



HP DaaS Proactive Security



Korzyści związane z usługą

- Większe bezpieczeństwo punktów końcowych
- Ochrona przed złośliwymi witrynami i załącznikami
- Ochrona danych i urządzeń użytkownika

Najważniejsze cechy usługi

- Zaawansowana technologia izolująca zabezpiecza przed złośliwym oprogramowaniem²
- Rozwiązanie analityczne HP TechPulse dostarcza dane i raporty dotyczące bezpieczeństwa
- Aon CyQu pozwala szacować poziom bezpieczeństwa³

Przegląd usługi

Rozszerz możliwości bezpiecznego zarządzania w ramach HP Device as a Service (DaaS) o usługę HP DaaS Proactive Security.¹ Zapewnia ona działającą w czasie rzeczywistym ochronę przed złośliwym oprogramowaniem dla punktów końcowych, funkcje analizy bezpieczeństwa i ryzyka oraz specjalistyczne dane, które pozwalają wzmocnić poziom bezpieczeństwa. Technologia izolowania zagrożeń chroni przed złośliwym oprogramowaniem infekującym systemy przez pocztę elektroniczną, przeglądarki oraz pliki pakietu Office i PDF. Rozszerza ona zakres danych i raportów bezpieczeństwa dzięki narzędziom analitycznym HP TechPulse. Dzięki temu możesz się chronić przed zagrożeniami, zrozumieć zasady ich działania oraz odpowiednio na nie reagować.

Funkcje i specyfikacje

Zaawansowana technologia izolująca

Wirusy, programy ransomware i inne rodzaje złośliwego oprogramowania cały czas stanowią główne zagrożenie dla infrastruktury IT. Wyjdź poza rozwiązania antywirusowe oparte na definicjach i przejdź na technologie izolowania zagrożeń w czasie rzeczywistym przez wykorzystanie mikromaszyn wirtualnych (VM) do powstrzymywania ataków zero-day z poziomu poczty e-mail, przeglądarek i plików, zabezpieczając tym samym swoją sieć.² Użytkownicy mogą wyświetlać załączniki i strony internetowe bez naruszania bezpieczeństwa sieci, przerywania swojej pracy oraz zmieniania obowiązujących procedur.

Narzędzia analityczne HP TechPulse

Otrzymuj informacje na bieżąco, zyskaj pełen wgląd w stan ochrony urządzeń oraz szczegółowe dane dotyczące bezskutecznych i zablokowanych ataków dzięki rozwiązaniu HP TechPulse – a wszystko to na pojedynczym pulpicie dostępnym przez portal HP DaaS.

Eksperci HP ds. usług

Popraw swoje bezpieczeństwo, przygotuj się na ataki i uniknij negatywnego wpływu na działalność przedsiębiorstwa dzięki naszym specjalistom, którzy śledzą raporty, analizują zagrożenia i pomagają w ustalaniu planów. Eksperci HP ds. usług przeprowadzają kwartalne analizy zagrożeń bezpieczeństwa i reagują na związane z nimi alerty.⁴

Aon

Wspólnie z firmą Aon oferujemy dodatkowe rozwiązania z dziedziny cyberbezpieczeństwa obejmujące usługi analityczne, reagowania na zdarzenia oraz ubezpieczeniowe. Narzędzie do samodzielnej analizy Aon Cyber Quotient (CyQu) pozwala oszacować poziom zabezpieczeń względem bliźniaczych firm z branży, a firma Aon zapewnia bezpłatną usługę reagowania na incydenty z godzinną konsultacją w wypadku zdarzenia naruszającego bezpieczeństwo.³

Plany DaaS Proactive Security

Funkcje oferowane w ramach usług	Plan standardowy (samodzielnie zarządzany)	Plan rozszerzony (zarządzany przez HP)
Ochrona przed załącznikami e-mail, linkami do stron wyludających dane oraz plikami do pobrania.	✓	✓
Dane analityczne dotyczące bezpieczeństwa od HP TechPulse.	✓	✓
Analityka Aon CyQu, reagowanie na incydenty i kwalifikacja do ubezpieczeń. ³	✓	✓
Wdrażanie polityki izolowania: eksperci HP ds. usług mogą zarządzać statusami zaawansowanej technologii zabezpieczającej.	—	✓
Analityka: w razie konieczności eksperci HP ds. usług przeprowadzą analizę wyizolowanych zagrożeń i przedstawiają zalecenia dotyczące najlepszych praktyk dla użytkowników i urządzeń narażonych na dużą ilość zagrożeń.	—	✓
Badanie i powiadamianie o zdarzeniach związanych z bezpieczeństwem: eksperci HP ds. usług powiadomią klienta o tym, że urządzenia nie są już chronione z powodu naruszenia ustawień przez użytkowników lub na skutek wprowadzenia zmian w konfiguracji systemowej.	—	✓

Opis realizacji

Charakterystyka usługi

- **Plan standardowy:** standardowa, samodzielnie zarządzana wersja usługi DaaS Proactive Security jest dostępna dla planów standardowych, rozszerzonych i premium DaaS. W przypadku wersji samzarządzanej użytkownik bierze na siebie odpowiedzialność wdrożenia urządzeń oraz za kontakt z firmą HP, jeśli będzie potrzebował pomocy.
- **Plan rozszerzony:** Rozszerzona wersja usługi DaaS Proactive Security jest dostępna tylko w planie rozszerzonym lub planie premium DaaS. W tym planie kierownik ds. programów wdrażania HP udziela pomocy podczas wprowadzania i konfiguracji usługi, natomiast eksperci HP ds. usług związanych z cyberbezpieczeństwem zapewniają stały monitoring i wsparcie.

Obowiązki HP

Obowiązki ekspertów ds. usług w planach standardowych:

- Rozwiązywanie problemów związanych z instalacją i łącznością.
- Udzielanie pomocy i porad w zakresie spraw serwisowych.
- Dodawanie adresów URL do białej listy witryn związanych z firmą.

Obowiązki ekspertów ds. usług w planach rozszerzonych:

- Zapewnienie prawidłowej instalacji i działania zaawansowanej technologii izolującej.
- Dostarczanie kwartalnych raportów analitycznych dotyczących zagrożeń dla bezpieczeństwa.
- Badanie alertów bezpieczeństwa i podejmowanie stosowanych działań.
- Monitorowanie usługi oraz koordynowanie procedur rozwiązywania problemów i działań pomocniczych.
- Zapewnianie wsparcia 2. i 3. poziomu oraz współpraca z działem pomocy technicznej klienta.

Obowiązki klienta

- Analizowanie pulpitów nawigacyjnych, raportów i zdarzeń w pulpicie HP DaaS Proactive Management.
- Analizowanie raportów dotyczących bezpieczeństwa i podejmowanie stosownych działań.
- Żądanie i przekazywanie adresów URL witryn z białej listy.
- Rozwiązywanie i kategoryzowanie częstych problemów związanych ze wsparciem użytkownika końcowego przed ich przekazaniem do działu wsparcia HP.
- Odnowienie, zmiana lub anulowanie konta HP DaaS.
- Wypełnienie internetowej ankiety CyQu.³

Wymagania systemowe

- Usługa HP DaaS Proactive Security wymaga urządzeń różnych marek z systemem Windows 10 w wersji 1703 lub nowszej, min. 8 GB pamięci i 6 GB wolnej przestrzeni na dysku twardym.
- HP DaaS Proactive Security wymaga dostępu do rozwiązania HP TechPulse, które jest uwzględnione w każdym planie usługi HP DaaS lub HP DaaS Proactive Management. Plan rozszerzony usługi HP DaaS Proactive Security wymaga wykupienia planu rozszerzonego lub premium usługi HP DaaS.
- Aby umożliwić komunikację między urządzeniami zarządzanymi a usługą zarządzania w chmurze HP, wymagane jest aktywne połączenie z internetem.
- Szczegółowe informacje znajdują się na stronie hpdaas.com/requirements.

Opis realizacji (ciąg dalszy)

Wdrażanie

Wdrażanie jest procedurą wprowadzania kwalifikujących się urządzeń do programu DaaS Proactive Security. Jeśli klient jest objęty planem rozszerzonym lub premium HP DaaS, do programu przypisany zostanie kierownik ds. procedur wdrażania. Jeśli klient jest objęty samodzielnie zarządzanym planem standardowym, ekspert ds. usług HP utworzy dla niego konto i przekaze wszystkie konieczne informacje w powitalnej wiadomości e-mail, w której znajdują się także instrukcje opisujące proces uzyskiwania potrzebnego wsparcia.

Wstępne wymagania związane z wdrażaniem

Przed przeniesieniem urządzeń do planu DaaS Proactive Security klient musi przekazać poniższe informacje swojemu kierownikowi ds. programu wdrażania, opiekunowi klienta HP i/lub partnerowi serwisowemu:

- główne dane kontaktowe (imię i nazwisko, adres e-mail, telefon, lokalizacja)
- adres firmy
- nazwę domeny DNS Active Directory
- listę administratorów raportujących
- listę urządzeń, które będą zarządzane w ramach usługi HP Proactive Management, z uwzględnieniem modelu i numeru seryjnego (tylko w przypadku planów rozszerzonych i premium DaaS)

Procedura wdrażania

- **Faza 1: rejestracja** – klient otrzymuje klucz licencyjny oraz link do internetowego formularza rejestracyjnego.
- **Faza 2: gromadzenie informacji** – klientowi przypisany zostaje kierownik ds. wdrażania, który zarządza całą procedurą. Ustala on rozmowę konferencyjną, podczas której przekazuje zalecenia dotyczące sposobu postępowania.
- **Faza 3: zalecenia i tworzenie konta** – firma HP tworzy dla klienta konto na platformie zabezpieczeń HP DaaS, zaczynając od ustalenia domyślnych konfiguracji zabezpieczeń oraz dodania do białej listy adresów URL, których potrzebuje klient.
- **Faza 4: wdrażanie** – kierownik ds. wdrażania spotyka się z klientem, aby rozpocząć procedurę wprowadzania urządzeń oraz w celu rozwiązania ewentualnych problemów.
- **Faza 5: przejście na stały program wsparcia i zarządzania (tylko plany rozszerzone)** – po zakończeniu procedury wdrażania program zostaje przejęty przez ekspertów HP ds. usług, którzy zapewniają stałe wsparcie i nadzór w okresie objętym umową.

Obowiązki kierownika ds. programu wdrażania

- Utworzenie konta HP DaaS Proactive Management.
- Dodawanie i usuwanie użytkowników pulpitów nawigacyjnych HP DaaS Proactive Management.
- Udzielanie dostępu do kont użytkowników.
- Gromadzenie i konsolidowanie wymaganych informacji środowiskowych.
- Dostarczenie dokumentacji i wskazówek pozwalających wdrożyć narzędzie analityczne.
- Opracowanie i implementacja planu związanego z projektem wdrażania.
- Udzielanie informacji o postępach.
- Weryfikacja pomyślnego wdrożenia.
- Przeniesienie obowiązku wsparcia klienta w zakresie HP DaaS Proactive Management na ekspertów HP ds. usług.
- Diagnozowanie i rozwiązywanie problemów związanych z instalacją.
- Zapewnianie stałego wsparcia.

Ograniczenia dotyczące usługi

- Dostępność ekspertów HP ds. usług w ramach planu rozszerzonego DaaS Proactive Security:
 - **Ameryka Północna:** wsparcie w języku angielskim jest dostępne od poniedziałku do piątku (z wyjątkiem dni wolnych od pracy w firmie HP) od 6.00 do 18.00 czasu MT.
 - **Ameryka Łacińska:** wsparcie w języku angielskim i hiszpańskim jest dostępne od poniedziałku do piątku (z wyjątkiem dni wolnych od pracy w firmie HP) od 7.00 do 18.00 czasu GMT-5.
 - **Europa, Bliski Wschód i Afryka:** wsparcie w języku angielskim, francuskim i niemieckim jest dostępne od poniedziałku do piątku (z wyjątkiem dni wolnych od pracy w firmie HP) od 8.00 do 18.00 czasu CET.
 - **Region Azji i Pacyfiku, Japonia:** wsparcie w języku angielskim i chińskim jest dostępne przez 24 godziny na dobę; wsparcie w języku japońskim jest zapewniane od 9.00 do 21.00 czasu japońskiego przez 7 dni w tygodniu (z wyjątkiem dni wolnych od pracy w firmie HP).
- Usługi Aon są obecnie dostępne tylko w Stanach Zjednoczonych.
- Platformy HP DaaS Proactive Management i HP DaaS Proactive Security są dostępne w ramach Amazon Web Services (AWS).

Warunki

Zapoznaj się z [warunkami](#) HP DaaS.

Dowiedz się więcej

Aby uzyskać szczegółowe informacje, skontaktuj się z lokalnym przedstawicielem lub partnerem kanałowym HP bądź odwiedź stronę hp.com/go/DaaS.

Zarejestruj się, aby otrzymywać aktualizacje
hp.com/go/getupdated



Podziel się ze współpracownikami

1. Wymagania systemowe dla usługi HP DaaS Proactive Security: urządzenia różnych marek z systemem Windows 10 w wersji 1703 lub nowszej, min. 8 GB pamięci i 6 GB wolnej przestrzeni na dysku twardym w celu instalacji klienta oprogramowania. HP DaaS Proactive Security wymaga dostępu do rozwiązań HP TechPulse, które jest uwzględnione w każdym planie usługi HP DaaS lub HP DaaS Proactive Management. Plan rozszerzony usługi HP DaaS Proactive Security wymaga wykupienia planu rozszerzonego lub premium usługi HP DaaS lub HP DaaS Proactive Management.
2. Technologia HP Sure Click Advanced wchodzi w zakres usługi HP DaaS Proactive Security i wymaga systemu operacyjnego Windows 10. Obsługiwane są przeglądarki Microsoft Internet Explorer, Google Chrome i Chromium. Obsługiwane załączniki obejmują pliki pakietu Microsoft Office (Word, Excel, PowerPoint) oraz pliki PDF, jeśli na komputerze zainstalowane jest oprogramowanie Microsoft Office lub Adobe Acrobat.
3. Usługi Aon są dostępne tylko w Stanach Zjednoczonych.
4. Usługi ekspertów są dostępne wyłącznie w ramach planu rozszerzonego usługi Proactive Security.

© Copyright 2019 HP Development Company, L.P. Informacje zawarte w niniejszym dokumencie mogą ulec zmianie bez powiadomienia. Jedyne gwarancje, jakich firma HP udziela na produkty i usługi, są określone w oświadczeniach gwarancyjnych dostarczanych wraz z tymi produktami i usługami. Żadne informacje przedstawione w niniejszym dokumencie nie powinny być interpretowane jako dodatkowa gwarancja. Firma HP nie ponosi odpowiedzialności za błędy techniczne lub redakcyjne oraz braki występujące w niniejszym dokumencie. Adobe i Acrobat są znakami towarowymi Adobe Systems Incorporated. Google, Chrome i Chromium są znakami towarowymi firmy Google Inc. Microsoft i Windows są zarejestrowanymi znakami towarowymi firmy Microsoft Corporation w Stanach Zjednoczonych i/lub w innych krajach.

4AA7-4656PLE, marzec 2019 r

