de soluções seguras de documentos para uma série de indústrias no mundo todo. Na verdade, cada produto e serviço da Xerox® que oferecemos foram desenvolvidos tendo a segurança em mente e de forma a se integrar continuamente a estruturas de segurança existentes. E mais, a segurança é gerenciada durante todo o ciclo de vida útil do produto a partir de análises de requisitos, projeto, desenvolvimento, fabricação, implantação e disposição - proporcionando a você e a seus clientes mais proteção e tranquilidade.

Na Xerox, ajudamos a proteger seus dados em cada ponto potencial de vulnerabilidade para que você não precise se preocupar. Ao se manter focado naquilo que fazemos melhor, você pode manter-se focado naquilo que faz melhor.

Metas de Segurança da Xerox

Identificamos as cinco principais metas de segurança em nossa jornada para fornecer soluções seguras a cada um de nossos clientes:

CONFIDENCIALIDADE

- Não há a divulgação não autorizada de dados durante o processamento, transmissão ou armazenagem

INTEGRIDADE

- Não há a alteração não autorizada de dados
- O sistema funciona conforme pretendido, sem uma manipulação não autorizada

DISPONIBILIDADE

- O sistema funciona corretamente
- Não há a negação de um serviço para usuários autorizados
- Proteção contra o uso não autorizado do sistema

RESPONSABILIDADE

- As ações de um órgão podem ser diretamente rastreadas para esse órgão

SEM REPÚDIO

- Garantia mútua de que a autenticidade e a integridade das comunicações de rede são mantidas

Vulnerabilidade de Segurança: Riscos e Custos da Indústria

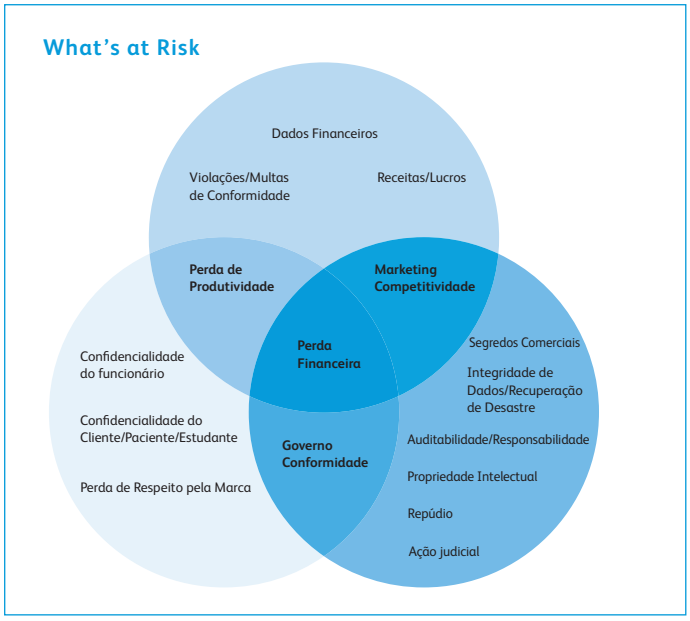
Negócios de todos os tamanhos tem informações sensíveis valiosas para criminosos cibernéticos que devem ser protegidas. O cenário de ameaça muda constantemente. Com um aumento no BYOD (Traga Seus Próprios Dispositivos), utilitários para dados de monitoramento de saúde, sistemas móveis de pagamento, armazenagem em nuvem e a Internet das Coisas, a ameaça é real e continua a crescer.

Os criminosos cibernéticos estão cada vez mais focando a atenção em negócios de pequeno e médio portes (SMBs), pois são alvos mais fáceis que as grandes empresas e porque, tipicamente, os SMBs carecem de recursos necessários para protegê-los contra ataques.

As violações de dados de grandes empresas ocupam as principais manchetes de jornais, mas, infelizmente, não ouvimos muitas notícias sobre ataques cibernéticos a SMBs.

Os interesses em SMBs são ainda mais altos que os de grandes corporações. As informações de clientes mantidas nos SMBs estão se tornando uma mercadoria mais valiosa e os custos dessas violações podem devastar um SMB. De acordo com um estudo realizado pela IBM e pelo Instituto Ponemon em 2015, o custo médio total de uma violação de dados para empresas participantes aumentou 23 % nos últimos dois anos para $3,79 milhões.[1] O custo médio pago por cada perda ou registro roubado contendo informações sensíveis e confidenciais aumentou de $145 em 2014 para $154 em 2015.[1]

Esses valores não contabilizam possíveis multas, perda de reputação e ruptura comercial. A segurança pode não ser sempre uma prioridade de negócio, mas manter as informações protegidas é essencial para a saúde da organização.



Cuidado da saúde

Avanços na tecnologia de informações - incluindo o uso de computadores portáteis - deram origem à necessidade de compartilhar dados médicos e informações de pacientes importantes por meio eletrônico - e é aí que a segurança se torna uma grande preocupação.

A Health Insurance Portability and Accountability Act (Lei de Portabilidade e Responsabilidade do Seguro de Saúde) de 1996 (HIPAA) foi implementada pelo governo federal para forçar todas as organizações de saúde a aplicar práticas uniformes de gerenciamento de dados para proteger as informações e a privacidade dos pacientes o tempo todo. De acordo com a HIPAA, é necessária uma trilha de auditoria para rastrear quem visualizou os dados, quando eles os visualizaram e se tinham autorização para isso.

A Health Information Technology for Economic and Clinical Health (HITECH) Act (Lei de Tecnologia de Informações de Saúde para a Saúde Econômica e Clínica) expandiu significativamente os esforços do governo americano para estabelecer um sistema nacional de registros eletrônicos para o setor de saúde. A HITECH entrou em vigor como parte da American Recovery and Reinvestment Act (Lei de Recuperação e Reinvestimento dos Estados Unidos) de 2009 para promover a adoção e o uso significativo da tecnologia de informações de saúde.

A não conformidade com a HIPAA pode resultar em sanções cíveis e criminais, mesmo se não houver uma violação.

Governo

Atualmente, governos locais, estaduais e federais enfatizam a simplificação de processos e a melhora da colaboração entre agências para oferecer melhores resultados aos cidadãos aos quais elas servem. Para realizar isso, empregam várias iniciativas para tirar vantagem das tecnologias mais modernas ao mesmo tempo em que impõem regulamentações rigorosas para garantir que as informações que serão compartilhadas estejam seguras e protegidas. Um exemplo é Lei de violação de dados do estado de Massachusetts, que é uma das mais agressivas do país. Os sistemas, software e serviços da Xerox® cumprem essas diretrizes rigorosas, assim como outras regulamentações.

Em 2014, o Departamento de Defesa adotou as normas 800-53 do National Institute of Standards and Technology (Instituto Nacional de Normas e Tecnologia) (NIST), que é uma publicação que recomenda controles de segurança para sistemas e organizações de informações federais e documenta os controles de segurança de todos os sistemas de informações federais, exceto aqueles concebidos para a segurança nacional.

1. 2015 Cost of Data Breach Study: Global Analysis, IBM and Ponemon Institute, maio de 2015.

Vulnerabilidade de Segurança: Riscos e Custos da Indústria

Além disso, o Departamento de Defesa adotou outras medidas de segurança com o uso de Cartões de Acesso Comuns (CAC) e as contrapartes do governo civil adotaram cartões de Verificação de Identidade Pessoal (PIV). Esses cartões exigem uma infraestrutura de KI para garantir uma autenticação e um ambiente de comunicação seguros.
Adicionalmente, muitas agências do governo federal adotaram a norma FIPS 140-2 para certificar os módulos de criptografia utilizados em impressoras e MFPs. E, por fim, muitos clientes do governo federal exigem que os produtos sejam certificados de acordo com a norma de Critérios Comuns.

Serviços financeiros

Depósito direto, serviços bancários on-line, cartões de débito e outros avanços na tecnologia de informações estão revolucionando o setor de serviços financeiros. Embora mais conveniente para clientes e negócios, esse uso intenso de tecnologia tem seu próprio conjunto de preocupações de segurança.

Uma troca segura de informações de cartão de crédito é vital e a conformidade com a Norma de Segurança de Dados (DSS) do Setor de Cartões de Pagamento (PCI) ajuda a diminuir as vulnerabilidades e a proteger os dados do portador do cartão. A DSS do PCI é uma norma proprietária de segurança de informações para organizações que lidam com cartões de crédito, incluindo Visa®, Mastercard®, American Express®, Discover® e JCB.

A Gramm-Leach-Bliley Financial Services Modernisation Act (Lei de Modernização de Serviços Financeiros de Gramm-Leach-Bliley) de 1999 (GLBA) foi instituída para garantir que instituições financeiras que coletam ou recebem dados privados de clientes tenham um plano de segurança implementado para protegê-los. Para obter a conformidade, as organizações devem preencher uma análise de riscos em seus processos atuais e implementar firewalls, restringir o acesso de usuários, monitorar impressões e muito mais.

A Dodd-Frank Wall Street Reform and Consumer Protection Act (Lei de Proteção do Consumidor e Reforma de Wall Street de Dodd-Frank) de 2010 aumenta ainda mais a necessidade de uma coleta e relatórios exatos de dados financeiros. Por meio do Escritório de Pesquisa Financeira e de agências membros, os dados serão coletados e analisados para identificar e monitorar riscos emergentes à economia e tornar essas informações públicas em relatórios periódicos e testemunhos anuais para o Congresso.

Educação

Com as instituições educacionais atuais - incluindo K-12, faculdades e universidades, solicitações de transcrição, aplicativos de auxílio financeiro e até mesmo notas podem ser encontrados on-line. Como certas escolas tem seus próprios centros médicos, elas também armazenam e compartilham informações médicas por via eletrônica. Esse ambiente interativo melhora a experiência do aluno e aumenta a produtividade da equipe, apesar de também tornar as escolas suscetíveis às ameaças de segurança.

Já que essas instituições gerenciam uma diversidade de informações, muitas regulamentações estaduais e federais se aplicam, incluindo a Computer Fraud and Abuse Act (Lei de Fraude de Computadores e Abuso), USA Patriot Act (Lei Patriota dos EUA), HIPAA e GLBA. No entanto, a regulamentação mais aplicável no setor de educação é a Family Education Rights and Privacy Act (Lei de Direitos de Educação e Privacidade da Família) (FERPA). Essa lei proíbe a divulgação de informações educacionais individualmente identificáveis sem a permissão escrita do aluno ou do tutor do aluno.

Com tantas medidas regulatórias e de conformidade exigindo uma resposta, a Xerox atende aos requisitos do governo federal, entre outros, como diretrizes. Ao desenvolver soluções que se esforçam para atender às normas de segurança mais rigorosas, podemos oferecer soluções extremamente seguras a todos os nossos clientes - independentemente do setor de negócio.

Visão Geral de Segurança

Na Xerox, nossa filosofia "Segurança = Proteção" direciona o desenvolvimento dos produtos, serviços e tecnologias infundidos com a segurança em cada nível.

A segurança é a frente e o centro no desenvolvimento de nossas "MFPs inteligentes." Como líder no desenvolvimento da tecnologia digital, a Xerox demonstra um comprometimento ao manter as informações digitais seguras e protegidas ao identificar possíveis vulnerabilidades e ao tratar delas de forma proativa para limitar os riscos. Os clientes respondem ao olhar para a Xerox como uma fornecedora confiável de soluções seguras que oferecem uma série de recursos de segurança modernos padronizados e opcionais.

Nossa Estratégia de Segurança

O desenvolvimento de produtos da Xerox® é orientado por um Processo Seguro de Desenvolvimento de Ciclo de Vida Útil, que leva as diretrizes do Software Assurance Maturity Model (Modelo de Maturidade em Garantia de Software) (SAMM) do Open Web Application Security Project (Projeto de Segurança de Aplicação em Rede Aberta) (OWASP) e do Instituto SANS em consideração. Isso envolve a definição de requisitos de segurança, avaliação de riscos, análise de vulnerabilidades e testes de penetração, bem como informações obtidas do OWASP e do Instituto SANS. Essa estratégia consiste em três pilares:

Recursos de Segurança de Última Geração

As impressoras e os dispositivos multifuncionais são sofisticados, com plataformas múltiplas de rede de sub-sistema e a Xerox oferece a mais ampla gama de funcionalidades de segurança no mercado, incluindo a criptografia, autenticação, autorização por usuário e auditoria.

Certificação

Os Critérios Comuns da ISO 15408 para Avaliação de Segurança da Tecnologia de Informações são a única norma internacionalmente reconhecida para certificação de segurança. A Xerox foi a primeira fabricante a buscar e obter certificações para dispositivos MFP "completos". Como cada elemento da plataforma multifuncional é um possível ponto de entrada, uma certificação de segurança significativa deve abranger todos os elementos, incluindo os sistemas operacionais, interface de rede, unidade(s) de disco rígido, servidor de Internet, intérprete(s) de PDL, interface de usuário de MFP, portas locais de hardware e sistema de fax.

Manutenção

Na Xerox, manter a segurança de nossa impressora e de dispositivos multifuncionais durante toda a vida útil exige uma diligência contínua para assegurar uma proteção constante contra brechas recentemente descobertas. Isso é realizado para:

- Garantir que as atualizações de software sejam emitidas continuamente
- Utilizar notificações de novos boletins de segurança com RSS feeds
- Responder às vulnerabilidades identificadas
- Fornecer diretrizes de instalação e de operação seguras
- Fornecer informações de Critérios Comuns
- Disponibilizar patches em www.xerox.com/security

O Modelo de Segurança da Xerox, em conjunto com o Ciclo de Vida Útil de Desenvolvimento Seguro, é um comprometimento que todos os recursos e funções do sistema, não apenas um ou dois, estejam seguros e protegidos.

Uma abordagem Abrangente à Segurança de Impressoras e MFPs

Pois, há anos, a Xerox reconheceu e adotou esse desvio na tecnologia e as necessidades evolutivas do local de trabalho. Oferecemos um conjunto abrangente de recursos de segurança para manter suas impressoras/MFPs e seus dados seguros. A Xerox protege cada parte da cadeia de dados, incluindo a impressão, cópia, digitalização, fax, downloads de arquivos e software do sistema. **Há quatro aspectos importantes em nossa abordagem multicamada.**

1. Prevenção de intrusão

Sua primeira e mais óbvia vulnerabilidade é a interface de usuário - que tem acesso físico à impressora e aos recursos. Usuário A autenticação é a base de garantia de acesso às impressoras e aos dispositivos multifuncionais da Xerox® para usuários locais e de rede autorizados. Uma vez autenticado, o usuário pode interagir com o dispositivo ou acessar aos dados do cliente, que estão sujeitos a restrições com base na função do usuário. As impressoras e MFPs da Xerox® utilizam uma diversidade de tecnologias para assegurar o acesso autorizado aos recursos e funções do dispositivo por meio de usuários e outros dispositivos de rede. Assim, tratamos de pontos menos óbvios de intrusão - o que é enviado para a impressora e como a Tecnologia Xerox® ConnectKey® interceptará os ataques de arquivos corrompidos e de um software malicioso. Nosso software de sistema, incluindo DLMs e weblets, é Digitalmente Assinado: quaisquer tentativas de instalação de versões infectadas e não assinadas resultarão na rejeição automática do arquivo. Os arquivos de impressão também serão excluídos se qualquer parte não for reconhecida como legítima.

AUTENTICAÇÃO DE REDE

Uma autenticação de rede permite que os usuários autenticam o dispositivo ao validar nomes de usuário e senhas antes do uso. Uma autenticação de rede autoriza um indivíduo a acessar a uma ou qualquer combinação dos serviços a seguir: impressão, cópia, fax, fax de servidor, reimpressão de trabalhos salvos, e-mail, fax por Internet e servidor de digitalização de fluxo de trabalho. Além disso, os usuários podem ser autorizados a acessar a uma ou qualquer combinação dos seguintes caminhos de máquina: serviços, status de trabalho ou status da máquina.

1. Prevenção de intrusão

Previna o acesso geral a dispositivos restritos com o acesso de usuário e um firewall interno na impressora.

2. Detecção de dispositivo

Fique atento na inicialização ou de acordo com a situação caso sejam detectadas alterações nocivas em sua impressora.

3. Proteção a documentos e dados

Mantenha as informações pessoais e confidenciais seguras com um disco rígido criptografado (AES 256 bits, FIPS validado para muitos produtos) e com a sobregravação de imagens.

4. Parcerias externas

Proteja seus dados e dispositivos contra intrusões maliciosas com a tecnologia de listas brancas da McAfee, a integração da Cisco® Identity Services Engine (ISE), órgãos de certificação e empresas de teste de compatibilidade.

MICROSOFT® ACTIVE DIRECTORY® SERVICES

O recurso Microsoft Active Directory Services (ADS) permite que o dispositivo autentique as contas de usuário em relação a um banco de dados centralizado de contas de usuário, em vez de utilizar exclusivamente o banco de dados de contas de usuário gerenciado localmente no dispositivo.

AUTENTICAÇÃO LDAP

A autenticação LDAP (BIND) é suportada para a autenticação com servidores LDAP para pesquisa e acesso de informações. Se um cliente LDAP conecta-se ao servidor, o estado padrão de autenticação da sessão é definido como anônimo. A operação BIND estabelece o estado de autenticação para uma sessão.

AUTENTICAÇÃO SMTP

Esse recurso valida a conta de e-mail do usuário e impede que usuários não autorizados enviem e-mail do dispositivo. Os Administradores de Sistema podem ativar TLS para todas as operações de envio e recebimento de SMTP.

Visão Geral de Segurança

AUTENTICAÇÃO POP3 ANTES DE SMTP

Como uma camada adicional de segurança, as MFPs Xerox® suportam a capacidade de os Administradores de Sistema habilitarem ou desabilitarem a autenticação POP3 antes do recurso SMTP. Uma autenticação POP3 antes de SMTP força um login bem sucedido em um servidor POP3 antes que possa enviar um e-mail via SMTP.

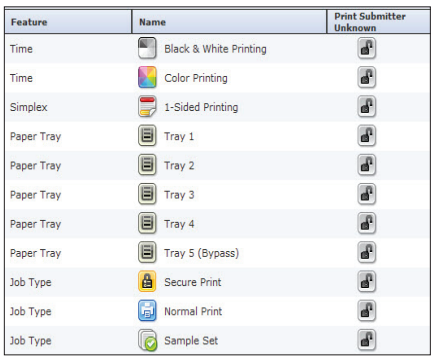
ROLE BASED ACCESS CONTROL (RBAC)

O recurso RBAC garante que usuários autenticados sejam atribuídos a uma função de usuário não conectado/usuário conectado, administrador de sistema ou administrador de contas. Cada função tem privilégios associados a níveis apropriados de acesso a recursos, tarefas e atributos de fila de impressão. Permite que os administradores escolham precisamente quais funções são permitidas para uma determinada função. Assim que um usuário se conecta ao dispositivo com o nome de usuário e a senha, o dispositivo pode determinar quais funções são atribuídas a esse usuário particular. As restrições são aplicadas com base nas funções atribuídas. Se toda uma função for restringida, ela poderá aparecer como bloqueada para o usuário após a autenticação ou não aparecerá de forma alguma.

Usuário não Conectado/ Usuário Conectado	Administrador de Sistema	Administrador de Contas

PRINT USER PERMISSIONS

Xerox user permissions provide the ability to restrict access to print features by user, by group, by time of day and by application. Users and groups can be set up with varying levels of access to print features. For example, limits can be set that allow colour print jobs only during certain hours of the day; Microsoft® PowerPoint® presentations automatically print in duplex mode; or Microsoft Outlook® emails always print in black and white.



Defina as permissões de cores do usuário e outras restrições de impressão com interfaces gráficas intuitivas.

AUTENTICAÇÃO DE CARTÃ O INTELIGENTE

Também conhecida como Autenticação de Cartão de Proximidade ou de Cartão Inteligente sem Contato, a Autenticação de Cartão Inteligente protege sua impressora e MFP contra o acesso local não autorizado. Os dispositivos da Xerox® suportam os principais cartões inteligentes (CAC/PIV, .NET, Rijkspas e outros cartões inteligentes e de proximidade), cerca de 30 tipos diferentes de leitores de cartões e 65 cartões de proximidade diferentes. Com a Autenticação de Cartão Inteligente, os usuários podem ser autenticados usando um sistema de identificação de dois fatores - posse do cartão e um número de identificação pessoal inserido na interface de usuário do dispositivo - para obter acesso aos recursos locais no dispositivo e na rede.

O Cartão de Acesso Comum/Verificação de Identidade Pessoal (CAC/PIV) é um cartão inteligente do Departamento de Defesa dos EUA emitido como uma identificação padrão para militares ativos, reservas, funcionários civis, outros funcionários não governamentais e pessoas elegíveis de empresas contratadas. O CAC/PIV pode ser utilizado para identificação geral, acesso controlado a edifícios e para autenticação de computadores pessoais, além de impressoras/MFPs e redes que os conectam.

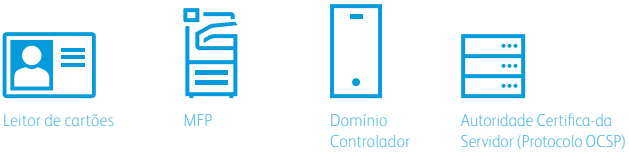
Visão Geral de Segurança

O CAC/PIV de 144k é uma versão do cartão inteligente. Os usuários podem ser autenticados usando uma identificação de dois fatores para obter acesso a serviços locais no dispositivo.

O CAC/PIV oferece os seguintes benefícios:

- Criptografia S/MIME para digitalizar para e-mail para si mesmo ou para qualquer destinatário no local da MFP ou no livro global de endereços LDAP
- Assinatura digital usando o Certificado de Assinatura de E-mail do cartão do usuário
- Preenchimento automático do campo "Para:" ao utilizar a função Digitalizar para E-mail da MFP
- Chave de certificado de até 2048 bits
- Transmissões de envio restritas para destinatários com certificados válidos
- Receber relatórios de confirmação de e-mail e manter registros de auditoria
- Assinatura única para Digitalizar para Página Principal e LDAP

Diagrama de configuração para Cartão de Acesso Comum (CAC)/Verificação de Identidade Pessoal (PIV)



1. Um cartão é inserido no leitor e é solicitado que o usuário digite um PIN na MFP.
2. A MFP verifica o servidor OCSP para confirmar se o certificado do cartão não expirou e então verifica a "Cadeia de Confiança" de volta para uma Autoridade Certificada conhecida.
3. O MFP inicia um diálogo criptografado de desafio/resposta entre o Controlador de Domínio e o Cartão de Acesso Comum. Se bem sucedido, o Controlador de Domínio emite um "Ticket Granting Ticket" e a autorização é concluída.
4. A autorização desbloqueia os recursos locais de MFP:
   - Digitalizar para e-mail
   - Cópia
   - Fax
   - Serviços Personalizados
   - Digitalização de fluxo de trabalho

SOFTWARE XEROX® PRINTSAFE

O Software Xerox® PrintSafe oferece uma autenticação de impressão segura para dados impressos na maioria das impressoras e MFPs, incluindo dispositivos da Xerox® e de outros fornecedores. Esse software está aberto para trabalhar com uma diversidade de leitores e cartões seguros padrão do setor.

Fluxos de trabalho de impressão seguros, convenientes e flexíveis

O usuário envia o documento.

Simplesmente ao pressionar "Imprimir", o documento é retido.

O usuário pode abordar qualquer impressora ou MFP em uma rede habilitada para aceitar um trabalho de PrintSafe e autenticar com uma simples passagem de cartão ou o PIN.

Assim que o usuário é autenticado, ele pode selecionar a liberação de um único trabalho ou todos os trabalhos seguros na impressora ou MFP.

O Software Xerox® PrintSafe não se limita aos dispositivos da Xerox®. Qualquer impressora ou MFP* registrada com o Software Xerox® PrintSafe pode emitir trabalhos PrintSafe.

Fluxos de trabalho flexíveis permitem que o usuário carregue um software no PC cliente para impressão direta ou sobre um servidor de impressão existente, que pode ser facilmente configurado para o Software Xerox® PrintSafe.

*Os dispositivos que não são da Xerox® exigem um acessório de rede; consulte o Representante de Vendas da Xerox para obter detalhes sobre fabricantes/modelos compatíveis.

ACESSO ÀS INTERFACES DE USUÁRIO DO DISPOSITIVO E DE USUÁRIO REMOTO

Os Administradores de Sistema podem bloquear o acesso às telas de configuração de dispositivos para usuários não autorizados a partir do painel de controle e do utilitário de Interface de Usuário Remoto em um esforço para proteger as informações de configuração.

2. Detecção de dispositivos

No improvável evento de seus dados e defesas de rede serem sobrepujados, a Tecnologia Xerox® ConnectKey® executará um teste abrangente de Verificação de Firmware na inicialização* ou quando ativado por usuários autorizados. Isso o alertará caso tenham sido detectadas alterações nocivas em sua impressora ou MFP.
Se quaisquer anomalias forem detectadas, o dispositivo emitirá uma mensagem aconselhando o usuário a recarregar o firmware. Nossas soluções integradas mais avançadas utilizam a tecnologia de Lista Branca** da McAfee® que monitora constantemente e previne automaticamente a execução de qualquer malware mal intencionado.

A Xerox, em parceria com a Cisco, implementou o nosso modelo de perfil no Cisco® Identity Services Engine (ISE). Essa integração com o Cisco Identity Services Engine (ISE) detecta automaticamente os dispositivos Xerox® na rede, classificando-os como impressoras para implantar e atender a políticas de segurança.

Para obter mais informações, consulte os documentos técnicos:

McAfee Whitelisting White Paper (somente em inglês):
http://www.office.xerox.com/latest/SECWP-03.PDF

Cisco ISE White Paper (somente em inglês):
http://www.office.xerox.com/latest/SECWP-04.PDF

*Impressoras e Impressoras Multifuncionais Xerox® VersaLink®
**Impressoras Multifuncionais Xerox® AltaLink® e i-Series

3. Proteção a documentos e dados

Proteção a Documentos

Mesmo quando todas as medidas de segurança necessárias de uma rede estão implementadas para proteger efetivamente dados críticos, já que eles percorrem os computadores de usuários e os dispositivos de impressão do escritório, as tecnologias de segurança também devem garantir que documentos impressos sensíveis sejam recebidos e visualizados apenas pelos destinatários pretendidos. A Xerox utiliza as tecnologias mais modernas para proteger sua emissão, seja imprimindo cópias impressas ou distribuindo documentos eletrônicos.

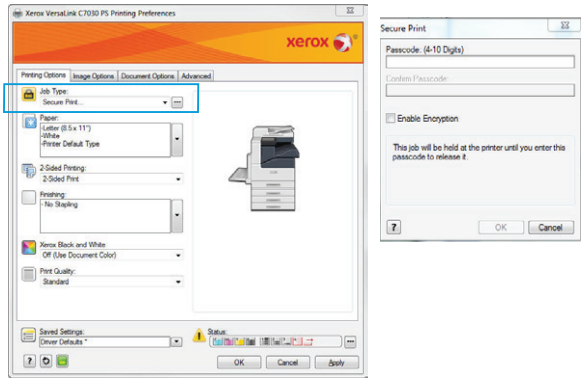
CRIPTOGRAFIA DE DADOS DE DIGITALIZAÇÃO

Os usuários de nossas MFPs inteligentes i-Series, VersaLink® e AltaLink® habilitadas para a Tecnologia Xerox® ConnectKey® também tem a opção de criptografar arquivos em PDF com uma senha ao utilizar o serviço Digitalizar para serviço de E-mail.

- Proteção externa ao firewall
  - Proteção de dados em um ambiente não seguro
  - Uso de protocolos padrão do setor como TLS e Secure PDF

CRIPTOGRAFIA DO FLUXO DE IMPRESSÃO

O Xerox® Global Print Driver® e certos drivers de produto suportam a criptografia de documentos ao enviar trabalhos de impressão do tipo impressão segura para dispositivos habilitados para a Tecnologia ConnectKey. As Impressoras Multifuncionais Xerox® AltaLink e i-Series também suportam a criptografia de documento para trabalhos de impressão periódicos. Não é necessário um hardware adicional para a criptografia de drivers de impressão.



IMPRESSÃO SEGURA

Os trabalhos de impressão sensíveis são retidos na impressora ou na MFP até que o dono do documento os libere ao digitar um PIN exclusivo por meio de uma interface de usuário do dispositivo. Isso garante que o destinatário de um documento esteja fisicamente presente ao imprimir informações confidenciais e possa remover imediatamente a saída da impressora ou MFP antes de a expor a outros usuários do dispositivo.

Uma impressão segura baseada em tecnologias de Cartão de Acesso Comum (CAC)/Verificação de Identidade Pessoal (PIV) associa o certificado de identidade do remetente do trabalho de impressão ao trabalho de impressão. No dispositivo, o usuário deve autenticar com o cartão CAC/PIV do usuário antes de o trabalho ser liberado.

PDF CRIPTOGRAFADO/PDF PROTEGIDO POR SENHA

Ao digitalizar um documento impresso para distribuição eletrônica via recurso Digitalizar para E-mail, as MFPs da Xerox® podem gerar PDFs criptografados por AES de 128 ou 256 bits ou PDFs protegidos por senha, que são então transmitidos de forma segura por uma rede e podem ser abertos, impressos ou alterados somente pelas pessoas que possuem a senha correta.

ENCAMINHAMENTO DE FAX PARA E-MAIL E REDE

As MFPs da Xerox® com capacidade de encaminhamento de fax podem direcionar os faxes recebidos para caixas de entrada de e-mail de destinatários específicos e/ou para um repositório de rede seguro, onde podem ser acessados apenas por observadores autorizados.

CONFIRMAÇÃO DE DESTINO DO FAX

Um remetente de fax recebe uma confirmação automática que o fax do remetente foi satisfatoriamente recebido pelo destinatário pretendido.

Visão Geral de Segurança

ASSINATURAS DIGITAIS

Uma assinatura digital é um esquema matemático que demonstra a autenticidade de uma mensagem ou um documento digital. Uma assinatura digital é utilizada para proteger o firmware do dispositivo contra a modificação não detectada e para fornecer uma autenticação da origem dos dados. Com cartões inteligentes, os e-mails podem ser digitalmente assinados com o certificado do remetente. Uma assinatura digital válida oferece ao destinatário a confiança para acredita que a mensagem foi criada por um remetente conhecido e que não foi alterada quando em trânsito.

MARCAS D'ÁGUA SEGURAS

Certas impressoras e MFPs da Xerox® tem um recurso de Marca d'água Segura que ajuda a prevenir que impressões originais com informações sensíveis sejam copiadas. Se um documento com uma marca d'água segura for copiado, a imagem de marca d'água ficará visível, tornando aparente que o documento contem informações sensíveis e que foi ilegalmente duplicado.

SELO DE USUÁRIO/HORA/DATA

Por meio de drivers da Xerox® , um selo de usuário/hora/data pode ser aplicado em qualquer documento impresso por um dispositivo em rede. Isso proporciona uma trilha de auditoria de quem o imprimi e em que momento.

FILTRAGEM DE ENDEREÇOS IP

A filtragem do Protocolo de Internet (IP) permite que os Administradores de Sistema criem regras para aceitar ou rejeitar informações que chegam no dispositivo MFP com base em endereços IP específicos ou em uma série de endereços. Isso proporciona ao Administrador de Sistema o controle sobre quem pode ou não acessar ao dispositivo.

Endereços IP registrados:
Disponível

Endereços IP não registrados:
Não Disponível

SECURE SOCKETS LAYER (SSL)/TRANSPORT LAYER SECURITY (TLS)

Muitas organizações tem obrigação de cumprir as políticas de segurança que exigem que todas as transações entre o cliente e a impressora ou a MFP sejam seguras via transações de Internet seguras, transferências de arquivo protegidas e e-mails seguros. Os dados transmitidos pela rede sem o uso de uma criptografia podem ser lidos por qualquer pessoa que vasculhar a rede. A Xerox diminui esse problema usando os protocolos Secure Sockets Layer/ Transport Layer Security para transmissões de dados em relação a certos protocolos como HTTPS e IPP.

CRIPTOGRAFIA IPSEC

Internet Protocol Security (IPsec) protege toda a comunicação na camada IP e é basicamente utilizado para criptografar os envios de impressão para o dispositivo. Criptografa todo o tráfego entre os Pontos A e B de forma que somente usuários confiáveis possam enviar e receber informações, que os dados não sejam alterados durante a transmissão e que somente usuários autorizados possam receber e ler as informações.

IPsec é concebido para fornecer os seguintes serviços de segurança:

- Criptografia de tráfego (impedindo que partes fortuitas leiam comunicações privadas)
- Validação de integridade (garantindo que o tráfego não tenha sido modificado ao longo do caminho)
- Autenticação de pares (garantindo que o tráfego seja de uma parte confiável)
- Anti-reprodução (proteção contra a reprodução da sessão segura)

ATIVAÇÃO/DESATIVAÇÃO DE PORTAS DE REDE

Com a capacidade de Ativação/Desativação de Portas de Rede, portas e serviços desnecessários podem ser desativados para evitar um acesso não autorizado ou mal intencionado. Em dispositivos desktop menores, essas opções podem ser ajustadas por meio do painel de controle ou do software de configuração baseado em PC. Em MFPs maiores, as ferramentas são fornecidas para definir níveis de segurança e desativar portas e serviços específicos.

Visão Geral de Segurança

CERTIFICADOS DIGITAIS

Os certificados digitais são documentos eletrônicos que utilizam uma assinatura digital para unir uma chave pública a uma identidade - informações como o nome de uma pessoa ou de uma organização, endereço etc. O certificado pode ser utilizado para verificar se uma chave pública pertence a um indivíduo.

As MFPs podem adicionar assinaturas que verificam a origem e a autenticidade de um documento em PDF. Se os destinatários abrirem um arquivo em PDF que foi salvo com uma assinatura digital, eles poderão visualizar as propriedades do documento para analisar o conteúdo da assinatura, incluindo a Autoridade Certificada, nome de produto do sistema, número de série e carimbo de hora/data de quando foi gerado. Se a assinatura for uma assinatura de dispositivo, também conterá o nome do dispositivo que gerou o documento ao mesmo tempo em que uma assinatura de usuário verifica a identidade do usuário autenticado que enviou ou salvou o documento.

As MFPs da Xerox® podem ser carregadas com um certificado assinado por uma autoridade certificada como a VeriSign ou o Administrador de Sistema pode gerar um certificado auto-assinado no dispositivo em si. Ao configurar um certificado em seu dispositivo, é possível habilitar uma criptografia para tipos específicos de fluxos de trabalho.

SNMPV3

Um Simple Network Management Protocol (SNMP) é um protocolo padrão de Internet para gerenciar dispositivos em redes IP, que fornece mais segurança ao proteger os dados contra uma violação, garantindo que o acesso seja limitado a usuários autorizados por meio de uma autenticação e de dados criptografados enviados através de uma rede.

Os dispositivos que tipicamente suportam SNMP incluem roteadores, switches, servidores, estações de trabalho, impressoras, modens e mais. É utilizado em grande parte nos sistemas de gerenciamento de rede para monitorar dispositivos conectados à rede em condições que garantem uma atenção administrativa. SNMP é um componente do Pacote de Protocolos de Internet conforme definido pela Internet Engineering Task Force (Força Tarefa de Engenharia de Internet) (IETF). O protocolo SNMPv3 fornece funções de segurança significativamente aprimoradas, incluindo a criptografia de mensagens e a autenticação.

STRINGS DE COMUNIDADE SNMP

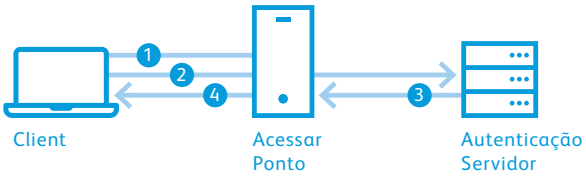
Dados MIB (Management Information Base (Base de Informações de Gerenciamento)) somente de leitura utilizam a string "pública" e as strings de comunidade de leitura/gravação definidas como "privadas." Por meio de strings de comunidade de leitura/gravação, um aplicativo pode alterar as definições de configuração do dispositivo usando as variáveis MIB. As strings de comunidade de leitura/gravação em dispositivos da Xerox® podem ser alteradas pelo Administrador de Sistema para aumentar a segurança ao gerenciar MFPs que utilizam SNMP.

AUTENTICAÇÃO 802.1X

IEEE 802.1X é um padrão IEEE para controle de acesso à rede baseado em portas (PNAC). Faz parte do grupo IEEE 802.1 de protocolo de redes de computadores. Ele fornece um mecanismo de autenticação para dispositivos que desejam conectar-se a uma rede de área local (LAN) ou a uma rede de área local sem fio (WLAN). A funcionalidade do protocolo IEEE 802.1X é suportada por muitos switches de Ethernet e pode impedir que sistemas convidados, nocivos ou não gerenciados que não conseguem realizar uma autenticação bem sucedida se conectem à sua rede.

Como funciona: Autenticação 802.1X

A autenticação 802.1X para LANs sem fio fornece uma autenticação centralizada baseada no servidor de usuários finais.



1. Um cliente envia uma mensagem "inicial" para um ponto de acesso, que solicita a identidade do cliente.
2. O cliente replica com um pacote de resposta contendo uma identidade e o ponto de acesso encaminha o pacote para um servidor de autenticação.
3. O servidor de autenticação envia um pacote de "aceitação" ao ponto de acesso.
4. O ponto de acesso coloca a porta cliente em um estado autorizado e o tráfego pode prosseguir.

Visão Geral de Segurança

O protocolo 802.1X tornou-se mais prevalente com o aumento da popularidade das redes sem fio. Muitas organizações bloqueiam o acesso de porta às redes internas usando esse protocolo. Isso impede que as informações passem na rede até que o dispositivo seja autenticado. De uma perspectiva de gestão de risco, isso permite que dispositivos sem fio e com fio comprovem quem são antes de qualquer informação passar pela rede. Se houver uma tentativa de acesso não autorizado, a porta ficará bloqueada até que o Administrador de Sistema a desbloqueie.

O Extensible Authentication Protocol (EAP) é uma estrutura de autenticação que realiza suas funções como parte da autenticação 802.1X. Os tipos de EAP atualmente suportados pelas MFPs da Xerox® são:

- EAP-MD5
- PEAPv0/EAP-MS-CHAPv2
- EAP-MS-CHAPv2
- EAP-TLS (produtos AltaLink® e i-Series)

FIREWALL

Um firewall é uma parte de um sistema de computador ou de rede desenvolvida para proteger o dispositivo contra ameaças externas e o acesso não autorizado ao mesmo tempo em que permite comunicações autorizadas. O dispositivo pode ser configurado para permitir ou negar transmissões de rede com base em um conjunto de regras e outros critérios. Os Administradores de Sistema podem restringir o acesso aos segmentos de rede, serviços e portas de dispositivos para protegê-los.

SEPARAÇÃO DE FAX E REDE

Separar a interface de fax do controlador de rede elimina o risco de segurança de invasão de uma rede de escritório por meio de uma linha de fax.

A MFP não fornece uma função para acessar à rede por meio da linha telefônica de fax. O protocolo Fax Class 1 utilizado na MFP responde apenas aos comandos de fax que permitem a troca de dados de fax. Os dados enviados do PC cliente somente podem ser dados de imagem compactados com informações de destino. Quaisquer dados diferentes de informações de imagem (como um vírus, código de segurança ou um código de controle que acessa diretamente à rede) são abandonados nessa etapa e a MFP finaliza imediatamente a chamada. Assim, não há um mecanismo pelo qual acessar ao sub-sistema de rede por meio da linha de fax.

Proteção de dados

A tecnologia transformou o modo como os funcionários realizam um negócio. Atualmente, os documentos assumem um formato não apenas nas tradicionais formas impressas, incluindo anotações manuscritas e versões de esboço das comunicações impressas, mas também nos formatos eletrônicos em desktops e no e-mail. Já que os funcionários criam, armazenam, compartilham e distribuem esses documentos eletrônicos de forma diferente da dos documentos impressos tradicionais, essas informações podem estar sujeitas a novos tipos de riscos. Para permanecer competitivo, uma empresa deve tratar dessas ameaças ao proteger os documentos e os sistemas de gerenciamento de documentos que contem o ativo mais valioso de uma empresa - o conhecimento.

Os sistemas de gerenciamento de informações e documentos enfrentam uma ampla gama de ameaças de segurança. Essas ameaças incluem atos de espionagem intencionais como invasão de computadores, furto, fraude e sabotagem, bem como atos involuntários como erro humano e desastres naturais. A segurança de informações é mais que uma proteção. Refere-se à garantia de acesso oportuno e disponibilidade de conteúdo do documento para melhorar o processo e o desempenho do negócio. Também está relacionada ao gerenciamento do conteúdo original e à conformidade com as regulamentações federais.

Desde a introdução dos primeiros produtos digitais, a Xerox reconhece o risco de dados retidos como sendo inadequadamente recuperados de uma armazenagem não volátil e cria recursos e contra medidas em nossos dispositivos para ajudar seus clientes a proteger seus dados.

CRIPTOGRAFIA DE DADOS DE IMAGEM

Usando a criptografia AES de 128 ou 256 bits, muitos dispositivos da Xerox® apresentam a criptografia de dados, incluindo dados de trabalho, imagem e cliente, que protege os dados em repouso de MFPs da Xerox® contra o acesso não autorizado. Com a criptografia de dados, o disco é particionado e somente a partição de dados do usuário é criptografada. As partições do sistema operacional não são nem podem ser criptografadas.

- Criptografia AES de 128 ou 256 bits, Federal Information Processing Standard (FIPS) 140-2 validados
- Todos os dados de imagem do usuário no disco rígido são criptografados

AES é um padrão de criptografia pequeno, rápido e difícil de decifrar e é adequado para uma ampla gama de dispositivos ou aplicativos. É a combinação moderna de segurança, desempenho, eficiência, facilidade de implementação e flexibilidade. Muitos dispositivos da Xerox® podem ser colocados no modo FIPS 140-2, o que significa que utilizarão somente algoritmos de criptografia certificados FIPS 140-2.

SOBREGRAVAÇÃO DE IMAGEM

Uma sobregravação de imagem apaga dados de disco rígido do dispositivo da Xerox® assim que esses não são mais necessários. Isso pode ser realizado automaticamente após a conclusão do processamento de cada trabalho, programado periodicamente e em caso de solicitação do Administrador de Sistema. Os dispositivos da Xerox® apresentam uma Sobregravação de Imagem Imediata e Sob Solicitação.

MEMÓRIAS VOLÁTIL E NÃO VOLÁTIL

Dentro de cada MFP da Xerox® , o controlador inclui uma memória volátil (RAM) e uma memória não volátil (disco rígido). Com a memória volátil, todos os dados de imagem são perdidos no desligamento ou na reinicialização do sistema. Com a memória não volátil, os dados de imagem são tipicamente armazenados na memória flash ou no disco rígido da MFP e são preservados até que sejam apagados.

À medida que as preocupações com a segurança de dados aumentam, os clientes querem saber como e onde os dados podem ser comprometidos. As Declarações de Volatilidade são documentos criados para ajudar a identificar onde os dados de imagem do cliente estão localizados nos dispositivos da Xerox® . Uma Declaração de Volatilidade descreve os locais, capacidades e conteúdo de dispositivos de memória volátil e não volátil dentro de certo dispositivo da Xerox® .

As Declarações de Volatilidade são criadas por muitos dispositivos da Xerox® para ajudar clientes cientes da segurança. Esses documentos podem ser obtidos ao entrar em contato com a equipe de suporte local da Xerox (para clientes existentes), um profissional de vendas da Xerox (para novos clientes) ou podem ser acessados em www.xerox.com/security.

FAX SEGURO

Faxes recebidos sensíveis são retidos até que o Administrador de Sistema os libere.

PROTEÇÃO DA SENHA PARA O RECURSO DIGITALIZAR PARA CAIXA DE CORREIO

Ao utilizar o recurso Digitalizar para Caixa de Correio de uma MFP, a caixa de correio designada pode ser protegida por senha para garantir que somente pessoas autorizadas possam acessar às digitalizações armazenadas nela. A segurança do recurso Digitalizar para Caixa de Correio é intensificada pela criptografia da partição de dados de imagem do disco rígido.

S/MIME PARA O RECURSO DIGITALIZAR PARA E-MAIL

O protocolo Secure/Multipurpose Internet Mail Extensions (S/MIME) fornece os seguintes serviços de segurança criptográficos para o recurso Digitalizar para E-mail: autenticação, integridade de mensagem e não repúdio de origem (usando assinaturas digitais), e segurança de privacidade e de dados (usando a criptografia).

Na comunicação S/MIME, ao enviar dados para a rede, uma assinatura é adicionada em cada mensagem de correio baseada nas informações de certificado retidas no dispositivo. A criptografia é realizada ao enviar dados com base no certificado correspondente a cada endereço designado da mensagem de correio. O certificado é verificado quando as informações da transmissão de dados são inseridas e quando os dados devem ser enviados. A comunicação S/MIME é realizada apenas quando a validade do certificado é confirmada.

CRIPTOGRAFIA PARA O RECURSO DIGITALIZAR PARA E-MAIL

A criptografia de e-mail via Autenticação de Cartão Inteligente permite que os usuários enviem até 100 e-mails criptografados para muitos destinatários no diretório LDAP de uma organização usando as chaves públicas dos destinatários. Muitas MFPs da Xerox® usando a Autenticação de Cartão Inteligente também proporcionam a capacidade de assinar digitalmente os e-mails. Os usuários podem visualizar os certificados de possíveis destinatários antes de enviar um e-mail. A MFP não permite o envio para usuários sem um certificado de criptografia. Além disso, a MFP registra todos os registros de e-mails enviados com uma opção de o administrador receber relatórios de confirmação.

OCULTAÇÃO DO REGISTRO DE TRABALHO

A função padrão de Ocultação do Registro de Trabalho garante que os trabalhos processados pelo dispositivo fiquem invisíveis para um usuário local ou por meio da Interface de Usuário Remoto. As informações de Registro de Trabalho, embora ocultas, continuam acessíveis pelo Administrador de Sistema, que pode imprimir o Registro de Trabalho para mostrar o uso de cópias, faxes, impressões e digitalizações no dispositivo.

OFERTA DE RETENÇÃO DO DISCO RÍGIDO

A Xerox fornece uma Oferta de Retenção do Disco Rígido para dispositivos da Xerox® àqueles clientes que se preocupam que os dados de imagem no disco rígido sejam mais sensíveis ou até mesmo classificados. Esse serviço possibilita que um cliente, por meio de uma taxa, retenha o disco(s) rígido e limpe-o ou destrua-o de forma que sinta que manterá os dados de imagem seguros.

VALIDAÇÃO DOS DADOS DE SERVIÇOS REMOTOS

Muitos dispositivos da Xerox® obtém o consentimento de compra do cliente antes de transmitir Informações Pessoais Identificáveis (PII) e Informações Identificáveis do Cliente (CII) via Serviços Remotos para a Xerox.

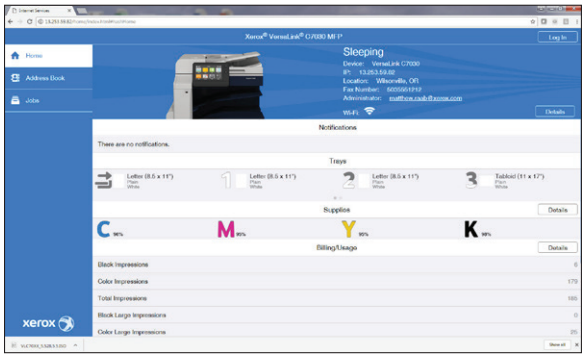
SENHAS POSTSCRIPT

Outra área de risco relacionada à impressão é ao imprimir com a linguagem de descrição da página (PDL) da Adobe® PostScript®. PostScript inclui comandos que permitem que trabalhos de impressão alterem os comportamentos padrão do dispositivo, o que poderia expor o equipamento. Como a linguagem de PostScript inclui utilitários muito poderosos que poderiam ser utilizados para comprometer a segurança de um dispositivo, os administradores podem configurar o dispositivo para que os trabalhos de PostScript tenham que incluir uma senha para mudar os comportamentos padrão do dispositivo. Os privilégios básicos do intérprete de PostScript dentro do controlador são limitados pelo projeto, mas os administradores tem certa capacidade de gerenciar a operação do sub-sistema de PostScript.

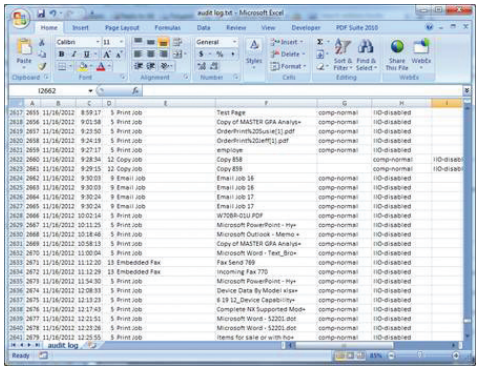
REGISTRO DE AUDITORIA

As MFPs da Xerox® e muitas de nossas impressoras podem manter Registros de Auditoria para rastrear a atividade por meio de documento, usuário e função. O Registro de Auditoria está ativado por padrão nos dispositivos mais novos e pode ser habilitado ou desabilitado pelo Administrador de Sistema. Ele pode rastrear o acesso e a tentativa de acesso ao dispositivo e transmitir registros de auditoria para um sistema SIEM ou para um servidor de registro de auditoria. Um exemplo de uma entrada de Registro de Auditoria: “User xx logged into the Xerox® AltaLink® MFP at 12:48 AM and faxed 10 pages to 888.123.1234. (Usuário xx conectou-se à MFP Xerox® AltaLink® às 12h48 e enviou um fax de 10 páginas para 888.123.1234.)”

Para impressoras multifuncionais habilitadas para a Tecnologia Xerox® ConnectKey®, o Registro de Auditoria pode ser enviado de forma automática e segura para um sistema SIEM para fornecer um monitoramento contínuo da MFP.



A interface de Registro de Auditoria é acessada da estação de trabalho de um Administrador de Sistema usando qualquer navegador de Internet padrão.



O registro pode ser então exportado em um arquivo .txt e aberto no Microsoft® Excel®.

4. Parcerias Externas

A Xerox trabalha com organizações de testes de conformidade e com líderes do setor de segurança como a McAfee para envolver as normas globais e o know-how deles com os nossos. Os recursos de proteção contra malwares a seguir estão disponíveis nas MFPs habilitadas para a Tecnologia Xerox® ConnectKey® (impressoras multifuncionais Xerox® AltaLink® e i-Series).

CONTROLE INTEGRADO DA MCAFEE® – AUMENTO DE SEGURANÇA

As MFPs da Xerox® que integram a Tecnologia Xerox® ConnectKey® incluem a incorporação de Controle Integrado da McAfee fornecido pela Intel® Security, resultando na primeira linha de impressoras multifuncionais do setor que se protegem contra possíveis ameaças externas. A tecnologia de lista branca da McAfee detecta tentativas não autorizadas de leitura, gravação ou adição de arquivos e diretórios protegidos e envia alertas caso ocorram. Além disso, a integração perfeita com o software Xerox® CentreWare® Web, o conjunto de ferramentas Xerox® MPS e o McAfee ePolicy Orchestrator® (McAfee ePO™) permitem o monitoramento a partir do console preferido.

CONTROLE INTEGRADO DA MCAFEE – CONTROLE DE INTEGRIDADE

O Controle de Integridade gera capacidades de Aumento de Segurança e impede que novos arquivos sejam executados de qualquer local por meios não confiáveis. Somente um software aprovado tem permissão de executar, o que previne ataques gerais e visados. Útil especialmente para implementações de segurança em grandes empresas, a Xerox e a Intel Security oferecem uma tecnologia de lista branca que garante que a única função executada nesses dispositivos seja os serviços que você deseja entregar. Essa mesma tecnologia é usada para proteger servidores, ATMs, terminais de ponto de vendas e dispositivos incorporados como, por exemplo, dispositivos móveis.

EPOLICY ORCHESTRATOR (EPO) DA MCAFEE

O ePolicy Orchestrator (ePO) da McAfee é uma ferramenta de software de gestão de segurança que facilita a gestão de risco e de conformidade de organizações de todos os tamanhos. É apresentada aos usuários com painéis do tipo "arrastar-soltar" que fornecem uma inteligência de segurança nos endpoints - dados, dispositivos móveis e redes - para percepção imediata e tempos de resposta mais rápidos. O ePolicy alavanca infraestruturas de TI existentes ao conectar o gerenciamento de soluções de segurança da McAfee e de terceiros ao LDAP, operações de TI e ferramentas de gerenciamento de configuração.

Para a comprovação independente de terceiros, nas quais atingimos os níveis principais de conformidade, os órgãos de certificação como Critérios Comuns (ISO/IEC 15408) e FIPS 140-2 medem nosso desempenho em comparação com as normas internacionais. Eles nos reconhecem por nossa abordagem abrangente de segurança de impressoras.

INTEGRAÇÃO DA CISCO® IDENTITY SERVICES ENGINE (ISE)

Gerencia e implementa de forma centralizada as políticas de segurança de impressoras. Nossa parceria com a Cisco fornece as maiores capacidades de detecção de dispositivos de impressão Xerox®, resultando na aplicação mais detalhada da política de segurança. Os dispositivos Xerox® são automaticamente reconhecidos e classificados por Cisco ISE, permitindo o controle de acesso de rede e a redução de despesas gerais pela eliminação da entrada manual de atributos da impressora. Nosso perfil de impressoras com Cisco ISE impede as tentativas de falsificação por sabotadores para obter acesso irrestrito a sistemas confidenciais. A integração do dispositivo de impressão Xerox® com Cisco ISE fornece uma abordagem operacionalmente eficiente para atingir os objetivos da política de segurança.

Conformidade regulatória e com as políticas

Impressoras e MFPs modernas são o foco de conformidade devido aos dados pessoais e sensíveis que elas acessam, armazenam e comunicam. Uma não conformidade pode conduzir à perda de oportunidades de negócio, perda de clientes existentes ou até mesmo uma ação judicial. Os níveis de conformidade exigida variam de acordo com o país e o mercado vertical.

A Health Insurance Portability and Accountability Act (Lei de Portabilidade e Responsabilidade do Seguro de Saúde) (HIPAA) nos EUA e a Data Protection Act (Lei de Proteção de Dados) no Reino Unido são exemplos de normas que podem ter que ser atendidas para que o negócio continue de forma legal.

A Certificação de Critérios Comuns é uma norma de segurança internacionalmente reconhecida que atende às especificações do Departamento de Defesa dos EUA.

Com os recursos de segurança líderes no setor e uma abordagem flexível de configuração e de implantação, os dispositivos da Xerox® podem estar conformes com qualquer norma e ter os controles disponíveis para atender a qualquer necessidade.

Os sistemas, software e serviços da Xerox® estão em conformidade com as normas reconhecidas do setor e as mais recentes regulamentações de segurança do governo. Nossos produtos oferecem recursos que permitem que nossos clientes atendam a essas normas. As normas a seguir são exemplos:

- Payment Card Industry (PCI) Data Security Standards Version 3.0
- Sarbanes-Oxley
- Basel II Framework
- The Health Insurance Portability and Accountability Act (HIPAA)
- E-Privacy Directive (2002/58/EC)
- Gramm-Leach-Bliley Act
- Family Educational Rights and Privacy Act
- The Health Information Technology for Economic and Clinical Health Act
- Dodd-Frank Wall Street Reform and Consumer Protection Act
- ISO-15408 Common Criteria for Information Technology Security Evaluation
- ISO-27001 Information Security Management System Standards
- Control Objectives for Information and Related Technology
- Statement on Auditing Standards No. 70
- NIST 800-53, adopted by Federal Government and DOD in 2014
- Federal Risk and Authorisation Program (FedRAMP)

Avaliação de segurança do produto

A segurança de um documento significa tranquilidade. Um dos diferenciais da linha de produtos da Xerox® é o compromisso com a segurança das informações. Nossos sistemas, software e serviços abrangem e estão em conformidade com as normas reconhecidas do setor e as mais recentes regulamentações de segurança do governo.

Certificação de Critérios Comuns

A Certificação de Critérios Comuns fornece uma validação independente e objetiva de terceiros da confiabilidade, qualidade e fiabilidade dos produtos de TI. É uma norma nas quais os clientes podem confiar para ajudá-los a tomar decisões informadas sobre as aquisições de TI. Os Critérios Comuns definem metas específicas de garantia de informações, incluindo níveis restritos de integridade, confidencialidade, disponibilidade de sistemas e dados, responsabilidade em nível individual e garantia que todas as metas serão atendidas. A Certificação de Critérios Comuns é uma exigência dos dispositivos de hardware e de software utilizados pelo governo federal em sistemas de segurança nacional.

Como obter a Certificação de Critérios Comuns

A Certificação de Critérios Comuns é um processo rigoroso que inclui testes de produto por um laboratório terceirizado que foi credenciado pelo National Voluntary Laboratory Accreditation Program (Programa Nacional de Credenciamento de Laboratórios Voluntários) (NVLAP) para realizar a avaliação de produtos em relação às exigências de segurança. Os produtos são testados quanto às exigências funcionais de segurança com base em Níveis de Garantia de Avaliação (EALs) predefinidos ou às exigências de garantia especializadas.

Para serviços de saúde, financeiros e de outros setores, a necessidade de segurança não é menos importante. Seja protegendo a privacidade dos clientes ou os ativos intelectuais e financeiros, a garantia que redes, discos rígidos e linhas telefônicos estejam seguras e protegidas contra hackers, vírus e outras atividades mal intencionadas é crítica. A Certificação de Critérios Comuns, embora não seja uma exigência externa ao governo federal, pode fornecer uma validação independente.

Com aproximadamente 150 dispositivos tendo concluído o processo de certificação, a Xerox tem um dos maiores números de MFPs certificadas para os Critérios Comuns. Além disso, a Xerox foi a primeira fabricante a certificar todo o dispositivo e a Xerox é a única fabricante a sempre certificar todo o dispositivo.

Visite www.xerox.com/information-security/common-criteria-certified para conhecer quais MFPs da Xerox® conseguiram a Certificação de Critérios Comuns.

Avaliação e Atenuação de Riscos

Segurança proativa para ameaças emergentes

Oferecera você os produtos e as soluções mais seguros do mercado atual é apenas uma parte de nossa história. Nossos cientistas e engenheiros trabalham duro no desenvolvimento da próxima geração de tecnologias de segurança inovadoras para combater ameaças futuras e manter seus documentos seguros: micro-impressão, segurança de impressão por fluorescência e infravermelho, Xerox® Glossmark® e tecnologia de marca de impressão Correlation Marks, apenas para citar algumas. Para obter mais informações sobre essas tecnologias, visite www.xerox.com/security.

Outras coisas que a Xerox faz:

Manter-se atenta aos riscos mais modernos

Monitoramos atentamente os centros de coordenação de vulnerabilidades para nos manter atualizados com as últimas informações - para que você não precise fazer isso.

Emitir boletins de segurança

Somos proativos no fornecimento de patches e atualizações de segurança quando necessário, mantendo seus equipamentos atualizados e seus dados seguros.

Distribuir RSS feeds

Atualizações minuto a minuto são automaticamente distribuídas aos leitores de RSS feed dos clientes.

Fornecer a você uma riqueza de informações

Se deseja aprender mais por conta própria, oferecemos uma biblioteca em constante expansão de artigos, periódicos e guias sobre segurança.

Visite www.xerox.com/security para acessar ao nosso leque completo de recursos de segurança.

Além de nossos próprios testes internos extensivos, a Xerox monitora regularmente os centros de coordenação de vulnerabilidades disponibilizados por órgãos e recursos como US-CERT e o relatório de Atualizações de Patch Críticas da Oracle®; Boletins de Segurança da Microsoft®, para vulnerabilidades de diversos softwares e sistemas operacionais; e bugtraq, SANS.org e secunia.com para vulnerabilidades de fonte aberta. Um robusto programa de testes internos de segurança também está incluído, o qual envolve a análise de vulnerabilidades e testes de penetração para fornecer patches totalmente testados. Visite www.xerox.com/security para ler a Política de Gerenciamento e de Divulgação de Vulnerabilidades.

Boletins de segurança e implantação de patches

Os desenvolvedores da Xerox obedecem a um ciclo de vida útil de desenvolvimento de segurança formal que gerencia problemas de segurança por meio da identificação, análise, priorização, codificação e testes. Esforçamo-nos para fornecer patches tão regularmente quanto possível com base na natureza, origem e gravidade da vulnerabilidade. Dependendo da gravidade da vulnerabilidade, do tamanho do patch e do produto, o patch pode ser implantado separadamente ou assumir a forma de uma nova versão de software para esse produto.

Dependendo de qual produto da Xerox® exige um patch, os clientes podem fazer o download de patches de segurança em www.xerox.com/security. Para outros produtos da Xerox®, o patch de segurança será disponibilizado como parte de uma nova versão de liberação de software do sistema. Você pode registrar-se para receber os boletins periodicamente. Nos EUA, os clientes devem assinar o RSS feed de segurança. Fora dos EUA, entre em contato com o centro de suporte local da Xerox.

No site de Internet www.xerox.com/security, você tem acesso a atualizações de informações oportunas e a recursos importantes:

- Boletins de segurança
- RSS Feed: Obter boletins de segurança
- Perguntas mais frequentes sobre a segurança do produto da Xerox®
- Artigos de divulgação de garantia de informações
- Produtos certificados para Critérios Comuns
- Política de gerenciamento e de divulgação de vulnerabilidades
- Orientação sobre segurança do produto
- Artigos e periódicos
- Declarações de volatilidade
- Tabela de pesquisa rápida de liberação de software
- Guia FTC para copiadoras digitais e MFPs

www.xerox.com/security é seu portal para um leque diverso de informações e atualizações relacionadas à segurança, incluindo boletins, artigos, patches e muito mais.

Práticas de segurança de fabricação e do fornecedor

A Xerox e nossos principais parceiros fabricantes são membros da Electronic Industry Citizenship Coalition (Coligação Civil da Indústria Eletrônica) (http://www.eicc.info).
Ao se inscrever no Código de Conduta da EICC, a Xerox e outras empresas demonstram que elas mantem uma supervisão rigorosa dos processos de fabricação.

Além disso, a Xerox tem relações contratuais com seus fornecedores primários e secundários que permitem que a Xerox realize auditorias no local para garantir a integridade do processo em relação ao nível de componente.

A Xerox também é membro da U.S. Customs Agency Trade Partnership Against Terrorism (Parceria Comercial de Agências Aduaneiras dos EUA contra o Terrorismo). Essa iniciativa está focada na segurança da cadeia de suprimentos. Exemplos de práticas adotadas pela Xerox nesse programa são aquelas implementadas para combater furto ou sequestro. Na América do Norte, todas as carretas que fazem o percurso entre a fábrica e os centros de distribuição de produtos (PDCs) e entre os PDCs e os Centros de Logística de Transporte (CLCs) são lacradas no ponto de origem. Todos os caminhões tem localizadores GPS e são continuamente monitorados.

Devoluções e Disposições de Produtos

Oferta de retenção do disco rígido para produtos da Xerox®

A Xerox fornece uma Oferta de Retenção do Disco Rígido para permitir que clientes nos Estados Unidos, por meio de uma taxa, retenham o disco rígido em produtos alugados da Xerox®. Esse serviço pode ser necessário para clientes com dados muito sensíveis, talvez até classificados, ou com políticas internas ou normas regulatórias que obrigam processos específicos de disposição para discos rígidos.

Na solicitação dessa oferta de serviço, um técnico de manutenção da Xerox se deslocará até o local do cliente, removerá o disco rígido e o fornecerá 'na forma em que está' para um representante do cliente. Nesse momento, a Xerox não fornece serviços de limpeza ou de destruição do disco rígido no local do cliente. Os clientes terão que tomar providências para a disposição final do disco rígido físico recebido do técnico.

Para determinar se seu produto da Xerox® contem um disco rígido ou analisar os recursos de segurança disponíveis para proteger dados nos discos rígidos, visite www.xerox.com/harddrive.

Para obter mais detalhes sobre esse programa, entre em contato com um representante de vendas da Xerox ou visite www.xerox.com/security em Security Resources (Recursos de Segurança) na seção Articles and White Papers (Artigos e Periódicos).

Além disso, basicamente todas as novas impressoras e MFPs da Xerox® vem padronizadas com a criptografia de disco AES de 256 bits, bem como a sobregravação de dados de imagem de passo triplo para garantir que os dados de nossos clientes fiquem protegidos a partir do dia um do novo equipamento.

Resumo

A segurança de rede e dos dados está entre os muitos desafios que os negócios enfrentam diariamente. E, como as impressoras e MFPs atuais servem como dispositivos de rede críticos para o negócio que recebem e enviam dados importantes por meio de uma série de funções, garantir uma segurança abrangente é primordial.

O sistema completo de uma MFP. juntamente com um software de gerenciamento de dispositivos na rede, deve ser avaliado e certificado para que a Segurança de Informações e todos os funcionários de uma organização tenham certeza de que os documentos e a rede estejam seguros e protegidos contra predadores de informações - ou até mesmo de violações de segurança interna. A esse respeito, as MFPs da Xerox® lideram o setor. Nossa abordagem abrangente, baseada em uma segurança fundamental, funcional, avançada e útil, é essencial para a proteção dos ativos de informações dos negócios atuais.

Ao reconhecer isso, a Xerox continua a desenvolver e projetar todos os seus produtos para garantir o mais alto nível possível de segurança em todos os possíveis pontos de vulnerabilidade. Estamos comprometidos com a proteção de seus dados de forma que você possa focar as buscas e as atividades que tornam seu negócio ou organização tão bem sucedidas quanto possível.

Para obter mais informações sobre as muitas vantagens de segurança oferecidas pela Xerox, visite www.xerox.com/security.

Lista de Verificação de Segurança

Os gerentes de segurança de TI já estão sobrecarregados com o gerenciamento das exigências de segurança. Os pequenos negócios devem depender de sistemas eficazes e de um software de segurança para fazer grande parte do trabalho para eles. A última coisa que você e sua equipe precisam é de mais atividade interativa ou de intervenções manuais para monitorar e manter cada dispositivo e fluxo de dados atualizados em seu ambiente, incluindo suas MFPs e impressoras.

Um plano abrangente de segurança de rede deve incluir três pontos enfáticos com uma estratégia implementada para cada um deles para garantir que você tenha um plano que funciona.

1. Dispositivos "sem as mãos, auto protegidos" que são resilientes a novos ataques
2. Conformidade com a maioria das normas e regulamentações de segurança atualizadas
3. Visibilidade completa na rede

Novo padrão de segurança para uma nova era

- A segurança não pode ser uma consideração posterior.
- As informações são uma propriedade intelectual cada vez mais valiosa.
- Os firewalls não são suficientes; as políticas de segurança devem ser holísticas e onipresentes.
- A proteção de dispositivos integrados é agora uma parte integral do imperativo de segurança moderno.

A Xerox oferece uma segurança abrangente e multicamada que é fácil de implantar e gerenciar, além de ajudar a manter seu negócio em conformidade com as normas industriais e governamentais. A tecnologia da Xerox® é testada e validada para proteger contra o acesso, dados e identidade não autorizados.

Ao comparar as MFPs da Xerox® com os produtos de outros fabricantes, utilize a lista de verificação a seguir para determinar se os dispositivos da concorrência fornecem o mesmo nível de segurança final que a oferecida pela Xerox.

		Concorrente		
	Xerox	1	2	3
Filtragem de endereços IP/MAC	✓			
Criptografia IPsec	✓			
IPv6	✓			
Autenticação 802.1X	✓			
Impressão protegida	✓			
Criptografia do recurso Digitalizar para E-mail	✓			
PDF criptografado/PDF protegido por senha	✓			
Assinaturas digitais	✓			
AES de 256 bits	✓			
Criptografia do disco rígido	✓			
Sobrescrever imagem	✓			
Fax protegido	✓			
Bloqueio de portas	✓			
Proteção da senha do recurso Digitalizar para Caixa de Correio	✓			
Oferta de retenção do disco rígido	✓			
Restrições de impressão	✓			
Registro de auditoria	✓			
Controle de acesso baseado em função	✓			
Autenticação de cartão inteligente	✓			
Cartão de acesso comum/ Verificação de identidade pessoal	✓			
Permissões de Usuários	✓			
Certificação de Critério Comuns do "Sistema Completo"	✓			
Integração com as ferramentas padrão de gerencia-mento de rede	✓			
Atualizações de segurança via RSS Feeds	✓			
Proteção integrada da McAfee fornecida pela Intel® Security	✓			
Controle de Integri-dade da McAfee®	✓			
Integração de McAfee® ePolicy Orches-trator®	✓			
Integração da Cisco® Identity Services Engine (ISE)	✓			

Para saber mais, visite www.xerox.com.

05/18 BR21699 SECGD-01PC