WHITE PAPER

Implementação da impressão segura

O que é uma identidade confiável?

Identidade confiável é uma identificação validada que utiliza a biometria ou uma credencial fornecida em um cartão, dispositivo móvel ou vestível. Em um ambiente de trabalho conectado, uma identidade confiável pode ser utilizada para acessar múltiplos sistemas, como acesso ao edifício, gestão de tempo e presença, e impressão segura.

Como aproveitar as suas credenciais de identidade confiável já existentes para uma impressão mais fácil e segura

Uma experiência mais segura e simples com a impressora

Quando um documento sensível é impresso, ele pode cair facilmente em mãos erradas, representando um enorme - e frequentemente ignorado - risco à segurança. Em realidade, 70% das organizações sofreram uma violação de dados relacionada à impressão. Muitas também enfrentam dificuldades com a complicação na alocação do rastreamento e erros, quando os usuários não são identificados corretamente. Além disso, muitos métodos comuns de impressão "segura" são complexos demais para os usuários ou muito suscetíveis a violações Por exemplo:

- Os teclados numéricos (pin pads) proporcionam a conveniência de não ter nada para portar, mas exigem que o usuário se recorde da senha — e não a revele a mais ninguém
- Senhas são frequentemente perdidas, esquecidas ou compartilhadas e exigem que o departamento de TI da organização as atualize, altere ou recupere constantemente
- Os códigos QR são extremamente fáceis de copiar e clonar, criando uma falsa impressão de segurança

Uma forma eficaz de solucionar essas questões é aplicar as credenciais de identificação, já utilizadas, para potencializar os programas de impressão segura. A agregação da impressão segura a credenciais de identidade confiáveis já existentes, como crachás, dispositivos móveis e biometria, não melhora apenas a segurança, mas proporciona também uma experiência mais conveniente aos usuários. Além disso, sua implementação se torna muito mais simples, com o auxílio e a experiência de um parceiro para o gerenciamento das impressões, ou do fabricante das impressoras. Este white paper auxilia as organizações a iniciar a descoberta no mundo da impressão segura, detalhando seus dois componentes mais importantes: credenciais e leitoras. Após a leitura, você entenderá os fundamentos da impressão segura e como ela pode funcionar em conjunto com sua atual solução de gerenciamento de identidade.

Impressão segura: mais assegurada, ecológica e simples

Sem a impressão segura, os documentos são enviados para a impressora e liberados imediatamente. Isso funciona adequadamente se o usuário recupera o impresso imediatamente, mas isso implica que o usuário esteja próximo da impressora no momento em que o impresso é liberado (por exemplo, quando a impressora fica ao lado do computador do usuário). No entanto, como não é viável que cada usuário tenha a sua própria impressora, a maioria das tarefas é impressa em uma impressora central, a uma certa distância do usuário.

Esse cenário é comum na área de saúde, onde os médicos atendem os pacientes em consultórios, inserem as informações dos pacientes em um laptop e imprimem em uma impressora no escritório central. Em seguida, as informações privadas do paciente permanecem na impressora até serem recuperadas pela equipe do escritório — ou qualquer outra pessoa que esteja na proximidade.

A privacidade não é o único aspecto que está atraindo mais atenção: as certificações ambientais e a reputação de "ambientalmente adequado" atraem cada vez mais o interesse dos clientes.

Com a impressão segura que utiliza uma identidade confiável, o documento não é liberado imediatamente para impressão. Em vez disso, o documento não será impresso até que o médico, ou um usuário autorizado, autenticar sua identidade na impressora usando o mesmo cartão, dispositivo ou biometria utilizado com os demais sistemas de controle de acesso (como para a entrada na edificação ou autorização para estacionamento). O médico e o paciente — assim como os auditores da HIPPA — sabem que essas informações confidenciais só podem ser acessadas com permissão. Empresas de todos os setores podem se beneficiar desse nível de privacidade, principalmente com as novas regulamentações mais estritas, como a norma GDPR, e a ênfase cada vez maior em sistemas empresariais bloqueados.

Evidentemente, a privacidade não é o único aspecto que está atraindo mais atenção: as certificações ambientais e a reputação de "ambientalmente adequado" atraem cada vez mais o interesse dos clientes. As empresas que adotam o tripé da sustentabilidade buscam agregar iniciativas relacionadas a isso, mas até mesmo as que não seguem filosofias expressamente ecológicas têm interesse em economizar recursos financeiros. A impressão segura pode contribuir. Estima-se que 20% das tarefas de impressão não sejam recuperadas pelo usuário original, resultando cotidianamente em desperdícios financeiros e ambientais, mas também complicando e aumentando desnecessariamente os custos do departamento. Com a impressão segura, os documentos permanecem na fila do servidor de impressão até serem liberados — reduzindo as despesas desnecessárias e, ao mesmo tempo, contribuindo ambientalmente para o planeta.

Entretanto, os métodos de impressão segura não são todos iguais. Para desenvolver o programa adequado, é necessário compreender suas necessidades e seus sistemas, além de contar com aliados desde o início do projeto. Afinal, não é ambientalmente correto, nem fiscalmente responsável, desenvolver um sistema apenas para eliminá-lo e substituí-lo por um novo. Para garantir o sucesso, os gerentes de TI devem considerar o seguinte:

Compreender as suas credenciais atuais

Iniciar questionando: qual mecanismo de autenticação sua organização gostaria de utilizar para a impressão segura? A maioria prefere utilizar as credenciais de controle de acesso já existentes, para que possam beneficiar de seus atuais sistemas, ao invés de começar do zero. Exceto, obviamente, se o seu sistema atual estiver desatualizado ou necessitar de um upgrade. Considere como você gostaria que os usuários experienciem a impressão segura agora e no futuro.

Se sua empresa está usando cartões/crachás:
os cartões são o tipo de credencial mais comum para ser estendido para impressão segura. Atualmente, há muitas novas tecnologias em uso. No futuro, os cartões podem deixar de ser predominantes, mas ainda continuarão sendo utilizados por muito tempo. O tipo do seu cartão, as necessidades e a marca determinarão as leitoras que o fabricante de impressoras irá fornecer, bem como o nível de segurança obtido. Os tipos mais comuns de cartões são:

- **Cartões de proximidade (prox):** esses cartões de 125 kHz são incrivelmente fáceis de utilizar: basta apresentar o cartão próximo da impressora e a tarefa será liberada. Infelizmente, eles proporcionam o mais baixo nível de segurança. Os cartões prox atribuem um número de série à um indivíduo, que é verificado pela leitora. Porém, esse número pode ser clonado com relativa facilidade.

- **Cartões inteligentes:** smart cards, como o HID Seos®, usam números de série randômicos para estabelecer a comunicação com a leitora, tornando a clonagem quase impossível. Eles também evitam a colisão de cartões — se dois usuários de cartões prox estão no mesmo espaço, a leitora pode não funcionar, já com os cartões inteligentes, a leitora pode selecionar o cartão correto.

Analise opções de credenciais móveis e vestíveis que não estejam "amarradas" a uma marca específica.

Etiquetas/Adesivos: se você tiver cartões desatualizados ou não suportados por seu fornecedor atual, você pode simplesmente acrescentar uma etiqueta ou um adesivo ao cartão para facilitar a comunicação com a leitora. No entanto, essas etiquetas são de 125 kHz e, portanto, não tão seguras quanto os cartões inteligentes.

Cartões de múltiplos tipos: organizações de grande porte podem ter diversos tipos de cartão, de acordo com o local e o nível de segurança. Por exemplo: a sede da empresa pode usar o Seos® para o acesso às edificações, mas os escritórios satélites podem usar cartões prox. Algumas leitoras podem ser configuradas para leitura de múltiplos tipos de cartão — certifique-se de que seu gerente de impressão ou o fabricante das impressoras entenda essa necessidade.

Se você usa ou considera utilizar credenciais móveis/vestíveis:
sem dúvida, o acesso móvel está em ascensão — se você não o está utilizando agora, provavelmente utilizará no futuro. Se sua empresa atualmente usa cartões, a opção por leitoras que operam com ambos, mobilidade e cartões, possibilitará uma transição com o mínimo de interrupções.

As credenciais móveis e vestíveis, como todas as opções, têm graus variados de segurança: os códigos QR exibidos em um celular são relativamente pouco seguros e podem ser copiados com facilidade. Os beacons de Bluetooth e as etiquetas de NFC, por sua vez, oferecem segurança adicional e não podem ser copiados. Além disso, as credenciais móveis são muito mais fáceis de implantar e gerenciar que os cartões — as atualizações podem ser enviadas imediatamente, sem necessidade de ajuda no local.

Analise opções de credenciais móveis e vestíveis que não estejam "amarradas" a uma marca específica. Por exemplo: sua solução de impressão segura móvel deve funcionar para ambos usuários, de iPhone e de Android.

Se sua empresa usa credenciais biométricas:
a biometria, como a leitura de impressões digitais, proporciona praticidade para o usuário e um nível de segurança extremamente elevado. Levando em consideração essa segurança avançada, não é de se admirar que essas opções sejam de alto custo. Muitas organizações optam por usar a biometria em conjunto com outra credencial, como uma credencial móvel ou um cartão. Além disso, até a biometria oferece níveis variados de segurança. Governos e outras organizações altamente seguras podem se beneficiar dos serviços agregados, como a detecção de vivacidade, que garante que a impressão digital esteja vinculada a uma identidade confiável de uma pessoa viva e respirando.

Identifique suas necessidades relacionadas à leitora

Quando você tiver um entendimento sólido sobre suas credenciais e seus recursos, será hora de considerar a melhor opção de leitora para habilitar a impressão segura. Inicialmente, determine se você precisa que a leitora libere uma tarefa de impressão a vários metros de distância, ou se você exigiria que o usuário estivesse diretamente na frente da impressora antes da liberação? Cartões, biometria e algumas aplicações móveis/vestíveis necessitam que o usuário toque na impressora com a sua credencial, para indicar que ele está presente para pegar o documento imediatamente. Talvez você prefira a facilidade de uma leitora que capte o sinal da credencial a vários metros de distância.

Em seguida, avalie se você prefere que a leitora esteja incorporada à impressora ou seja instalada externamente. Leitoras incorporadas são mais atraentes esteticamente, mas requerem espaço interno na carcaça da impressora e recursos técnicos robustos para instalação e manutenção. As leitoras de mesa ou com carcaça, por sua vez, se parecem com um pequeno disco rígido que pode ser conectado à impressora e trocado conforme

A solução correta de impressão segura combina segurança e conveniência. É mais um passo rumo a um ambiente de trabalho realmente conectado.

a necessidade. As leitoras de mesa também previnem que a carcaça da impressora interfira no sinal.

A interoperabilidade das leitoras também varia. Até mesmo se todos os cartões utilizados em uma organização forem Seos®, é possível que uma leitora não consiga verificar cartões estabelecidos em um site e utilizados em outro. Além disso, nem toda leitora opera com todo tipo de cartão; por exemplo: se você usa cartões atualmente, mas pensa em adotar credenciais móveis, escolha uma leitora que funcione com ambos.

Por fim, identifique as conexões e os conectores disponíveis. Por exemplo:

- i conexões USB são realizadas externamente, permitem o ajuste automático da antena da leitora de cartões e são ajustados facilmente no local. No caso das leitoras biométricas, a conectividade USB é a mais fácil de configurar e implementar.
- i As conexões UART requerem instalação interna, dentro da impressora e seu ajuste pode ser difícil.

Consulte o seu principal aliado — o fabricante das impressoras ou o parceiro de gerenciamento de impressão

Para concluir, você precisa ter uma minuciosa conversa com o fabricante das impressoras ou com o gerente de impressão. Embora seja tecnicamente possível comprar leitoras independentemente e deixar a instalação nas mãos da sua experiente equipe de TI, conforme o mencionado anteriormente, esse método não é recomendável e pode ser um desperdício de tempo e dinheiro. Uma conversa com o fabricante das impressoras ou com o parceiro de gerenciamento de impressão sobre sua preferência de credencial para o presente e o futuro, a experiência que se deseja para o usuário em termos de distância e comprovação de presença, e o posicionamento das leitoras garante uma implementação econômica e sem dificuldades.

Descubra a sua solução

A compreensão dos fundamentos da impressão segura e de suas necessidades atuais e futuras, ajudará a guiar a conversa com o fabricante das impressoras ou com o parceiro de gerenciamento de impressão. Eles são a variável mais importante para a implementação da impressão segura e podem prestar assessoria para determinar de que, exatamente, a sua organização precisa — ou não precisa. A solução correta de impressão segura combina segurança e conveniência. É mais um passo rumo a um ambiente de trabalho realmente conectado. As organizações conseguem realizar economias substanciais ao eliminar impressoras pessoais e documentos impressos sem necessidade, reduzindo o desperdício e aprimorando a alocação dos custos.

E o melhor de tudo é que, com a utilização das credenciais atuais, já conhecidas pelos usuários e pela TI, o treinamento necessário é mínimo. Você pode sentir-se confiante de que a sua solução de impressão segura será simplesmente uma extensão de sua solução de identidade confiável, e o próximo passo para que o seu ambiente de trabalho esteja realmente conectado.

Acesse o nosso site para saber mais sobre o portfólio de impressão segura líder do mercado.

2019-05-06-hid-eat-secure-print-wp-pt

PLT-04761

[1] *Pesquisa realizada pela Quocirca: http://quocirca.com/wp-content/uploads/2018/06/Quocirca-Print-Security-Jan-2017-Report- Excerpt.pdf*

[2] *Pesquisa realizada pela Nuance: https://whatsnext.nuance.com/office-productivity/orphaned-print-jobs-silent-security-leak/*