

SMARTSHIELD



Technologia bezpieczeństwa danych
W ploterach serii ColorWave i PlotWave

Canon

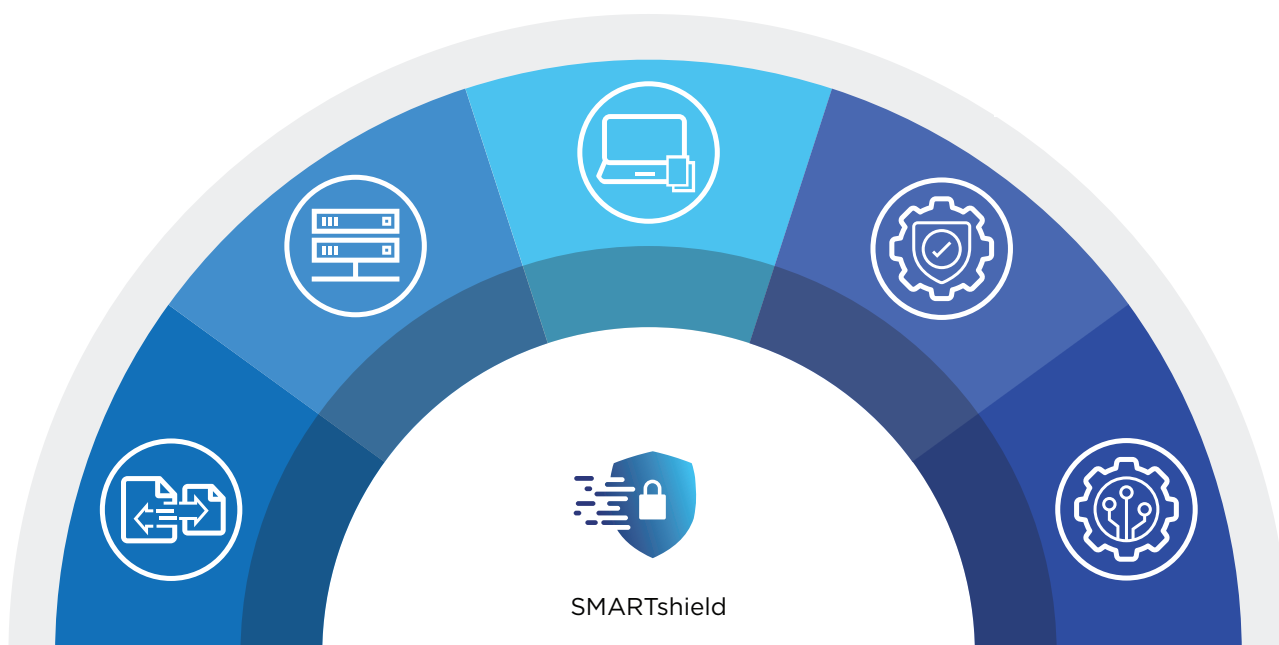
DLA NAS JEST WAŻNE BEZPIECZEŃSTWO TWOICH DANYCH

Zagrożenia związane z atakiem informatycznym rosną z roku na rok. Nic zatem dziwnego, że bezpieczeństwo sieciowe to temat coraz częściej poruszany w biznesie. W przypadku profesjonalnego druku wielkoformatowego, na przykład podczas tworzenia dokumentacji inżynierskiej, bezpieczeństwo i poufność danych to absolutna podstawa.

Dlatego właśnie powstał Canon SmartShield – inteligentny system ochrony wielkoformatowych profesjonalnych systemów druku.



ColorWave 3800



Bardziej niż kiedykolwiek firmy i organizacje samorządowe i rządowe muszą chronić dane i poufne informacje zarówno biurze jak i w sieciach komputerowych. Ochrona danych musi się odbywać na każdym etapie ich obiegu w organizacji. A więc na etapie przesłane pliku od osoby na stację roboczą a także na urządzenia peryferyjne takie jak chociażby plotery wielkoformatowe.

Dane też muszą być zabezpieczone przed nieautoryzowanym dostępem zarówno poprzez blokowanie niewykorzystywanych protokołów oraz blokowanie niebezpiecznych aplikacji jak i poprzez możliwość blokady panelu do którego odblokowania musi nastąpić uwierzytelnienie użytkownika.

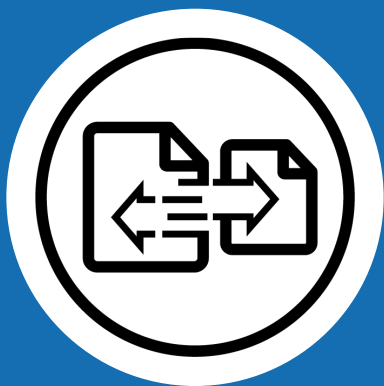
Dane są też gromadzone na dysku twardym kontrolera, a więc ważne jest by dysk oraz dane na dysku były zaszyfrowane a start dysku był pod bezpieczną kontrolą systemu z możliwością trwałego a zatem bezpiecznego usunięcia danych z dysku.

SMARTshield, jest w pełni zintegrowaną technologią zabezpieczeń drukowania w najnowszych systemach ColorWave i Plotwave i jest zaprojektowany specjalnie w celu zabezpieczenia potrzeb organizacji w zakresie bezpieczeństwa. Jest zintegrowaną odpowiedzią na obecne potrzeby w tym zakresie.

SMARTshield stanowi parasol ochronny nad danymi i oferuje wiele zabezpieczeń łącznie z opcją fizycznego wyjmowania dysku w celu jego bezpiecznego przechowywania np. w sejfie lub też fizycznego zniszczenia dysku w przypadku np. odsprzedaży całego systemu.

Dzięki SMARTshield dane są zabezpieczone na każdym etapie procesu przepływu prac.

SMARTshield zabezpiecza dane teraz jak i w przyszłości dzięki długo wspieranemu kontrolerowi, który jest oparty na systemie operacyjnym Windows 10 IOT i opcjonalnemu systemowi antywirusowemu McAfee.



BEZPIECZNA TRANSMISJA DANYCH

Chroń dane podczas wysyłania plików do plotera wielkoformatowego z dowolnego urządzenia.

Dzięki pakietowi oprogramowania do przesyłania plików ClearConnect użytkownicy mogą przysyłać pliki z komputera lub urządzenia mobilnego. Przy takim poziomie elastyczności i dostępie mobilnym jest to niezbędne.

Cenne dane są przekazywane w bezpieczny sposób do drukarki przez cały czas i ze wszystkich urządzeń.

- Kompatybilność z bezpiecznym protokołem IPsec.
- Kompatybilność z IPv6 i IPv4.
- HTTPS.





BEZPIECZNE PRZECHOWYWANIE DANYCH

Chroń poufne dane przechowywane na dysku twardym plotera wielkoformatowego. Ważne jest, aby chronić poufne dane zapisane na drukarce A0, które mogą być skradzione lub przez przypadek mogą wyciec. SMARTshield szyfruje dane na dysku i ogranicza dostęp poprzez identyfikację i autoryzację użytkownika. Skutecznie i zgodnie z najnowszymi standardami usuwa dane, więc użytkownicy mogą być pewni, że ich poufne pliki są niedostępne dla osób nie powołanych także poprzez szyfrowanie danych i możliwości niszczenie dysku twardego np. po zakończeniu umowy dzierżawy.

- Bezpieczne usuwanie plików.
- E-Shredding.
- Wyjmowany dysk twardy (opcja).
- Bezpieczny start dysku.
- Szyfrowanie danych na dysku twardym.
- Możliwość fizycznego zniszczenia dysku twardego.





AUTORYZACJA UŻYTKOWNIKA

SMARTshield umożliwia wielopoziomą autoryzację użytkowników i ogranicza dostęp do poufnych plików. Umożliwia też blokadę panelu użytkownika a do odblokowania i autoryzacji wykorzystuje Active Directory. Pozwala też na wdrożenie Smart Card. Posiada funkcję osobistej skrzynki odbiorczej Smart Inbox co pozwala na drukowanie i skanowanie z i do osobistego folderu. Opcjonalnie umożliwia kontrolę nas ilością wykonywanych wydruków przez poszczególnych użytkowników.



- Blokada panelu użytkownika.
- Bezpieczny druk za pomocą Active Directory.
- Umożliwia bezpieczny druk za pomocą smartcard (konieczny opcjonalny czytnik kart).
- Pozwala kierować pliki do osobistej skrzynki odbiorczej.
- Umożliwia skanowanie do osobistego folderu.
- Pozwala drukować z osobistego folderu.
- Umożliwia blokowanie portów i interfejsów.
- Możliwość podłączenia oprogramowania Uniflow.



ZABEZPIECZENIE PRZED NIEAUTORYZOWANYM DOSTĘPEM (HAKERAMI)

Jedno z największych wyzwań dla każdej firmy, czy też organizacji jest powstrzymanie hakerów przed atakiem na sieć firmową. Przez plotery wielkoformatowe często przewija się ogromna ilość danych wrażliwych. Jest niezbędnym by ograniczyć dostęp z zewnątrz do wrażliwych danych na dysku twardej kontrolera. Warto mieć pewność, że drukarka wielkoformatowa nie może zostać przejęta i używana przeciwko firmowej sieci. SMARTshield rozwiązuje problem włamań i jest narzędziem do profilaktyki na wielu frontach:

- Wyłączanie niewykorzystywanych protokołów.
- SNMP v3.
- Kompatybilność z IEE 802.1x.
- Opcjonalny program antywirusowy McAfee.
- Opcjonalna kontrola aplikacji za pomocą McAfee Whitelisting.





BEZPIECZEŃSTWO TERAZ I W PRZYSZŁOŚCI

SMARTshield został zaprojektowany, aby zapewnić bezpieczeństwo danych i sieci teraz a także i w przyszłości. Kontroler w oparciu o system operacyjny Windows 10 IOT, zapewnia zdalne poprawki bezpieczeństwa i zdalny serwis przez długie lata.

Nasi specjaliści ds. bezpieczeństwa stale monitorują najnowsze ryzyka tak by móc zapewnić dane firmowe podczas korzystania z systemu wielkoformatowego były bezpieczne.

- Oprogramowanie kontrolera oparto na systemie OPERACYJNYM Windows 10 IoT Enterprise LTSC.
- Wsparcie systemu operacyjnego co najmniej do 2029 roku i dłużej.
- Zdalne aktualizacje bezpieczeństwa na kontrolerze.
- Możliwość zdalnych aktualizacji za pomocą On Remote Service.

Rozumiemy Twoje o bezpieczeństwo i z tego powodu przygotowaliśmy zestaw funkcji przeciwdziałających zagrożeniom na jakie są narażone w obecnym czasie firmy i organizacje. Myślimy o bezpieczeństwie danych nie tylko dzisiaj, ale także w przyszłości.



Canon to Twój partner w zakresie bezpiecznego środowiska drukowania.

KOMPATYBILNOŚĆ SMARTSHIELD

SMARTshield jest zintegrowany z następującymi systemami:

ColorWave 3600



ColorWave 3800



Seria PlotWave 3000



Seria PlotWave 5000



PlotWave 7500



SMARTSHIELD

W SZCZEGÓŁACH

BEZPIECZNE PRZESŁANIE

Zgodność z bezpiecznym protokołem internetowym IPsec

IPsec to protokół zapewniający uwierzytelnianie, poufność danych i integralność w komunikacji sieciowej pomiędzy kontrolerem a innymi urządzeniami.

**IPsec
Zgodność z IPv6 i IPv4**

Protokół internetowy w wersji 4 (IPv4) jest jednym z podstawowych protokołów opartych na standardach metody pracy w Internecie i innych sieciach z komutacją pakietów. Protokół ten używa 32-bitowe adresy. IPv6 jest najnowszą wersją protokołu, który używa 128-bitowych adresów i dlatego może obsługiwać większą ilość urządzeń.

HTTPs

W celu ochrony ruchu sieciowego podczas wykorzystywania narzędzi takich jak WebTools Express, Publisher Express i Publisher Select zamiast używania protokołu HTTP można użyć bezpiecznego protokołu HTTPs. Ponadto można uruchomić autoryzację certyfikatu. Autoryzacja może być osadzona w kontrolerze, aby zapobiec atakowi typu „man-in-the-middle”, gdzie złośliwa strona, która znajduje się na ścieżce do serwera kontrolera, udaje, że jest kontrolerem.

BEZPIECZNE PRZECHOWYWANIE I USUWANIE

Bezpieczne usuwanie plików

Automatyczne usuwanie zadań drukowania, skanowania i kopiowania z inteligentnej skrzynki odbiorczej po czasie zdefiniowanym przez użytkownika. Kasowanie plików jest bezpieczne po włączeniu funkcji E-Shredding.

E-shredding

Funkcja e-niszczenia jest zabezpieczeniem, które pozwala systemowi nadpisać dowolny plik będący rezultatem procesów drukowania/kopiowania/skanowania danych i trwale usunąć ich z systemu. Ta funkcja zapobiega odzyskiwaniu wszelkich usuniętych danych użytkownika, w tym zawartości plików i atrybutów plików, na przykład jeśli dysk jest skradziony

Wymienny dysk twardy

Opcjonalny zestaw wymiennego dysku twardego umożliwia administratorom fizyczne usunięcie go z plotera wielkoformatowego. Wewnętrzny dysk twardy, dzięki czemu można go zamknąć w bezpiecznym miejscu po godzinach pracy. Dysk może być następnie łatwo ponownie zainstalowany do użytku w normalnych godzinach pracy.

Bezpieczny start

Bezpieczny start (Secure Boot) jest standardem bezpieczeństwa. Pozwala upewnić się, że urządzenie uruchamia się tylko przy użyciu oprogramowania, który jest godny zaufania. Po uruchomieniu koparki wielkoformatowej, oprogramowanie sterownika sprawdza podpis każdego z elementów oprogramowania rozruchowego.

Szyfrowanie danych

Na dysku twardym kontrolera POWERSync szyfrowane są wszystkie pliki. Szyfrowany jest cały dysk (łącznie z systemem operacyjnym i wszystkimi danymi (także te używane do szyfrowanie przestrzeni dyskowej).

Mechanizm szyfrowania jest oparty na module Trusted Platform Module (TPM) i Microsoft BitLocker mechanizm, który jest zgodny z certyfikatem FIPS 140-2. Używana metoda szyfrowania to AES 256.

Zniszczenie dysku twardego na zakończenie umowy

Na życzenie klienta, wewnętrzny dysk twardy sterownika POWERSync może być usunięty i fizycznie zniszczony, dzięki czemu na wielkoformatowej drukarce nie pozostaną żadne dane dotyczące druku klienta. Opcjonalnie dysk może być wyjmowany by go bezpiecznie przechowywać w zabezpieczonym miejscu.

AUTORYZACJA

Blokada dostępu do panelu sterowania

Po włączeniu funkcji zarządzania dostępem, wszystkie rodzaje paneli obsługi urządzeń przez użytkownika zgromadzone w pakiecie ClearConnect mogą być dostępne jedynie po odblokowaniu za pomocą danych uwierzytelniających w danej domenie lub za pośrednictwem karty elektronicznego dostępu (niezbędny opcjonalny czytnik).

Bezpieczne drukowanie przez autoryzację w domenie (active directory)

Wrażliwe zadania drukowania wysłane przez właściciela zadania nie są drukowane do momentu, gdy ten nie uwierzyteli na panelu użytkownika systemu, że ma prawo druku.

Dostępność wydruków w Smart Inbox

Po włączeniu tej funkcji zadanie z wydrukami będzie czekało w osobistej inteligentnej skrzynce odbiorczej, aż do momentu aktywacji zadania druku z panelu użytkownika ClearConnect lub z poziomu narzędzia WebTools Express. Ta funkcja zapobiega przypadkowemu lub intencjonalnemu zabraniu wydrukowanej dokumentacji przez innych pracowników biurowych.



Skanuj do swojego osobistego folderu

Funkcja Scan to Home Folder jest dostępna poprzez uwierzytelnienie domenowego użytkownika poprzez podanie hasła. Po wprowadzeniu uwierzytelnienia na panelu drukarki, użytkownik może zeskanować plik do jego katalogu domowego w sieci uprzednio odpowiednio skonfigurowanego w firmowej sieci.

Drukuj z osobistego folderu

Funkcja drukowania z Home Folder jest poprzez uwierzytelnienie domenowego użytkownika przez podanie hasła. Po wprowadzeniu uwierzytelnienia na panelu drukarki, użytkownik może drukować z katalogu domowego w sieci firmowej uprzednio odpowiedni skonfigurowanego w firmowej sieci.

Wyłączanie portów i interfejsów

Aby zabezpieczyć kontroler POWERsync przed nieautoryzowanym dostępem jest możliwość wyłączenia wszystkich portów, które w danej chwili nie są używane.

Oprogramowanie firm trzecich jak np. uniFLOW

Systemy drukujące PlotWave i ColorWave z interfejsem użytkownika ClearConnect mogą być zintegrowane w środowisku uniFLOW klienta. Daje to użytkownikom dodatkowe możliwości i funkcjonalności i może pomóc kontrolować i redukować koszty druku i kopiowania, a także zwiększać bezpieczeństwo dokumentów i poprawić wydajności pracowników.

ZABEZPIECZENIE PRZED NIEAUTORYZOWANYM DOSTĘPEM

Wyłączanie nieużywanych protokołów

Administratorzy sieci mają możliwość skonfigurowania konkretnych protokołów, które mają być dostępne. W rezultacie niechciana komunikacja z urządzeniem i dostęp do systemu za pośrednictwem określonych protokołów mogą być skutecznie blokowane.

SNMP V3

Jest bezpieczna wersja SNMP, która zapewnia uwierzytelnianie i integralność protokołami transportowymi Network Management Station (NMS) a zarządzanymi drukarkami.

Urządzenie IEEE 802.1X Uwierzytelnianie

Zapewnienie mechanizmu uwierzytelniania opartego na porcie (zgodnie ze standardem IEEE802.1X) pozwalające na uwierzytelnienie urządzenia przez organ centralny w celu komunikacji z innymi urządzeniami.

Antywirus McAfee (Opcja)

Opcjonalna możliwość zainstalowania oprogramowania antywirusowego McAfee na kontrolerze POWERsync jako dodatkową barierę ochronną przed wirusami.

McAfee Whitelisting Biała lista (opcja)

Opcjonalna funkcja aktywowana za pomocą licencji. Po aktywowaniu i włączeniu tworzy szczegółowy wykaz wszystkich dozwolonych plików na kontrolerze przez co zapobiega wszelkim nieuprawnionym zmianom dokonywanym przez złośliwe oprogramowanie, wirusy lub przez nieautoryzowanych użytkowników. Stale sprawdza integralność plików i sprawdza z listą. Zablokuje wszelkie manipulacje lub nieautoryzowane zmiany.

BEZPIECZEŃSTWO TERAZ I W PRZYSZŁOŚCI

Kontroler oparty na systemie operacyjnym Windows 10 IoT Enterprise LTSC

Kontroler POWERsync w drukarce używa systemu operacyjnego Windows 10 IoT Enterprise LTSC.

Wsparcie techniczne do 2029 r. lub dłużej

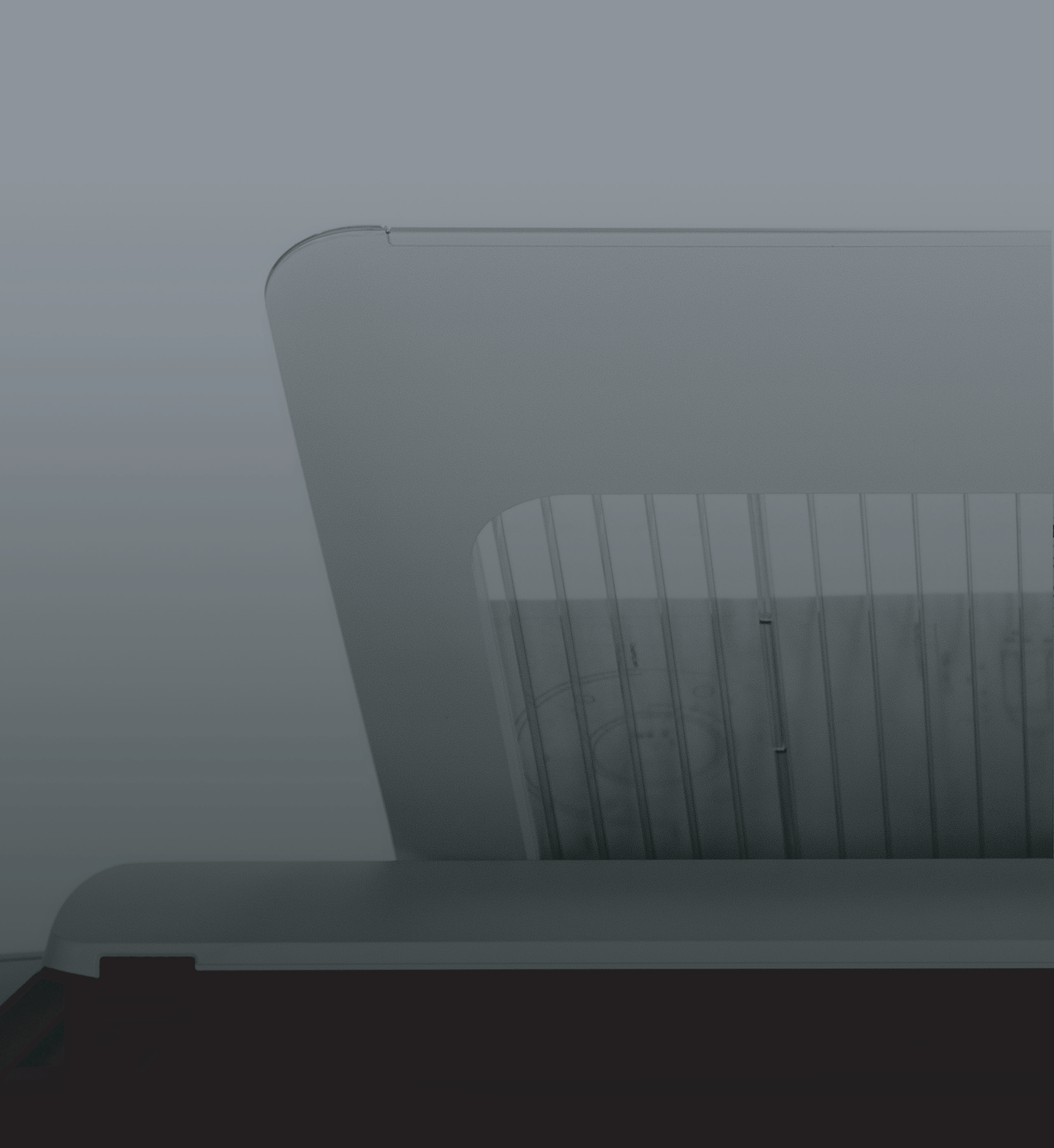
Firma Microsoft gwarantuje obsługę systemu Windows 10 IoT Enterprise LTSC do przynajmniej 2029 roku. Prawdopodobnie przedłuży ten okres. Oznacza to, że w tym okresie będą dostarczane aktualizacje zabezpieczeń.

Zdalna aktualizacja zabezpieczeń

Za pomocą WebTools Express administrator systemu może zdalnie przysyłać i zainstalować aktualizacje. Pozwala to na szybką reakcję i wysoką dyspozycyjność, ponieważ nie ma potrzeby angażowania serwisu w celu dokonania aktualizacji systemu.

On Remote Service

On Remote Service to usługa opracowana przez firmę Canon w celu zapewnienia jak największej sprawności całego systemu. Funkcjonalność jest częścią kontrolera PowerSynch. On Remote Service oferuje zdalną pomoc techniczną obejmującą zdalną diagnostykę, zdalny odczyt licznika i zdalny serwis. W rezultacie zwiększona jest dostępność systemu dla użytkowników, zmniejszona administracja, ulepszona obsługa po sprzedażowa, a także umożliwiony jest szybszy czas reakcji serwisu. Same plusy i spokojny sen.



© 2020 Canon Production Printing

Canon jest zastrzeżonym znakiem towarowym firmy Canon Inc. Wszystkie inne znaki towarowe są własnością odpowiednich właścicieli i niniejszym zostają uznane. Żadna część tej publikacji nie może być kopiowana, modyfikowana, reprodukowana ani przesyłana w jakiegokolwiek formie lub w jakikolwiek sposób, elektroniczny, ręczny bez uprzedniej pisemnej zgody firmy Canon Production Printing. Ilustracje oraz specyfikacja nie muszą odnosić się do produktów i usług oferowanych na poszczególnych lokalnych rynkach. Treść tej publikacji nie powinna być interpretowana jako jakakolwiek gwarancja lub rękojmia w odniesieniu do określonych właściwości lub specyfikacji lub właściwości technicznych lub przydatności do określonych zastosowań. Treść tej publikacji może od czasu do czasu ulegać zmianom bez powiadomienia. Canon Production Printing nie ponosi odpowiedzialności za jakiegokolwiek bezpośrednie, pośrednie lub wtórne szkody jakiegokolwiek rodzaju lub straty lub wydatki wynikające z korzystania z treści tej publikacji.

Canon

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