



CONTROL

SEGURIDAD PARA LOS MFP, LAS COMUNICACIONES EN RED Y LOS DOCUMENTOS

Su organización depende de redes complejas de personas conectadas, procesos y tecnología, para lograr los resultados que se desean. Además, hoy es más importante que nunca asegurar los datos. Sus impresoras multifuncionales son una parte integral de esta red conectada ya que ayudan a salvaguardar la información confidencial, a proteger los datos de los empleados y de los clientes y le ayudan en sus esfuerzos por cumplir con las normas. Con características de seguridad integradas y actualizadas con frecuencia, la Serie imageRUNNER ADVANCE de Canon le puede ayudar a obtener altos niveles de control sobre sus MFP, sus comunicaciones en red y sus documentos.

CONTROL

SUS IMPRESORAS MULTIFUNCIONALES



Características de seguridad avanzadas para sus MFP: para su tranquilidad, muchas son estándares y todas son uniformes en toda la línea de productos.



CONTROL DE ACCESO A LOS DISPOSITIVOS

Por medio de una variedad de métodos de autenticación flexibles, los administradores pueden controlar quién tiene acceso al MFP y a qué características. Esto se puede realizar mediante un PIN, un nombre de usuario y una contraseña, o con una tarjeta de conexión (con la adición de un lector de tarjetas opcional). Se pueden aplicar restricciones, tales como el acceso a las funciones de copiado y escaneo en color. Estas pueden ser individuales, grupales o mediante funciones personalizadas. También se puede definir si se permite que usuarios no registrados, tales como los visitantes, se conecten como invitados y luego especificar su nivel de acceso.

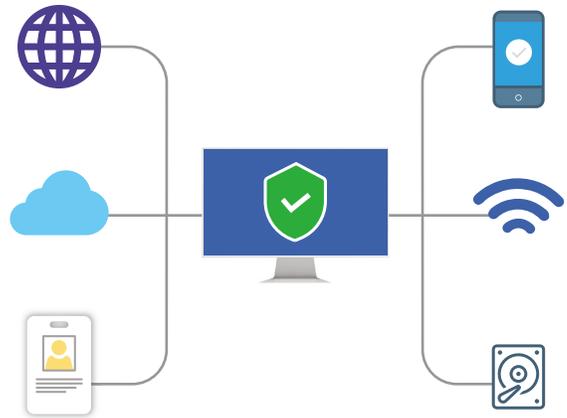
ACCESO DE CONTROL A

LAS FIJACIONES DE ADMINISTRACIÓN

Las configuraciones de los dispositivos, tales como las fijaciones de red y otras opciones de control, están disponibles solo para los usuarios con privilegios de administrador. Esto mejora la seguridad al ayudar a evitar cambios intencionales o accidentales a las funciones y permisos de los dispositivos. Los administradores pueden fijar los requisitos para las contraseñas, tales como el periodo de expiración, el tiempo de bloqueo y la complejidad. Incluso pueden acceder al dispositivo de forma remota y con completo control, desde cambiar los permisos hasta supervisar la actividad, incluso activar o desactivar los dispositivos, o bloquear funciones o equipos específicos.

CONFIGURACIONES CENTRALIZADAS DE SEGURIDAD

Las configuraciones de seguridad se pueden configurar desde una ubicación centralizada, protegida por contraseña y accesible solo a los usuarios autorizados. Esto les da a las organizaciones la capacidad de separar la administración de la seguridad de la administración de los dispositivos, y de reservar el acceso a ciertos controles para los profesionales de la seguridad. Las configuraciones de la política de seguridad se pueden supervisar a intervalos regulares, con notificaciones configuradas para alertar a los administradores cuando se realizan cambios. Después de establecer estas configuraciones, el administrador puede usar las herramientas de administración del dispositivo para exportar a otros dispositivos en el grupo. Esto crea configuraciones de seguridad uniformes en todo el sistema, con poco tiempo y esfuerzo.



SUS DATOS VALIOSOS

Los modelos imageRUNNER ADVANCE ofrecen asistencia estándar para la Encriptación de la HDD, aprovechando un módulo criptográfico que cumple con el estándar de seguridad FIPS 140-2. Esto ayuda a proteger la información confidencial que se guarda en el disco duro. El sistema también incluye características robustas de borrado de datos que pueden sobrescribir los datos anteriores como parte del procesamiento rutinario de trabajos, así como inicializar y borrar permanentemente todos los datos al final de la vida útil del equipo. La sobrescritura del disco duro se puede llevar a cabo por demanda o mediante programación, y se puede proporcionar un informe de confirmación.*

Los modelos imageRUNNER ADVANCE ofrecen la posibilidad de ayudar a verificar que el proceso de arranque del dispositivo, el firmware y las aplicaciones se inicializan al activarse, sin alteración ni manipulación por parte de terceros malintencionados. Durante la operación, el Control Integrado de McAfee utiliza una lista blanca para la protección contra la ejecución de programas malignos (malware) y la manipulación del firmware y de las aplicaciones.**



* El Programador de Borrado de Datos de la HDD con informe de confirmación es opcional.
** Compatible con los modelos imageRUNNER ADVANCE de tercera generación (primera, segunda y tercera edición) e imageRUNNER ADVANCE DX solamente. El Control Integrado de McAfee requiere la Plataforma de firmware unificada v3.9.

CONTROLE

SUS COMUNICACIONES EN RED



Un rango de soluciones de seguridad para ayudar a mantener los datos seguros contra ataques internos y externos a medida que viajan por la red.

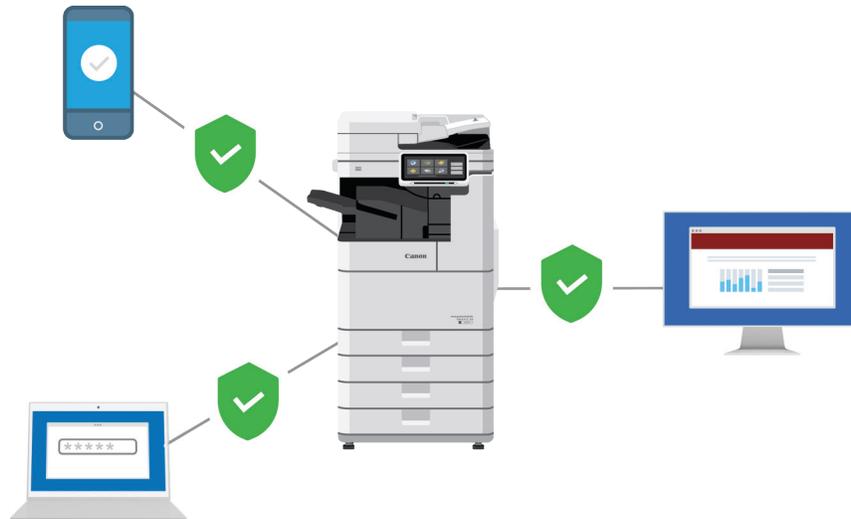
ENCRIPCIÓN DEL TRÁFICO POR LA RED

Los modelos imageRUNNER ADVANCE incluyen varias características de seguridad para ayudar a proteger los datos que se envían a través de la red. IPsec (Seguridad del Protocolo de Internet) protege el intercambio de los datos a nivel de las comunicaciones mediante la encriptación del tráfico de red entrante y saliente, la confirmación de la identidad del emisor y la garantía de que la recepción de la transmisión sea inalterada. La encriptación TLS 1.2 (Seguridad de la Capa de Transporte) previene aún más el acceso a los datos que se intercambian y la alteración de los mismos, y ayuda a mantener la seguridad de la información durante el tránsito.



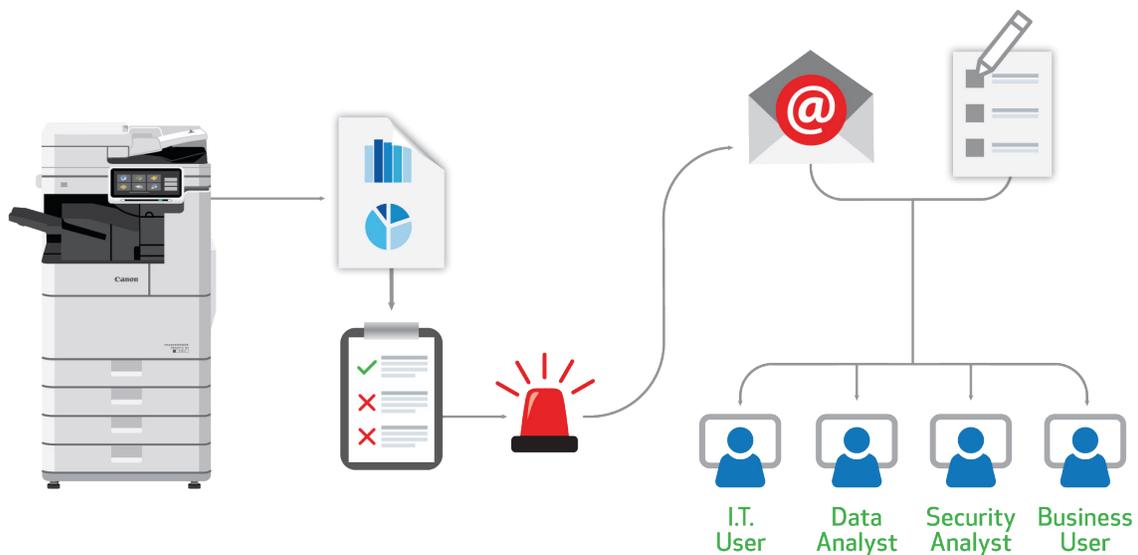
CONEXIONES EN RED

Los sistemas imageRUNNER ADVANCE de Canon son compatibles con el protocolo IEEE 802.1x, proporcionan autenticación a los dispositivos en red y establecen una conexión cerrada. El protocolo está diseñado para evitar que usuarios no deseados se conecten a la red, ya sea que utilicen una conexión con cables o un dispositivo móvil.



SE INTEGRA CON LOS SISTEMAS SIEM

Los sistemas de Información de Seguridad y de Administración de Eventos (SIEM, por sus siglas en inglés) pueden ser herramientas valiosas, que ofrecen a los administradores de redes información completa referente a la actividad de su red. La plataforma imageRUNNER ADVANCE está conformada para integrarse con su infraestructura SIEM actual, y se comunica directamente con estas herramientas de terceros para ayudar a entregar la información a su entorno de Impresión. Los administradores pueden establecer alertas para recibir notificaciones de problemas posibles tales como intentos de autenticación fallidos, cambios en las fijaciones, nuevas solicitudes y más. Esta comunicación entre los MFP imageRUNNER ADVANCE y los sistemas SIEM puede permitirle detectar las potenciales amenazas a su red e impresoras.



CONTROLE SUS DOCUMENTOS



Diversas soluciones de seguridad para ayudar a proteger documentos confidenciales a lo largo de su ciclo de vida.



MANTENGA LOS DOCUMENTOS EN LAS MANOS CORRECTAS

Todas las organizaciones gestionan documentos confidenciales. Si los documentos caen en las manos incorrectas, las consecuencias pueden ir desde daños a la reputación hasta altas multas o incluso acciones legales. La información confidencial, incluyendo los expedientes de los empleados, la información de los clientes y la propiedad intelectual exclusiva, es vulnerable cuando queda desatendida en las bandejas de salida. Para evitar que tales documentos queden en la impresora, los usuarios pueden crear un PIN que se debe ingresar en el dispositivo para liberar el trabajo. Los administradores también pueden exigir que los usuarios se conecten antes de imprimir sus trabajos mediante uno de los diversos métodos de autenticación.



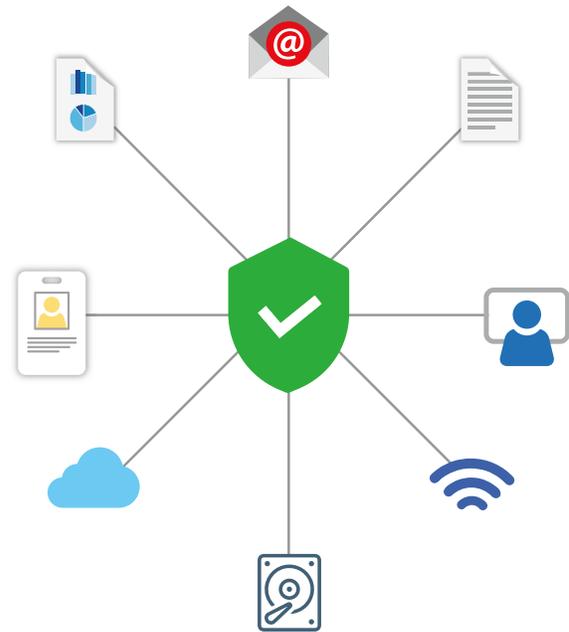
SEGURIDAD DEL FLUJO DE TRABAJO

Ya sea por error humano o con mala intención, los flujos de trabajo diarios pueden conducir a información mal dirigida, y potencialmente causar graves problemas de seguridad. Los dispositivos imageRUNNER ADVANCE tienen varias características que pueden ayudar: todas son fáciles de usar y están bajo el control del administrador. Los destinos de escaneo se pueden restringir para todos los usuarios o para ciertos grupos, tales como los invitados. Esto limita la capacidad de enviar documentos a aquellos destinatarios en una libreta de direcciones específica o dominio. Incluso para niveles más altos de control, a los usuarios se les puede permitir enviar documentos solo a ellos mismos. Las libretas de direcciones se pueden mantener confidenciales para proteger los detalles privados. Además, se pueden proteger mediante contraseña de manera que solo los usuarios autorizados puedan añadir, editar o eliminar la información.

Para las transmisiones por fax, los documentos entrantes se guardan en un formato de propiedad exclusiva que ayuda a protegerlas de actividad mal intencionada. Los faxes entrantes legítimos se pueden dirigir a buzones específicos o se pueden proteger mediante un PIN bajo el control del administrador. También se puede limitar y controlar el destino de los faxes salientes.

PROTEJA SUS PDF

A menudo los PDF representan algunos de los documentos más confidenciales en una organización, con el formato que generalmente se utiliza para contratos, informes, propuestas, estados financieros e información confidencial similar. La característica* integrada de PDF Encriptado permite varios niveles de encriptación para mejorar la seguridad al enviar estos documentos. Se pueden incluir permisos y contraseñas para controlar quién puede abrir, leer o imprimir el archivo. Para ayudar a garantizar la legitimidad de los documentos altamente confidenciales, los usuarios pueden agregar firmas digitales para verificar la fuente y la autenticidad de los documentos. Esta firma se puede ver por medio de las propiedades del documento o se puede desplegar de forma prominente en las páginas de los PDF.



ADMINISTRACIÓN DEL CONTENIDO DE LA NUBE

La información comercial importante se puede guardar en diversos lugares dentro de una organización. La tecnología del flujo de trabajo que pueda simplificar la comunicación y ofrecer características de seguridad es una prioridad. La fuerte interacción de Canon con Box y mxHero** ofrece a los clientes capacidades poderosas, basadas en la nube, para tratar muchos problemas que a suceden con frecuencia al enviar y recibir archivos grandes, incluyendo la necesidad de medidas de seguridad y los altos costos relacionados con el almacenamiento de correo electrónico. A medida que los correos electrónicos pasan por mxHero, el contenido del mensaje y los archivos adjuntos se pueden enviar de forma automática a una cuenta de almacenamiento en la nube con acceso restringido e indexada, tal como Box, para transformar buzones voluminosos y potencialmente vulnerables en buzones livianos y controlados. Las soluciones de Box les ofrecen a los usuarios una diversidad de características de seguridad, incluyendo la capacidad de restringir cuándo se puede acceder a los archivos y quién puede hacerlo.



* Estándar en los modelos imageRUNNER ADVANCE de tercera generación (primera, segunda y tercera edición) e imageRUNNER ADVANCE DX. Opcional en los modelos de la primera edición.

** La integración de Box y mxHero requiere de soluciones opcionales.

Los modelos imageRUNNER ADVANCE de tercera generación (primera, segunda y tercera edición) e imageRUNNER ADVANCE DX

CARACTERÍSTICAS DE SEGURIDAD		Serie C7500, Serie C5500, Serie C3700, Serie C356iF, Serie C475iF, Serie 8500, Serie 6500, Serie 4700, Serie 715iF
Administración de los dispositivos		
Verificación del sistema en el arranque		Estándar (Disponible en los modelos imageRUNNER ADVANCE de tercera generación y imageRUNNER ADVANCE DX)
Control Integrado de McAfee		Estándar (Disponible en los modelos imageRUNNER ADVANCE de tercera generación y imageRUNNER ADVANCE DX)
Administración de seguridad		
Configuraciones de la política de seguridad		Estándar
Integración con SIEM		Estándar
Autenticación		
Active Directory/SSO		Estándar
Universal Login Manager		Estándar
uniFLOW Online Express		Estándar
uniFLOW/uniFLOW Online		Opcional
Tarjeta de proximidad o CAC/PIV		Opcional
Control de acceso		
Configuración del sistema mediante contraseña		Estándar
Sistema de administración de acceso		Estándar
Bloqueo de USB		Estándar
Seguridad de los datos		
TPM (Módulo de Plataforma Confiable)		Estándar
Bloqueo de contraseña del disco duro		Estándar
Formateo de los datos del disco duro (EOL)		Estándar (9x)
Borrado de los datos del disco duro		Estándar
Programador del borrado de los datos del disco duro de MEAP		Opcional
Encriptación de los datos del disco duro		Estándar (FIPS 140-2 Validated)
Copias impresas y seguridad del sistema		Opcional (Criterios Comunes IEEE2600)*
Kit del disco duro extraíble		Opcional/NA**
Seguridad de los documentos		
Impresión segura (Basada en el software controlador)		Estándar
Impresión segura encriptada (Basada en el software controlador)		Estándar (Disponible en los modelos imageRUNNER ADVANCE de segundo y tercera generación e imageRUNNER ADVANCE DX)***
Impresión segura (Servidor/Nube)		Opcional
Sello de agua seguro		Estándar (Disponible en los modelos imageRUNNER ADVANCE de segundo y tercera generación e imageRUNNER ADVANCE DX)***
Seguridad del buzón		Estándar
PDF encriptado (Compatible con AES 256)		Estándar (Disponible en los modelos imageRUNNER ADVANCE de segundo y tercera generación e imageRUNNER ADVANCE DX)***
PDF con firma digital del dispositivo		Estándar (Disponible en los modelos imageRUNNER ADVANCE de segundo y tercera generación e imageRUNNER ADVANCE DX)***
Bloqueo de escaneo de documentos		Opcional/NA*
Seguridad de la red		
Administración de puerto, dirección IP, filtro MAC		Estándar
IPSec		Estándar
Selección del algoritmo de cifrado		Estándar
Compatibilidad con TLS1.1/1.2 e inhabilitación de SSL 3.0		Estándar
Certificaciones		
Criterios Comunes IEEE 2600		Opcional*
FIPS 140-2		IPSEC/CAC/PIV/Encriptación de la HDD/TLS

* Es posible que el kit IEEE 2600 no esté disponible al mismo tiempo que se lance el producto; verifique la disponibilidad con su distribuidor autorizado de Canon.

** No disponible con la serie imageRUNNER ADVANCE 715iF/615iF/525iF/C356iF/C475iF.

*** Opcional en modelos de tercera generación de imágenesRUNNER ADVANCE primera edición.

♦ No disponible con la serie imageRUNNER ADVANCE 715iF/615iF/525iF/C475iF.

Nota: Algunas características requieren de actualización conforme a la versión más reciente de United Firmware Platform.

 www.cla.canon.com/imageRUNNER_ADV_Series



Canon U.S.A., Inc.
Latin America Group
One Canon Park
Melville, NY 11747
U.S.A.

Consulte la disponibilidad de los productos. Canon U.S.A. no brinda asesoría jurídica ni consultoría de cumplimiento regulatorio, incluyendo sin limitación las leyes Sarbanes-Oxley, HIPAA, GLBA, Check 21 ni la Ley Patriota de los Estados Unidos de América. Cada cliente debe tener su propio asesor jurídico idóneo para determinar la conveniencia de una solución en particular en lo que se refiere al cumplimiento normativo y legal.

Como socio de ENERGY STAR®, Canon U.S.A., Inc. certificó que estos modelos cumplen con los criterios de eficiencia energética de ENERGY STAR mediante un organismo de certificación reconocido por la EPA, ENERGY STAR y la marca ENERGY STAR son marcas registradas en los Estados Unidos de América. Canon, imageRUNNER, imageWARE y el logotipo de GENUINE son marcas registradas o marcas de fábrica de Canon Inc. en los Estados Unidos de América y también pueden ser marcas registradas o marcas de fábrica en otros países. Therefore es una marca registrada de Therefore Corporation. uniFLOW es una marca registrada de NT-ware Systemprogrammierung GmbH. Google Cloud Print™ es una marca registrada o una marca de fábrica de Google Inc. AirPrint y el logotipo de AirPrint son marcas de fábrica de Apple Inc. Todos los otros nombres de productos y marcas a los cuales se hace referencia son marcas de fábrica de sus respectivos propietarios. McAfee y el logotipo de McAfee son marcas de fábrica de McAfee LLC en los Estados Unidos de América y/o en otros países. Todas las imágenes de pantalla son simuladas. Es posible que todas las características que aparecen en este folleto no se apliquen a todas las series o productos y que puedan ser opcionales; consulte estos detalles con su distribuidor autorizado Canon. Los productos se muestran con accesorios opcionales. Las especificaciones y la disponibilidad podrían cambiar sin previo aviso. No nos hacemos responsables por errores tipográficos.
©2020 Canon U.S.A., Inc. Todos los derechos reservados.

