Visão Geral de Segurança da Ricoh

RICOH
imagine. change.

Quer saber se seus dispositivos estão vulneráveis?

As ameaças à segurança não estão mais limitadas a computadores, servidores ou redes pessoais. Os equipamentos de impressão -- até mesmo impressoras a laser básicas -- precisam de medidas de proteção contra uma gama diversificada de ameaças. À medida que as impressoras multifuncionais se transformaram em verdadeiros terminais de informação, elas se tornaram os principais ativos de TI por si só. A capacidade de computação do que tradicionalmente é classificado como “Impressoras/Copiadoras” cresceu, juntamente com o potencial de ameaças , que podem incluir:

- Acesso criminoso através de redes
- Interceptação e alteração de informações pela rede
- Vazamento de informações da mídia de armazenamento HD
- Acesso não autorizado através do painel de operação de um dispositivo
- Acesso inadequado através de linhas telefônicas de fax
- Vazamento de informações via cópia impressa
- Violações da política de segurança devido à negligência

Simplesmente esperar que você não seja atingido não é a resposta. Tecnologia superior, compromisso e conhecimento são essenciais. A Ricoh pode ajudá-lo a lidar com possíveis problemas causados por vulnerabilidades em seus dispositivos, os dados que eles processam e as redes às quais eles se conectam.

O método de camadas da Ricoh

No coração do nosso modelo de segurança está o próprio equipamento. O Sistema Operacional (SO) no núcleo dos nossos atuais equipamentos projetados pela Ricoh foi especificamente projetado e reforçado pela Ricoh para nossos equipamentos e muitos dos nossos modelos de equipamentos MFP são certificados pelo IEEE 2600.2 Standard Protection Profile for Hardcopy Devices, ou Perfil de Proteção Padrão IEEE 2600.2 para Equipamentos de Impressos. A criptografia do disco rígido e a segurança por sobregravação do disco vem por padrão em alguns de nossos equipamentos e ajudam a garantir que os dados processados permaneçam confidenciais. A Ricoh trabalhou arduamente para garantir que a segurança do equipamento não seja enfraquecida pela introdução do Painel de Operação Inteligente (SOP) — que também usa um SO exclusivo da Ricoh. A Ricoh não instala componentes desnecessários e o acesso ao root não está disponível. Os aplicativos embutidos devem passar no teste de Compatibilidade da Ricoh e ser assinados digitalmente antes que possam ser executados no Painel de Operação Inteligente. A Ricoh está comprometida em trabalhar com nossos clientes para fornecer produtos e serviços que estejam em sincronia com suas políticas de segurança de TI e de rede. Usamos várias técnicas para ajudar a proteger contra ameaças ''man-in-the-middle'' ou ''trabalho interno''— incluindo criptografia ponta a ponta de arquivos de impressão e digitalização, criptografia de dados em servidores e separação de funções de administrador. Uma gama de serviços de segurança líder de mercado — incluindo consultoria e gestão de serviços — envolve as outras camadas para monitorar, otimizar e gerenciar com eficácia a segurança de documentos e informações .

Aplicativos Embutidos

- Fornecer recursos estendidos
- Testados, Compatibilidade certificada e assinados digitalmente pela Ricoh
- Exemplos: Autenticação, impressão segura, criptografia, fluxo de trabalho

Rede (transporte e camada de ligação de dados)

- Aplicar e cumprir as medidas e políticas de segurança de rede do cliente
- Criptografia de ponta a ponta de arquivos de impressão e digitalização para proteger contra o "man-in-the-middle"

Interface de usuário (Painel de Operação Inteligente)

- A Ricoh endureceu o SO com base no uso de módulos específicos
- Componentes e ferramentas desnecessárias, com problemas conhecidos, não são instaladas
- Kernel e serviços são personalizados
- O Acesso ao root não está disponível

Segurança do Servidor

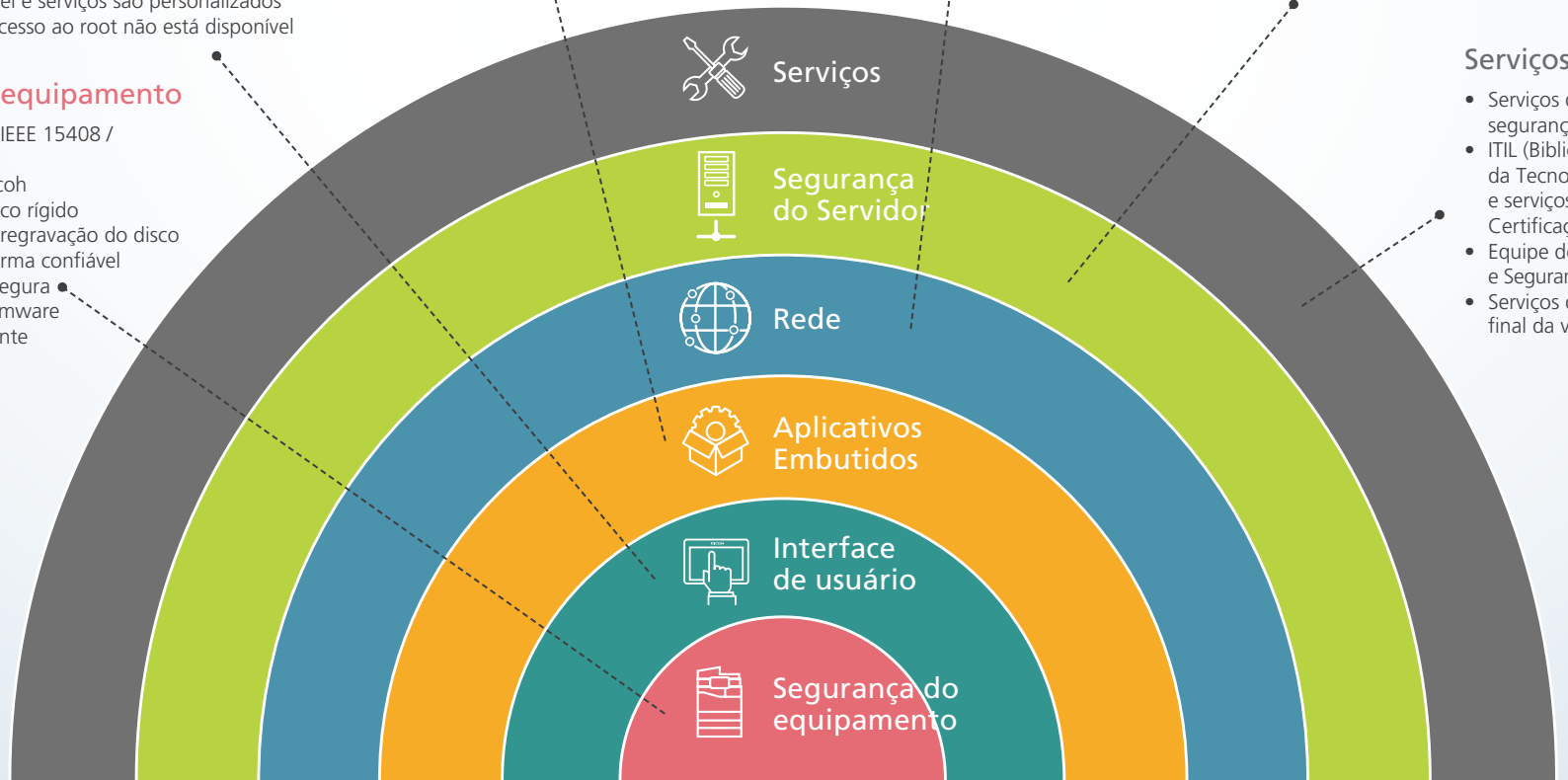
- Aplicar e cumprir as medidas e políticas de segurança de rede do cliente
- Arquivos criptografados
- Separação das funções do administrador

Segurança do equipamento

- Certificação ISO / IEEE 15408 / IEEE 2600.2
- SO exclusivo da Ricoh
- Criptografia do disco rígido
- Segurança por sobregravação do disco
- Módulo de plataforma confiável para inicialização segura
- Atualizações de firmware assinado digitalmente

Serviços

- Serviços de otimização da segurança
- ITIL (Biblioteca da Infraestrutura da Tecnologia da Informação) e serviços e processos com Certificação ISO
- Equipe de Resposta a Incidentes e Segurança
- Serviços de descarte ao final da vida útil



Segurança está no nosso DNA

Os equipamentos da Ricoh são projetados, fabricados e implementados com segurança como um requisito básico. O pensamento focado na segurança está presente desde o início, desde o design do produto até as vendas. Está em nosso DNA, informando nossa filosofia de design e nosso compromisso de trabalhar continuamente para oferecer suporte aos nossos clientes com soluções conforme as ameaças evoluem.

Governança da informação e cibersegurança

O conhecimento, capacidades e serviços da Ricoh também se estendem além do equipamento (consulte a página 33).

Segurança do equipamento

Nossos recursos de segurança do equipamento podem ajudar a proteger equipamentos multifuncionais e impressoras a laser contra ameaças potenciais, incluindo comprometimento de firmware, unidade de disco rígido de um equipamento, memória não volátil, portas de rede abertas e sistema de autenticação. A Ricoh obteve certificação para uma ampla gama de produtos com base nos Critérios Comuns (ISO/IEC 15408). Em equipamentos submetidos à certificação dos Critérios Comuns, as funções de segurança são testadas por laboratórios licenciados pelo governo independentes para garantir que os recursos de segurança funcionem corretamente e estejam em conformidade com os padrões definidos pelo governo e pela indústria.

Como parte de nosso compromisso contínuo de impedir que seus ativos de informações importantes sejam expostos a ameaças, desenvolvemos e oferecemos recursos e produtos de segurança para ajudar a proteger seus documentos eletrônicos e impressos, sem prejudicar a produtividade e processos fáceis de usar.

Firmware inseguro pode ser comprometido

Atualizações de firmware assinado digitalmente

Se um software incorporado da impressora ou MFP, também conhecido como firmware, for alterado ou comprometido, esse equipamento poderá ser usado como um método de intrusão na rede corporativa, como um meio de danificar o equipamento ou como uma plataforma para outros fins maliciosos. Os equipamentos projetados pela Ricoh são criados usando um Trusted Platform Module (TPM) da Ricoh e são projetados para não inicializar se o firmware tiver sido comprometido. O TPM da Ricoh é um módulo de segurança de hardware que valida os principais programas do controlador, Sistema Operacional, BIOS, carregador de inicialização e firmware do aplicativo.

As multifuncionais e impressoras da Ricoh usam uma assinatura digital para avaliar a validade do firmware. A chave pública usada para essa verificação é armazenada em uma região não volátil e protegida contra gravação do Trusted Platform Module (TPM) da Ricoh. Uma chave de criptografia raiz e funções criptográficas também estão contidas no TPM e não podem ser alteradas a partir do exterior. A Ricoh usa um procedimento de Trusted Boot que emprega dois métodos para verificar a validade dos programas/firmware:

1. Detecção de alterações
2. Validação de assinaturas digitais

Um equipamento da Ricoh não inicializa a menos que seus programas/firmware sejam verificados como autênticos e seguros para os usuários.

Dados temporários são dados vulneráveis

Sistema de Segurança por Sobregravação de Dados (DOSS)

Quando um documento é digitalizado ou quando os dados são recebidos de um PC, alguns dados podem ser armazenados temporariamente na unidade de disco rígido ou no equipamento de memória. Isso pode incluir digitalizar/imprimir/copiar dados de imagem, dados inseridos pelo usuário e configuração do equipamento. Esses dados temporários, ou "latentes", representam uma possível vulnerabilidade na segurança.

O Sistema de Segurança por Sobregravação de Dados (DOSS) da RICOH fecha esta vulnerabilidade, destruindo dados temporários armazenados no disco rígido de MFP, sobrescrevendo-os com sequências aleatórias de "1" e "0". Os dados temporários são sobrescritos e, assim, excluídos toda vez que um trabalho é executado.

- Em conformidade com as recomendações da Agência de Segurança Nacional (NSA) e Departamento de Defesa (DoD) para lidar com informações classificadas
- Torna virtualmente impossível acessar dados latentes de trabalhos de fax/digitalização/cópia/impressora, uma vez que o processo por sobregravação estiver concluído (processo por sobregravação pode ser selecionado de 1 a 9 vezes)
- Funciona com o sistema de segurança Removable Hard Drive (RHD) da RICOH, proporcionando uma abordagem em várias camadas
- Auxilia clientes em conformidade com os requisitos HIPAA, GLBA e FERPA
- Fornece feedback visual sobre o processo por sobregravação (ou seja, Concluído ou Em Processo) com um simples ícone no painel de exibição

Criptografia protege contra roubo de dados

Criptografia de disco rígido

Mesmo que o disco rígido seja fisicamente removido de uma máquina da Ricoh, os dados criptografados não poderão ser lidos. A função de criptografia do disco rígido pode ajudar a proteger o disco rígido de uma impressora multifuncional contra roubo de dados enquanto ajuda as organizações a cumprirem com as políticas de segurança corporativa. A criptografia inclui dados armazenados em um catálogo de endereços do sistema, reduzindo o risco de funcionários, clientes ou fornecedores de uma organização terem suas informações usadas de forma inadequada e potencialmente segmentadas. Os seguintes tipos de dados, que são armazenados na memória não volátil ou na unidade de disco rígido das impressoras multifuncionais, podem ser criptografados:

- Catálogo de endereços
- Dados de autenticação do usuário
- Documentos armazenados
- Documentos armazenados temporariamente
- Registros
- Configurações da interface de rede
- Informações de configuração

A Ricoh fornece criptografia de disco rígido usando a metodologia Advanced Encryption Standard (AES) para 256 bits.

A sua linha de fax fornece uma entrada?

Segurança da linha de fax

Habilitar o recurso de fax de um equipamento pode significar conectá-lo ao exterior por meio de uma linha telefônica, o que significa que bloquear o possível acesso não autorizado por meio da linha de fax é fundamental. O software incorporado da Ricoh foi projetado para processar apenas tipos apropriados de dados (ou seja, dados de fax) e enviar esses dados diretamente para as funções adequadas dentro do equipamento. Como exclusivo dados de fax podem ser recebidos da linha de fax, o possível acesso não autorizado da linha de fax para a rede ou para programas dentro do equipamento é eliminado.

A Ricoh utiliza vários métodos para ajudar a proteger as operações seguras de fax:

- O Controlador de Fax contém apenas um modem de fax e não um modem de dados, portanto, toda a comunicação é feita através do protocolo de fax G3.
- Os dados de imagem não são salvos na Memória da Página do Controlador do Motor ou Área de Armazenamento Temporária, impossibilitando o acesso a esses dados do Controlador de Fax.
- Os dados armazenados na Memória da Página do Controlador do Motor ou Área de Armazenamento Temporária são enviados para a Unidade de Impressão.
- Não há conexão ativa entre os Barramentos de Vídeo para Impressão/Digitalização e o Controlador do Motor, tornando impossível acessar os dados armazenados na Memória da Páginas do Controlador do Motor ou na Área de Armazenamento Temporária do Controlador de Fax.
- Os dados de Localização de Página são apagados após a conclusão de todos os trabalhos.

Certificação de segurança independente

IEEE 2600

O padrão IEEE 2600 de segurança define os requisites mínimos para recursos de segurança usados por equipamentos que exigem um alto nível de segurança de documentos, estabelecendo uma referência comum de expectativas de segurança para MFPs e impressoras. Para garantir que um equipamento demonstre a conformidade com o padrão estabelecido, um laboratório terceirizado independente testa e fornece a verificação dos recursos de segurança do fabricante.

Essas áreas, que foram identificadas como as mais vulneráveis a possíveis violações de dados, foram validadas em muitos equipamentos da Ricoh para o padrão IEEE 2600 e podem ser habilitadas:

- Sistemas de autenticação e identificação de usuários
- Tecnologia de criptografia de dados disponível para impressoras multifuncionais
- Validação do firmware do sistema
- Separação da linha de fax analógica e o controlador de cópia/impressão/digitalização
- Validação de algoritmos de criptografia de dados
- Operação de segurança por sobregravação de dados

A Ricoh oferece uma ampla linha de MFPs e impressoras que foram certificadas em conformidade com o padrão IEEE 2600 de segurança, e nossa linha de produtos está sendo constantemente aprimorada para atender aos requisitos em constante mudança de nossos clientes.

Controlar o acesso e reduzir riscos

Autenticação do usuário do equipamento

Os recursos de autenticação permitem aos usuários autorizados acessar uma impressora multifuncional da Ricoh e, ao mesmo tempo, impedir o acesso de pessoas sem as credenciais adequadas. A Ricoh também oferece a capacidade de controlar o nível de recursos concedidos a cada usuário ou grupo de usuários. Isso pode incluir a restrição da capacidade de alterar as configurações da máquina e exibir entradas do catálogo de endereços ou conceder acesso a fluxos de trabalho de digitalização, servidores de documentos e outras funções específicas. Além disso, a função Bloqueio de Usuário, que é acionada se detectar uma alta frequência de tentativas de login fracassadas ou com sucesso, ajuda a proteger contra um ataque de negação de serviço ou uma quebra de senha por força bruta.

Métodos de autenticação incluem:

- Autenticação Básica — Usuários inserem um nome de usuário e senha, que são registrados localmente no catálogo de endereços da impressora multifuncional.
- Autenticação de Código do Usuário — Usuários inserem um código de até 8 dígitos, que é comparado aos dados registrados no catálogo de endereços.
- Autenticação de Windows/LDAP — Acesso às impressoras multifuncionais da Ricoh pode ser vinculado aos controladores de domínio do Windows® e servidores LDAP.
- Autenticação de Cartão — Em vez de inserir um nome de usuário e senha, um usuário mantém um cartão registrado adequadamente em um leitor de cartão opcional para autenticação.
- Autenticação de Cartão de Acesso Comum (CAC) — O Cartão de Acesso Comum é um sistema de autenticação baseado em cartão de identificação especializado do Departamento de Defesa dos EUA, projetado para usuários do governo que devem estar em conformidade com a Diretiva Presidencial de Segurança Doméstica 12 (HSPD-12).
- Verificação de Identidade Pessoal (PIV) — Verificação de Identidade Pessoal é a versão civil do cartão CAC.
- Solução de Autenticação de Token SIPRNet —Token SIPRNet é uma variação da ID de CAC, projetado para redes controladas.

Segurança de dados

É fácil vazar acidentalmente informações. Um documento deixado na bandeja de uma impressora multifuncional pode se tornar um risco de segurança tão facilmente quanto um arquivo digital de apropriação indevida ou impacto de erro humano. As impressoras multifuncionais da Ricoh ajudam a proteger seus dados, quer você esteja imprimindo, copiando, digitalizando ou enviando fax. O sistema de criptografia de dados da Ricoh, que usa o módulo de criptografia RSA BSAFE e é validado para FIPS 140-2, ajuda a proteger seus dados quando estão em trânsito e quanto estão em repouso.

174 milhões

registros digitais foram comprometidos por intrusos de dados em 2011 — um aumento de mais de 4.000% em relação a 2010.*

*Relatório de investigações sobre violação de dados da Verizon® 2012

A Ricoh ajuda a proteger seus dados com tecnologias e recursos que são projetados para suportar políticas de segurança, proteger contra uso indevido ou descuido e incentivar a conformidade por meio de contabilização.

Proteção para documentos digitalizados

Soluções seguras de digitalização

O processo de digitalizar documentos impressos e rotear os arquivos eletrônicos resultantes, seja para sistemas de back-end ou por e-mail, pode ser um ponto de comprometimento de dados se não for adequadamente protegido. Os processos de digitalização, embora projetados para serem fáceis para os usuários, também devem fornecer proteção robusta para informações digitais roteadas. Isso começa com a restrição de acesso. Limitar as operações de digitalização somente para usuários autorizados com várias opções de autenticação, incluindo login via rede, autenticação Kerberos opcional ou single sign-on via cartão.

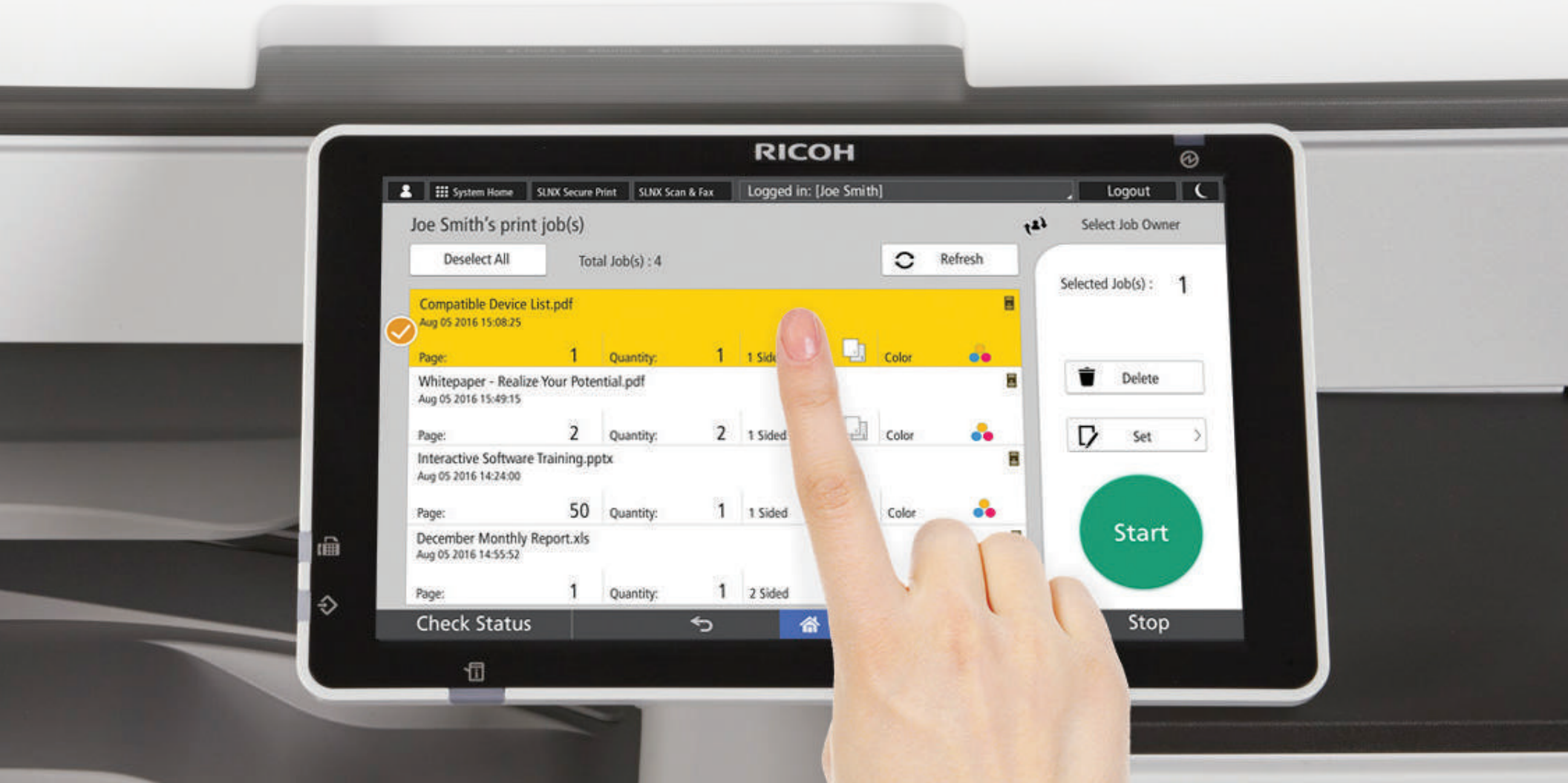
Criptografar as comunicações de digitalização para e-mail ajuda a reduzir o risco de comprometimento das informações. Envie mensagens de e-mail usando criptografia de chave pública e um certificado de verificação de usuário que foi registrado no catálogo de endereços do equipamento de digitalização. Você também pode impedir a falsificação de e-mails e a alteração de mensagens, anexando uma assinatura eletrônica que usa uma chave secreta, com base em um certificado de equipamento.

As impressoras multifuncionais, copiadoras e scanners projetados pela Ricoh são equipados com protocolos Secure Sockets Layer (SSL) e Transport Layer Security (TLS) e podem utilizar algoritmos de criptografia robustos (AES e SHA-2 de 256 bits), além de fornecer trilhas de auditoria e controle administrativo.

Impressoras não assistidas podem vazar informações

Impressora bloqueada

Os documentos impressos colocados na bandeja de papel ou deixados na abertura podem ser pegos por qualquer pessoa. Isso coloca em risco as informações do documento e o impacto potencial aumenta drasticamente ao imprimir documentos confidenciais. Os recursos de impressão bloqueados da Ricoh podem manter documentos criptografados no disco rígido do equipamento até que o proprietário do documento apareça e insira o código PIN correto. Além dessa função de impressão bloqueada baseada em driver, a Ricoh também oferece impressão bloqueada aprimorada, que está vinculada às contas de usuário e pode ser acoplada à autenticação de cartão. Para obter ainda mais recursos, softwares como o Streamline NX da RICOH (na foto) podem fornecer liberação de documentos segura com todos os recursos, oferecendo aos usuários opções sobre sua fila de impressão segura e permitindo aos administradores manter o controle.

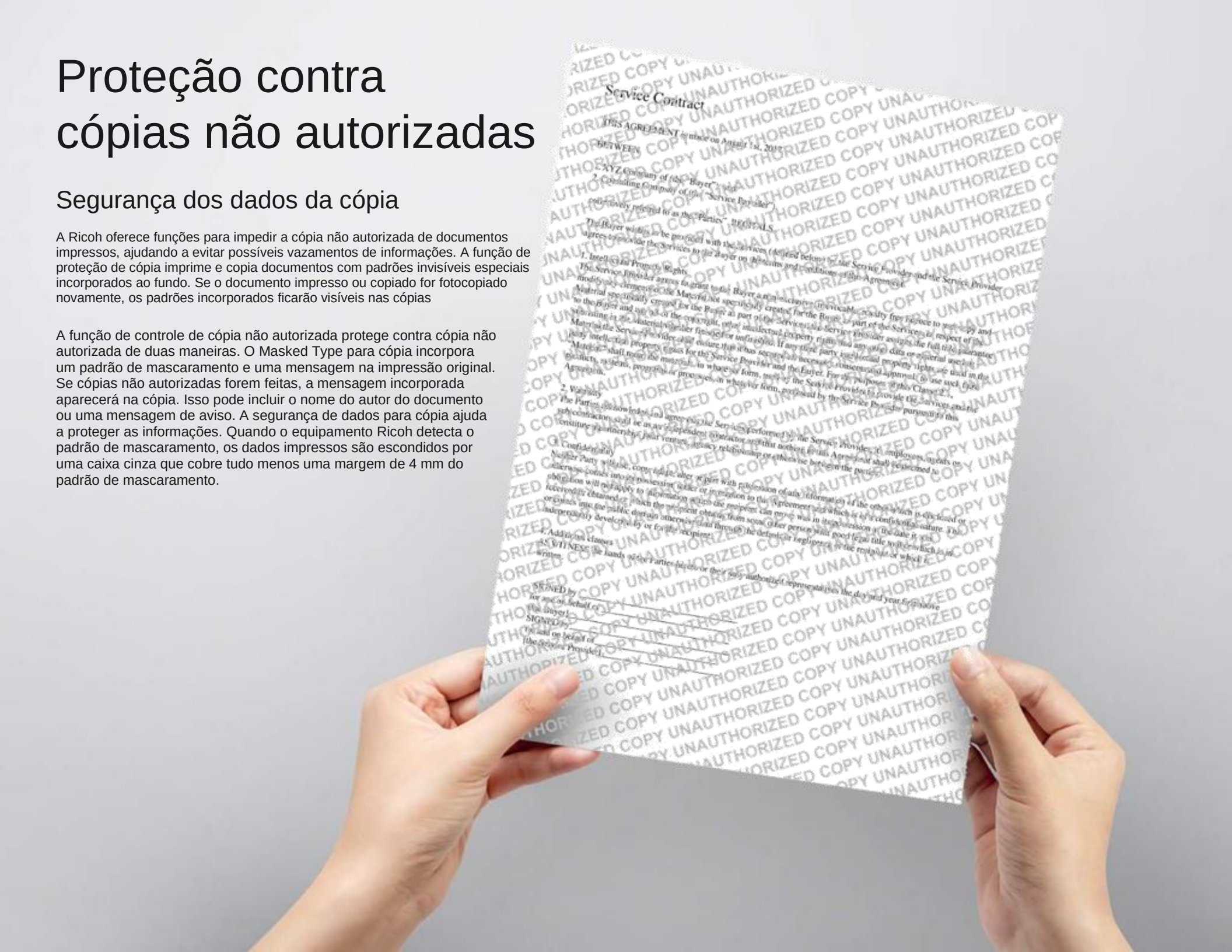


Proteção contra cópias não autorizadas

Segurança dos dados da cópia

A Ricoh oferece funções para impedir a cópia não autorizada de documentos impressos, ajudando a evitar possíveis vazamentos de informações. A função de proteção de cópia imprime e copia documentos com padrões invisíveis especiais incorporados ao fundo. Se o documento impresso ou copiado for fotocopiado novamente, os padrões incorporados ficarão visíveis nas cópias

A função de controle de cópia não autorizada protege contra cópia não autorizada de duas maneiras. O Masked Type para cópia incorpora um padrão de mascaramento e uma mensagem na impressão original. Se cópias não autorizadas forem feitas, a mensagem incorporada aparecerá na cópia. Isso pode incluir o nome do autor do documento ou uma mensagem de aviso. A segurança de dados para cópia ajuda a proteger as informações. Quando o equipamento Ricoh detecta o padrão de mascaramento, os dados impressos são escondidos por uma caixa cinza que cobre tudo menos uma margem de 4 mm do padrão de mascaramento.



Documentos anônimos são difíceis de controlar

Impressão segura de informações obrigatórias

Carimbar documentos com informações de identificação importantes para maior responsabilidade e controle de gerenciamento. A impressão obrigatória de informações de segurança é um recurso que força as principais informações, incluindo quem imprimiu um documento, quando foi impresso e de qual equipamento, a ser impresso com um documento. Este recurso pode ser ativado para funções de cópia, impressão, fax e servidor de documentos. Os administradores podem selecionar a posição de impressão e quais tipos de informações serão impressos automaticamente na saída, o que pode incluir:

- Data e hora em que o trabalho foi impresso
- Nome ou login de ID do usuário de quem imprimiu o trabalho
- Endereço IP e/ou número de série do equipamento usado

Proteger equipamentos contra uso indevido

Recuperação e contabilização de custos

O uso descontrolado de equipamentos de imagem pode levar a despesas imprevistas e possíveis violações das políticas da empresa. O software de recuperação e contabilização de custos da Ricoh rastreia o uso para o indivíduo e automatiza o processo de alocação de custos para usuários ou departamentos. Cria uma maior responsabilidade, estabelecendo cotas de usuários e limites de conta orçamentária. Estabelece permissões de usuário para restringir o acesso a determinados recursos com base na necessidade, por exemplo, a capacidade de imprimir em cores. Controlar quem pode usar equipamentos por meio da autenticação e designar o que eles podem ou não fazer reduz as oportunidades de uso indevido e fornece uma visão de gerenciamento útil.

Segurança da rede

Os produtos e tecnologias da Ricoh oferecem recursos que podem ajudar a proteger contra acesso não autorizado

As impressoras multifuncionais trocam informações essenciais com computadores e servidores em redes. Se deixadas desprotegidas, estas informações correm o risco de ser alteradas por pessoas com intenção maliciosa que possam explorar as redes. As técnicas empregadas incluem criptografia de comunicações de rede e fluxos de impressão, autenticação de usuário de rede e uma série de contramedidas administrativas, como fechar portas de rede e gerenciamento proativo de equipamentos.

Os recursos de segurança da Ricoh podem ajudar a reduzir o risco de exploração de rede ou vazamento de informações decorrentes de um equipamento ou impressora multifuncional violada.

Usuários não autorizados podem ser uma ameaça

Autenticação do usuário de rede

Os equipamentos da Ricoh oferecem suporte à autenticação do usuário de rede para limitar o acesso a usuários autorizados. Por exemplo, a autenticação do Windows® verifica a identidade de um usuário na impressora multifuncional comparando as credenciais de login (nome de usuário e senha) com o banco de dados de usuários autorizados no servidor de rede do Windows. No caso de acesso ao catálogo de endereços global, a autenticação LDAP valida um usuário no servidor LDAP (Lightweight Directory Access Protocol), assim, apenas aqueles com um nome de usuário e senha válidos podem pesquisar e selecionar endereços de e-mail armazenados no servidor LDAP.

Softwares como o RICOH Streamline NX, um conjunto modular que abrange os processos de segurança e contabilização, gerenciamento do equipamento, digitalização, fax e impressão, fornecem opções adicionais de autenticação de rede. Isso inclui a autenticação no LDAP, a autenticação Kerberos e um SDK disponível para integrações personalizadas.

Tornar os equipamentos “invisíveis” para o exterior

Fecha as portas de rede não utilizadas

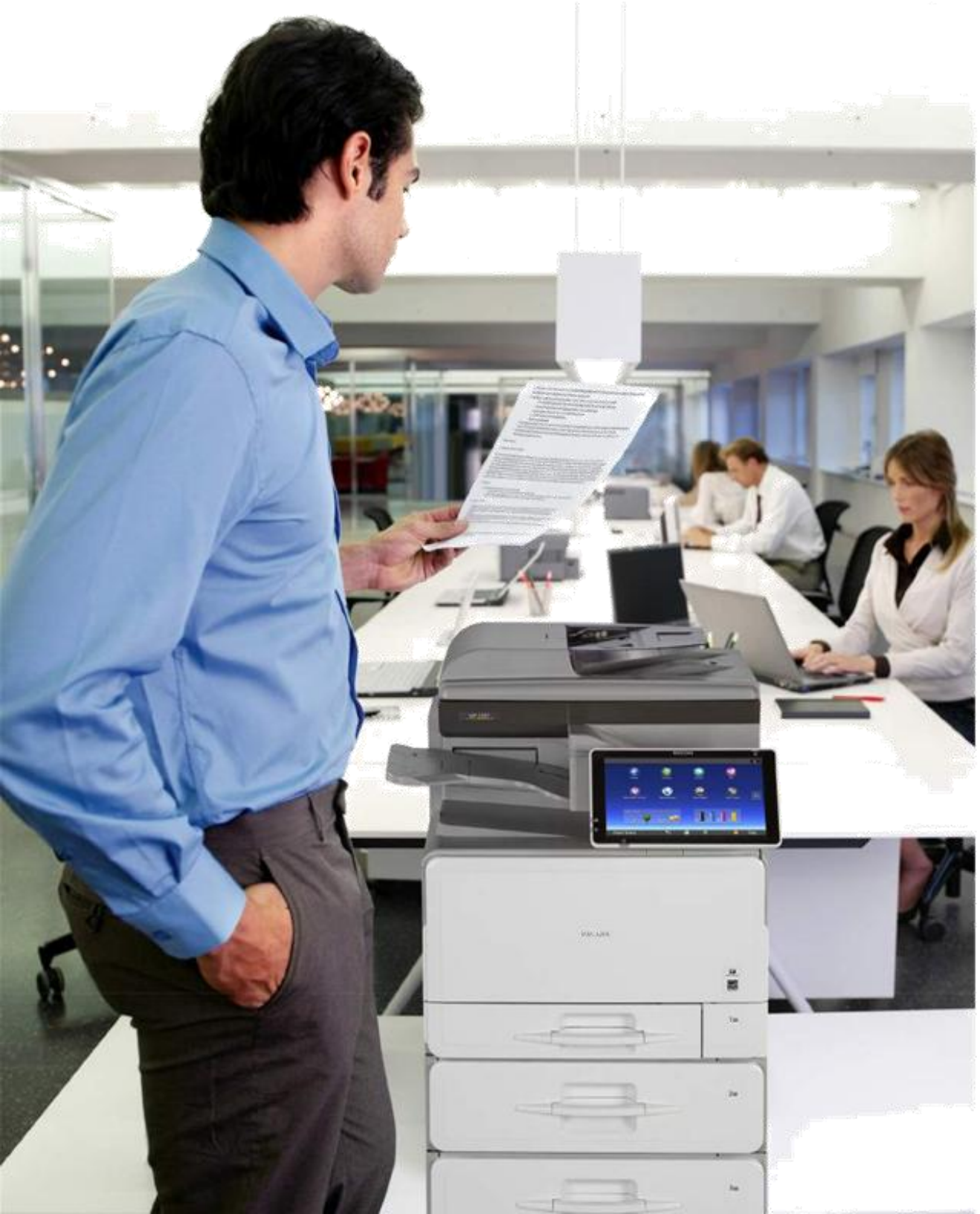
Em um esforço para facilitar a adição de equipamentos de rede, os sistemas habilitados para rede de muitos fornecedores são enviados rotineiramente ao cliente com todas as portas definidas como "abertas", mas as portas abertas não usadas em impressoras e MFPs representam um risco de segurança. As portas comprometidas podem levar a várias ameaças externas, incluindo a destruição ou falsificação de dados armazenados, ataques de Negação de Serviço (DoS) e vírus ou malware que entram na rede. Existe uma solução simples, mas muitas vezes negligenciada, para essa fonte específica de risco: feche as portas. Os administradores de equipamentos da Ricoh podem facilmente bloquear portas de rede desnecessárias, ajudando a tornar os equipamentos virtualmente “invisíveis” para hackers. Além disso, protocolos específicos, como SNMP ou FTP, podem ser completamente desativados para não ter risco de serem explorados.

Dados não criptografados na rede estão em risco

Criptografia de rede

À medida que os dados passam pela rede, é possível que um hacker experiente intercepte fluxos de dados brutos, arquivos e senhas. Sem proteção, informações inteligíveis podem ser roubadas, modificadas ou falsificadas e reinseridas na rede com intenção maliciosa. A Ricoh usa protocolos robustos de segurança de rede que também podem ser configurados de acordo com as necessidades dos clientes. O protocolo Transport Layer Security (TLS) é usado para ajudar a manter a integridade dos dados que estão sendo comunicados entre dois pontos finais.

Os equipamentos da Ricoh suportam WPA2, WPA2-PSK usando criptografia AES (Acesso Protegido por Wi-Fi), um sistema de criptografia para redes sem fio que oferece maior segurança do que o sistema convencional de criptografia WEP (Wired Equivalent Privacy). WPA2, WPA2-PSK possui uma função de autenticação do usuário e um protocolo de criptografia chamado CCMP (AES), que atualiza automaticamente a chave de criptografia em determinados intervalos.



Dados enviados para impressoras podem ser explorados

Criptografia de fluxo de impressão

Os dados enviados em um fluxo de impressão podem ser explorados se não forem criptografados e capturados em trânsito. A Ricoh pode ativar a criptografia de dados de impressão por meio de Secure Sockets Layer/Transport Layer Security (SSL/TLS) via Internet Printing Protocol (IPP), criptografando dados de estações de trabalho para equipamentos de rede ou impressoras multifuncionais. Isso pode ser feito usando o IPP sobre SSL/TLS. Como esse é um protocolo que ajuda a manter a integridade dos dados, as tentativas de interceptar os fluxos de dados de impressão criptografados em trânsito produziriam apenas dados indecifráveis.

Gerenciar equipamentos pode ser demorado

Device Manager NX

Como o gerenciamento de equipamentos pode ser demorado, as lacunas de segurança podem surgir de forma não intencional quando aspectos de gerenciamento de equipamentos adequados não são atendidos. O software de gerenciamento de equipamentos da Ricoh, como o Device Manager NX e o Streamline NX, fornece aos gerentes de TI um ponto de controle central para monitorar e gerenciar um número praticamente ilimitado de equipamentos de impressão conectados em rede, espalhados por vários servidores ou regiões geográficas. As comunicações criptografadas por SNMPv3 são usadas para monitorar o status operacional de equipamentos e seus serviços, incorporando funções de autenticação de usuário e criptografia de dados que ajudam a proteger os dados do usuário e as informações do equipamento de rede.

Com o controle central, os administradores podem determinar quem pode acessar e usar um equipamento ou uma impressora multifuncional, monitorar as configurações da Solução de Segurança por Sobregravação de Dados (DOSS) e gerenciar os certificados do equipamento. As tarefas automatizadas também podem reduzir a exposição do firmware desatualizado. O firmware do equipamento da Ricoh é comparado com a versão de firmware aprovada pelo cliente ou com o firmware mais recente disponível para

Ajudar os prestadores de serviços a responderem rapidamente

@Remote

@Remote Connector NX da Ricoh coleta alertas de serviço críticos e pode comunicá-los diretamente ao seu Prestador de Serviços utilizando um método seguro. O seu Prestador pode agendar atualizações de firmware remotas, usando o conector para enviar atualizações críticas imediatamente. O @Remote Connector também coleta medidores de equipamentos e os disponibiliza em um cronograma pré-definido, junto com notificações de níveis consumíveis, para manter o tempo de atividade e reduzir a carga administrativa.

Programas e recursos

As organizações que usam e armazenam informações médicas, informações financeiras, informações pessoalmente identificáveis (PII) ou outros tipos de dados sensíveis podem estar sujeitos a vários requisitos regulamentares, como HIPAA, Gramm-Leach-Bliley ou a Lei dos Direitos Educacionais e Privacidade da Família. Se a sua organização precisa aderir à conformidade externa ou demonstrar suporte às suas próprias políticas de segurança, a Ricoh pode ajudar.

Nós fornecemos aos nossos clientes programas e recursos para ajudar a satisfazer seus requisitos específicos de conformidade regulamentar.

Na Ricoh, oferecemos suporte aos nossos clientes, fornecendo assistência técnica, conhecimento e treinamento, e documentação de segurança relacionados aos nossos equipamentos. Além disso, também oferecemos a remoção de dados dos equipamentos em fim de vida útil como um serviço.

Programas de fim de vida do equipamento

As informações latentes sobre equipamentos desativados podem apresentar um risco de segurança até que sejam completamente destruídas. Se comprometidos, terceiros mal-intencionados poderiam usar as informações adquiridas para uma violação de segurança maior. Os programas da Ricoh limpam as informações do equipamento no fim de sua vida útil ou quando são devolvidos na conclusão de um contrato de aluguel ou locação.

Serviços por sobregravação de disco rígido

Geralmente executado quando um equipamento é desativado ou na conclusão de uma locação de equipamento, o Serviço por sobregravação de Dados sobrescreve completamente os dados do cliente no disco rígido da máquina. Vários métodos por sobregravação de dados estão disponíveis, incluindo os métodos compatíveis com a Agência Nacional de Segurança (NSA) e o Departamento de Defesa (DoD). Além disso, NV-RAM é inicializado com valores padrão para impedir que informações identificáveis, como endereços IP, catálogos de endereços e outros dados administrativos, sejam expostas a terceiros.

Serviços de eliminação de disco rígido

O Programa de Devolução de Disco Rígido permite aos clientes manter o disco rígido de sua MFP ou da impressora no final de uma locação ou a vida útil da máquina. Um técnico certificado da Ricoh remove o disco rígido antes de sair do local do cliente e transfere-o para a custódia de um representante do cliente. Os clientes mantêm o controle de suas informações e podem optar por destruí-las através de um método de sua escolha.

Serviços de limpeza da MFP

O Serviço de Limpeza da MFP da Ricoh foi projetado para remover todas as informações de identificação de uma MFP ou impressora antes que o equipamento deixe a localização do cliente. As informações armazenadas na memória do equipamento, como catálogos de endereços e informações de endereço de rede, são excluídas. As marcas de identificação, como rótulos com nomes de departamentos, endereços IP e informações da central de atendimento, também são removidas, juntamente com qualquer papel específico do cliente ou estoque de formulários. Remover essas informações pode ajudar a impedir tentativas mal-intencionadas de reunir informações de TI de uma organização.

Suporte técnico global/nacional

A Ricoh estabeleceu Centros de Tecnologia em todas as regiões para fornecer suporte técnico aos nossos clientes em todo o mundo, respondendo às suas necessidades com rapidez e eficiência. A equipe da Ricoh Global Services fornece soluções completas, consistentes e padronizadas. Com cobertura em aproximadamente 200 países e territórios em todo o mundo, a Ricoh emprega mais de 30.000 profissionais de prestação de serviços. Nossa incomparável rede de suporte a parceiros de revenda e vendas diretas tem capacidade de atender 95% dos funcionários da empresa Fortune Global 500, o que significa que você pode confiar em um parceiro para todas as suas necessidades globais. Com escritórios e profissionais de prestação de serviços em muitos países do mundo, podemos responder rapidamente às solicitações do cliente, onde quer que eles estejam.

Documentação de apoio de segurança

A Ricoh fornece documentação técnica para fundamentar os requisitos de segurança de informações de nossos clientes, incluindo os Documentos de Certificação IEEE 2600 e ISO 15408 para ofertas de produtos selecionados. Esta documentação fornece validação de terceiros independente das reclamações de segurança e pode ser fornecida mediante solicitação. Além disso, os Livros Brancos da Segurança que abrangem equipamentos e configurações de rede e os Guias de Instalação de Segurança do Equipamento também estão disponíveis para os clientes. Esses guias fornecem informações detalhadas sobre como o equipamento Ricoh comunica os dados dentro do equipamento e como o equipamento interage com a rede.

Treinamento do administrador e usuário final

Manter um alto grau de vigilância e aderir às melhores práticas de segurança envolve mais do que apenas tecnologia, envolve as pessoas. A Ricoh oferece treinamento em nossos equipamentos destinados a usuários finais e administradores. Com o conhecimento certo na ponta dos dedos, a sua equipe pode entender os recursos de segurança disponíveis e aprender como seu uso adequado pode ajudar a sua organização a proteger suas informações e a cumprir as políticas.

Segurança além do equipamento

As melhores práticas de segurança exigem uma “defesa profunda” que vai além do equipamento. A Ricoh está abordando as crescentes preocupações de segurança de nossos clientes por meio de Governança, Risco e Conformidade (GRC) e Gestão de serviços de Segurança. Esses serviços abrangem o ciclo de vida dos dados e avaliação e gerenciamento de riscos, eDiscovery, segurança do endpoint e servidor, acesso a identidade, segurança de e-mail e proteções contra ameaças de rede avançadas.

Procure a Ricoh para ajuda com os seus principais desafios de segurança

Roubo/perda de dados

A perda de dados está no centro das preocupações de liderança do nível C, e manter os dados confidenciais e seguros é uma luta constante. Os invasores estão continuamente buscando uma lacuna em sua armadura que pode ser explorada. O equipamento de imagem da Ricoh pode ser um componente essencial de prevenção de perda de dados.

Alteração/corrupção de dados

Os ataques de vírus em manchetes globais destacam como todas as organizações são vulneráveis a ataques cibernéticos. Malware, vírus, trojans e worms atacam plataformas amplamente implementadas com vulnerabilidades bem conhecidas. As plataformas da Ricoh, embora amplamente implementadas, utilizam Sistemas Operacionais exclusivos para impedir tentativas de adulteração.

Disponibilidade de dados

A disponibilidade de informações e dados é um ato de equilíbrio multifacetado entre permitir e impedir o acesso. Os produtos da Ricoh abordam a agilização da troca sancionada de informações através de impressão, cópia, digitalização e roteamento, impondo controles desses processos, criptografando dados em trânsito e determinando quem pode consumir as informações processadas pelo nosso equipamento.

Entendendo os regulamentos

As organizações devem observar várias regulamentações globais, nacionais e do setor, sem mencionar as políticas de segurança e os requisitos de auditoria da empresa exigidos internamente. A Ricoh fornece ferramentas e conhecimento para atender às necessidades relacionadas à conformidade de nossos clientes.

Comprovando a conformidade

As penalidades pelo não conformidade podem ser severas, e novas regulamentações estão aumentando a barreira sobre o potencial impacto adverso no negócio. A documentação adequada está no centro de demonstrar efetivamente a conformidade. A certificação IEEE 2600 fornece validação independente de terceiros e essas reivindicações de segurança de TI operam como anunciadas. A Ricoh pode fornecer esta certificação, juntamente com outra documentação, para apoiar nossos clientes.

Iniciar uma Avaliação de Risco de Segurança

Uma Avaliação de Risco de Segurança realizada pela Ricoh engloba hardware, software e dados e é construída sobre padrões NIST* aceitos. As pontuações de risco de baixa a alta são calculadas com base nos padrões do Governo Federal dos EUA e DoD**, juntamente com uma expectativa de perda anual (ALE) para ativos de dados, resultados e recomendações. A Avaliação de Riscos de Segurança informa o Plano de Gerenciamento de Risco subsequente, Criação de Políticas, as ações de Remediação de Risco e a auditoria independente por terceiros.

Envolver nossos profissionais de segurança

Os clientes estão procurando organizações nas quais possam confiar e que possam ajudá-los a permanecer seguros e comprovar a conformidade. A Ricoh está empenhada em fornecer aos nossos clientes a melhor tecnologia, serviços, programas e recursos, juntamente com a disposição para ajudar nossos clientes a atender aos requisitos de políticas de segurança. Se você tiver dúvidas ou gostaria de obter mais informações, entre em contato com o profissional de vendas da Ricoh ou visite nosso site.

Saiba mais em **www.Ricoh-USA.com**.

** Instituto Nacional de Normas e Tecnologia*
*** Departamento de Defesa*

RICOH
imagine. change.

090717