OCHRONA BIURA

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

CZY INFORMACJE PRZETWARZANE W TWOIM BIURZE SĄ BEZPIECZNE?

Współczesne firmy w dużym stopniu polegają na informacjach, tworząc złożone sieci połączonych technologii, ludzi i organizacji, mające wymiar międzynarodowy. W erze cyfrowej transformacji pojawiają się nowe, elastyczne metody pracy, które odmieniają biura oraz sposoby tworzenia, udostępniania i wykorzystywania informacji. Zabezpieczanie danych w tym skomplikowanym środowisku jest jeszcze trudniejsze niż kiedykolwiek, a większość firm inwestuje w zaawansowane technologie, takie jak wytrzymałe zapory sieciowe, nieustannie aktualizowaną ochronę antywirusową, oprogramowanie zabezpieczające oraz w wiele innych rozwiązań. Często jednak nie zdają sobie sprawy z konieczności rozszerzenia tej ochrony na drukarki biurowe, co sprawia, że są bardziej podatne na zagrożenia, niż im się wydaje.

WARTO POMYŚLEĆ O DRUKARKACH

Nowoczesne drukarki wielofunkcyjne ewoluowały i stały się zaawansowanymi narzędziami, które – podobnie jak komputery i serwery – mają systemy operacyjne, pojemne dyski twarde, zapewniają połączenie z siecią oraz Internetem i są udostępniane wielu użytkownikom w ramach codziennego przetwarzania ogromnej liczby dokumentów biznesowych o kluczowym znaczeniu.

JAKIE RYZYKO SIĘ Z TYM WIĄŻE?

- Uzyskanie dostępu do poufnych informacji zapisanych w pamięci niezabezpieczonych urządzeń wielofunkcyjnych przez nieupoważnionych do tego użytkowników
- Zagrożenie dostępności infrastruktury drukowania na skutek wykonania nieprawidłowej operacji
- Uzyskanie dostępu do sieci za pośrednictwem drukarki przez osoby z zewnątrz mające zamiar wykorzystać urządzenie do kolejnych ataków
- Możliwość przypadkowego pozostawienia poufnych dokumentów na tacy wyjściowej po zakończeniu drukowania
- Wymieszanie wydruków należących do różnych użytkowników
- Wysłanie dokumentów faksem lub za pośrednictwem wiadomości e-mail do niewłaściwych osób w wyniku pomyłki przy wpisywaniu danych kontaktowych odbiorców
- Możliwość przechwycenia przesyłanych danych drukowania lub skanowania przez hakerów
- Utrata danych z powodu nieostrożnej utylizacji drukarek pod koniec okresu dzierżawy

„W środowisku biurowym, w którym mogą być przetwarzane ogromne ilości danych, warto wdrożyć podstawowe standardy bezpieczeństwa informacji. Obecnie drukarka nie jest już zwykłym urządzeniem – to serwer, który przy okazji drukuje dokumenty”.

(dyrektor ds. bezpieczeństwa informatycznego Publicis Groupe)

BEZPIECZNE ROZWIĄZANIA W ZAKRESIE DRUKOWANIA DLA TWOJEJ FIRMY

Z myślą o bezpieczeństwie i ochronie prywatności danych

Projektując lub wybierając technologie, produkty i usługi dla naszych klientów, bierzemy pod uwagę prawdopodobny wpływ tych rozwiązań na bezpieczeństwo informacji w środowisku danego klienta. Dlatego nasze biurowe drukarki wielofunkcyjne są wyposażone w wiele funkcji zabezpieczeń, zarówno standardowych, jak i opcjonalnych, które umożliwiają firmom dowolnej wielkości osiągnięcie żądanego poziomu ochrony w następującym kontekście:

URZĄDZENIA | SIECI | DOKUMENTY | CAŁA FIRMA

STANDARDY I CERTYFIKATY UZNAWANE NA CAŁYM ŚWIECIE

Nasze drukarki wielofunkcyjne imageRUNNER ADVANCE są regularnie oceniane i certyfikowane przy użyciu metodologii Common Criteria oraz zgodnie z wymaganiami związanymi z normą IEEE2600 w zakresie bezpieczeństwa wydruków.

TESTOWANIE ZABEZPIECZEŃ

Firma Canon stosuje jeden z najbardziej rygorystycznych systemów testowania bezpieczeństwa w branży urządzeń biurowych. Technologie zastosowane w ramach naszej oferty podlegają tym samym testom o wysokim standardzie, jakich używamy w kontekście naszej własnej firmy.

Jako lider w dziedzinie tworzenia innowacyjnych rozwiązań w zakresie druku oraz zarządzania informacjami dla biur i przedsiębiorstw firma Canon współpracuje ze swoimi klientami, aby pomóc im w przyjęciu kompleksowego podejścia do bezpieczeństwa informacji – uwzględniającego wpływ technologii biurowej na bezpieczeństwo w ramach szerszego ekosystemu informacyjnego.

CHROŃ SWOJE URZĄDZENIE

Kompleksowa ochrona zasobów fizycznych

ROZWIĄZANIA ZWIĄZANE Z UWIERZYTELNIANIEM UŻYTKOWNIKÓW

Wdrożenie kontroli dostępu użytkowników za pośrednictwem uwierzytelniania umożliwia zabezpieczenie urządzenia przed nieautoryzowanym użyciem. Zapewnia także dodatkową korzyść w postaci szybszego uzyskiwania dostępu do preferowanych ustawień i zadań drukowania danej osoby, a jednocześnie zwiększa możliwości monitorowania sposobu użytkowania urządzenia. Drukarki wykorzystywane przez pracowników jednego działu są wyposażone w aplikację uniFLOW Online Express – elastyczne rozwiązanie do logowania umożliwiające uwierzytelnianie użytkowników na podstawie bazy danych użytkowników utworzonej w urządzeniu oraz uwierzytelnianie domen za pośrednictwem usługi Active Directory lub serwera uniFLOW. Dzięki temu firmy mogą kontrolować dostęp do urządzeń, zachowując równowagę pomiędzy wygodą użytkowników a bezpieczeństwem.

OCHRONA DANYCH ZAPISANYCH NA DYSKU TWARDYM

Urządzenie wielofunkcyjne przez cały czas dysponuje dużą ilością danych – od oczekujących zadań drukowania, odebrane faksy, zeskanowane dane, książki adresowe i dzienniki aktywności po historię zadań – które należy chronić. Urządzenia firmy Canon zapewniają wiele możliwości ochrony danych na każdym etapie eksploatacji urządzenia i gwarantują poufność, integralność oraz dostępność danych.

SYSTEM ZARZĄDZANIA DOSTĘPEM

Ta opcja zapewnia precyzyjną kontrolę dostępu do funkcji urządzenia. Administratorzy mogą korzystać z dostępnych, standardowych ról lub tworzyć odpowiednio dostosowane role z określonym poziomem uprawnień dostępu. Na przykład niektórych użytkowników można pozbawić możliwości kopiowania dokumentów lub korzystania z funkcji wysyłania.

USTAWIENIA ZWIĄZANE Z POLITYKĄ BEZPIECZEŃSTWA

Najnowsze urządzenia imageRUNNER ADVANCE DX są również wyposażone w funkcję zasad bezpieczeństwa, która zapewnia administratorowi dostęp do wszystkich ustawień związanych z zabezpieczeniami w ramach jednego menu oraz możliwość ich edytowania przed zastosowaniem w odniesieniu do danego urządzenia. Po wdrożeniu ustawień korzystanie z urządzenia i zmiana ustawień musi być zgodna z przyjętymi zasadami. Zasady bezpieczeństwa można chronić osobnym hasłem. Dzięki temu dostęp do nich będzie ograniczony i możliwy jedynie dla specjalisty ds. bezpieczeństwa IT, co pozwoli zapewnić wyższy poziom kontroli i nadzoru.

KONTROLA ADMINISTROWANIA URZĄDZENIAMI

Konfiguracji urządzenia, obejmującej między innymi ustawienia sieci i inne opcje sterowania, mogą dokonywać wyłącznie użytkownicy z uprawnieniami administratora, co uniemożliwia wprowadzenie zamierzonych lub przypadkowych zmian przez nieupoważnione do tego osoby.

ZABEZPIECZENIA PREWENCYJNE

Urządzenia imageRUNNER ADVANCE DX są wyposażone w rozmaite ustawienia związane z bezpieczeństwem, które zabezpieczają drukarkę przed atakami. Funkcja weryfikacji systemu dba o poprawność działania uruchamianego urządzenia, a oprogramowanie McAfee Embedded Control umożliwia niezakłóconą pracę przez cały okres eksploatacji produktu poprzez zapobieganie ingerencjom w działanie programów i blokowanie ich nieautoryzowanego uruchamiania. Ponadto dane Syslog zapewniają bieżące informacje o stanie zabezpieczeń urządzenia i umożliwiają monitorowanie pracy (dane mogą być odczytywane przez odpowiedni system SIEM innego producenta).

CZY TWOJE URZĄDZENIA SĄ BEZPIECZNE?

1
Czy Twoje urządzenia są wykorzystywane przez wielu użytkowników i znajdują się w ogólnodostępnych miejscach?

2
Czy użytkownicy mogą uzyskać niezabezpieczony dostęp do tych urządzeń?

3
Czy stosujesz jakiekolwiek zabezpieczenia w celu ochrony informacji zapisanych na dyskach twardych swoich urządzeń?

4
Czy nieupoważnieni do tego użytkownicy mogą zmieniać ustawienia urządzeń?

5
Czy bierzesz pod uwagę okres eksploatacji swojego urządzenia i myślisz o jego bezpiecznej utylizacji?

SZYFROWANIE DYSKU TWARDEGO

Nasze urządzenia imageRUNNER ADVANCE DX szyfrują wszystkie dane zapisywane na dysku twardym, zwiększając tym samym bezpieczeństwo. Układ zabezpieczający odpowiedzialny za szyfrowanie danych jest zgodny ze standardem bezpieczeństwa FIPS 140-2 poziomu 2, ustanowionym przez amerykański rząd i jest certyfikowany w ramach programu walidacji modułów kryptograficznych (ang. Cryptographic Module Validation Program, CMVP) stworzonego przez Stany Zjednoczone i Kanadę, a także Japońskiego programu walidacji modułów kryptograficznych (ang. Japan Cryptographic Module Validation Program, JCMVP).

USUWANIE DANYCH Z DYSKU TWARDEGO

Niektóre dane, na przykład skopiowane lub zeskanowane, a także dokumenty drukowane z komputera, są jedynie tymczasowo przechowywane na dysku twardym i usuwane po zakończeniu danej operacji.

W celu uniknięcia dłuższego przechowywania danych nasze urządzenia z dyskiem twardym umożliwiają rutynowe usuwanie pozostałych danych w ramach przetwarzania zadań.

RESETOWANIE WSZYSTKICH DANYCH I USTAWIEŃ

Aby zapobiec utracie danych podczas wymiany lub utylizacji dysku twardego, można nadpisać wszystkie dokumenty i dane zapisane na dysku twardym oraz przywrócić domyślne ustawienia urządzenia.

TWORZENIE KOPII LUSTRZANEJ DYSKU TWARDEGO*

Firmy mogą tworzyć kopie zapasowe danych na dyskach twardych swoich urządzeń, korzystając przy tym z dodatkowego dysku twardego. Podczas wykonywania kopii lustrzanej dane na obu dyskach twardych są również w pełni szyfrowane.

* Opcja w wybranych modelach. Aby uzyskać szczegółowe informacje na temat dostępności danych funkcji i opcji w ramach oferty biurowego sprzętu do druku, należy skontaktować się z przedstawicielem firmy Canon.

ZABEZPIECZENIE SIECI

CZY DRUKARKA MOŻE STANOWIĆ ZAGROŻENIE DLA SIECI?

- Czy pozostawiasz porty sieciowe otwarte, umożliwiając w ten sposób dokonanie ataku?
- Czy osoby z zewnątrz mogą drukować i skanować dokumenty przy użyciu Twoich urządzeń bez narażania sieci na zagrożenia?
- Czy zasady związane z przynoszeniem do pracy własnych urządzeń są bezpieczne i akceptowalne?
- Czy strumienie danych drukowania przesyłane z komputera do urządzenia wyjściowego są szyfrowane?
- Czy dane drukowania i skanowania są zabezpieczone podczas ich przesyłania?

Firma Canon oferuje szereg rozwiązań zabezpieczających sieć oraz dane przed wewnętrznymi i zewnętrznymi atakami.

FILTROWANIE ADRESÓW IP ORAZ MAC

Możesz zabezpieczyć swoją sieć przed nieupoważnionym dostępem poprzez zezwolenie na komunikację tylko z urządzeniami o określonym adresie IP lub MAC, zarówno w zakresie komunikacji wychodzącej, jak i przychodzącej.

KONFIGURACJA SERWERA PROXY

Możesz ustawić serwer proxy, aby obsłużyć komunikację bez użycia komputera i wykorzystywać ten serwer do łączenia się z urządzeniami spoza sieci.

UWIERZYTELNIANIE IEEE 802.1X

Nieupoważniony dostęp do sieci jest blokowany przez przełącznik LAN, który przyznaje uprawnienia dostępu jedynie urządzeniom klienckim autoryzowanym przez serwer uwierzytelniania.

KOMUNIKACJA W STANDARDZIE IPSEC

Komunikacja w standardzie IPSec uniemożliwia osobom trzecim przechwytywanie pakietów IP przesyłanych przez sieć IP i ingerowanie w nie. Szyfrowana komunikacja TLS pozwala zapobiec przechwytywaniu i fałszowaniu danych przesyłanych pomiędzy Twoim urządzeniem i innymi urządzeniami (takimi jak komputery), a także ingerowaniu w te dane.

KONTROLA NAD PORTAMI

Porty należy skonfigurować w ramach zasad bezpieczeństwa.

AUTOMATYCZNE REJESTROWANIE CERTYFIKATÓW

Funkcja ta pozwala w znacznym stopniu wyeliminować trudności związane z zachowywaniem certyfikatów bezpieczeństwa. Korzystając z uznanej w branży technologii, administrator systemu może automatycznie aktualizować i wydawać certyfikaty, tak aby zasady bezpieczeństwa były przestrzegane przez cały czas.

MONITOROWANIE DZIENNIKÓW

Różne dzienniki umożliwiają monitorowanie aktywności urządzenia, w tym żądań zablokowania komunikacji.

WI-FI DIRECT

Umożliwia korzystanie z połączenia peer-to-peer w przypadku drukowania mobilnego, dzięki czemu urządzenie przenośne nie musi uzyskiwać dostępu do sieci.

SZYFROWANIE DANYCH PRZESYŁANYCH DO I Z URZĄDZENIA

Opcja ta umożliwia szyfrowanie zadań drukowania przesyłanych z komputera użytkownika do drukarki wielofunkcyjnej. Po włączeniu zestawu uniwersalnych funkcji zabezpieczeń dane zeskanowane w formacie PDF również mogą być szyfrowane.

FUNKCJA DRUKOWANIA GOŚCINNEGO

Nasze bezpieczne oprogramowanie do zarządzania drukowaniem i skanowaniem w sieci eliminuje typowe zagrożenia związane z drukowaniem mobilnym i gościnnym, umożliwiając zewnętrzne przesyłanie zadań za pośrednictwem poczty e-mail, Internetu i aplikacji mobilnej. Minimalizuje to liczbę ścieżek ataku poprzez powiązanie urządzeń wielofunkcyjnych wyłącznie z bezpiecznymi źródłami.

DWIE SIECI

Najnowsza technologia umożliwia teraz obsługę dwóch sieci: podstawową siecią zawsze będzie sieć przewodowa, a dodatkowa sieć może opierać się na rozwiązaniu bezprzewodowym lub przewodowym, co ma umożliwić bardziej bezpieczne rozdzielenie sieci.

OCHRONA DOKUMENTÓW

Wszystkie firmy operują poufnymi dokumentami, takimi jak umowy, informacje o listach płac personelu, dane klientów, plany badań i rozwoju i inne. Dostanie się dokumentów w niepowołane ręce może zaszkodzić reputacji firmy, skutkować wysokimi karami finansowymi, a nawet doprowadzić do wytoczenia procesu firmie.

Canon oferuje szereg rozwiązań pozwalających chronić poufne dokumenty przez cały okres ich wykorzystywania.

POUFNOŚĆ DRUKOWANYCH DOKUMENTÓW

Bezpieczne drukowanie
Użytkownik może ustawić kod PIN odblokowujący drukowanie, tak aby można było wydrukować dokument dopiero po wprowadzeniu poprawnego kodu. Umożliwia to użytkownikom zabezpieczenie dokumentów, które uznają za poufne.

Wstrzymanie wszystkich zadań drukowania
Urządzenie imageRUNNER ADVANCE DX umożliwia administratorowi wymuszenie wstrzymania wszystkich przesłanych zadań drukowania, tak aby użytkownicy musieli się zalogować przed wydrukowaniem dokumentów. Ma to na celu ochronę poufności wszystkich drukowanych materiałów.

Skrzynki pocztowe
Zadania drukowania lub zeskanowane dokumenty mogą być przechowywane w skrzynce pocztowej, co pozwala uzyskać do nich dostęp w późniejszym czasie. Skrzynki pocztowe mogą być chronione kodem PIN, aby tylko ich właściciel mógł przeglądać ich zawartość. To bezpieczne miejsce zapewniane przez urządzenie jest odpowiednie do przechowywania dokumentów, które muszą być często drukowane (np. formularzy), ale wymagają ostrożnego obchodzenia się z nimi.

Bezpieczne drukowanie uniFLOW*
Dzięki rozwiązaniu uniFLOW MyPrintAnywhere do bezpiecznego drukowania użytkownicy mogą przesyłać zadania drukowania za pośrednictwem uniwersalnego sterownika i pobierać je z dowolnej drukarki w sieci.

ZAPOBIEGANIE POWIELANIU DOKUMENTÓW

Drukowanie z widocznymi znakami wodnymi
Sterowniki umożliwiają nadrukowanie widocznych oznaczeń na treści dokumentu lub w jej tle. Utrudnia to kopiowanie pewnych dokumentów poprzez sygnalizowanie poufnego charakteru takich materiałów.

Drukowanie/kopiowanie z niewidocznymi znakami wodnymi
Po włączeniu tej opcji dokumenty mogą być drukowane lub kopiowane z osadzonym w tle ukrytym tekstem, dzięki czemu po powieleniu tekst pojawia się na dokumencie i pełni funkcję odstraszającą.

Zapobieganie utracie danych na poziomie korporacyjnym
Rozszerz podstawowe funkcje zapobiegania utracie danych o rozwiązanie iW SAM Express w połączeniu z uniFLOW. To oparte na serwerze rozwiązanie umożliwia przechwytywanie i archiwizowanie dokumentów wysyłanych do i z drukarki, ich analizę i interpretację za pomocą tekstu lub atrybutów, co ma zapewnić bezpieczeństwo.

Śledzenie pochodzenia dokumentu*
Dzięki osadzonemu kodowi można określić źródło pochodzenia dokumentu.

CZY TWOJE DOKUMENTY SĄ BEZPIECZNE?

1
Czy nieupoważnieni użytkownicy mają zablokowany dostęp do poufnych dokumentów w drukarce?

2
Czy możesz zapewnić poufność wszystkich dokumentów przechodzących przez współdzielone urządzenie?

3
Czy możesz śledzić pochodzenie drukowanych dokumentów?

4
Czy ktoś mógłby wyciągnąć z drukarki poufne dokumenty?

5
Czy jesteś w stanie zapobiec występowaniu typowych błędów podczas wysyłania dokumentów z urządzenia?

KONTROLA NAD WYSYŁANIEM I FAKSOWANIEM DOKUMENTÓW

Ograniczenie zakresu odbiorców
Aby zmniejszyć ryzyko wycieku informacji, administratorzy mogą ograniczyć listę dostępnych odbiorców do pozycji zapisanych w książce adresowej lub na serwerze LDAP, adresu zalogowanego użytkownika lub niektórych domen.

Wyłączanie automatycznego uzupełniania adresów
Wyłączenie funkcji automatycznego uzupełniania adresów e-mail pomoże zapobiec wysyłaniu dokumentów do niewłaściwych odbiorców.

Ochrona książki adresowej
Możesz ustawić kod PIN, aby chronić książkę adresową urządzenia przed jej edycją przez nieupoważnionych do tego użytkowników.

Potwierdzanie numeru faksu
Zobligowanie użytkowników do dwukrotnego wprowadzania numeru faksu w celu jego potwierdzenia przed wysłaniem pomaga zapobiegać wysyłaniu dokumentów do przypadkowych odbiorców.

Poufność odbieranych faksów
Urządzenie można skonfigurować w taki sposób, by dokumenty były przechowywane w jego pamięci bez ich drukowania. Można również chronić poufność dokumentów otrzymywanych za pośrednictwem faksu poprzez określenie miejsca przechowywania tych dokumentów (w postaci poufnej skrzynki odbiorczej), a także ustawienie kodów PIN.

WERYFIKACJA POCHODZENIA I AUTENTYCZNOŚCI DOKUMENTU DZIĘKI PODPISOM CYFROWYM

Podpis urządzenia
Na zeskanowane dokumenty w formacie PDF lub XPS może być naniesiony podpis urządzenia za pomocą klucza i mechanizmu certyfikatu, tak aby odbiorca mógł zweryfikować pochodzenie dokumentu, a także jego autentyczność.

Podpis użytkownika*
Opcja ta umożliwia użytkownikom wysyłanie plików PDF lub XPS z unikatowym cyfrowym podpisem użytkownika uzyskanym od urzędu certyfikacji. W ten sposób odbiorca może sprawdzić, który użytkownik podpisał dany dokument.

WDRAŻANIE ZASAD DZIĘKI INTEGRACJI Z ADOBE LIFECYCLE MANAGEMENT ES

Użytkownicy mogą zabezpieczać pliki PDF oraz stosować stałe i dynamiczne zasady dotyczące kontroli dostępu oraz praw użytkowania w celu ochrony poufnych i cennych informacji, tak aby nie trafiły one w ręce przypadkowych osób lub osób o wrogich zamiarach. Zasady bezpieczeństwa obowiązują na poziomie serwera, dzięki czemu prawa można zmienić nawet po rozpowszechnieniu pliku. Urządzenia z serii imageRUNNER ADVANCE DX można skonfigurować celem integracji z systemem Adobe® ES.

* Opcjonalne. Aby uzyskać szczegółowe informacje na temat dostępności danych funkcji i opcji w ramach oferty biurowego sprzętu do druku, należy skontaktować się z przedstawicielem firmy Canon.

BEZPIECZEŃSTWO INFORMACJI W PRZEDSIĘBIORSTWIE

Firma Canon może wspomóc całościową ochronę informacji w Twojej organizacji.

PEŁNA KONTROLA W ZAKRESIE KOMPLEKSOWEGO PRZECHWYTYWANIA I DRUKU

Dzięki naszemu modułowemu oprogramowaniu do zarządzania wydrukiem firmy mogą bezpiecznie korzystać z urządzeń funkcjonujących w ramach sieci. To umożliwia bezpieczne drukowanie zadań na dowolnej drukarce podłączonej do serwera zarządzania wydrukiem. Użytkownicy mobilni są obsługiwani przy użyciu centralnie sterowanych usług, dzięki którym zarówno użytkownicy wewnętrzni, jak i goście mogą bezpiecznie drukować z urządzeń mobilnych. Moduł skanowania dla przedsiębiorstw umożliwia przechwytywanie, kompresję, konwersję i dystrybucję dokumentów z poziomu urządzenia wielofunkcyjnego do wielu miejsc docelowych, w tym systemów opartych na chmurze. Istnieje również możliwość bezpiecznego przekierowania zadania drukowania do najbardziej odpowiedniej drukarki, co pozwala zoptymalizować koszt wydruku dla każdego dokumentu.
Nasze rozwiązanie zwiększa bezpieczeństwo dokumentów w całej firmie. Umożliwia też kompleksowe rozliczanie obsługi dokumentów poprzez zapewnienie wglądu w aktywność poszczególnych użytkowników, urządzeń i działów.

SCENTRALIZOWANE ZARZĄDZANIE FLOTĄ

Nasze oprogramowanie do zarządzania urządzeniami IW MC umożliwia aktualizowanie ustawień urządzeń, zasad bezpieczeństwa, haseł i certyfikatów, a także oprogramowania układowego urządzeń firmy Canon w ramach całej sieci. Pozwala to oszczędzać cenny czas pracowników działu IT oraz na bieżąco aktualizować zabezpieczenia infrastruktury druku.

KOMPLEKSOWE AUDYTY DOKUMENTÓW

Nasza architektura usług dla dokumentów biurowych może zostać wzbogacona o opcje przechwytywania całych rekordów (tj. skanowanie i metadane zadań) wszystkich dokumentów przetwarzanych przez urządzenia imageRUNNER ADVANCE DX.

USŁUGI ZARZĄDZANIA DRUKIEM

Usługi zarządzania drukiem firmy Canon łączą innowacyjną technologię i oprogramowanie z odpowiednim zakres usług, aby umożliwić drukowanie i obsługę dokumentów bez angażowania zespołów IT. Dzięki proaktywnemu zarządzaniu i ciągłemu usprawnianiu infrastruktury druku oraz przepływu dokumentów możemy pomóc w osiągnięciu celów związanych z bezpieczeństwem przy jednoczesnej optymalizacji kosztów i zwiększeniu wydajności w całej firmie.

OPRACOWYWANIE NIESTANDARDOWYCH ROZWIĄZAŃ

Dysponujemy wewnętrznym zespołem specjalistów, którzy mogą zaproponować i opracować niestandardowe rozwiązanie dostosowane do konkretnej sytuacji lub konkretnych wymagań.

CZY TWOJE PODEJŚCIE DO BEZPIECZEŃSTWA FIRMY JEST WŁĄCZAJĄCE CZY IZOLUJĄCE?

- Czy zasady bezpieczeństwa obejmuje również flotę urządzeń wielofunkcyjnych?
- W jaki sposób zapewniasz regularne aktualizowanie infrastruktury drukowania oraz terminowe i skuteczne wdrażanie ulepszeń oraz poprawek błędów?
- Czy osoby z zewnątrz mogą drukować i skanować dokumenty przy użyciu Twoich urządzeń bez narażania sieci na zagrożenia?
- Czy zasady dotyczące przynoszenia własnych urządzeń są bezpieczne i akceptowalne w ramach całej floty urządzeń drukujących?
- Czy Twój zespół IT ma wystarczająco dużo czasu, by zajmować się problemami związanymi z bezpieczeństwem?
- Czy udaje Ci się zachować równowagę pomiędzy zapewnianiem bezpieczeństwa a wygodą użytkownika?

DLACZEGO WARTO WYBRAĆ FIRMĘ CANON?

SPECJALISTYCZNA WIEDZA

Integracja sprzętu i oprogramowania zmniejsza ryzyko naruszenia zabezpieczeń systemu.

WSPÓŁPRACA

Pomagamy naszym klientom w skuteczniejszym prowadzeniu działalności. Mogą się w pełni na niej skoncentrować, wiedząc, że my **aktywnie zajmiemy się zagrożeniami związanymi z bezpieczeństwem danych.**

USŁUGI

Ten **sam zespół ds. bezpieczeństwa informacji**, który zajmuje się klientami, dba również o bezpieczeństwo naszego wewnętrznego systemu IT.

Bierzemy pod uwagę wszystkie potencjalne zagrożenia, zarówno te wewnętrzne, jak i te pochodzące zza firmowej zapory.

INNOWACJE

Nasze produkty i usługi **są wyposażone w mechanizmy, które skuteczniej** minimalizują ryzyko występowania zagrożeń dla bezpieczeństwa danych.

SC 2017 awards EUROPE

BLI PACESETTER MOBILE Print 2017-2018

„Bardzo polecany” w kategorii najlepszych zespołów ds. zabezpieczeń na gali **2017 SCA Awards Europe,** podczas której nagradzane są osiągnięcia w dziedzinie cyberbezpieczeństwa.

Firma Canon U.S.A. otrzymała dwie nagrody **BLI PaceSetter Awards 2017** (Bezpieczne przetwarzanie obrazów dokumentów i mobilne drukowanie).

Canon Inc.
Canon.com

Canon Europe
canon-europe.com

Canon Polska Sp. z o.o.
ul. Gottlieba Daimlera 2
02-460 Warszawa
tel. +48 22 430 60 00
canon.pl

Polish edition

Canon

McAfee PROTECTED