



HP DaaS Proactive Security



Voordelen van de service

- Maakt endpoints veiliger
- Beschermst tegen kwaadaardige websites en bijlagen
- Beschermst uw gegevens en apparaten

Kenmerken van de service

- Geavanceerde isolatietechnologie beschermt tegen malware²
- Inzicht in beveiliging en rapporten met HP TechPulse analytics
- Evaluatie van uw beveiligingsniveau met Aon CyQu³

Overzicht van de service

Versterk de mogelijkheden voor beveiligingsbeheer van HP Device as a Service (DaaS) met HP DaaS Proactive Security.¹ Dit biedt realtime bescherming tegen malware voor computerendpoints, veiligheids- en dreigingsanalyse en gespecialiseerde expertise om uw beveiliging te helpen verbeteren. Technologie voor het isoleren van aanvallen beschermt het apparaat tegen malware die binnenkomt via e-mail, browsers en Office- en pdf-bestanden. De technologie vormt een aanvulling op de inzichten in de beveiliging en rapporten van HP TechPulse analytics. Zo kunt u zich beschermen tegen aanvallen, ze begrijpen en erop reageren.

Kenmerken en specificaties

Geavanceerde isolatietechnologie

Virussen, ransomware en andere malware vormen een voortdurende bedreiging van IT-infrastructuur. Ga een stap verder dan de bekende antivirusoplossingen en pas realtime gevarenisolatie toe met behulp van micro-virtuele machines (VM) om zero-day aanvallen op e-mail, browser en bestanden af te slaan en uw netwerk te beschermen.² Gebruikers kunnen bijlagen en websites bekijken zonder dat de beveiliging van hun netwerk in gevaar komt en zonder de werkstroom te onderbreken of hun werkwijzen te wijzigen.

HP TechPulse analytics

Blijf op de hoogte en ontvang een holistisch overzicht van de beschermingsstatus van uw apparatuur en uitvoerige informatie over aanvalspogingen en -blokkeringen met HP TechPulse, allemaal op een alles-in-één dashboard dat beschikbaar is via het HP DaaS-portaal.

HP Service Experts

Verbeter uw beveiliging, blijf aanvallen voor en voorkom dat uw bedrijf negatieve gevolgen ondervindt dankzij onze gespecialiseerde Service Experts die rapporten monitoren, dreigingen analyseren en u helpen met de planning. HP Service Experts zullen ieder kwartaal de veiligheidsdreiging analyseren en reageren op veiligheidswaarschuwingen.⁴

Aon

Wij werken samen met Aon zodat wij aanvullende cyberveiligheidsoplossingen kunnen aanbieden, waaronder beoordeling, respons bij incidenten en verzekeringsservices. Met de Aon Cyber Quotient (CyQu) zelfbeoordelingstool en veiligheidsscore kunt u uw veiligheidsniveau evalueren en vergelijken met andere bedrijven in de industrie. Daarnaast rekent Aon \$0 voor respons bij incidenten met een uur advies in geval van een beveiligingsinbreuk.³

DaaS Proactive Security-plannen

Servicekenmerken	Standaardpakket (zelfbeheer)	Uitgebreid pakket (beheerd door HP)
Bescherming tegen dreiging uit e-mailbijlagen, phishinglinks en downloads	✓	✓
Veiligheidsinzichten via HP TechPulse	✓	✓
Aon CyQu evaluatie, respons bij incidenten en verzekeringsdekking ³	✓	✓
Handhaving van isolatiebeleid: HP Service Experts kunnen zorgen voor een geavanceerde beveiligingsstatus	—	✓
Analyse: HP Service Experts maken een doeltreffende analyse van geïsoleerde dreigingen en doen waar nodig aanbevelingen voor de beste praktijken voor gebruikers en apparaten waarvoor veel dreiging bestaat.	—	✓
Onderzoeken en melden van beveiligingsincidenten: HP Service Experts sturen een melding wanneer uw apparaten niet langer beschermd zijn ten gevolge van manipulatie door eindgebruikers of wijzigingen in de systeemconfiguratie.	—	✓

Leveringsspecificaties

Serviceopties

- **Standaard:** De standaard, zelfbeheerde versie van DaaS Proactive Security is beschikbaar voor de DaaS-plannen standaard, uitgebreid en premium. Bij de zelfbeheeroptie bent u zelf verantwoordelijk voor het aanmelden van uw apparaten en kunt u desgewenst contact opnemen met HP voor assistentie.
- **Uitgebreid:** De uitgebreide versie van DaaS Proactive Security is alleen beschikbaar als u tevens een uitgebreid of premium DaaS-plan heeft. In het plan Uitgebreid krijgt u assistentie van een programmamanager onboarding bij het installeren en configureren van de service en zorgen HP Service Experts met expertise op het gebied van cyberveiligheid voor continue monitoring en ondersteuning.

Verantwoordelijkheden HP

Verantwoordelijkheden van de Service Expert in het standaardplan:

- Oplossen van installatie- en verbindingsproblemen.
- Assistentie bieden en service-gerelateerde vragen beantwoorden.
- Nieuwe URL's toevoegen aan de whitelist van bedrijfsspecifieke websites.

Verantwoordelijkheden van de Service Expert in het uitgebreide plan:

- Zorgen voor installatie en activatie van de geavanceerde isolatietechnologie
- Leveren van kwartaalverslagen van de analyse van veiligheidsdreiging.
- Onderzoeken van veiligheidswaarschuwingen en ondernemen van adequate actie.
- Monitoring en coördinatie van probleemoplossing en assistentie.
- Leveren van niveau 2- en niveau 3-ondersteuning en coördinatie met uw servicedesk.

Verantwoordelijkheden van de klant

- Bekijken van dashboards, verslagen en incidenten op het HP DaaS Proactive Management-dashboard.
- Bekijken van veiligheidsrapporten en zo nodig reageren.
- Aanvragen en leveren van URL-whitelistingpagina's.
- Probleemopsporing en -oplossing van gangbare eindgebruikersproblemen, voordat deze aan HP support worden doorgegeven.
- Uw HP DaaS-account tijdig vernieuwen, wijzigen of annuleren.
- Invullen van de CyQu online enquête.³

Systeemvereisten

- DaaS Proactive Security vereist multi-vendor klantapparaten met Windows 10 1703 of hoger, minimaal 8 GB werkgeheugen en 6 GB vrije ruimte op de harde schijf.
- DaaS Proactive Security vereist HP TechPulse, dat in alle HP DaaS of HP DaaS Proactive Management-plannen inbegrepen is. Voor het HP DaaS Proactive Security plan Uitgebreid moet de klant zijn aangemeld voor een Uitgebreid of Premium HP DaaS-plan.
- Voor communicatie tussen beheerde apparaten en HP cloudbeheer is een actieve internetverbinding vereist.
- Zie hpdaas.com/requirements voor meer informatie.

Leveringsspecificaties (vervolg)

Onboarding

Onboarding is het proces waarbij gedekte apparaten worden ingevoerd in DaaS Proactive Security. Als u over een Uitgebreid of Premium-plan beschikt, wordt een onboarding-manager toegewezen om het proces te beheren. Als u een Standaardplan hebt met zelfbeheer, zal een HP Service Expert een account voor u aanmaken en de benodigde accountinformatie leveren in een welkomstmail, samen met uitleg hoe u assistentie kunt krijgen wanneer u deze nodig heeft.

Voorwaarden voor onboarding

Voordat u uw apparaten overzet naar DaaS Proactive Security levert u de volgende informatie aan uw onboarding-manager, HP accountmanager en/of servicepartner:

- Belangrijke contactgegevens (naam, e-mail, telefoon, locatie)
- Bedrijfsadres
- Actieve DNS-domeinnaam
- Lijst van rapportbeheerders
- Lijst van te beheren apparaten door HP Proactive Management inclusief model en serienummer (alleen voor Uitgebreid en Premium DaaS-plannen)

Onboardingproces

- **1e fase: Registratie:** U ontvangt een licentiecode en een link naar een online registratieformulier.
- **2e fase: Verzamelen van informatie:** Er wordt een onboardingmanager toegewezen om uw onboarding te beheren. Deze plant een conferencecall in om aanbevelingen te doen over de vervolgstappen.
- **3e fase: Aanbevelingen en account aanmaken:** HP zal een account voor u aanmaken in het HP DaaS veiligheidsplatform en begint met standaard veiligheidsinstellingen en het whitelisten van aanvullende URL's waarom u verzoekt.
- **4e fase: Implementatie:** De onboardingmanager maakt een afspraak met u om het apparaat aan te melden en eventuele problemen op te lossen.
- **5e fase: Overgang naar continue ondersteuning en beheer (alleen uitgebreide plannen):** Zodra de onboarding is voltooid, zal de service worden overgedragen naar HP Service Experts, die continue ondersteuning en beheer leveren voor de duur van het contract.

Verantwoordelijkheden van de onboardingmanager

- Aanmaken van een HP DaaS Proactive Management account.
- Toevoegen of verwijderen van HP DaaS Proactive Management dashboardgebruikers.
- Toegang verlenen tot een gebruikersaccount.
- Verzamelen en bewaren van vereiste omgevingsinformatie.
- Zorgen voor documenten en begeleiding om de analyticsagent te installeren.
- Ontwikkelen en implementeren van het onboarding-plan.
- Leveren van voortgangsupdates.
- Verifiëren van succesvolle implementatie.
- Overdragen van klantenondersteuning van HP DaaS Proactive Management naar HP Service Experts.
- Diagnosticeren en oplossen van installatieproblemen.
- Bieden van continue ondersteuning.

Beperkingen van de service

- Beschikbaarheid van een HP Service Expert voor het DaaS Proactive Security-plan Uitgebreid:
 - **Noord-Amerika:** Engelse ondersteuning beschikbaar van maandag t/m vrijdag (uitgezonderd HP feestdagen) van 6.00 tot 18.00 uur MT.
 - **Latijns-Amerika:** Engelse en Spaanse ondersteuning beschikbaar van maandag t/m vrijdag (uitgezonderd HP feestdagen) van 7.00 tot 18.00 uur GMT -5.
 - **Europa, Midden-Oosten en Afrika:** Engelse, Franse en Duitse ondersteuning beschikbaar van maandag t/m vrijdag (uitgezonderd HP feestdagen) van 8.00 tot 18.00 uur CET.
 - **Azië-Pacific en Japan:** Engelse en Chinese ondersteuning 24 uur per dag beschikbaar; Ondersteuning in het Japans is er van 9.00 tot 21.00 uur Japan-Standaardtijd, 7 dagen per week (uitgezonderd HP feestdagen).
- Aon-diensten zijn momenteel alleen beschikbaar in de Verenigde Staten.
- HP DaaS Proactive Management en HP DaaS Proactive Security platforms worden gehost op Amazon Web Services (AWS).

Algemene voorwaarden

Zie de [Algemene voorwaarden](#) van HP DaaS.

Meer informatie

Neem contact op met uw lokale HP salesmedewerker of channel partner voor meer informatie of kijk op hp.com/go/DaaS.

Meld u aan voor updates op
hp.com/go/getupdated



Delen met collega's

1. Systeemvereisten voor HP DaaS Proactive Security zijn: apparaten van de klant van verschillende leveranciers die Windows 10 1703 of nieuwer gebruiken en minimaal 8 GB geheugen en 6 GB ruimte op de harde schijf vrij hebben om de software te installeren. HP DaaS Proactive Security vereist HP TechPulse, dat in alle HP DaaS of HP DaaS Proactive Management-plannen is inbegrepen. Voor het HP DaaS Proactive Security-plan Uitgebreid moet de klant zijn aangemeld voor een Uitgebreid of Premium HP DaaS- of HP DaaS Proactive Management-plan.
2. HP Sure Click Advanced is inbegrepen in HP DaaS Proactive Security en vereist Windows 10 en Microsoft Internet Explorer, Google Chrome en Chromium worden ondersteund. Ondersteunde bijlagen zijn onder meer Microsoft Office (Word, Excel, PowerPoint) en pdf-bestanden, maar enkel als Microsoft Office of Adobe Acrobat is geïnstalleerd.
3. Aon-diensten zijn alleen in de Verenigde Staten beschikbaar.
4. Service Experts zijn alleen beschikbaar in het Uitgebreid Proactive Security-plan.

© Copyright 2019 HP Development Company, L.P. De informatie in dit document kan zonder voorafgaande kennisgeving worden gewijzigd. De van toepassing zijnde garanties voor HP producten en diensten zijn vastgelegd in de uitdrukkelijke garantie bepalingen die bij dergelijke producten en diensten op fysieke en/of elektronische wijze worden meegeleverd of gepubliceerd op de website(s) van HP. Niets in dit document mag als een aanvullende garantie worden opgevat. HP is niet aansprakelijk voor technische en/of redactionele fouten c.q. weglatingen in dit document. Adobe en Acrobat zijn handelsmerken van Adobe Systems Incorporated. Google, Chrome en Chromium zijn handelsmerken van Google Inc. Microsoft en Windows zijn geregistreerde handelsmerken van Microsoft Corporation in de Verenigde Staten en/of andere landen.

4AA7-4656NLE, maart 2019

