



HP DaaS Proactive Security



Avantages du service

- Rendre les terminaux plus sûrs
- Vous protéger contre les pièces jointes et les sites Web malveillants
- Protéger vos données et vos appareils

Caractéristiques du service

- Une technologie d'isolation avancée vous protège contre les logiciels malveillants²
- L'analyse HP TechPulse fournit des informations et des rapports sur la sécurité
- L'évaluation Aon CyQu vous aide à évaluer votre niveau de sécurité³

Présentation du service

Améliorez les capacités de gestion sécurisée de HP Device as a Service (DaaS) avec HP DaaS Proactive Security¹. HP DaaS Proactive Security assure une protection en temps réel contre les logiciels malveillants susceptibles d'attaquer les appareils impliqués dans le traitement des données. Cette solution analyse la sécurité et les menaces et vous fait bénéficier d'une expertise spécialisée qui vous aide à renforcer votre sécurité globale. La technologie d'isolation des menaces protège contre les logiciels malveillants introduits par le biais du courrier électronique, des navigateurs et des fichiers Office ou PDF. Elle étend les connaissances et les rapports de sécurité fournis par l'analyse HP TechPulse. Vous pouvez ainsi vous protéger contre les menaces, les comprendre et réagir.

Caractéristiques et spécifications

Technologie d'isolation avancée

Les virus, les logiciels de rançon et autres logiciels malveillants représentent une menace majeure pour l'infrastructure informatique. Allez au-delà des solutions antivirus basées sur la définition grâce à la technologie d'isolation des menaces en temps réel, en utilisant des micro-machines virtuelles pour contenir les attaques de courrier électronique, de navigateurs et de fichiers de type jour-zéro et les empêcher de nuire à votre réseau². Les utilisateurs peuvent visualiser les pièces jointes et les sites Web sans compromettre la sécurité de votre réseau et sans interrompre leur flux de production ni modifier leurs comportements.

Analyse HP TechPulse

Avec HP TechPulse, bénéficiez d'un tableau de bord centralisé sur le portail HP DaaS qui vous permet de rester informé, et vous offre une vue d'ensemble de l'état de protection de vos appareils et des résultats détaillés sur les tentatives d'attaque et sur les attaques bloquées.

Experts HP

Renforcez votre sécurité et gardez une longueur d'avance sur les attaques. Évitez les impacts négatifs sur votre entreprise grâce à nos experts, qui supervisent les rapports, analysent les menaces et vous aident à planifier vos activités. Des experts HP effectueront des analyses trimestrielles des menaces pour la sécurité et répondront aux alertes de sécurité⁴.

Aon

Nous collaborons avec Aon pour offrir des solutions de cybersécurité supplémentaires, notamment des services d'évaluation, d'intervention en cas d'incident et d'assurance. L'outil d'auto-évaluation du Cyber Quotient Aon (CyQu) et le score de sécurité vous aident à évaluer votre niveau de sécurité par rapport à vos pairs de l'industrie, et Aon intervient gratuitement pendant une heure en cas de violation de sécurité³.

Forfait DaaS Proactive Security

Caractéristiques du service	Forfait standard (autogéré)	Forfait amélioré (géré par HP)
Protection contre les menaces liées aux pièces jointes de courriers électroniques, aux liens d'hameçonnage et aux téléchargements	✓	✓
Informations de sécurité de HP TechPulse	✓	✓
Évaluation Aon CyQu, intervention en cas d'incident et admissibilité à l'assurance ³	✓	✓
Application des politiques d'isolation : Les experts HP peuvent gérer le niveau de protection avancée de la technologie HP	—	✓
Analyse : les experts HP effectueront une analyse des menaces isolées et interrompus. Ils recommanderont les meilleures pratiques pour les utilisateurs et les dispositifs qui subissent un volume élevé de menaces, si nécessaire.	—	✓
Enquêtes et avis sur les événements liés à la sécurité : les experts HP vous avertiront lorsque les appareils ne sont plus protégés en raison d'une altération par les utilisateurs finaux ou de modifications de la configuration du système.	—	✓

Modalités du service

Options du service

- **Standard** : la version standard autogérée de DaaS Proactive Security est disponible pour les forfaits DaaS Standard, Avancé et Premium. Dans le cadre de l'option autogérée, vous êtes responsable de l'enregistrement de vos appareils et devez contacter HP si vous avez besoin d'assistance.
- **Avancé** : la version avancée de DaaS Proactive Security n'est disponible que si vous disposez également d'un forfait DaaS Avancé ou Premium. Avec le forfait Avancé, un responsable du programme d'intégration HP vous assiste dans l'installation et la configuration du service, et des experts HP dotés d'une grande expertise en matière de cybersécurité assurent une surveillance et un support permanents.

Responsabilités de HP

Responsabilités de l'expert dans le cadre du forfait Standard :

- Résolution des problèmes d'installation et de connectivité
- Assistance des clients et réponse aux questions relatives au service
- Ajout de nouvelles URL à la liste blanche des sites Web propres à votre entreprise

Responsabilités de l'expert dans le cadre du forfait Avancé :

- Vérification de l'installation et de l'activation de la technologie d'isolation avancée
- Fourniture de rapports trimestriels d'analyse des menaces pour la sécurité
- Enquête sur les alertes de sécurité et mise en place des mesures appropriées
- Surveillance de l'entretien et coordination du dépannage et de l'assistance
- Assistance de niveau 2 et de niveau 3 et prise en charge de la coordination avec votre service d'assistance

Responsabilités du client

- Consultation des tableaux de bord, des rapports et des incidents sur le tableau de bord de HP DaaS Proactive Management
- Examen des rapports de sécurité et intervention si nécessaire
- Recherche et fourniture des pages Web de liste blanche d'URL.
- Dépannage et tri des erreurs fréquemment rencontrées par les utilisateurs avant de faire appel au support HP
- Renouvellement, modification ou annulation d'un compte HP DaaS
- Réalisation de l'analyse CyQu en ligne³

Configuration système requise

- DaaS Proactive Security nécessite des appareils client multiconstructeurs fonctionnant sous Windows 10 1703 ou une version ultérieure, avec au moins 8 Go de mémoire et 6 Go d'espace disque disponible.
- Le service HP DaaS Proactive Security exige HP TechPulse, qui est inclus dans tous les forfaits HP DaaS et HP DaaS Proactive Management. Le forfait HP DaaS Proactive Security Avancé exige la souscription d'un forfait HP DaaS Avancé ou Premium.
- Les communications entre les appareils gérés et le service de gestion cloud HP nécessitent une connexion Internet active.
- Pour plus de détails, consultez hpdaas.com/requirements.

Modalités du service (suite)

Intégration

L'intégration est le processus qui consiste à intégrer les appareils couverts à la solution DaaS Proactive Security. Un gestionnaire de programme d'intégration sera désigné pour gérer le processus d'intégration si vous disposez d'un forfait HP DaaS Avancé ou Premium. Si vous disposez d'un forfait standard autogéré, un expert HP créera un compte pour vous et vous fournira, dans un e-mail de bienvenue, les informations nécessaires ainsi que les instructions pour obtenir de l'aide si vous en avez besoin.

Conditions préalables à l'intégration

Avant de transférer vos appareils vers DaaS Proactive Security, vous devez fournir les informations suivantes à votre responsable de programme d'intégration, votre responsable de compte HP et/ou votre partenaire de service :

- Coordonnées principales (nom, adresse e-mail, téléphone, emplacement)
- Adresse de votre entreprise
- Votre nom de domaine DNS Active Directory
- Une liste des administrateurs de rapports
- Une liste des appareils à gérer par HP Proactive Management, y compris les numéros de modèle et de série (pour les forfaits HP DaaS Avancé ou Premium uniquement)

Processus d'intégration

- **Phase 1 – Inscription** : vous recevrez une clé de licence et un lien vers un formulaire d'inscription en ligne.
- **Phase 2 – Partage d'informations** : un gestionnaire de programme d'intégration sera affecté à la gestion de votre processus d'intégration. Il organisera une conférence téléphonique pour indiquer la façon de procéder.
- **Phase 3 – Recommandations et création des comptes** : HP créera votre compte dans la plateforme de sécurité HP DaaS, en commençant par les configurations de sécurité par défaut et en mettant sur liste blanche toutes les URL supplémentaires dont vous avez besoin.
- **Phase 4 – Déploiement** : le responsable du programme d'intégration vous rencontrera pour commencer l'enregistrement des appareils et résoudre tout problème.
- **Phase 5 – Transition vers un soutien et une gestion continus (forfait Avancé seulement)** : une fois l'intégration terminée, le service sera assuré par des experts HP, qui assureront une assistance et une gestion continues pendant toute la durée du contrat.

Responsabilités du gestionnaire de programme d'intégration

- Créer le compte HP DaaS Proactive Management
- Ajouter ou supprimer des utilisateurs du tableau de bord HP DaaS Proactive Management
- Accorder l'accès au compte de l'utilisateur
- Recueillir et consolider les informations requises sur l'environnement
- Fournir de la documentation et des conseils pour déployer l'agent d'analyse
- Élaborer et mettre en œuvre le projet d'intégration du forfait
- Fournir des mises à jour sur les progrès réalisés
- Vérifier la réussite de la mise en œuvre
- Transmettre à des experts HP le support client de la fonctionnalité HP DaaS Proactive Management
- Diagnostiquer et résoudre les problèmes d'installation
- Offrir un soutien continu

Limites du service

- Disponibilité des experts HP pour le forfait DaaS Proactive Security Avancé :
 - **Amérique du Nord** : support technique en anglais disponible du lundi au vendredi (sauf jours fériés HP) de 6 h à 18 h, heure des Rocheuses.
 - **Amérique latine** : support technique en anglais et en espagnol disponible du lundi au vendredi (sauf jours fériés HP) de 7 h à 18 h, heure GMT -5.
 - **Europe/Moyen-Orient, Afrique** : support technique en anglais, français et allemand disponible du lundi au vendredi (sauf jours fériés HP) de 8 h à 18 h, heure d'Europe Centrale/CET.
 - **Asie, Pacifique, Japon** : support technique en anglais et en chinois disponible 24 heures sur 24. le support en japonais est disponible de 9 h à 21 h, heure normale du Japon, 7 jours sur 7 (sauf les jours fériés HP).
- Les services Aon ne sont actuellement disponibles qu'aux États-Unis.
- Les plateformes HP DaaS Proactive Management et HP DaaS Proactive Security sont hébergées sur Amazon Web Services (AWS).

Conditions générales

Consultez les [conditions générales](#) de HP Daas.

En savoir plus

Prenez contact avec votre représentant commercial ou votre partenaire revendeur local pour plus d'informations ou rendez-vous sur hp.com/go/DaaS.

Abonnez-vous à notre liste de diffusion
hp.com/go/getupdated



Partagez ce document

1. Configuration requise pour le forfait HP DaaS Proactive Security : appareils clients multiconstructeurs sous Windows 10 1703 ou version ultérieure avec un minimum de 8 Go de mémoire et 6 Go d'espace disque disponible pour installer le client logiciel. Le service HP DaaS Proactive Security exige HP TechPulse, qui est inclus dans tous les forfaits HP DaaS et HP DaaS Proactive Management. Le forfait HP DaaS Proactive Security Avancé exige la souscription d'un forfait HP DaaS ou HP DaaS Proactive Management Avancé ou Premium.
2. La technologie HP Sure Click Advanced est incluse dans HP DaaS Proactive Security et exige Windows 10. Prise en charge Microsoft Internet Explorer, Google Chrome et Chromium. Les pièces jointes prises en charge incluent les fichiers Microsoft Office (Word, Excel, PowerPoint) et PDF lorsque Microsoft Office et/ou Adobe Acrobat sont installés.
3. Les services Aon sont disponibles uniquement aux États-Unis.
4. Les experts sont disponibles uniquement avec le forfait Proactive Security Avancé.

© Copyright 2019 HP Development Company, L.P. Les informations contenues dans le présent document peuvent être modifiées à tout moment et sans préavis. Les seules garanties relatives aux produits et services HP sont énoncées dans les déclarations de garantie expresses fournies avec ces produits et services. Aucune information du présent document ne saurait être considérée comme constituant une garantie complémentaire. HP décline toute responsabilité quant aux éventuelles erreurs ou omissions techniques ou rédactionnelles qui pourraient être constatées dans le présent document. Adobe et Acrobat sont des marques commerciales d'Adobe Systems Incorporated. Google, Chrome et Chromium sont des marques déposées de Google Inc. Microsoft et Windows sont des marques déposées de Microsoft Corporation aux États-Unis et/ou dans d'autres pays.

4AA7-4656FRE, mars 2019

