LIBRO BLANCO

Implementación de la impresión segura

¿Qué es una identificación confiable?

Una identificación confiable es una identificación validada que utiliza una credencial biométrica o una credencial aprovisionada en una tarjeta o un dispositivo móvil o en una prenda o accesorio electrónico. En un lugar de trabajo conectado se puede utilizar una identificación confiable para ingresar a varios sistemas, como acceso a edificios, control de asistencia y tiempo de trabajo e impresión segura.

Cómo aprovechar sus credenciales de identificación confiables actuales para imprimir de forma más fácil y segura

Una experiencia de impresión más segura y sencilla

Después de que se imprime un documento confidencial, puede caer fácilmente en las manos equivocadas, lo cual plantea un enorme riesgo de seguridad que se suele pasar por alto. De hecho, el 70% de las organizaciones han sufrido una filtración de información relacionada con la impresión. Muchas de ellas también se enfrentan a complicadas asignaciones y errores de seguimiento cada vez que los usuarios no son adecuadamente identificados. Además, muchos métodos corrientes de impresión "segura" son demasiado engorrosos para los usuarios o demasiado vulnerables a las filtraciones de información. Por ejemplo:

- Los teclados para el ingreso del PIN ofrecen la comodidad de no tener que llevar nada consigo, pero requieren que el usuario recuerde su código y que no lo comparta con nadie
- Las contraseñas se pierden, se olvidan o comparten con frecuencia, lo cual hace necesario que el departamento informático de una organización tenga que actualizarlas, cambiarlas o recuperarlas constantemente
- Los códigos QR son sorprendentemente fáciles de copiar y clonar, lo cual genera una falsa sensación de seguridad

Una manera efectiva de hacer frente a estas preocupaciones es emplear las credenciales de identificación que ya están en uso para poner en marcha programas de impresión segura. El hecho de incorporar una impresión segura a las credenciales de identificación confiables con las que ya cuenta la organización, como escarapelas, dispositivos móviles y biometría, no solo aumenta la seguridad, sino que además ofrece una experiencia más fácil de usar para los usuarios y es bastante simple de implementar con la ayuda de un fabricante experimentado de impresoras o de un socio proveedor de impresión gestionada. El presente libro blanco ayuda a las organizaciones a comenzar a explorar el mundo de la impresión segura, mediante el análisis de sus dos componentes fundamentales: las credenciales y los lectores. Después de leerlo, comprenderá los conceptos básicos de la impresión segura y la forma en que esta puede funcionar dentro de su solución actual de gestión de identificaciones confiables.

Más segura, ecológica y eficiente: Impresión segura

Sin la impresión segura, los documentos son enviados a la impresora y su impresión es autorizada de inmediato. Eso no representa ningún problema si el usuario retira inmediatamente el documento impreso, pero es necesario que dicho usuario esté en la impresora en el momento en que el documento se imprima (por ejemplo, cuando la impresora está justo al lado del computador del usuario). Sin embargo, dado que no es factible que cada usuario tenga su propia impresora, la mayoría de los trabajos se imprimen en una impresora central, la cual se encuentra a cierta distancia del usuario.

La confidencialidad no es el único aspecto que está recibiendo mayor atención, la certificación ambiental y tener una buena reputación de respeto por el medio ambiente son cada vez más atractivos para los consumidores.

Este tipo de situaciones es común en el sector de la atención médica, donde los médicos tratan a los pacientes en las salas de examen, ingresan su información en un computador portátil y la imprimen en una impresora de una oficina central. Así, la información confidencial del paciente permanece en la impresora hasta que el personal de oficina, u otra persona que esté cerca, retire el documento impreso.

Gracias a la impresión segura, que utiliza una identificación confiable, la autorización de impresión del documento no se lleva a cabo de inmediato. En cambio, el documento no se imprime hasta que el médico o usuario autorizado autentique su identidad en la impresora, utilizando la misma tarjeta, el mismo dispositivo o los mismos datos biométricos que utiliza con otros sistemas de control de acceso (por ejemplo, para entrar al edificio o tener permiso de estacionar). Tanto el médico como el paciente, así como los auditores de la ley HIPAA (Ley de Transferencia y Responsabilidad de Seguro Médico), saben que solo se puede tener acceso a esa información confidencial mediante la debida autorización. Las empresas de todos los sectores industriales pueden beneficiarse de este nivel de confidencialidad, especialmente ante la aparición de nuevas y más estrictas reglamentaciones como la GDPR (Normativa de protección de datos) y la importancia cada vez mayor que se da a los sistemas empresariales con restricción de acceso a la información.

Por supuesto, la confidencialidad no es el único aspecto que está recibiendo mayor atención, la certificación ambiental y tener una buena reputación de respeto por el medio ambiente son cada vez más atractivos para los consumidores. Las compañías que reportan sus resultados ambientales, sociales y financieros están ansiosas por incorporar iniciativas de sostenibilidad, pero incluso aquellas que no tienen una filosofía explícita de protección del medio ambiente tienen interés en ahorrar dinero. La impresión segura puede ayudar Se estima que el usuario original nunca recoge el 20% de los trabajos que imprime, lo cual se traduce no sólo en considerables desperdicios financieros y ambientales diarios, sino que además complica innecesariamente y eleva de forma excesiva las asignaciones de costos de los distintos departamentos. Con la impresión segura, los documentos permanecen en la cola del servidor de impresión hasta que su impresión sea autorizada, lo cual permite reducir gastos innecesarios y al mismo tiempo cuidar el planeta.

Sin embargo, no todos los métodos de impresión segura son iguales. Diseñar el programa adecuado implica comprender los sistemas y las necesidades de su organización, así como contar con aliados al comienzo del proyecto. Después de todo, no es ni ecológica ni fiscalmente responsable construir un sistema y luego desmontarlo y reemplazarlo por uno nuevo. Para garantizar el éxito, los encargados de los sistemas informáticos deben tener en cuenta lo siguiente:

Entender sus credenciales actuales

Comience por preguntarse: ¿Qué mecanismo de autenticación le gustaría usar a su organización para la impresión segura? La mayoría prefiere trabajar con sus credenciales de control de acceso actuales, las cuales les permiten partir de la base de los sistemas existentes en lugar de empezar desde cero. A menos, por supuesto, que su sistema actual esté desactualizado y que sea necesario actualizarlo. Piense en la forma en que desea que sus usuarios experimenten la impresión segura ahora y en el futuro.

Si utiliza tarjetas o credenciales:

Las tarjetas son el tipo de identificación más común que se puede ampliar para implementar una impresión segura. Hay una gran número de nuevas tecnologías que se usan actualmente. Si bien en el futuro las tarjetas podrían llegar a ser menos predominantes, se seguirán empleando por mucho tiempo. El tipo de tarjeta, las necesidades y la marca determinarán el tipo de lectores que deberá proporcionar su fabricante de impresoras, así como el nivel de seguridad alcanzado. Los siguientes son los tipos más comunes de tarjetas:

Asegúrese de averiguar opciones de identificaciones móviles y prendas y accesorios electrónicos que no estén vinculadas a una marca específica.

Tarjetas de proximidad (prox): Estas tarjetas de 125 kilohercios son increíblemente fáciles de usar: todo lo que hay que hacer es sostener la tarjeta cerca de la impresora y se autoriza la impresión del trabajo. Desafortunadamente, ofrecen el nivel más bajo de seguridad. Las tarjetas de proximidad asignan un número de serie a una persona que el lector verifica, pero este número se puede clonar con relativa facilidad.

Tarjetas inteligentes: Las tarjetas inteligentes como HID Seos® utilizan números de serie aleatorios para establecer la comunicación con el lector, lo cual hace que la clonación sea casi imposible. También ayudan a evitar la colisión de tarjetas: Si dos usuarios de tarjetas de proximidad se encuentran en el mismo espacio, es posible que el lector de tarjetas no funcione, mientras que las tarjetas inteligentes permiten que el lector seleccione la indicada.

Etiquetas/adhesivos: Si tiene tarjetas obsoletas o tarjetas a las que su proveedor actual no brinde soporte, podría agregarles una etiqueta o un adhesivo para facilitar la comunicación con el lector. Sin embargo, estas etiquetas son de 125 kHz y por lo tanto no son tan seguras como las tarjetas inteligentes.

Varios tipos de tarjetas: Las organizaciones más grandes pueden tener diferentes tipos de tarjetas según la ubicación y el nivel de seguridad. Por ejemplo, es posible que en la sede principal de la empresa se utilice Seos® para el acceso a los edificios, mientras que en las oficinas satélite se utilicen tarjetas de proximidad. Algunos lectores se pueden configurar para que lean varios tipos de tarjetas. Asegúrese de que el encargado o el fabricante de las impresoras comprenda esta necesidad.

Si utiliza o está considerando utilizar credenciales móviles o portátiles:
El acceso móvil está defintivamente en auge, y si su organización no lo está utilizando en este momento, es probable que lo haga en el futuro. Si actualmente utiliza tarjetas, el hecho de optar por lectores que funcionen tanto con dispositivos móviles como con tarjetas le permitirá realizar el cambio con un nivel mínimo de interrupción de las actividades de su compañía.

Las credenciales móviles y las prendas y accesorios electrónicos, como cualquier otra opción, ofrecen diferentes grados de seguridad: los códigos QR que aparecen en un teléfono móvil son relativamente poco seguros y fáciles de copiar. Las balizas Bluetooth y las etiquetas NFC, por otro lado, ofrecen mayor seguridad y no se pueden copiar. La credencial móvil también es mucho más fácil de implementar y administrar que las tarjetas; las actualizaciones se pueden enviar inmediatamente sin asistencia en las instalaciones de la organización.

Asegúrese de averiguar opciones móviles y de prendas y accesorios electrónicos que no estén vinculados a una marca específica. Por ejemplo, su solución móvil de impresión segura debería funcionar para los usuarios de iPhone y Android.

Si utiliza credenciales biométricas:
las opciones biométricas, como el escaneo de huellas dactilares, ofrecen un nivel sumamente alto de seguridad y comodidad para el usuario. Teniendo en cuenta este avanzado nivel de seguridad, no es de extrañar que también sean una opción costosa. Muchas organizaciones optan por utilizar biometría junto con otra credencial, como identificaciones móviles y tarjetas. Además, incluso la biometría ofrece diferentes niveles de seguridad. Los gobiernos y otras organizaciones que requieren de alta seguridad utilizan servicios adicionales, como la detección de dedo vivo, que garantiza que la huella dactilar está vinculada a una identidad confiable y viva.

La solución de impresión segura ideal combina seguridad y comodidad, acercando así a su organización al propósito de convertirse en un lugar de trabajo verdaderamente conectado.

Determine cuáles son los lectores que necesita

Una vez tenga una comprensión clara de sus credenciales y las funciones de estas, es hora de considerar la mejor opción de lector que le permita implementar la impresión segura. En primer lugar, determine si necesita un lector para autorizar trabajos de impresión desde varios metros de distancia, o si es necesario que el usuario esté directamente frente a la impresora antes de autorizar el trabajo. Las tarjetas, la biometría y algunas aplicaciones con dispositivos móviles/prendas o accesorios electrónicos requieren que el usuario toque la impresora con su credencial, asegurando así que el usuario esté allí para recoger el documento de inmediato. Por otro lado, es posible que desee la comodidad que brinda un lector que detecta la señal de una credencial a varios metros de distancia.

A continuación, analice si prefiere que el lector esté alojado dentro de la impresora o que esté instalado en el exterior. Los lectores integrados ofrecen un aspecto más agradable, pero necesitan espacio dentro de la carcasa de la impresora y habilidades técnicas robustas para su instalación y mantenimiento. Los lectores de escritorio o los que vienen en una carcasa, por otro lado, tienen la apariencia de un pequeño disco duro que se puede conectar a la impresora e intercambiarse según sea necesario. Los lectores de escritorio también evitan que la carcasa de la impresora interfiera con la señal.

El nivel de interoperabilidad de los lectores también varía, incluso si una organización utiliza todas las tarjetas Seos®, es posible que un lector no pueda verificar las tarjetas asignadas en una ubicación y utilizadas en otra. Además, no todos los lectores funcionan con todas las credenciales; por ejemplo, si en este momento su organización utiliza tarjetas pero está contemplando cambiar a identificaciones móviles, elija un lector que funcione con ambas.

Por último, determine las conexiones y los conectores disponibles. Por ejemplo:

- ¡ Las conexiones USB se conectan externamente, permiten el ajuste automático de la antena del lector de tarjetas y son fáciles de ajustar en el lugar de la instalación. En el caso de los lectores biométricos, la conectividad USB es más fácil de configurar e implementar.
- ¡ Las conexiones UART requieren la instalación interna en la impresora y pueden ser difíciles de ajustar.

Consulte con su más importante aliado: El fabricante de sus impresoras o su socio de impresión gestionada

Por último, deberá tener una conversación a fondo con el fabricante o administrador de sus impresoras. Si bien es técnicamente posible comprar lectores de forma independiente y pedir a su experimentado equipo de informática que los instale, como se mencionó antes, esta alternativa no es recomendable y podría constituir una pérdida de tiempo y dinero. Analizar con su fabricante de impresoras o socio de impresión gestionada la credencial de su elección para el presente y el futuro, la experiencia que desea ofrecer al usuario en cuanto a distancia y prueba de presencia, así como la ubicación de los lectores le garantizará una implementación sin complicaciones y económica.

Encuentre su solución ideal

Entender los fundamentos de la impresión segura y sus necesidades actuales y futuras le ayudará a encauzar la conversación con el fabricante de impresoras o el socio de impresión gestionada. Ellos constituyen la variable más importante a la hora de implementar una impresión segura, pues tienen la capacidad de asesorarlo con precisión sobre lo que su organización necesita, o sobre aquello que puede no necesitar en absoluto. La solución de impresión segura ideal combina seguridad y comodidad, acercando así a su organización al propósito de convertirse en un lugar de trabajo verdaderamente conectado. Las organizaciones logran ahorros sustanciales al eliminar las impresoras

personales y documentos que se imprimen de forma innecesaria, reducir el desperdicio y asignar mejor los costos.

Lo mejor de todo es que dado que se aprovechan las credenciales actuales con las que los usuarios y el departamento informático ya están familiarizados, se requiere muy poca capacitación. Puede tener la certeza de que su solución de impresión segura es simplemente una extensión de su solución de identificación confiable y un paso más hacia la transformación de su organización en un lugar de trabajo verdaderamente conectado.

Visite nuestro sitio web para obtener más información sobre el portafolio de lectores para impresión segura más destacado del mercado.

---

[1] *Investigación de Quocirca: http://quocirca.com/wp-content/uploads/2018/06/Quocirca-Print-Security-Jan-2017-Report- Extracto.pdf*

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

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

PLT-04760