



Chroń swoją sieć dzięki najlepszym zabezpieczeniom procesu drukowania oferowanym przez firmę HP¹

94%

firm z branży finansów twierdzi, że bezpieczeństwo kopiarki/drukarki jest ważne lub bardzo ważne²



61%

organizacji zgłosiło w ostatnich latach przynajmniej jedno naruszenie danych związane z drukowaniem³



43%

firm ignoruje drukarki w swoich praktykach dotyczących bezpieczeństwa urządzeń końcowych⁴





Tylko 18% firm monitoruje drukarki pod kątem zagrożeń.⁴ A jak jest w Twojej firmie?

Dostrzegaj ukryte zagrożenia

Dział IT nieprzerwanie zajmuje się ochroną poufnych informacji na wielu urządzeniach i w wielu różnych środowiskach, odpowiadając na przykład za dane osobowe pracowników czy dane klientów. Choć w wielu działach IT stosuje się restrykcyjne zasady zabezpieczeń do poszczególnych komputerów i całej sieci, urządzenia drukujące są często pomijane, a tym samym narażone na atak. Niezabezpieczone urządzenia narażają na cyberatak całą sieć.

Poznaj potencjalne koszty

Nawet pojedyncze naruszenie zabezpieczeń może być kosztowne. Następstwem naruszenia poufności informacji wskutek braku zabezpieczeń urządzeń drukujących może być kradzież tożsamości, kradzież danych istotnych dla konkurencji, nadszarpnięty wizerunek marki i reputacja, a nawet spór sądowy. Niezgodność z przepisami może zaś skutkować wysokimi grzywnami.

HP może pomóc

Chroń swoją sieć dzięki najlepszym zabezpieczeniom procesu drukowania oferowanym przez firmę HP.¹ Drukarki HP są zawsze chronione, automatycznie wykrywając i powstrzymując zagrożenia, a jednocześnie przystosowując się do zwalczania nowych. Firma HP może pomóc w zautomatyzowaniu funkcji ochrony urządzeń, danych i dokumentów dzięki szerokiej ofercie rozwiązań. Nasi specjaliści mogą pomóc w opracowaniu i wdrożeniu wszechstronnej strategii zabezpieczeń urządzeń drukujących.

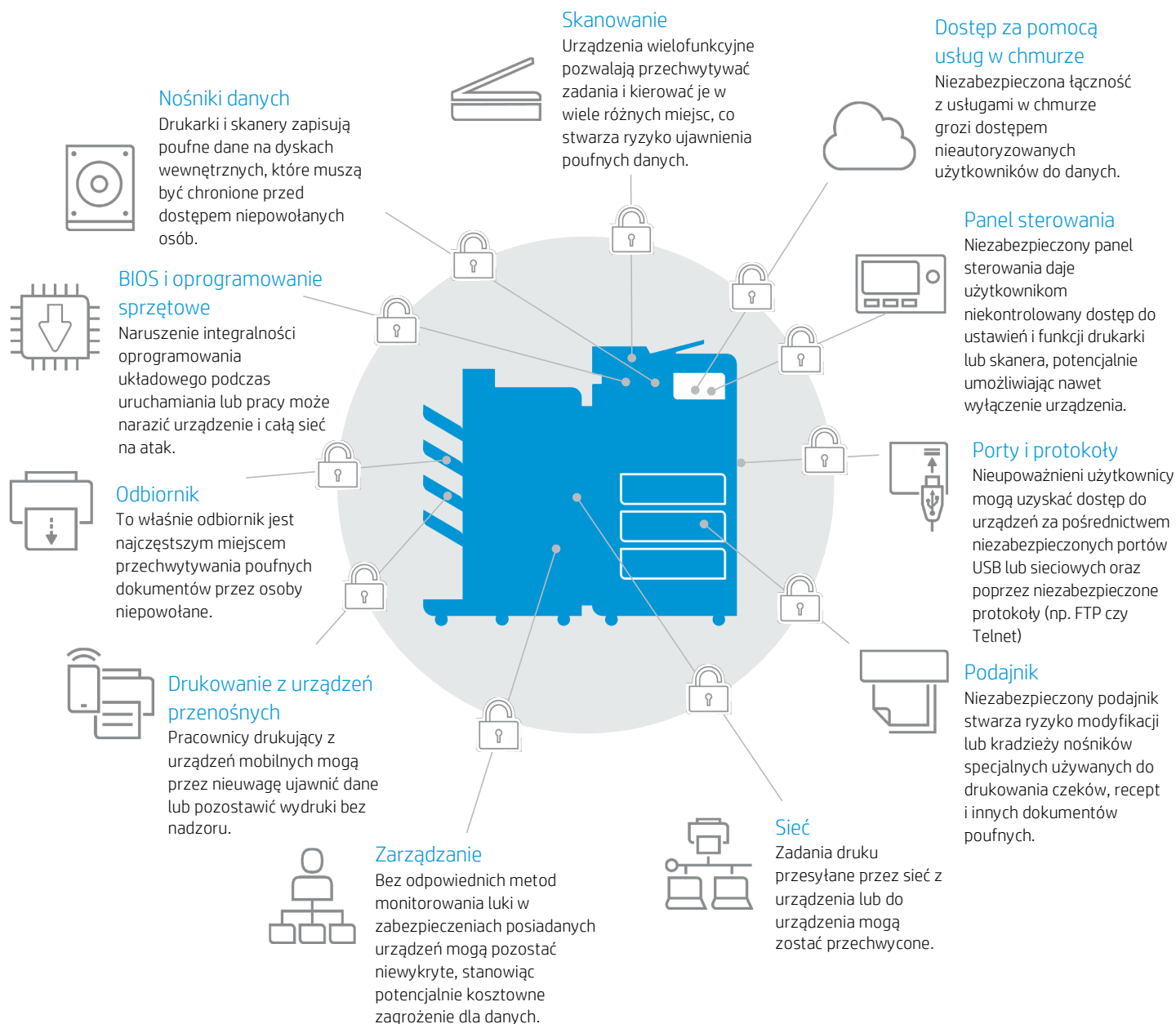
„Jako potwierdzenie długoterminowych inwestycji w bezpieczeństwo druku HP posiada najszersze i najbardziej zróżnicowane portfolio rozwiązań i usług w zakresie bezpieczeństwa na rynku”.

– Quocirca, styczeń 2017⁵

Chroń swoje urządzenia, dane i dokumenty

Kluczowe luki w zabezpieczeniach mogą się pojawiać w wielu punktach środowiska druku i przetwarzania obrazu. Dokładne zrozumienie zagrożeń pozwala nad nimi skuteczniej zapanować.

Wrażliwe punkty systemów druku i przetwarzania obrazu





Ochrona urządzenia



Więcej informacji

Usługi recyklingowe HP
hp.com/go/businessrecycling

Usługi HP Secure Managed Print Services
hp.com/go/securemps

Drukarki HP zostały zaprojektowane tak, aby w połączeniu z rozwiązaniami z zakresu monitorowania zabezpieczeń i zarządzania ograniczać ryzyko, utrzymywać zgodność i skutecznie chronić całą sieć. (Niektóre funkcje i rozwiązania są niedostępne na niektórych urządzeniach HP⁶).

Podstawowe metody zabezpieczeń

Szyfrowana pamięć masowa z bezpiecznym wymazywaniem

Wszelkie poufne informacje przechowywane na dysku wewnętrznym są narażone na kradzież. Wiele urządzeń HP ma fabrycznie wbudowane szyfrowanie w celu ochrony danych. Gdy przechowywane dane przestaną być potrzebne, można użyć wbudowanych funkcji urządzenia, aby bezpiecznie zastąpić dane i usunąć poufne informacje.

Bezpieczna utylizacja

Usługi niestandardowego przetwarzania wtórnego HP umożliwiają wyczyszczenie danych z dysków twardych przed odpowiedzialnym recyklingiem starych produktów.

Bezpieczny dostęp do drukarki w celu naprawy

Wiedza o metodach zabezpieczeń konserwatorów drukarki ułatwia ochronę poufnych danych. Warto wybrać usługi *HP Secure Managed Print Services (MPS)* lub partnerów HP, aby uzyskać fachową pomoc.

Wyłączanie nieużywanych portów i protokołów

Prawidłowa konfiguracja urządzenia zmniejszy obszar możliwego ataku. Wyłącz porty fizyczne i niezabezpieczone protokoły (takie jak FTP lub Telnet), aby uniemożliwić nieautoryzowany dostęp lub użycie.

Administracyjna kontrola dostępu do urządzenia

Ustaw hasła administratorów, aby tylko pracownicy działu IT lub inne upoważnione osoby mogły konfigurować ustawienia urządzeń.

Białe listy kodu oprogramowania układowego

Następna strona zawiera informacje o tym, w jaki sposób białe listy pomagają chronić flotę urządzeń przed szkodliwym oprogramowaniem.

Zaawansowane metody zabezpieczeń

Common Criteria Certification

Drukarki HP dla firm są certyfikowane jako zgodne z uznanymi międzynarodowo standardami bezpieczeństwa, takimi jak Common Criteria Certification (CCC) i FIPS 140. Sprawdzaj, czy aktualizacje oprogramowania układowego urządzeń mają podpisany kod w celu potwierdzenia autentyczności i integralności kodu oraz zachowania zgodności.



Więcej informacji

Wbudowane funkcje zabezpieczeń drukowania

- HP Sure Start (integralność systemu BIOS)
- Białe listy kodu oprogramowania układowego
- Wykrywanie problemów z uruchomieniem
- HP Connection Inspector

hp.com/go/PrintersThatProtect

HP JetAdvantage Security Manager:

hp.com/go/securitymanager

Funkcje zabezpieczeń drukowania automatycznie wykrywają i powstrzymują ataki

Drukarki HP dla firm mają funkcje zabezpieczeń ułatwiające ochronę przed wykorzystaniem ich jako punktów wejścia ataków do sieci. Zabezpieczenia drukowania oferowane przez HP zapewniają możliwość wykrywania zagrożeń w czasie rzeczywistym, zautomatyzowane monitorowanie oraz walidację wbudowanego oprogramowania, co pomaga zatrzymać niebezpieczeństwa już w momencie ich pojawienia się.⁷

Drukarki HP dla firm, od modeli Pro⁸ po modele Enterprise,⁷ zawsze są chronione, automatycznie wykrywając i powstrzymując zagrożenia we wszystkich fazach działania:

- **Podczas uruchomienia.** Kod rozruchowy (w przypadku urządzeń klasy Pro) lub system BIOS (w przypadku urządzeń klasy Enterprise) to zestaw instrukcji służący do ładowania krytycznych składników sprzętowych i inicjowania oprogramowania układowego. Integralność kodu jest weryfikowana w każdym cyklu rozruchu, co ułatwia ochronę urządzenia przed atakiem.
- **Podczas ładowania oprogramowania układowego.** Funkcja *białej listy* automatycznie sprawdza oprogramowanie układowe podczas rozruchu urządzenia, aby określić, czy jest to autentyczny, prawidłowy kod podpisany cyfrowo przez HP. W razie wykrycia nieprawidłowości urządzenie jest bezpiecznie uruchamiane ponownie w trybie offline i powiadamia dział IT.
- **Podczas pracy.** Wbudowane funkcje HP chronią pamięć urządzeń, gdy są one uruchomione i podłączone do sieci – czyli wtedy, kiedy dochodzi do większości ataków. W razie ataku urządzenie jest wyłączane.

Urządzenia HP Enterprise mogą przeprowadzić samonaprawę

Drukarki HP Enterprise nie tylko potrafią wykryć i powstrzymać zagrożenia, lecz także automatycznie przeprowadzić samonaprawę po atakach, dzięki czemu nie musi interweniować dział IT.⁷ Funkcje te automatycznie przeprowadzają ponowny rozruch w razie ataku lub anomalii. Administratorzy mogą otrzymywać powiadomienia za pośrednictwem narzędzi do zarządzania zdarzeniami i informacjami dotyczącymi bezpieczeństwa, takich jak ArcSight, Splunk i SIEMonster.

- *HP Sure Start* to doskonały BIOS z możliwością samonaprawy.⁷ W razie naruszenia integralności systemu BIOS program HP Sure Start przeprowadza ponowne uruchomienie przy użyciu „kopii wzorcowej” systemu BIOS.
- Funkcja *wykrywania włamań w trakcie pracy urządzenia* monitoruje skomplikowane operacje oprogramowania układowego i pamięci, automatycznie powstrzymuje włamanie i przeprowadza ponowne uruchomienie w razie ataku.
- Oprogramowanie *HP Connection Inspector* analizuje wychodzące połączenia sieciowe, aby określić, co jest normalne, powstrzymać podejrzane żądania i udaremnić działanie destrukcyjnego oprogramowania, automatycznie wykonując ponowny rozruch urządzenia.

Dzięki chroniącemu inwestycję, uaktualnianemu oprogramowaniu układowemu HP FutureSmart można dodać białe listy, wykrywanie włamań w trakcie pracy i funkcję HP Connection Inspector do wielu już używanych drukarek HP Enterprise.⁷

Cykl sprawdzania jest uzupełniony przez narzędzie HP JetAdvantage Security Manager

Po ponownym rozruchu lub dodaniu każdego nowego urządzenia do sieci program *HP JetAdvantage Security Manager* automatycznie sprawdza zgodność ustawień zabezpieczeń urządzenia z zasadami firmowymi i w razie potrzeby koryguje ustawienia.⁹ Interwencja informatyków nie jest potrzebna.

Jak to działa?

Wbudowane funkcje zabezpieczeń dotyczą czterech podstawowych etapów cyklu pracy urządzenia HP.

W razie ataku urządzenia HP Enterprise mogą przeprowadzić ponowny rozruch i samonaprawę.

Cykl sprawdzania jest uzupełniony przez narzędzie HP JetAdvantage Security Manager.

Cztery. Stały nadzór

Chroni operacje i powstrzymuje ataki podczas pracy urządzenia. Kontroluje wychodzące połączenia sieciowe, aby powstrzymać podejrzane żądania (tylko klasa Enterprise).

Trzy. Sprawdzenie ustawień

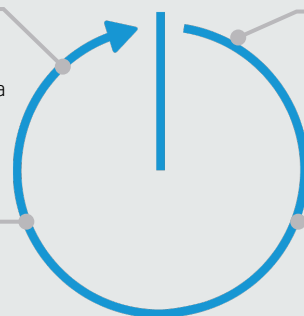
Po ponownym rozruchu program HP JetAdvantage Security Manager sprawdza i w razie potrzeby poprawia odpowiednie ustawienia zabezpieczeń na urządzeniu.

Jeden. Sprawdzenie kodu BIOS/rozruchowego

Zapobiega wykonaniu destrukcyjnego kodu podczas rozruchu, zezwalając na załadowanie jedynie oryginalnego kodu podpisanego przez HP.

Dwa. Sprawdzenie oprogramowania układowego

Dozwolone jest załadowanie jedynie autentycznego, prawidłowego oprogramowania układowego, podpisanego cyfrowo przez HP.





Ochrona danych

Dane wymagają nieprzerwanej ochrony zarówno podczas przechowywania, jak i przy przesyłaniu. Oto kilka kluczowych kroków do zapewnienia bezpiecznego przesyłania danych oraz korzystania z nich.⁶



Więcej informacji

Oprogramowanie HP Web Jetadmin
hp.com/go/wja

Uniwersalny sterownik drukarki HP z funkcją bezpiecznego drukowania szyfrowanego
hp.com/go/upd

Rozwiązania z zakresu organizacji pracy HP JetAdvantage
hp.com/go/documentmanagement

HP Access Control
hp.com/go/hpac

Podstawowe metody zabezpieczeń

Standardy sieciowe 802.1x lub IPsec

Użyj standardów szyfrowania sieci do ochrony danych przesyłanych między urządzeniem a narzędziami zarządzania, takimi jak *HP Web Jetadmin* lub *wbudowany serwer internetowy HP*.

Szyfrowanie przesyłanych danych

Chroń zadania drukowania przesyłane do urządzeń za pomocą szyfrowania, na przykład przy użyciu protokołu Internet Print Protocol over TLS (IPPS). *Uniwersalny sterownik drukarki HP z bezpiecznym szyfrowanym drukowaniem* wykorzystuje pełny algorytm symetryczny AES256 do szyfrowania i odszyfrowywania zadań drukowania na całej trasie od klienta do wydruku. Dane są szyfrowane hasłem określonym przez użytkownika, a do odszyfrowywania są używane biblioteki kryptograficzne firmy Microsoft® zgodne ze standardem FIPS 140.

Podczas skanowania *rozwiązania z zakresu organizacji pracy HP JetAdvantage* ułatwiają ochronę poufnych informacji, zarazem zwiększając wydajność. Funkcja HP Capture and Route na przykład integruje się z łatwością z funkcją HP Access Control, zapewniając wzmocnienie zabezpieczeń, a przy tym wygodę płynącą z jednokrotnego uwierzytelniania i możliwości monitorowania zawartości w celu zarządzania informacjami.¹⁰

Szyfrowanie danych przy spoczynku

Za pomocą wbudowanego szyfrowania chroń poufne informacje firmowe przechowywane na dysku twardym. Opcjonalny produkt HP Trusted Platform Module (TPM) pozwala dodać do urządzenia kolejną warstwę ochrony szyfrowanych poświadczeń i danych poprzez automatyczne hermetyzowanie kluczy szyfrowania. Moduł generuje i chroni klucze prywatne certyfikatów, udostępniając w bezpieczny sposób dane urządzenia.

Zapora

Uniemożliwia przedostanie się do sieci destrukcyjnemu oprogramowaniu i wirusom, ograniczając drukarce dostęp do urządzeń komputerowych w sieci.

Natywne uwierzytelnianie użytkowników

Zmniejsz koszty i zagrożenia bezpieczeństwa, żądając, aby użytkownicy logowali się przy użyciu protokołów uwierzytelniania PIN/PIC, LDAP lub Kerberos. Można je również zintegrować z usługą Active Directory.

Kontrola dostępu na podstawie ról

Funkcja *HP Access Control Rights Management* zmniejsza koszty i zagrożenia bezpieczeństwa za pomocą ograniczeń funkcji drukarki. Kontrola dostępu oparta na rolach umożliwia przydzielanie różnych funkcji różnym użytkownikom, a nawet całym działom, w zależności od ich potrzeb. Można na przykład ograniczyć dostęp do faksowania, skanowania do poczty elektronicznej lub skanowania do faksu.

Zaawansowane metody zabezpieczeń

Zaawansowane uwierzytelnianie i śledzenie

Stosuj zaawansowane metody uwierzytelniania (takie jak hasła, karty zbliżeniowe, karty elektroniczne lub metody biometryczne) i rozwiązania śledzenia, aby zwiększyć zabezpieczenia i kontrolę.



Więcej informacji

HP Access Control
hp.com/go/hpac

HP JetAdvantage Connect
hp.com/go/JetAdvantageConnect

Rozwiązanie HP Capture and Route
hp.com/go/hpcr

- Funkcja *HP Access Control Secure Authentication* przywraca kontrolę, wzmacnia zabezpieczenia i obniża koszty. Uzyskaj wiele różnych narzędzi i opcji kontroli, takich jak uwierzytelnianie na podstawie odcisku palca przy użyciu urządzeń przenośnych obsługujących komunikację NFC.
- Funkcja *HP Access Control Job Accounting* umożliwia ścisłe śledzenie i zbieranie danych, analizowanie wyników, a następnie tworzenie i wysyłanie raportów. Stosuj wydobyte dane w celu przypisywania kosztów druku, motywowania pracowników do inteligentniejszego drukowania i zapewniania działowi IT informacji niezbędnych do udoskonalania prognoz dotyczących całej floty.

Urządzenia przenośne uwzględnione w dostępie sieciowym

Wykorzystaj urządzenia przenośne jako część ogólnych zasad zabezpieczeń drukowania w celu kontroli dostępu do drukarki. HP oferuje rozwiązania oparte na serwerze, zapewniające bezpieczne drukowanie ściągane, a także zaawansowane funkcje zarządzania i raportów.

- Funkcja *HP JetAdvantage Connect** zapewnia intuicyjne i niezawodne funkcje drukowania z urządzeń przenośnych zaprojektowane specjalnie dla firm. Korzystanie z istniejących narzędzi i zasad sieci IT do zarządzania drukiem z urządzeń przenośnych pozwala zaoszczędzić czas i pieniądze.¹¹ Użytkownicy mogą bezpiecznie drukować ze smartfonów i tabletów w dowolnym miejscu i czasie, tak łatwo, jak przy użyciu komputera.
- Oprogramowanie *HP Access Control* zawiera funkcje zarządzania drukowaniem z urządzeń przenośnych. Wykorzystuje ono istniejącą infrastrukturę poczty e-mail, umożliwiając użytkownikom urządzeń przenośnych wysłanie zadania drukowania do kolejki druku pocztą elektroniczną, a następnie pobranie go z dowolnej drukarki lub urządzenia wielofunkcyjnego z obsługą tego rozwiązania. Dostęp do sieciowych urządzeń drukujących można chronić funkcjami bezpiecznego uwierzytelniania, między innymi funkcją Mobile Release.

Zapobiegaj wyciekom danych

Rozwiązania HP oferują funkcje zabezpieczające przed utratą danych. Rozwiązanie *HP Capture and Route Data Loss Prevention* umożliwia zapobieganie skanowaniu lub faksowaniu poufnych informacji. Z kolei dzięki funkcji *HP Access Control Print Data Loss Prevention* możliwa jest ochrona przed drukowaniem poufnych dokumentów. Śledź najważniejsze dane w celu zapobiegania naruszeniom bez spowalniania toku pracy. Otrzymuj inteligentne powiadomienia bezpieczeństwa utworzone na podstawie Twoich indywidualnych ustawień.

Zastosuj certyfikaty cyfrowe do drukarek

Popraw bezpieczeństwo swojego środowiska druku, stosując certyfikaty cyfrowe do drukarek i urządzeń wielofunkcyjnych podłączonych do sieci. Program HP JetAdvantage Security Manager pozwala zaoszczędzić czas dzięki automatycznemu instalowaniu i odnawianiu certyfikatów.⁹



Ochrona dokumentów

Zintegruj inteligentne rozwiązania sprzętowe i programowe z szerszym planem zabezpieczeń IT, aby chronić poufne informacje w drukowanych dokumentach.⁶

Podstawowe metody zabezpieczeń

Kontroluj dostęp do wydrukowanych formularzy

Wyposaż posiadane drukarki i urządzenia wielofunkcyjne w blokowane podajniki, pozwalające zapobiegać kradzieżom papierów specjalnych używanych do drukowania czeków, recept i innych poufnych dokumentów.

Użyj opcjonalnego kodu PIN lub drukowania ściąganego, aby chronić poufne dokumenty

Użytkownicy mogą korzystać z opcji kodu PIN lub drukowania ściąganego, co zmniejsza zależność od drukarek osobistych, jak również ryzyko dostania się zadań drukowania w niepowołane ręce. Takie zabezpieczenia pozwalają dodatkowo ograniczyć liczbę nieodebranych wydruków, obniżając koszty i zmniejszając ilość odpadów.

W przypadku drukowania z kodem PIN użytkownicy wysyłający poufne zadania drukowania przypisują kod PIN, który trzeba wprowadzić na urządzeniu, aby uruchomić zadanie.

W przypadku drukowania ściąganego zadanie drukowania jest przechowywane w chmurze lub na komputerze użytkownika. Użytkownicy dokonują uwierzytelniania w wybranej lokalizacji drukarki w celu ustawienia zadań do drukowania w kolejce. HP oferuje dwa rozwiązania drukowania ściąganego oparte na chmurze:*

- *HP JetAdvantage Secure Print* to przystępne rozwiązanie opracowane dla małych i średnich firm, przechowujących zadania drukowania w chmurze lub na komputerze użytkownika. Jest łatwe w konfiguracji i obsłudze, umożliwia użytkownikom uruchamianie zadań za pomocą urządzenia przenośnego i obsługuje urządzenia wielu producentów.¹²
- *HP JetAdvantage Private Print* to bezpłatne, oparte na chmurze rozwiązanie HP, pozwalające korzystać z zalet drukowania ściąganego bez wprowadzania złożoności. Usługa jest łatwa w konfiguracji i nie wymaga serwera, instalowania ani utrzymywania.¹³

Zaawansowane metody zabezpieczeń

Korzystaj z drukowania w trybie pull printing w przypadku każdego zadania druku

Rozwiązanie *HP Access Control Secure Pull Printing* chroni poufne informacje, wzmacnia zabezpieczenia urządzeń i zwiększa wydajność. To solidne rozwiązanie serwerowe oferuje wiele form uwierzytelniania, w tym wydawanie plaketek, a także funkcje zabezpieczeń i zarządzania na poziomie przedsiębiorstwa.

Stosuj MICR, znaki wodne lub inne funkcje, aby zapobiegać kopiowaniu lub modyfikacji

Dostępnych jest wiele rozwiązań HP i TROY do zapobiegania fałszerstwom*, między innymi stosowanie bezpiecznego tonera, który plami papier w razie próby modyfikacji środkami chemicznymi, dodawanie zmiennych znaków wodnych do drukowanych stron lub stosowanie kodów czytelnych dla urządzeń, umożliwiających śledzenie i kontrolowanie poszczególnych dokumentów. Urządzenia wielofunkcyjne mogą zabezpieczać poufne dokumenty drukowane, na przykład recepty, akty urodzenia lub protokoły sądowe, umieszczając na nich elementy zapobiegające fałszowaniu, w tym własne podpisy, logotypy firmy czy czcionki zabezpieczające.



Więcej informacji

HP JetAdvantage Secure Print
hp.com/go/JetAdvantageSecurePrint

HP JetAdvantage Private Print
hp.com/go/JetAdvantagePrivatePrint

HP Access Control
hp.com/go/hpac

Ochrona dokumentów HP i TROY
hp.com/go/HPandTROY



Monitoruj środowisko druku i zarządzaj nim



Więcej informacji

HP JetAdvantage Security Manager
hp.com/go/securitymanager

Rozwiązania monitorowania zabezpieczeń i zarządzania mogą ułatwić identyfikację luk w zabezpieczeniach i ustanowić jednolite, oparte na zasadach podejście do ochrony danych, zmniejszania ryzyka i utrzymywania zgodności z przepisami.⁶ Zapobiegaj lukom w ochronie i unikaj kosztownych grzywien.

Podstawowe metody zabezpieczeń

Aktualizuj urządzenia za pomocą najnowszego oprogramowania układowego / systemu operacyjnego

Użyj oprogramowania HP Web Jetadmin¹⁴ do wysyłania aktualizacji oprogramowania układowego do całej floty, dzięki czemu urządzenia będą mieć najnowszą ochronę i funkcje zabezpieczeń.

Sprawdzaj dzienniki zdarzeń zabezpieczeń drukarki

Urządzenia HP wysyłają zdarzenia drukarki / powiadomienia do serwera syslog, dzięki czemu dział IT w razie potrzeby może rozwiązać problemy.

Analizuj i koryguj ustawienia urządzeń

Zarządzaj podstawowymi ustawieniami zabezpieczeń drukarek w całej flocie dzięki zestawowi *HP Print Manageability Integration Kit (MIK)*, dodatkowi plug-in do programu Microsoft® System Center Configuration Manager (SCCM). Microsoft SCCM to powszechnie używane rozwiązanie zarządzania, umożliwiające zdalne planowanie, instalowanie, konfigurowanie i monitorowanie systemów końcowych. Zestaw HP Print MIK może wykrywać, analizować i korygować 15 najważniejszych ustawień zabezpieczeń oraz generować raport dotyczący wyników.

Wszechstronne zarządzanie zabezpieczeniami w całej flocie zapewnia narzędzie *HP JetAdvantage Security Manager*.⁹ To rozwiązanie zmniejsza koszty i zasoby niezbędne do wdrożenia zasad zabezpieczeń w całej flocie i zautomatyzowania korekty ustawień urządzeń, a także instaluje i odnawia niepowtarzalne certyfikaty, zarazem generując raporty niezbędne do zapewnienia zgodności z przepisami.



Więcej informacji

HP JetAdvantage Security Manager
hp.com/go/securitymanager

Zaawansowane metody zabezpieczeń

Zainstaluj oprogramowanie SIEM w celu wykrywania i dokumentowania zagrożeń

Dane zdarzeń z urządzeń z oprogramowaniem układowym HP FutureSmart można wysyłać do narzędzi do wykrywania incydentów, takich jak ArcSight, Splunk i SIEMonster, zapewniających monitorowanie w czasie rzeczywistym. Osoby odpowiedzialne za bezpieczeństwo informatyczne mogą z łatwością zobaczyć systemy końcowe drukarek jako część szerszego ekosystemu informatycznego, aby wykrywać i rozwiązywać alerty zabezpieczeń drukarek.

Automatycznie konfiguruje nowe urządzenia drukujące dodawane do sieci

Funkcja Instant-on Security oprogramowania HP JetAdvantage Security Manager automatycznie konfiguruje nowe urządzenia w chwili ich dodania do sieci lub po ich ponownym uruchomieniu.

Raporty inspekcji zgodności zabezpieczeń floty urządzeń drukujących z przepisami

Używaj oprogramowania HP JetAdvantage Security Manager do tworzenia raportów stanowiących dowód zgodności z przepisami, demonstrujących stosowanie zasad zabezpieczeń do drukarek i ochrony danych klientów.

Naruszenie zgodności z przepisami może zaszkodzić firmie

Niechronione lub zbyt słabo chronione systemy końcowe stwarzają więcej okazji do cyberprzestępstw. Aby przeciwdziałać rosnącemu zagrożeniu, organy rządowe z całego świata wdrażają surowe przepisy bezpieczeństwa, które wymuszają na organizacjach lepszą ochronę danych klienta.

Organizacje nieosiągające zgodności z przepisami mogą napotkać poważne koszty obejmujące grzywny, utratę

zamówień, nadszarpniętą reputację oraz pozwy zbiorowe.

Niezbędne jest wdrożenie urządzeń i rozwiązań takich jak drukarki HP Enterprise i oprogramowanie HP JetAdvantage Security Manager, które mogą zapewnić spełnienie wymogów zgodności z przepisami oraz ochronę informacji firmowych przed zagrożeniami bezpieczeństwa.



Pomoc, jakiej potrzebujesz

Możesz liczyć na pomoc w tworzeniu systemu zabezpieczeń. Zespół konsultantów z działu pomocy technicznej może przedstawić metody zwiększania bezpieczeństwa danych, urządzeń i dokumentów.

Przeanalizuj bieżące luki w zabezpieczeniach drukowania z ekspertami w dziedzinie bezpieczeństwa drukowania. Pomagamy w utworzeniu wszechstronnych zasad zabezpieczeń drukowania odpowiednich do potrzeb firmy i opartych na sprawdzonych metodach, a także w utworzeniu planu osiągnięcia lepszych zabezpieczeń w danym środowisku.

Lider w branży

Firma HP została mianowana liderem w pierwszym raporcie IDC MarketScape na temat rozwiązań dotyczących bezpieczeństwa oraz oceny sprzedawców Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment (z raportem można się zapoznać [tutaj](#)). Zgodnie z raportem: „W kwestii bezpieczeństwa firma HP Inc. bierze pod uwagę całą infrastrukturę druku i dokumentów, poczynwszy od zablokowania urządzenia, na wszelkich aspektach użytkowania urządzenia oraz ochrony treści skończywszy”. Niniejszy wykres pochodzi z raportu IDC 2017 Vendor Assessment.¹⁵

Celem modelu analizy sprzedawców IDC MarketScape jest dostarczenie przeglądu konkurencyjności dostawców ICT na danym rynku. Metodologia badania wykorzystuje rygorystyczną metodę punktacji bazującą zarówno na kryteriach ilościowych, jak i jakościowych, dzięki której powstaje graficzne przedstawienie pozycji każdego sprzedawcy na danym rynku. Wynik w kategorii Capabilities (potencjał) stanowi ocenę produktu sprzedawcy, strategii wprowadzania go na rynek oraz realizacji celów biznesowych w krótkim terminie. Wynik w kategorii Strategy (strategia) jest miarą zgodności strategii sprzedawcy z wymaganiami klientów w okresie od 3 do 5 lat. Udział sprzedawcy w rynku został zilustrowany odpowiednim rozmiarem ikony.¹⁵

Pierwsze kroki

Skontaktuj się z przedstawicielem handlowym, aby uzyskać więcej informacji o oferowanych przez HP funkcjach zabezpieczeń, rozwiązaniach i usługach, dzięki którym zyskasz większą ochronę i spokojny sen.

Więcej informacji

hp.com/go/printsecurity

¹ Stwierdzenie „najbezpieczniejsze na świecie drukowanie” na podstawie analizy HP dotyczącej udostępnionych w 2017 r. funkcji zabezpieczeń drukarek HP tej samej klasy. Firma HP oferuje zestaw funkcji zabezpieczeń, które monitorują, wykrywają i automatycznie powstrzymują ataki, a następnie kontrolują poprawność oprogramowania po ponownym uruchomieniu. Lista produktów znajduje się na stronie internetowej hp.com/go/LJCompatibility.

² InfoTrends, „Projektowanie sprzętu i oprogramowania”, Brendan Morse, październik 2016.

³ Quocirca, „Obszar usług zarządzania drukiem, 2016”, quocirca.com/content/managed-print-services-landscape-2016, lipiec 2016.

⁴ Przeprowadzona na zlecenie HP ankieta firmy Spiceworks wśród 309 osób decyzyjnych w dziedzinie IT w regionach Ameryki Północnej, EMEA i APAC, listopad 2016 r.

⁵ Quocirca, „Bezpieczne drukowanie: konieczność w erze Internetu rzeczy”, quocirca.com/content/print-security-imperative-iot-era, styczeń 2017.

⁶ Rozwiązania mogą nie być obsługiwane przez niektóre urządzenia HP. Rozwiązania mogą wymagać zakupu dodatkowych opcji.

⁷ Najbardziej zaawansowane funkcje zabezpieczeń HP są dostępne w urządzeniach HP klasy Enterprise dzięki oprogramowaniu FutureSmart w wersji 4.5 lub nowszej. Stwierdzenie na podstawie analizy HP dotyczącej udostępnionych w 2017 r. wbudowanych funkcji zabezpieczeń drukarek HP tej samej klasy. HP oferuje takie połączenie funkcji zabezpieczeń, które umożliwia sprawdzanie integralności do poziomu systemu BIOS i obejmuje możliwość samonaprawy.

⁸ Wybrane urządzenia HP LaserJet Pro i PageWide Pro posiadają wbudowane funkcje, które umożliwiają automatyczne wykrywanie i zatrzymywanie ataków. Więcej informacji można znaleźć na stronie hp.com/go/LJCompatibility.

⁹ Oprogramowanie HP JetAdvantage Security Manager należy zakupić oddzielnie. Aby dowiedzieć się więcej, odwiedź stronę hp.com/go/securitymanager.

¹⁰ Dodatkowe hasło jest wymagane, kiedy informacje są wysyłane do chronionego hasłem repozytorium końcowego.

¹¹ Funkcja HP JetAdvantage Connect jest zgodna z czołowymi urządzeniami przenośnymi. Urządzenia z systemami operacyjnymi Android™, Google Chrome™ i Microsoft® wymagają jednorazowego zainstalowania specjalnego dodatku. Pełna lista obsługiwanych systemów operacyjnych jest dostępna na stronie hp.com/go/JetAdvantageConnect.

¹² HP JetAdvantage Secure Print: funkcja pull printing działa we wszystkich podłączonych do sieci drukarkach lub urządzeniach wielofunkcyjnych. Uwierzytelnianie za pomocą urządzenia jest dostępne w przypadku wielu urządzeń HP LaserJet, PageWide i OfficeJet Pro oraz w przypadku urządzeń innych firm. Niektóre urządzenia mogą wymagać uaktualnienia oprogramowania sprzętowego. Do przechowywania w chmurze i odbierania zadań drukowania wymagane jest połączenie internetowe. Wysyłanie zadania drukowania z urządzenia przenośnego wymaga połączenia sieciowego i kodu QR. Więcej informacji oraz lista obsługiwanych drukarek i urządzeń wielofunkcyjnych znajduje się na stronie hp.com/go/JetAdvantageSecurePrint.

¹³ Oprogramowanie HP JetAdvantage Private Print jest dostępne bezpłatnie i wymaga połączenia drukarki z Internetem oraz włączenia usług internetowych. Nie jest dostępne w niektórych krajach. Więcej informacji na stronie hp.com/go/JetAdvantagePrivatePrint.

¹⁴ Narzędzie HP Web Jetadmin można bezpłatnie pobrać ze strony hp.com/go/webjetadmin.

¹⁵ Na podstawie przeglądu sprzedawców autorstwa IDC oraz opinii dotyczącej czołowej roli HP: „Firma HP ma przewagę dzięki wysokiej jakości usługom i możliwościom w zakresie IT... oraz zapewnianiu kompleksowej i zintegrowanej strategii w zakresie bezpieczeństwa w całej infrastrukturze IT”. ŹRÓDŁO: IDC MarketScape: Raport Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment, Allison Correia i Robert Palmer, październik 2017, IDC Doc #US41988517.

* Dostępność rozwiązań w zakresie drukowania może się różnić w zależności od kraju.

Zarejestruj się, aby otrzymywać aktualizacje

hp.com/go/getupdated



Udostępnij współpracownikom

© Copyright 2014–2018 HP Development Company, L.P. Informacje zawarte w tym dokumencie mogą ulec zmianie bez powiadomienia. Jedyne gwarancje na produkty i usługi HP są określone w dokumentach gwarancyjnych dołączonych do tych produktów i usług. Żadne informacje przedstawione w tym dokumencie nie powinny być interpretowane jako dodatkowa gwarancja. Firma HP nie ponosi odpowiedzialności za błędy techniczne, redakcyjne lub pominięcia w treści niniejszego dokumentu.

Android i Google Chrome są zastrzeżonymi znakami towarowymi firmy Google Inc. Windows jest zastrzeżonym znakiem towarowym grupy kapitałowej Microsoft w Stanach Zjednoczonych.

4AA3-1295PLE, styczeń 2018, wersja 11

