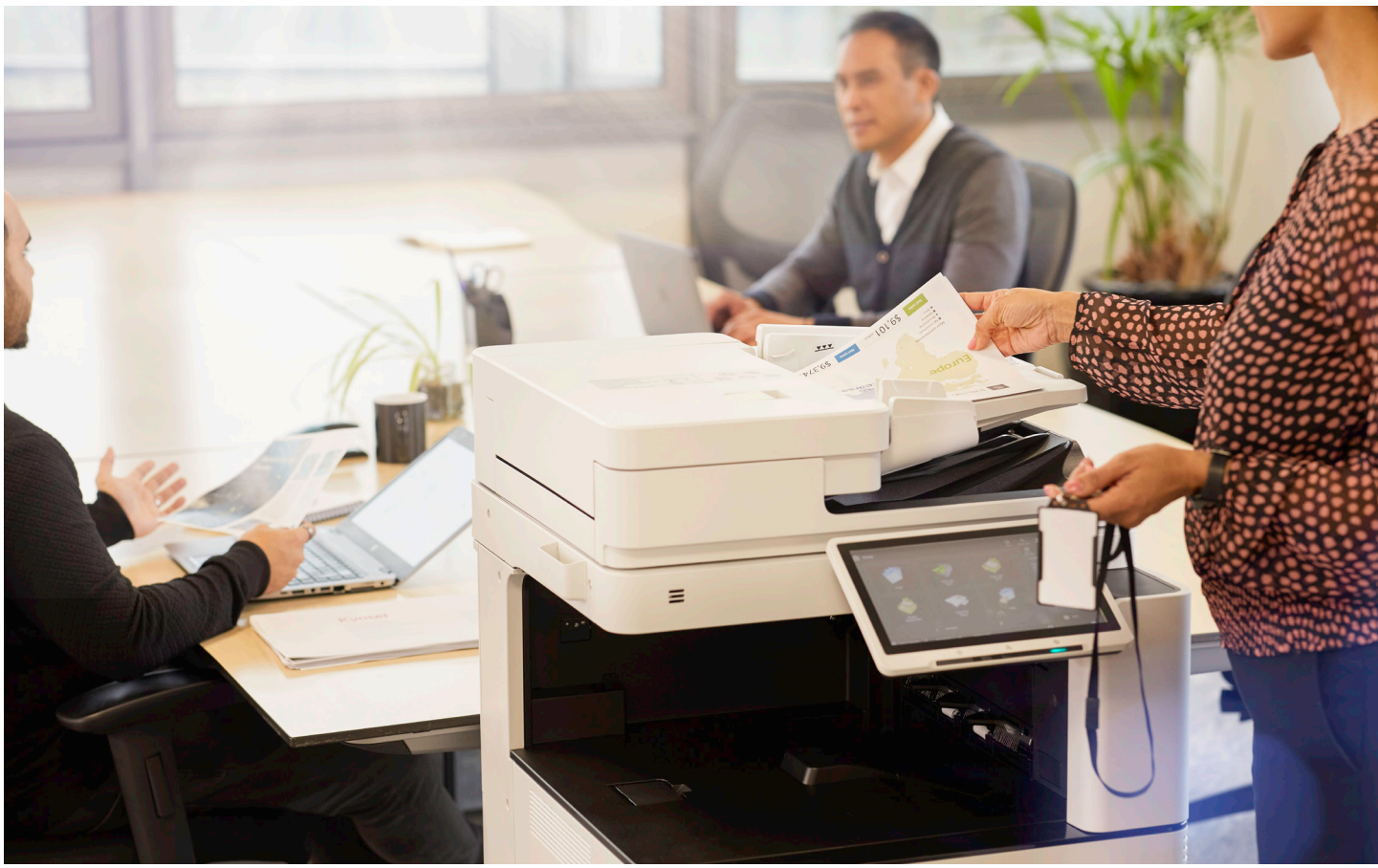

SCHÜTZEN SIE IHR BÜRO

McAfee PROTECTED

COPIER MFP LINE OF THE YEAR 2018 BLI BUYERS LAB LINE OF THE YEAR

BLI BUYERS LAB 2019 PICK
Canon uniFLOW Online
Outstanding Cloud Output-Management Solution

COPIER MFP LINE OF THE YEAR 2020 BLI BUYERS LAB LINE OF THE YEAR

Canon

WIE SICHER SIND INFORMATIONEN IN IHREM BÜRO?

Moderne Unternehmen sind auf Daten angewiesen. Dies bedingt komplexe technische Netzwerke, die Prozesse, Menschen und Organisationen länderübergreifend verbinden. In Zeiten des digitalen Wandels entstehen neue agile Arbeitsformen, die das Büro und die Art und Weise verändern, wie Menschen Informationen erstellen, teilen und nutzen. Der Schutz von Daten ist in diesen komplexen Umgebungen schwieriger als je zuvor. Die meisten Unternehmen investieren deshalb in höchst anspruchsvolle Technologien wie robuste Firewalls, aktuellen Virenschutz, Sicherheits-Software und vieles mehr. Doch die Notwendigkeit, diesen Schutz auf Bürodrucker auszudehnen, wird oft nicht erkannt, wodurch diese verwundbarer sind, als vielen bewusst ist.

DENKEN SIE AN IHRE DRUCKER

Moderne Multifunktionsdrucker (MFPs) haben sich zu leistungsstarken Geräten entwickelt, die wie Computer und Server ein Betriebssystem und Festplatten enthalten sowie mit dem Netzwerk und Internet verbunden sind und von vielen Personen gemeinsam genutzt werden, die täglich enorme Mengen unternehmenswichtiger Dokumente verarbeiten.

WELCHE RISIKEN GIBT ES?

- Unbefugte Benutzer erhalten Einblick in vertrauliche Daten, die auf ungeschützten MFPs gespeichert sind.
- Eine Fehlbedienung gefährdet die Druckinfrastruktur.
- Böswillige Außenstehende erhalten über den Drucker Zugriff auf Ihr Netzwerk, sodass sie weitere Angriffe starten können.
- Vertrauliche Dokumente, die nach dem Drucken im Ausgabefach vergessen wurden, werden verbreitet.
- Gedruckte Dokumente, die von verschiedenen Benutzern gesendet wurden, geraten im Ausgabefach durcheinander.
- Dokumente werden aufgrund eines Tippfehlers an den falschen Empfänger per Fax oder E-Mail gesendet.
- Hacker fangen die Druck- oder Scandaten während der Übertragung ab.
- Die unsachgemäße Entsorgung von Druckern am Ende der Leasingdauer führt zur unbeabsichtigten Offenlegung von Daten.

„Für die Datensicherheit im Büro, in dem große Datenmengen verarbeitet werden, sind grundlegende Standards unabdingbar. Ein Drucker ist heutzutage keine dumme Maschine mehr, sondern vielmehr ein Server, der nebenbei auch noch druckt."

(CISO, Publicis Groupe)

SICHERE DRUCKLÖSUNGEN FÜR IHR UNTERNEHMEN

Sicherheit und Datenschutz serienmäßig

Wenn wir Produkte und Dienstleistungen für unsere Kunden entwickeln oder auswählen, stellen wir ihren möglichen Einfluss auf die Datensicherheit in der Kundenumgebung in den Mittelpunkt. Deshalb sind unsere Büro-Multifunktionsdrucker mit einer Vielzahl standardmäßiger oder optionaler Sicherheitsfunktionen ausgestattet, mit denen Unternehmen aller Größen den optimalen Schutz für alle Bereiche erzielen:

GERÄTE | NETZWERKE | DOKUMENTE | IHR UNTERNEHMEN

INTERNATIONAL ANERKANNTE NORMEN UND ZERTIFIZIERUNGEN

Unsere multifunktionalen Drucker der imageRUNNER ADVANCE Serie werden anhand der Common-Criteria-Methodik und in Übereinstimmung mit den Anforderungen der IEEE2600-Sicherheitsstandards für Drucksysteme regelmäßig evaluiert und zertifiziert.

SICHERHEITSPRÜFUNGEN

Bei Canon wird eines der strengsten Sicherheitsprüfprogramme in der Bürogerätebranche angewendet. Technologien, die in unsere Produktpalette eingehen, durchlaufen dieselben hohen Prüfstandards, die wir auch für unser eigenes Unternehmen ansetzen.

Als Branchenführer in der Entwicklung innovativer Druck- und Informationsmanagementlösungen für Büro und Unternehmen erarbeiten wir bei Canon gemeinsam mit unseren Kunden integrative Konzepte für die Datensicherheit, bei denen die Sicherheitsaspekte unserer Bürotechnologien als Teil des größeren Ökosystems berücksichtigt werden.

SCHÜTZEN SIE IHR GERÄT

Umfassender Schutz für Ihre physischen Vermögenswerte

LÖSUNGEN FÜR DIE NUTZERERKENNUNG

Schützen Sie Ihr System vor unbefugtem Zugriff, indem Sie eine Nutzerzugangskontrolle (via Authentifizierung) einrichten. Dies hat den zusätzlichen Vorteil, dass Nutzer schnelleren Zugriff auf ihre bevorzugten Einstellungen und Druckjobs haben. Zudem verbessert es die Haftungs- und Kontrollmöglichkeiten. Unsere Abteilungsdrucker verfügen über uniFLOW Online Express. Diese flexible Lösung ermöglicht die Nutzererkennung über eine auf dem System erstellte Datenbank sowie die Domain-Authentifizierung über Active Directory oder uniFLOW Server. So haben Unternehmen die Möglichkeit, den Zugang zum System zu kontrollieren und zugleich die richtige Balance zwischen Bedienkomfort und Sicherheit zu finden.

SCHUTZ DER DATEN AUF DER FESTPLATTE

Permanent enthält der multifunktionale Drucker eine große Menge an Daten, die geschützt werden sollten – von Druckaufträgen in der Warteschlange bis zu empfangenen Faxen, gescannten Daten, Adressbüchern, Aktivitätsprotokollen und Auftragsverläufen. Canon Systeme bieten fortdauernd ein Bündel von Maßnahmen zum Schutz Ihrer Daten. So stellen Sie die Vertraulichkeit, Integrität und Verfügbarkeit von Daten sicher.

ZUGRIFFSVERWALTUNGSSYSTEM

Dieses Feature sorgt für eine punktgenaue Kontrolle des Zugriffs auf die Systemfunktionen. Administratoren können die verfügbaren Rollen nutzen oder eigene maßgeschneiderte mit den gewünschten spezifischen Zugriffsrechten erstellen. Zum Beispiel können bestimmte Nutzer daran gehindert werden, Dokumente zu kopieren oder zu versenden.

SICHERHEITSRICHTLINIEN

Die aktuellen imageRUNNER ADVANCE DX Systeme verfügen über eine Sicherheitsrichtlinien-Funktion, die es dem Administrator ermöglicht, in einem einzigen Menü auf alle sicherheitsbezogenen Einstellungen zuzugreifen und sie zu bearbeiten, bevor sie auf die Maschine angewandt werden. Sobald Letzteres geschehen ist, müssen Systemverwendung und Einstellungsänderungen im Einklang mit den Richtlinien erfolgen. Die Sicherheitsrichtlinien können über ein separates Kennwort geschützt werden, sodass der Zugang zu diesem Bereich auf den zuständigen IT-Sicherheitsbeauftragten beschränkt ist. Dadurch wird eine weitere Kontrollebene geschaffen.

KONTROLLE DER SYSTEMVERWALTUNG

Systemkonfigurierungen, wie Netzwerkeinstellungen und andere Steuerungsoptionen, stehen nur den Nutzern zur Verfügung, die Administratorrechte besitzen. So werden absichtliche oder versehentliche Änderungen durch Unbefugte verhindert.

PRÄVENTIVE SICHERHEIT

Die imageRUNNER ADVANCE DX Produkte bieten eine Reihe von Sicherheitseinstellungen, die Sie vor Angriffen schützen. Die Funktion „Sicherer Start“ stellt die Geräteintegrität nach dem Einschalten des Computers sicher, während die eingebettete McAfee Kontrollsoftware die Integrität während der gesamten Lebensdauer des Geräts gewährleistet, indem verhindert wird, dass Programme während der Laufzeit manipuliert oder nicht autorisierte Programme ausgeführt werden. Darüber hinaus bieten Syslog-Daten Echtzeitinformationen zum Sicherheitsstatus des Systems sowie Überwachungsfunktionen (Daten können von einem geeigneten SIEM-System eines Drittanbieters gelesen werden).

WIE SICHER SIND IHRE GERÄTE?

1
Werden Ihre Systeme gemeinsam genutzt und sind öffentlich zugänglich?

2
Können Nutzer ungesicherten Zugriff auf die Systeme erlangen?

3
Werden die Daten auf der Systemfestplatte in irgendeiner Weise geschützt?

4
Können unbefugte Nutzer die Systemeinstellungen ändern?

5
Haben Sie schon einmal über den Lebenszyklus Ihres Systems nachgedacht, und wie man es danach sicher entsorgen kann?

FESTPLATTENVERSCHLÜSSELUNG

Unsere imageRUNNER ADVANCE DX Systeme verschlüsseln alle Daten auf der Festplatte. Der Sicherheits-Chip, der für die Datenverschlüsselung verantwortlich ist, erfüllt den FIPS 140-2 Level 2-Sicherheitsstandard der US-Regierung und ist zertifiziert gemäß dem Cryptographic Module Validation Program (CMVP) der USA und Kanada sowie dem Japan Cryptographic Module Validation Program (JCMVP).

FESTPLATTENLÖSCHUNG

Einige Daten, wie kopierte oder gescannte Bilddaten, aber auch Dokumentendaten, die von einem Computer aus gedruckt werden, werden nur vorübergehend auf der Festplatte gespeichert und nach Auftragserledigung gelöscht. Um sicherzustellen, dass keine Daten verbleiben, bieten unsere Systemfestplatten die Möglichkeit, die Auftragsdaten routinemäßig nach Auftragsabschluss zu löschen.

INITIALISIERUNG ALLER DATEN UND EINSTELLUNGEN

Um beim Ersetzen oder Entsorgen der Festplatte Datenverlust zu vermeiden, können Sie alle Dokumente und Daten auf der Festplatte überschreiben und für die Maschineneinstellungen die Standardwerte wiederherstellen.

FESTPLATTENSPIEGELUNG*

Unternehmen haben die Möglichkeit, die Daten zusätzlich auf einer optionalen zweiten Festplatte zu speichern. Nach Abschluss der Spiegelung werden die Daten auf beiden Festplatten komplett verschlüsselt.

*Optional bei ausgewählten Modellen. Nähere Informationen über die Verfügbarkeit der Funktionen und Optionen innerhalb unseres Portfolios erfahren Sie bei Ihrem Canon Partner.

SICHERN SIE IHR NETZWERK

IST IHR DRUCKER EINE GEFAHR FÜR IHR NETZWERK?

- Sind die Netzwerkanschlüsse einem Angriff schutzlos ausgesetzt?
- Können Gäste drucken und scannen, ohne Ihr Netzwerk zu gefährden?
- Sind Ihre BYOD-Richtlinien („Bring Your Own Device“, Arbeiten mit benutzereigenen Geräten) sicher und vertretbar?
- Werden die Druckdatenströme vom Computer zum Ausgabegerät verschlüsselt?
- Werden Druck- und Scandaten bei der Übertragung verschlüsselt?

Canon bietet eine Reihe von Sicherheitslösungen, mit denen Sie Ihr Netzwerk und Ihre Daten gegen interne und externe Angriffe schützen.

IP- UND MAC-ADRESSFILTERUNG

Schützen Sie Ihr Netzwerk vor unbefugtem Zugriff durch Dritte, indem Sie die Kommunikation nur mit Systemen erlauben, die eine bestimmte IP- oder MAC-Adresse für aus- wie eingehende Kommunikation haben.

PROXYSERVER-KONFIGURIERUNG

Richten Sie anstelle Ihres Systems einen Proxyserver für Kommunikationsabläufe ein, und verwenden Sie ihn, wenn Sie Systeme außerhalb des Netzwerks anschließen.

IEEE 802.1X-AUTHENTIFIZIERUNG

Über einen LAN-Switch werden unbefugte Netzwerkzugriffe abgeblockt. Zugangsrechte haben nur Clientsysteme, die vom Authentifizierungsserver erkannt und freigegeben werden.

IPSEC-KOMMUNIKATION

IPSec-Kommunikation verhindert, dass Dritte IP-Pakete über das IP-Netzwerk abfangen oder manipulieren können. Verwenden Sie TLS 1.3 verschlüsselte Kommunikation, um zu verhindern, dass Daten, die zwischen dem Druck-/Multifunktionssystem und anderen Geräten (wie PCs) ausgetauscht werden, ausgespäht, gefälscht oder manipuliert werden.

PORTKONTROLLE

Konfigurieren Sie Ports im Rahmen Ihrer Sicherheitsrichtlinien-Einstellungen.

AUTOMATISCHE ZERTIFIKATS-REGISTRIERUNG

Durch diese Funktion wird der Aufwand zur Verwaltung der Sicherheitszertifikate deutlich reduziert. Diese branchenübliche Technik erlaubt es einem Systemadministrator, Zertifikate automatisch zu aktualisieren und freizugeben und dadurch die Sicherheitsrichtlinien stets einzuhalten.

PROTOKOLLÜBERWACHUNG

Verschiedene Protokolle ermöglichen es, die Aktivitäten an Ihrem System (einschl. blockierter Kommunikation) zu überwachen.

WI-FI DIREKT

So wird eine Peer-to-Peer-Verbindung für mobiles Drucken möglich, ohne dass das Mobilgerät auf das Netzwerk zugreifen müsste.

VERSCHLÜSSELUNG DER DATENÜBERTRAGUNG ZUM UND VOM GERÄT

Diese Option verschlüsselt Druckaufträge, die vom Nutzer-PC zum multifunktionalen Drucker unterwegs sind. Durch die Aktivierung des umfassenden Sicherheitsfunktionssets können auch PDF-Scans verschlüsselt werden.

MOBILES DRUCKEN FÜR GÄSTE

Unser sicheres Druck- und Scan-Management im Netzwerk kümmert sich um die allgemeinen Sicherheitsrisiken beim mobilen Drucken, z.B. für Gäste. Es werden externe Job-Verteilungswege per Mail, Web und Mobil-App bereitgestellt. Indem das Multifunktionssystem mit einer sicheren Datenquelle verbunden ist, werden die Angriffsmöglichkeiten stark eingeschränkt.

DUALES NETZWERK

Durch neueste Technologie wird jetzt duale Netzwerkfähigkeit geboten: Während das primäre Netzwerk immer kabelgebunden ist, kann das zweite aus Gründen einer strengeren Netzwerktrennung sowohl kabelgebunden als auch kabellos sein.

SCHÜTZEN SIE IHRE DOKUMENTE

Dies betrifft alle Unternehmen mit sensiblen Dokumenten (wie Verträge, Gehaltsabrechnungen, Kundendaten, Forschungs- und Entwicklungspläne u.v.m.). Wenn solche Dokumente in die falschen Hände gelangen, reichen die Folgen vom Imageschaden über Strafgebühren bis hin zum Rechtsstreit.

Canon bietet eine Reihe von Sicherheitslösungen zum Schutz Ihrer vertraulichen Dokumente während ihres gesamten Lebenszyklus.

VERTRAULICHKEIT GEDRUCKTER DOKUMENTE

Sicherer Druck
Der Nutzer kann nur über einen PIN-Code den Druck auslösen, d.h. erst nach Eingabe des richtigen PIN-Codes an der Maschine wird das Dokument gedruckt. So können Mitarbeiter Dokumente schützen, die sie als vertraulich einstufen.

Anhalten aller Druckjobs
Der Administrator kann Druckaufträge zurückhalten, die an imageRUNNER ADVANCE DX Systeme versandt wurden. Erst wenn der Nutzer sich angemeldet hat, wird sein Auftrag gedruckt. So ist die Vertraulichkeit aller Drucksachen gewährleistet.

Mailboxen
Druckaufträge oder gescannte Dokumente können zwecks späteren Zugriffs in einem Postfach gespeichert werden. Postfächer können über einen PIN-Code geschützt werden. So ist sichergestellt, dass nur befugte Nutzer die gespeicherten Inhalte sehen können. Der gesicherte Bereich auf der Maschine ist prädestiniert, um Dokumente zurückzuhalten, die häufig ausgegeben werden, aber einen gewissenhaften Umgang erfordern (z.B. Formulare).

uniFLOW Sicheres Drucken*
Mit uniFLOW MyPrintAnywhere Sicheres Drucken können Nutzer Druckaufträge über den universellen Treiber erteilen und sie dann an jedem beliebigen vernetzten Drucker ausgeben lassen.

ERSCHWEREN ODER VERHINDERN EINER VERVIELFÄLTIGUNG VON DOKUMENTEN

Druck mit sichtbaren Wasserzeichen
Die Treiber bieten eine Funktion, die die Druckseiten mit einer sichtbaren Markierung im Vorder- oder Hintergrund des eigentlichen Dokumentinhalts versieht. Die Benutzer werden damit auf die Vertraulichkeit des Dokuments hingewiesen und vom Kopieren des Dokuments abgehalten.

Drucken/Kopieren mit unsichtbaren Wasserzeichen
Wenn diese Option aktiviert ist, erscheint beim Drucken oder Kopieren ein eingebetteter (zuvor unsichtbarer) Text – eine wirkungsvolle Abschreckung.

Unternehmensweiter Schutz vor Datenverlust
Verbessern Sie Ihren Schutz vor Datenverlusten durch iW SAM Express in Verbindung mit uniFLOW. Mit dieser serverbasierten Lösung können Sie Dokumente erfassen und archivieren, die zum und vom Drucker gesendet werden. Das geschieht mithilfe von Text oder Attributen, die analysiert und interpretiert werden.

* Optional. Nähere Informationen über die Verfügbarkeit der Funktionen und Optionen innerhalb unseres Büroportfolios erfahren Sie bei Ihrem Canon Partner.

WIE SICHER SIND IHRE DOKUMENTE?

1
Werden unbefugte Nutzer daran gehindert, auf sensible Dokumente am Drucker zuzugreifen?

2
Können Sie die Vertraulichkeit aller Nutzerdokumente gewährleisten, die das gemeinsam genutzte System durchlaufen?

3
Können Sie die Herkunft gedruckter Dokumente zurückverfolgen?

4
Könnte ein Benutzer ein vertrauliches Dokument am Drucker an sich nehmen?

5
Können Sie häufig vorkommende Fehler beim Versand von Dokumenten zum System verhindern?

KONTROLLE ÜBER DAS VERSENDEN VON DOKUMENTEN PER E-MAIL UND FAX

Beschränkung der Sendeziele
Um die Gefahr von Datenlecks zu mindern, können Administratoren die verfügbaren Sendeziele auf solche im Adressbuch oder LDAP-Server, auf die angemeldete Nutzeradresse oder bestimmte Domains beschränken.

Deaktivierung der automatischen Adressvervollständigung
Indem Mailadressen nicht automatisch vervollständigt werden, verhindern Sie, dass Dokumente an falsche Ziele geschickt werden.

Adressbuchschutz
Ein eingerichteter PIN-Code verhindert, dass unbefugte Nutzer das Adressbuch des Systems bearbeiten können.

Faxnummerbestätigung
Indem Nutzer aufgefordert werden, die Faxnummer zur Bestätigung erneut einzugeben, wird verhindert, dass Dokumente unbeabsichtigt beim falschen Empfänger landen.

Vertraulichkeit für eingehende Faxnachrichten
Eingegangene Faxe werden nicht gedruckt, sondern in einem Speicher abgelegt.
Sie können die Diskretion empfangener Faxdokumente auch gewährleisten, indem Sie Bedingungen für den Zugang zu einer vertraulichen Eingangsbox festlegen oder PIN-Codes einrichten.

PRÜFEN DES URSPRUNGS UND DER ECHTHEIT VON DOKUMENTEN ANHAND VON DIGITALEN SIGNATUREN

Gerätesignatur
Die Systemsignatur kann auf gescannte Dokumente im PDF- oder XPS-Format angewandt werden. Dies geschieht über einen Schlüssel und einen Zertifikatsmechanismus. So kann der Empfänger die Herkunft und die Echtheit des Dokuments überprüfen.

Nutzersignatur
Die Option ermöglicht es, eine PDF- oder XPS-Datei mit einer eindeutigen digitalen Signatur des Nutzers zu verschicken, die dieser von einer Zertifizierungsstelle erhalten hat. Auf diese Weise kann der Empfänger prüfen, welcher Nutzer unterschrieben hat.

ANWENDUNG VON RICHTLINIEN DURCH ADOBE LIFECYCLE MANAGEMENT ES

Anwender können PDFs sichern und permanent dynamische Richtlinien anwenden, um den Zugang und die spezifischen Nutzungsrechte zu kontrollieren. So sind vertrauliche geschäftskritische Informationen vor fahrlässiger oder mutwilliger Verbreitung geschützt. Sicherheitsrichtlinien werden auf Serverebene gesteuert, damit Rechte auch dann geändert werden können, nachdem eine Datei bereits verteilt worden ist. Die imageRUNNER ADVANCE DX Serie kann so konfiguriert werden, dass sich Adobe® ES einbinden lässt.

* Optional. Nähere Informationen über die Verfügbarkeit der Funktionen und Optionen innerhalb unseres Büroportfolios erfahren Sie bei Ihrem Canon Partner.

SCHUTZ DER UNTERNEH-MENSDATEN

Canon kann einen Beitrag zum umfassenden Schutz von Informationen in Ihrem Unternehmen leisten.

VOLLSTÄNDIGE KONTROLLE VON DER ERFASSUNG BIS ZUR AUSGABE

Mit unserer modularen Ausgabemanagement-Software erreichen Unternehmen eine sichere gemeinsame Nutzung der Netzwerksysteme. Dadurch können Jobs sicher auf jedem an den Server angeschlossenen Drucker ausgegeben werden. Mobile Benutzer werden durch einen zentral gesteuerten Service unterstützt, über den sowohl interne Anwender als auch externe Gäste sicher von Mobilgeräten drucken können. Für die Anforderungen größerer Unternehmen gibt es das Scanmodul, mit dem sich Dokumente via Multifunktionssystem erfassen, komprimieren, umwandeln und zu einer Vielzahl von Zielen versenden lassen (einschl. cloudbasierten Systemen). Sie können auch Druckaufträge zum bestgeeigneten Drucker sicher umleiten und so die Druckkosten für jedes Dokument optimieren.
Unsere Lösung erhöht die Dokumentensicherheit in Ihrem Unternehmen. In Verbindung mit einer vollständigen Protokollierung haben Sie jederzeit im Blick, welche Mitarbeiter oder Abteilungen welches System wie nutzen.

ZENTRALES FLOTTENMANAGEMENT

Unsere Systemmanagement-Software IW MC ermöglicht es, Systemeinstellungen, Sicherheitsrichtlinien, Kennwörter, Zertifikate und Firmware zu aktualisieren und netzübergreifend auf Ihre Canon Flotte zu übertragen. So spart Ihr IT-Team wertvolle Zeit. Zugleich ist die Sicherheit Ihrer Infrastruktur jederzeit auf dem neuesten Stand.

UMFASSENDE NACHVERFOLGUNG VON DOKUMENTEN

Unsere Dokumentenservices-Architektur kann optional erweitert werden, um einen kompletten Datensatz (d.h. Scan plus Auftragsmetadaten) aller Dokumente zu erfassen, die auf imageRUNNER ADVANCE DX Systemen verarbeitet wurden.

MANAGED PRINT SERVICES

Canon MPS verbindet zukunftsweisende Technik und Software mit den passenden Dienstleistungen. Auf diese Weise können Sie entspannt nach Ihren Wünschen drucken und Dokumente handhaben – ohne die damit verbundenen Probleme für Ihre IT-Abteilung. Durch vorausschauende Steuerung und kontinuierliche Optimierung Ihrer Infrastruktur und Ihrer Dokumentenworkflows können wir dazu beitragen, dass Sie nicht nur Ihre Sicherheitsziele erreichen, sondern auch unternehmensweit die Kosten senken und die Produktivität steigern.

NUTZERSPEZIFISCHE ENTWICKLUNG

Unser unternehmensinternes Entwicklungsteam konzipiert eine Lösung, die auf Ihre spezifische Situation oder besonderen Anforderungen zugeschnitten ist.

WIE UMFASSEND IST IHR SICHERHEITSANSATZ?

- Gilt Ihre Sicherheitsrichtlinie auch für Ihre Multifunktionsgeräteflotte?
- Wie stellen Sie sicher, dass Ihre Infrastruktur stets auf dem neuesten Stand ist und Verbesserungen und Bugfixes zeitnah und effizient erfolgen?
- Sind Sie in der Lage zu drucken und zu scannen, ohne dass Ihr Netzwerk gefährdet ist?
- Sind Ihre Richtlinien in puncto „Geschäftliche Nutzung privater Geräte“ (BYOD) sicher und umsetzbar an Ihrer gesamten Druckerflotte?
- Hat Ihr IT-Team genügend Zeit, um Sicherheitsanliegen nachzugehen?
- Haben Sie die richtige Balance zwischen Sicherheit und Bedienkomfort?

WARUM CANON?

KOMPETENZ

Verknüpfung von Hardware und Software verringert die Möglichkeit von System-Sicherheitsverletzungen.

PARTNERSCHAFT

Wir helfen unseren Kunden, indem wir ihre Geschäftsabläufe verbessern und in der beruhigenden Gewissheit, **dass wir uns vorbeugend um Sicherheitsrisiken kümmern.**

SERVICE

Bei uns ist **das gleiche Team** sowohl für die Informationssicherheit unserer Kunden als auch für unsere eigene IT-Sicherheit zuständig.

Wir denken an alle potenziellen Gefahren, innerhalb und außerhalb Ihres Unternehmens.

INNOVATION

Unsere Produkte und Dienstleistungen eröffnen intelligente Möglichkeiten, mit denen mögliche Risiken für die Datensicherheit auf ein Minimum reduziert werden.

SC 2017 awards EUROPE

BLI PACESETTER MOBILE Print 2017-2018

„Sehr empfehlenswert“ – so unsere Bewertung in der besten Team-Kategorie anlässlich der **2017 SCA Awards Europe,** bei denen das Fachwissen bezüglich Cyber-Sicherheit ausgezeichnet wurde.

Canon U.S.A. hat zwei **BLI PaceSetter Awards 2017 erhalten** (Document Imaging Security and Mobile Print).

Canon Inc.
Canon.com

Canon Europe
canon-europe.com

Canon Deutschland GmbH
Europark Fichtenhain A10
D-47807 Krefeld
Canon Helpdesk
Tel.: +49 2151 3450
Fax: +49 2151 345 102
canon.de

Canon Austria GmbH
Oberlaaer Straße 233
A-1100 Wien
Canon Helpdesk
Tel. (01) 360 277 4567
canon.at

Canon (Schweiz) AG
Richtistrasse 9
CH-8304 Wallisellen
Tel. +41 (0)22 567 58 58
canon.ch

German edition

Canon

McAfee PROTECTED