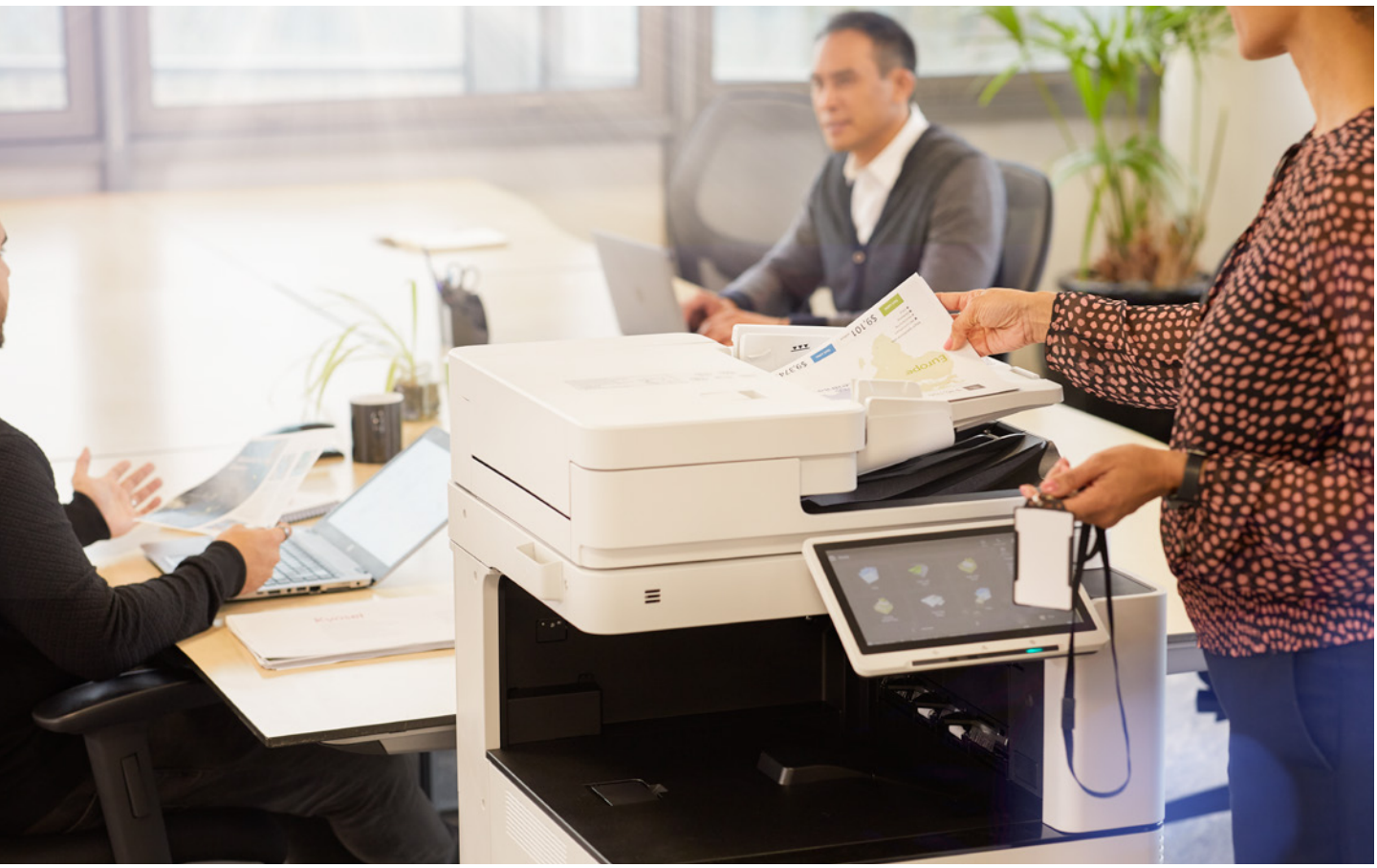


حماية مكتبك

McAfee PROTECTED

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

New to the Line

BLI BUYERS LAB 2019 PICK

Canon uniFLOW Online

Outstanding Cloud Output-Management Solution

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

Canon

ما مدى أمان المعلومات في مكتبك؟

تعتمد الشركات حاليًا على المعلومات إلى حد كبير، وهذا ما أدى إلى إنشاء شبكات معقدة من التقنيات والعمليات والأشخاص والمؤسسات ذات الصلة التي تتجاوز نطاق الحدود الوطنية. تظهر ممارسات عمل ذكية جديدة في عصر التطور الرقمي، وهذا ما يؤدي إلى إعادة تصميم المكاتب وتشكيل طريقة الأشخاص في إنتاج المعلومات ومشاركتها واستخدامها. أصبح تأمين البيانات في هذه البيئة المعقدة أكثر صعوبة من أي وقت مضى، وتستثمر معظم الشركات في تقنيات متطورة مثل جدران الحماية القوية وبرامج الحماية من الفيروسات الحديثة وبرامج الأمان وغير ذلك الكثير. ورغم ذلك، لم تتمكن في كثير من الأحيان من إدراك الحاجة إلى توسيع نطاق هذه الحماية بحيث يشمل طابعات المكاتب، وهذا ما يجعلهم أكثر عرضة للمخاطر مما يتوقعون.

فكِّر بشأن طابعاتك

تطورت الطابعات الحديثة متعددة الوظائف (MFP) إلى أدوات فائقة الإمكانات، مثلما تطورت أجهزة الكمبيوتر والخوادم التي لديها أنظمة تشغيل ومحركات أقراص صلبة كبيرة ومتصلة بالشبكة والإنترنت، ويشاركها المستخدمون لمعالجة أعداد هائلة من المستندات المهمة للأعمال يوميًّا.

ما المخاطر؟

- عرْض المستخدمين غير المصرح لهم المعلومات الحساسة المُخزَّنة على الطابعات متعددة الوظائف غير المحمية
- إمكانية اختراق البنية الأساسية للطباعة بسبب التشغيل الخاطئ
- إمكانية وصول الجهات الخارجية الضارة إلى الشبكة عبر الطابعة واستخدامها لشن المزيد من الهجمات الإلكترونية
- كشف المستندات السرية المنسية في درج الإخراج بعد الطباعة
- خلط المطبوعات الخاصة بمستخدمين مختلفين
- إرسال المستندات عبر الفاكس أو البريد الإلكتروني إلى المستلمين غير المقصودين بسبب أخطاء مطبعية
- اعتراض المتطفلين لعمليات الطباعة أو المسح الضوئي للبيانات أثناء نقلها
- فقدان البيانات نتيجة التخلص من الطابعات من دون توخي الحذر في نهاية مدة الإيجار.

"أصبح اعتماد المعايير الأساسية لأمن المعلومات أمرًا لا بد منه في المكاتب التي من المحتمل أن تتعامل فيها مع كميات هائلة من البيانات. لم تَعُد الطابعة حاليًا مجرد جهاز بسيط، بل إنها يمكن أن تؤدي دور الخادم الذي يتحكم في طباعة الورق".

(كبير موظفي أمن المعلومات بمجموعة Publicis Groupe)

حلول طباعة آمنة لأعمالك

الأمان والخصوصية حسب التصميم

عندما نصمم تقنيات ومنتجات وخدمات أو نحددها لعملائنا، نضع في اعتبارنا تأثيرها المحتمل بشأن أمن المعلومات في بيئة العملاء. ومن ثَمَّ، تأتي الطابعات المكتبية متعددة الوظائف المتوفرة لدينا مزودة بمجموعة متنوعة من ميزات الأمان القياسية والاختيارية على حد سواء، وهذا ما يتيح لجميع الشركات -بغض النظر عن حجمها- تحقيق مستوى الحماية المطلوب بخصوص:

الأجهزة | **الشبكات** | **المستندات** | **مؤسستك**

المعايير والشهادات المُعترف بها دوليًا

يتم تقييم طابعات imageRUNNER ADVANCE متعددة الوظائف واعتمادها دوريًا باستخدام منهجية المعايير العامة ووفقًا لمتطلبات معايير IEEE2600 لأمن جهاز النسخ الورقية.

اختبار الأمان

تستخدم Canon نظامًا من أكثر أنظمة اختبارات الأمان صرامة في صناعة أجهزة المكاتب. وتخضع التقنيات المعتمَدة في مجموعة منتجاتنا لمعايير الاختبارات العالية نفسها التي نأملها لشركتنا.

وبصفتها شركة رائدة في مجال تطوير حلول مبتكرة لإدارة الطباعة والمعلومات للمكاتب والشركات، تعمل Canon مع العملاء لمساعدتهم على تبني منهج شامل لأمن المعلومات، والذي يتناول الآثار الأمنية للتقنية المكتبية كجزء من نظام المعلومات الأشمل.

حماية جهازك

حماية متكاملة لأصولك المادية

حلول مصادقة المستخدم

يمكنك حماية جهازك من الاستخدام غير المصرح به عن طريق تطبيق التحكم في وصول المستخدمين من خلال المصادقة. وهذا يوفر أيضًا ميزة إضافية تتمثل في تزويد المستخدمين بالوصول السريع إلى إعداداتهم المفضلة ومهام الطباعة، مع تعزيز المساءلة والتحكم. تم تزويد الطابعات الإدارية لدينا ببرنامج uniFLOW Online Express، وهو حل مرن لتسجيل الدخول يتيح مصادقة المستخدم من خلال قاعدة بيانات المستخدم التي تم إنشاؤها على الجهاز، ومصادقة النطاق من خلال خدمة Active Directory أو خادم uniFLOW. وهذا يتيح للشركات الفرصة للتحكم في الوصول إلى الأجهزة، فضلاً عن تحقيق التوازن المناسب بين راحة المستخدم وأمانه.

حماية البيانات الموجودة على محرك الأقراص الصلبة

في أي وقت من الأوقات، تتضمن الطابعة متعددة الوظائف كمية هائلة من البيانات التي ينبغي حمايتها – بدايةً من مهام الطباعة المُنتظَرة حتى رسائل الفاكس المستلمة والبيانات الممسوحة ضوئيًا ودفاتر العناوين وسجلات النشاط وسجل المهام. تُقدم أجهزة Canon عددًا من الإجراءات لحماية بياناتك في كل مرحلة من عمر الجهاز وضمان سرية البيانات وسلامتها وتوفرها.

نظام إدارة الوصول

توفر هذه الميزة تحكمًا دقيقًا في الوصول إلى وظائف الجهاز. ويمكن للمسؤولين استخدام الأدوار القياسية المتوفرة أو إنشاء أدوار مخصصة بالمستوى المطلوب من امتيازات الوصول. على سبيل المثال، قد يتم منع بعض المستخدمين من نسخ المستندات أو استخدام وظيفة الإرسال.

إعداد سياسة الأمان

تم أيضًا تزويد أحدث أجهزة imageRUNNER ADVANCE DX بوظيفة سياسة الأمان التي تمكن المسؤول من الوصول إلى كل الإعدادات المتعلقة بالأمان في قائمة واحدة وتحريرها قبل تطبيقها على الجهاز. وبمجرد تطبيقها، يجب أن يتوافق استخدام الجهاز وتغيرات الإعدادات مع سياسة الأمان. ويمكن حماية سياسة الأمان بكلمة مرور منفصلة، بحيث يقتصر الوصول إلى هذه المنطقة على أخصائي الأمن المسؤول في قسم تكنولوجيا المعلومات، وهذا ما يؤدي إلى إضافة مستوى آخر من التحكم والتأكيد.

التحكم في إدارة الأجهزة

تتوفر تهيئة الجهاز، مثل إعدادات الشبكة وخيارات التحكم الأخرى، فقط للمستخدمين الذين لديهم امتيازات المسؤول التي تمنع أي تعديلات متعمدة أو غير مقصودة.

الأمن الوقائي

تقدم منتجات imageRUNNER ADVANCE DX عددًا من إعدادات الأمان التي تتيح لك حماية الطابعات من الهجمات الإلكترونية. توفر وظيفة التحقق من النظام عند بدء التشغيل سلامة الجهاز بمجرد تشغيله، بينما يضمن برنامج McAfee Embedded Control سلامة الجهاز طوال العمر الافتراضي له وذلك من خلال منع التلاعب بالبرامج أو تنفيذ البرامج غير المصرح بها خلال وقت التشغيل. علاوة على ذلك، توفر بيانات سجل النظام معلومات الأمان والسلامة للجهاز في الوقت الفعلي، بالإضافة إلى إمكانات المراقبة (يمكن قراءة البيانات بواسطة نظام مناسب لمعلومات الأمان وإدارة الأحداث (SIEM) لجهة خارجية).

ما مدى أمان أجهزتك؟

1
هل أجهزتك مشتركة وموجودة في أماكن عامة؟

2
هل يمكن للمستخدمين الحصول على وصول غير آمن إلى الأجهزة؟

3
هل لديك إجراءات لحماية المعلومات الموجودة على القرص الصلب للجهاز؟

4
هل يمكن للمستخدمين غير المصرح لهم تغيير إعدادات الجهاز؟

5
هل وضعت في اعتبارك العمر الافتراضي للجهاز وطريقة التخلص منه بأمان؟

تشفير القرص الصلب

تعمل أجهزة imageRUNNER ADVANCE DX لدينا على تشفير كل البيانات الموجودة على محرك الأقراص الصلبة لتعزيز الأمان. تتوافق شريحة الأمان المسؤولة عن تشفير البيانات مع معيار الأمان FIPS 140-2 من المستوى 2 الذي وضعته حكومة الولايات المتحدة وتم اعتماده بموجب برنامج التحقق من صحة وحدة التشفير (CMVP) الذي وضعته الولايات المتحدة وكندا، بالإضافة إلى برنامج التحقق من وحدة التشفير الخاص باليابان (JCMVP).

مسح القرص الصلب

يتم تخزين بعض البيانات، مثل بيانات الصور المنسوخة أو الممسوحة ضوئيًا بالإضافة إلى بيانات المستندات المطبوعة من جهاز كمبيوتر، مؤقتًا فقط على محرك الأقراص الصلبة ويتم حذفها بعد اكتمال العملية. لضمان عدم الاحتفاظ بأي بيانات متبقية، توفر أجهزتنا المزودة بمحرك الأقراص الصلبة إمكانية مسح البيانات المتبقية دوريًا كجزء من معالجة المهام.

تهيئة جميع البيانات والإعدادات

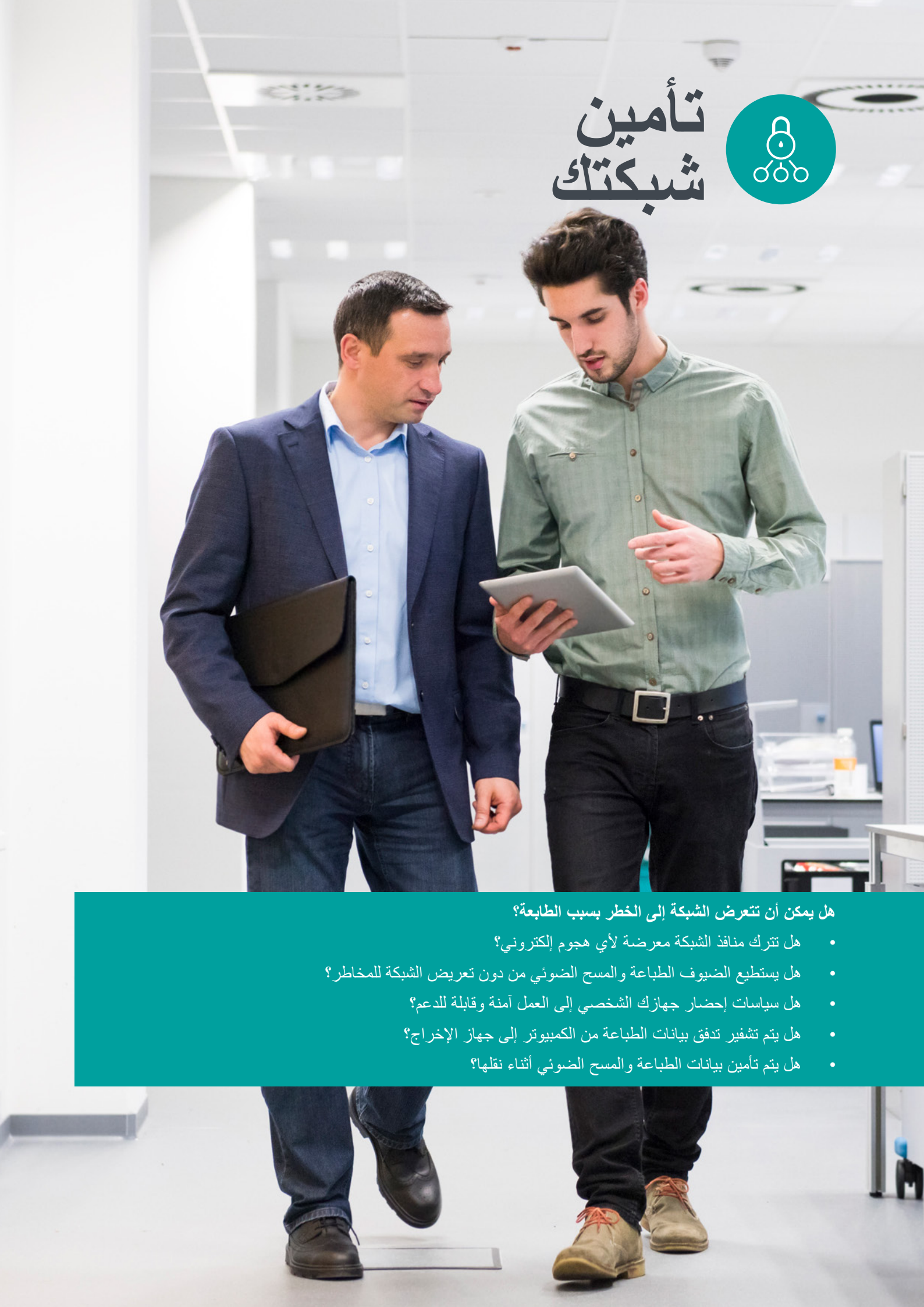
لمنع فقدان البيانات عند استبدال القرص الصلب أو التخلص منه، يمكنك استبدال جميع المستندات والبيانات الموجودة على القرص الصلب، واستعادة إعدادات الجهاز إلى الإعدادات الافتراضية.

النسخ المتطابق للقرص الصلب*

يمكن للشركات إجراء نسخ احتياطي للبيانات الموجودة على محركات الأقراص الصلبة الخاصة بأجهزتها باستخدام قرص صلب إضافي اختياري. عند إجراء النسخ المتطابق، يتم تشفير البيانات الموجودة على كلا محركي الأقراص الصلبة بالكامل.

*اختياري للطُرز المحددة. للحصول على معلومات مفصلة حول توفر المزايا والخيارات في مجموعة الطباعة المكتبية، يُرجى الاتصال بمندوب Canon لديك.

تأمين شبكتك



هل يمكن أن تتعرض الشبكة إلى الخطر بسبب الطابعة؟

- هل تترك منافذ الشبكة معرضة لأي هجوم إلكتروني؟
- هل يستطيع الضيوف الطباعة والمسح الضوئي من دون تعريض الشبكة للمخاطر؟
- هل سياسات إحضار جهازك الشخصي إلى العمل آمنة وقابلة للدعم؟
- هل يتم تشفير تدفق بيانات الطباعة من الكمبيوتر إلى جهاز الإخراج؟
- هل يتم تأمين بيانات الطباعة والمسح الضوئي أثناء نقلها؟

تُقدم Canon مجموعة من الحلول الأمنية للحفاظ على أمان شبكتك وبياناتك من الهجمات الداخلية والخارجية.

تصفية عناوين IP وMAC

يمكنك حماية شبكتك من الوصول غير المصرح به بواسطة الجهات الخارجية من خلال السماح فقط بالاتصال بالأجهزة التي لديها عنوان IP أو MAC محدد لكل من الاتصالات الصادرة والواردة.

إعداد خادم الوكيل

قم بتعيين وكيل لمعالجة الاتصالات بدلاً من جهازك، واستخدمه عند الاتصال بأجهزة خارج نطاق الشبكة.

مصادقة IEEE 802.1X

يتم حظر الوصول غير المصرح به إلى الشبكة بواسطة مفتاح LAN الذي يمنح امتيازات الوصول فقط لأجهزة العميل المصرح بها من خادم المصادقة.

اتصالات IPSEC

تمنع اتصالات IPSec الجهات الخارجية من اعتراض حزم IP المنقولة عبر شبكة IP أو التلاعب بها.
وتُستخدم اتصالات TLS المشفرة لمنع مراقبة البيانات واعتراضها والتلاعب بها والتي يتم تبادلها بين الجهاز والأجهزة الأخرى مثل الكمبيوتر.

التحكم في المنفذ

احرص على تهيئة المنافذ كجزء من إعداد سياسية الأمان لديك.

التسجيل التلقائي للشهادة

بفضل هذه الميزة، يقل الجهد المبذول للحفاظ على شهادات الأمان بدرجة كبيرة. باستخدام تقنية معترَف بها في الصناعة، يمكن لمسؤول النظام تحديث الشهادات وإصدارها تلقائيًا مع التأكد من استيفاء سياسات الأمان في جميع الأوقات.

مراقبة السجلات

تتيح لك السجلات المتنوعة مراقبة أنشطة الأجهزة، بما في ذلك طلبات الاتصال المحظورة.

شبكة WI-FI DIRECT

تتيح لك الاتصال المباشر للطباعة عبر الأجهزة المحمولة من دون الحاجة إلى وصول الجهاز المحمول إلى الشبكة.

تشفير البيانات أثناء نقلها من الجهاز وإليه

يقوم هذا الخيار بتشفير مهام الطباعة أثناء نقلها من كمبيوتر المستخدم إلى الطابعة متعددة الوظائف. ومن خلال تمكين مجموعة ميزات الأمان العام، قد يتم أيضًا تشفير البيانات الممسوحة ضوئيًا بتنسيق PDF.

الطباعة الخارجية عبر الأجهزة المحمولة

تتعامل برامج إدارة الطباعة والمسح الضوئي الآمنة الموجودة على الشبكة مع المخاطر الأمنية الشائعة للطباعة الخارجية وعبر الأجهزة المحمولة عن طريق توفير مسارات خارجية لتسليم المهام عبر البريد الإلكتروني والويب وتطبيقات الأجهزة المحمولة. وهذا ما يقلل من الهجمات الإلكترونية عن طريق تثبيت الأجهزة متعددة الوظائف في مصدر آمن.

الشبكة المزدوجة

تتميز أحدث التقنيات الآن بإمكانية الاتصال عبر الشبكة المزدوجة: بالرغم من أن الشبكة الأساسية ستصبح سلكية دائمًا، يمكن أن يكون الخط الثانوي الآن لاسلكيًا أو سلكيًا بهدف الفصل الآمن للشبكات بصورة أكثر صرامة.

حماية مستنداتك

تتعامل جميع الشركات مع المستندات الحساسة، مثل الاتفاقيات التعاقدية ومعلومات رواتب الموظفين وبيانات العملاء وخطط البحث والتطوير والمزيد. وفي حالة وصول المستندات إلى الأشخاص غير المقصودين، ستتراوح العواقب بين الإضرار بسمعة الشركة والغرامات المالية الباهظة أو حتى الإجراءات القانونية.

تُقدم Canon مجموعة من الحلول الأمنية لحماية مستنداتك الحساسة طوال دورة حياتها.

سرية المستندات المطبوعة

الطباعة الآمنة
يمكن للمستخدم تعيين رمز PIN للطباعة، بحيث لا يمكن طباعة المستند إلا بعد إدخال رمز PIN الصحيح على الجهاز. وهذا يتيح للأفراد تأمين هذه المستندات التي يعتبرونها سرية.

إيقاف جميع مهام الطباعة
باستخدام imageRUNNER ADVANCE DX، يمكن للمسؤول فرض إيقاف كل مهام الطباعة المقدَّمة، بحيث يطلب من المستخدمين تسجيل الدخول أولاً قبل طباعة المهام لحماية سرية كل المواد المطبوعة.

علب البريد
يمكن تخزين مهام الطباعة أو المستندات الممسوحة ضوئيًا في علبة بريد للوصول إليها في مرحلة لاحقة. ويمكن حماية علب البريد باستخدام رمز PIN لضمان أنه يمكن لمالكها المُخصص فقط عرض المحتوى المخزن فيها. وهذه المساحة الآمنة على الجهاز مناسبة للاحتفاظ بالمستندات التي يمكن استخدمها كثيرًا (مثل النماذج)، ولكنها تتطلب التعامل بحذر.

تقنية uniFLOW للطباعة الآمنة*
بفضل تقنية uniFLOW MyPrintAnywhere للطباعة الآمنة، يرسل المستخدمون مهام الطباعة عبر برنامج التشغيل العالمي ويجمعونها من أي طابعة على الشبكة.

منع تكرار المستندات أو حظره

الطباعة باستخدام علامات مائية مرئية
لدى برامج التشغيل القدرة على طباعة علامات مرئية على الصفحة يمكن أن تظهر في أعلى محتوى المستند أو خلفه. وهذا يحظر النسخ عن طريق رفع مستوى وعي المستخدم بسرية المستندات.

الطباعة/النسخ باستخدام علامات مائية غير مرئية
أثناء تمكين هذا الخيار، يمكن طباعة المستندات أو نسخها مع تضمين نص مخفي في الخلفية، بحيث يظهر النص في المستند عند النسخ ويحول دون إتمام العملية.

منع فقدان البيانات على مستوى الشركة
بادر بترقية إمكاناتك الأساسية لمنع فقدان البيانات باستخدام iW SAM Express مع uniFLOW. وهذا الحل المستند إلى الخادم يتيح لك تصوير المستندات المرسَلة من الطابعة وإليها وحفظها وتحليلها وتفسيرها باستخدام نص أو سمات ذات هدف رئيسي يتمثل في التصدي للتهديدات الأمنية.

تعقب أصل المستند*
من خلال الرمز المضمن، يمكن تعقب أصل المستند للوصول إلى مصدره.

ما مدى أمان مستنداتك؟

1. هل يتم منع المستخدمين غير المصرح لهم من الوصول إلى المستندات الحساسة في الطابعة؟
2. هل يمكنك ضمان سرية جميع مستندات المستخدمين التي تمر عبر الجهاز المشترك؟
3. هل يمكنك تعقب أصول المستندات المطبوعة؟
4. هل يمكن لشخص ما سرقة المستندات الحساسة من طابعتك؟
5. هل يمكنك منع الأخطاء الشائعة عند إرسال المستندات من الجهاز؟

التدريب على التحكم في ارسال المستندات وإرسالها عبر الفاكس

تقليل وجهات الإرسال

للحد من مخاطر تسرب المعلومات، يمكن للمسؤولين اقتصار وجهات الإرسال المتوفرة فقط على الأفراد المسجلين في دفتر العناوين أو خادم LDAP أو عنوان المستخدم المسجَّل أو بعض النطاقات.

تعطيل الإكمال التلقائي للعنوان

امنع إرسال المستندات إلى وجهات غير مقصودة عن طريق تعطيل الإكمال التلقائي لعناوين البريد الإلكتروني.

حماية دفتر العناوين

قم بتعيين رمز PIN لحماية دفتر عناوين الجهاز من التعديل غير المصرح به بواسطة المستخدمين.

تأكيد رقم الفاكس

امنع إرسال المستندات إلى المستلمين غير المقصودين من خلال مطالبة المستخدمين بإدخال رقم الفاكس مرتين للتأكيد قبل الإرسال.

سرية الفاكس المستلَم

اضبط الجهاز لتخزين المستندات في الذاكرة من دون طباعتها. يمكنك أيضًا حماية سرية مستندات الفاكس المستلَمة من خلال تطبيق الشروط لتحديد موقع التخزين في علبة الوارد الخاصة بالمستندات السرية، بالإضافة إلى تعيين رموز PIN.

تحقَّق من أصل المستندات وصحتها من خلال التوقيعات الرقمية

توقيعات الجهاز

يمكن تطبيق توقيع الجهاز على المستندات الممسوحة ضوئيًا بتنسيق PDF أو XPS، باستخدام آلية المفتاح والشهادة، حتى يتمكن المستلم من التحقق من مصدر المستند وصحته.

توقيع المستخدم*

يتيح الخيار للمستخدمين إرسال ملف PDF أو XPS باستخدام توقيع رقمي فريد من نوعه مخصص للمستخدم يتم الحصول عليه من هيئة إصدار الشهادات. وبهذه الطريقة، يتمكن المستلم من التحقق من هوية المستخدم الموقع على المستند.

تطبيق السياسات باستخدام التكامل مع نظام ADOBE LIFECYCLE MANAGEMENT ES

يمكن للمستخدمين تأمين ملفات PDF وتطبيق سياسات مستمرة وديناميكية للتحكم في حقوق الوصول والاستخدام لحماية المعلومات الحساسة وذات القيمة العالية من الكشف غير المقصود أو الضار. تُحفَظ سياسات الأمان على مستوى الخادم، بحيث يمكن تغيير الحقوق حتى بعد نشر الملف. يمكن إعداد الفئة imageRUNNER ADVANCE DX series للتكامل مع Adobe® ES.

*اختياري. للحصول على معلومات مفصلة حول توفر المزايا والخيارات في مجموعة الطباعة المكتبية، يُرجى الاتصال بمندوب Canon لديك.

تأمين معلومات المؤسسة

يمكن لشركة Canon المساهمة في الحماية الشاملة للمعلومات في مؤسستك.

التحكم الكامل في احتياجات التصوير والإخراج الشاملة

من خلال برامج إدارة الإخراج القياسية لدينا، تتمتع الشركات بمشاركة آمنة لأجهزة الشبكة، وهذا ما يمكِّنها من طباعة المهام بأمان على أي طابعة متصلة بخادم إدارة الإخراج. يتم دعم مستخدمي الأجهزة المحمولة من خلال خدمة يتم التحكم فيها مركزيًّا، حيث يتمتع المستخدمون الداخليون والخارجيون بالوصول الآمن إلى الطباعة من الأجهزة المحمولة.

بالنسبة إلى احتياجات التصوير لدى المؤسسات، توفر وحدة المسح الضوئي تصوير المستندات وضغطها وتحويلها ونشرها من الجهاز متعدد الوظائف إلى مجموعة متنوعة من الوجهات، بما في ذلك الأنظمة المستندة إلى الشبكة السحابية. يمكنك أيضًا إعادة توجيه مهام الطباعة بأمان إلى الطابعة الأكثر ملاءمة، وهذا ما يؤدي إلى تحسين تكلفة الطباعة لكل مستند.

يعزز الحل المتوفر لدينا أمان المستندات في جميع أقسام شركتك، فضلاً عن المحاسبة الكاملة للمستندات التي توفر رؤية كاملة حول النشاط لكل مستخدم وجهاز وقسم.

إدارة المجموعة المركزية

يتيح لك برنامج IW MC لإدارة الأجهزة إعدادات الجهاز وسياسات الأمان وكلمات المرور والشهادات، فضلاً عن تحديث البرنامج الثابت وترقيته إلى مجموعة أجهزة Canon لديك عبر الشبكة، وهذا ما يوفر الوقت الثمين لفريق تكنولوجيا المعلومات ويساعد في الحفاظ على تحديث أمان البنية الأساسية للطباعة لديك.

تدقيق المستندات الشامل

يمكن تحسين بنية خدمات المستندات المكتبية من خلال خيارات الطلب للحصول على سجل كامل (بيانات المسح الضوئي وتعريف المهمة) بكل المستندات التي تتم معالجتها من خلال أجهزة imageRUNNER ADVANCE DX.

خدمات الطباعة المُدارة

تَجمع خدمات الطباعة المُدارة لدى Canon بين التقنية المبتكرة والبرامج ذات الخدمات المناسبة، لتوفر لك تجربة الطباعة والمستندات التي ترغب فيها من دون المتاعب المرتبطة بفرق تكنولوجيا المعلومات لديك. من خلال الإدارة الاستباقية والتحسين المستمر لبنية الطباعة الأساسية وآليات عمل المستندات، يمكننا مساعدتك على تحقيق أهدافك الأمنية مع تحسين التكلفة وزيادة الإنتاجية في جميع أقسام شركتك.

تخصيص التطوير

لدينا فريق من المطورين الداخليين الذين يمكنهم اقتراح حل مخصص وتطويره بما يتناسب مع وضعك المحدد أو متطلباتك الفريدة.

ما مدى شمولية نهج أمن مؤسستك؟

- هل تمتد سياستك الأمنية أيضًا إلى مجموعة الأجهزة متعددة الوظائف لديك؟
- كيف تضمن تحديث البنية الأساسية للطباعة لديك وتحسينها وتنفيذ إصلاحات الأخطاء في الوقت المناسب وبكفاءة؟
- هل يستطيع الضيوف الطباعة والمسح الضوئي من دون تعريض الشبكة للمخاطر؟
- هل سياسات إحضار جهازك الشخصي آمنة وقابلة للدعم عبر مجموعة الطباعة لديك؟
- هل فريق تكنولوجيا المعلومات لديه الوقت الكافي للتحقيق في المخاوف الأمنية؟
- هل لديك التوازن الصحيح بين توفير الأمان وراحة المستخدم؟

لماذا تختار CANON؟

الخبرة
يقلل التكامل بين الأجهزة والبرامج من احتمال حدوث انتهاكات للنظام.

الشراكة
نحن نساعد العملاء على تحسين أعمالهم وهم يعلمون أننا سنتعامل مع **تهديدات أمن البيانات استباقيًّا.**

الخدمة
يدير **فريق أمن المعلومات نفسه** المخصص للعملاء الأمن الداخلي لتكنولوجيا المعلومات لدينا.

نحن نراعي جميع التهديدات المحتملة داخل جدار حماية المؤسسة وخارجه.

الابتكار
تتضمن منتجاتنا وخدماتنا **طرقًا أكثر ذكاءً** للحد من مخاطر أمن المعلومات المحتملة.

"إشادة كبيرة" كأفضل فريق أمان حاصل على **جوائز SCA لعام 2017 بأوروبا** تقديرًا لخبرته في مجال الأمن الإلكتروني.

حصلت Canon U.S.A. على جائزتين من **جوائز BLI PaceSetter لعام 2017** (أمن تصوير المستندات والطباعة عبر الأجهزة المحمولة).

Canon Inc.
Canon.com

Canon Europe
canon-europe.com

Canon Europe Ltd.
3 The Square
Stockley Park
Uxbridge
Middlesex
UB11 1ET UK

Canon Ireland
Lake Drive 3006
Citywest, Saggart
Co. Dublin, Ireland
هاتف رقم: 01 2052400
فاكس رقم: 01 2052525
canon.ie

Canon (UK) Ltd
Woodhatch
Reigate
Surrey RH2 8BF
هاتف رقم: 01737 220000
فاكس رقم: 01737 220022
canon.co.uk