HP WOLF SECURITY

HP WOLF ENTERPRISE SECURITY

POWERED BY Bromium®

RÉDUIRE LA COMPLEXITÉ INFORMATIQUE DES ENTREPRISES GRÂCE À UNE INTELLIGENCE EXPLOITABLE ET À L'ISOLEMENT DES APPLICATIONS

TABLE DES MATIÈRES

SYNTHÈSE

Les entreprises d'aujourd'hui mènent une bataille de plus en plus ardue contre les cyberattaques perfectionnées et ciblées qui passent inaperçues. Malgré l'augmentation des dépenses et la complexité accrue des solutions de sécurité en couches, les entreprises doivent redéfinir leur stratégie de sécurité des terminaux, réduire la complexité, réévaluer les exigences commerciales et supprimer les flux de travail des utilisateurs sur les réseaux non fiables ou malveillants.

En outre, les entreprises doivent garantir l'intégrité de leur infrastructure et fournir des renseignements sur les menaces en temps réel comme mesures défensives sur une plateforme unifiée. Les entreprises sont victimes de violations et les systèmes des utilisateurs sont entravés par la surconsommation de ressources due à la multiplicité des solutions de sécurité. Enfin, le manque de protection et de visibilité des menaces en temps réel entrave les exigences des entreprises. L'utilisation du confinement dans le cadre d'une architecture d'entreprise bien instrumentée et agile améliore la sécurité des terminaux et assure l'intégrité, la confidentialité et la résilience.

L'approche de HP en matière de confinement des menaces offre un meilleur moyen de vaincre les cyberattaques visant les terminaux, où plus de 80 % des intrusions se produisent. HP propose une solution d'isolement et de confinement des applications qui intègre l'isolement des menaces sur les terminaux, l'analyse des menaces et le partage des renseignements sur les menaces via syslog et STIX/TAXII, tout en prenant en charge le cadre ATT&CK de MITRE et en réduisant la complexité.

La technologie HP de confinement des menaces permet à l'entreprise d'isoler, de protéger et de répondre aux attaques ciblées, aux menaces de type zero-day et aux tentatives d'intrusion en temps réel. L'entreprise dispose ainsi d'une meilleure connaissance de la situation de cybersécurité.

Les principales caractéristiques de la solution de confinement de HP sont les suivantes :

- Isolement et confinement des applications renforcés par une sécurité intégrée au matériel
- Protection non fondée sur la signature, ne repose pas sur la détection
- Isolement au niveau des tâches avec des machines virtuelles non persistantes
- Alertes haute-fidélité et analyse complète de la chaîne d'élimination, sans analyse commerciale basée sur le cloud
- Tactique : protection réseau désactivée/limitée
- Intégration à l'infrastructure existante de visibilité et de gestion des actifs de l'entreprise
- Protection des applications Windows anciennes et récentes
- Fonctionne sur toutes les plateformes matérielles des fournisseurs d'ordinateurs
- Déploiements éprouvés en production dans des environnements civils et de défense américains

HP possède une vaste expérience dans le domaine du confinement auprès de clients civils et militaires du monde entier :

- Défense du gouvernement américain
- Secteur public du gouvernement américain
- Forces de l'ordre américaines
- Gouvernement du Royaume-Uni
- Forces de l'ordre du Royaume-Uni
- Gouvernement canadien
- Gouvernement allemand
- Forces de l'ordre allemandes

Ce document explique en détail comment la solution de confinement des applications HP Sure Click Enterprise[1], est une solution inégalée pour répondre aux exigences d'isolation des applications du gouvernement américain. Ce document couvre :

- L'acquisition des technologies Bromium par HP
- La réduction de la complexité en augmentant la visibilité et la gestion
- La protection des appareils tactiques
- La collecte de données enrichies en temps réel sur les menaces avec HP Sure Click Enterprise
- Le partage des renseignements sur les menaces pour soutenir les cybercapacités du gouvernement américain et des organisations conjointes
- L'isolement d'internet avec HP Sure Click Enterprise

ACQUISITION DE BROMIUM INC. PAR HP INC.

Bromium a été fondée en 2010 avec pour mission de restaurer la *confiance dans l'informatique*. Les fondateurs de la société, les docteurs Ian Pratt et Simon Crosby, avaient une longue expérience approfondie en innovation dans la virtualisation et la sécurité. Inspirée par les principes d'isolement de la virtualisation classique, l'équipe de Bromium a créé une technologie qui change la donne, appelée microvirtualisation, pour assurer une sécurité renforcée des terminaux des entreprises en protégeant les utilisateurs finaux contre les logiciels malveillants évolués grâce à une technologie d'isolement et de confinement des applications. L'équipe détient 48 brevets délivrés, et 10 brevets sont en attente pour sa technologie. L'expression « *isolement et confinement des applications* », inventée par l'Agence nationale de sécurité dans son document intitulé Symposium 2016 sur l'assurance de l'information, a été par la suite connue simplement sous le nom de *confinement*.

Bromium, Inc. et HP Inc. sont entrés dans une relation constructeur officielle en 2016. HP a reconnu la nécessité de différencier ses offres de plateformes de sécurité en s'appuyant sur des solutions de sécurité matérielles. À partir de 2017, HP a commencé avec succès à expédier une version constructeur (OEM) du confinement Bromium sous la marque HP Sure Click sur des millions d'appareils professionnels.

Suite au succès de Sure Click, HP a fait l'acquisition de Bromium le 19 septembre 2019. Par la suite, HP a créé une nouvelle unité commerciale mondiale, HP Security, avec l'équipe existante de Bromium à sa tête. À la suite de l'acquisition, HP a mis à jour la convention de dénomination de l'ancien produit Bromium Secure Platform pour mieux l'aligner sur sa marque HP Sure Click. HP s'engage à prendre en charge la solution HP Sure Click sur tout ordinateur, quel que soit le fabricant, fonctionnant sous Windows 10. Aujourd'hui, l'ancienne plateforme sécurisée Bromium est connue sous le nom de HP Sure Click Enterprise.

HP est depuis 20 ans un leader incontesté en matière de sécurité dans le secteur des ordinateurs. En 1999, HP a cofondé le groupe de normalisation Trusted Computing et, en 2003, a été le premier à installer des modules de plateforme sécurisée (TPM) dans ses ordinateurs. En 2005, HP a été le premier à introduire la signature cryptographique des mises à jour du micrologiciel du BIOS, faisant ainsi progresser le secteur en collaborant avec le National Institute of Standards and Technology (NIST) pour créer des normes de sécurité pour les BIOS.

En 2013, HP a introduit un contrôleur axé sur la sécurité , et intégré dans la plateforme des ordinateurs, fournissant un environnement informatique sécurisé distinct du processeur principal, qui peut être utilisé pour mettre en œuvre les fonctions de sécurité critiques de la plateforme. Le contrôleur intégré est utilisé pour mettre en œuvre la fonction HP Sure Start, qui permet au BIOS et à d'autres microprogrammes d'être vérifiés de manière cryptographique à chaque démarrage, ce qui permet à la plateforme de réparer elle-même le microprogramme s'il a été altéré.

La fonctionnalité HP Sure Run utilise le contrôleur embarqué pour créer des signaux de détection de collision cryptographique entre le contrôleur et le système d'exploitation hôte, ce qui permet de surveiller les processus critiques de sécurité du système d'exploitation hôte et de prendre des mesures correctives en cas de défaillance. HP Sure Recover[2] a été ajouté à la plateforme pour permettre aux systèmes de réinstaller le système d'exploitation hôte en toute sécurité s'il est corrompu. L'image du système d'exploitation peut être téléchargée à partir d'une image signée de manière cryptographique et stockée sur le réseau de l'entreprise ou sur le cloud, ou à partir d'une puce mémoire flash spéciale qui est protégée par le contrôleur embarqué. Ainsi, les systèmes HP sont les seuls à pouvoir réinstaller le système d'exploitation hôte en quelques minutes pour faciliter la récupération après la suppression d'informations essentielles sur le disque, telles que l'enregistrement d'amorçage maître de la table de partition, par un logiciel malveillant.

En 2019, HP a lancé HP Sure Admin[3], une solution de pointe pour la gestion sécurisée des données de configuration du BIOS à l'aide d'une cryptographie à clé publique, permettant une solution beaucoup plus évolutive et sécurisée pour les entreprises que le classique mot de passe du BIOS. Cette solution permet aussi bien l'administration à distance via le réseau que l'accès local sécurisé des utilisateurs aux menus de configuration du BIOS.

En plus des capacités de sécurité sous le système d'exploitation, HP a créé une pile de sécurité des terminaux qui offre une protection de pointe du système d'exploitation hôte. HP Sure Click Enterprise utilise les capacités de virtualisation matérielle des processeurs modernes pour isoler les activités à haut risque telles que la navigation sur le Web et l'ouverture de documents provenant de sources Internet.

En 2021, HP a consolidé l'ensemble de son portefeuille de sécurité des terminaux.

RÉDUCTION DE LA COMPLEXITÉ ET ACCROISSEMENT DE LA VISIBILITÉ DES MENACES

HP Sure Click Enterprise est conçu pour fournir un isolement et un confinement des applications renforcés par le matériel, grâce à l'exploitation des fonctions existantes du processeur, notamment Intel VT-x/EPT et/ou AMD V/RVI. En tant que solution basée sur un hyperviseur, HP Sure Click Enterprise est une solution spécialement conçue pour assurer l'isolement et le confinement des applications, en prenant en charge les clients lourds et l'infrastructure de bureau virtuel (VDI). En outre, Bromium (HP) travaille depuis des années avec les principaux fournisseurs de solutions de cybersécurité, tels que McAfee, Microsoft et Forescout, afin de garantir la compatibilité et l'intégration transparente.

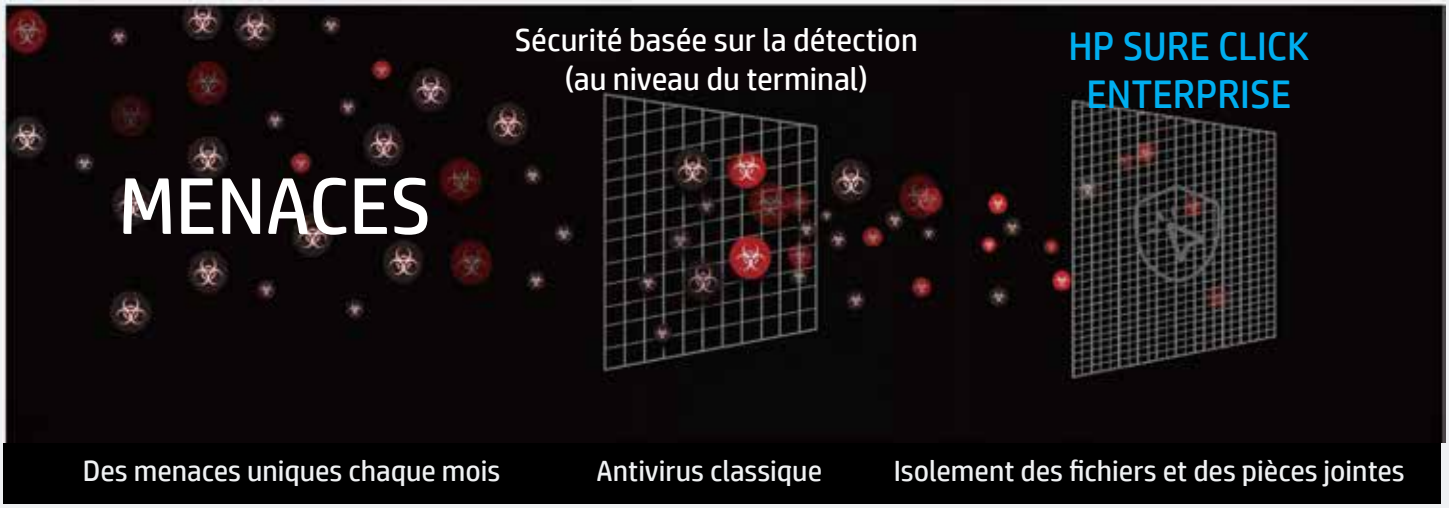
HP Sure Click Enterprise est la seule solution de confinement à offrir tous les éléments suivants :

- Conteneurs de micromachines virtuelles (microVM) non persistants par tâche
- Prise en charge des systèmes d'exploitation et des applications modernes et anciens
- Isolement et protection sans exigence de connexion au cloud
- Capture complète de la chaîne d'élimination et partage des informations sur les menaces pour permettre l'exécution complète d'une attaque
- Serveur de gestion centralisé sur site ou dans le cloud .GOV avec intégration AD
- Un aperçu immédiat des nouveaux vecteurs de menace fourni au gouvernement américain, potentiellement même avant la communauté des vendeurs et de la sécurité, ce qui donne au gouvernement un avantage concurrentiel sur ses adversaires

ISOLEMENT ET CONFINEMENT DES APPLICATIONS :

L'isolement et le confinement des applications HP encapsulent chaque fichier non fiable (entrant) et chaque onglet de navigateur Web dans un conteneur de micromachine virtuelle (microVM) jetable à usage unique, sans s'appuyer sur une détection imparfaite pour déterminer l'intention malveillante.

- Isolement renforcé par le matériel sur l'hôte, en exploitant les capacités de virtualisation intégrées au processeur
- Fonctionne sous le noyau, ce qui réduit la surface d'attaque à un hyperviseur renforcé
- L'isolement et le confinement des applications s'appliquent également aux menaces liées au Web et aux fichiers
- Les menaces malveillantes ne peuvent pas atteindre le système d'exploitation hôte, le noyau, le registre, les informations d'identification ou le réseau interne
- Les faux positifs ne nécessitent aucune réponse active et sont rares ; les menaces potentielles ont déjà été isolées et contenues.
- Aucun impact des faux négatifs (détections manquées), car les vraies menaces sont toujours isolées et contenues.
- Élimine l'utilisateur en tant que décideur final en matière de cybersécurité ; permet à l'utilisateur d'effectuer son travail sans compromis.



HP SURE CLICK ENTERPRISE OFFRE UNE PROTECTION CONTRE LES VECTEURS D'ATTAQUE SUIVANTS :

- Pièces jointes de courriers électroniques malveillants (Outlook, clients de messagerie tiers, messagerie électronique)
- Liens d'hameçonnage malveillants (Outlook, clients de messagerie tiers, messagerie électronique, Skype, clients de discussion en ligne tiers)
- Téléchargements de fichiers malveillants (http/https/FTP, etc.) : tous les navigateurs sont pris en charge
- Fichiers malveillants provenant de périphériques USB, y compris les fichiers enregistrés sur l'hôte ou le réseau
- Exploitations de navigateur et logiciels malveillants sans fichier provenant du navigateur (IE, Chrome, FF, Edge)
- Vol d'informations d'identification par une activité malveillante dans le navigateur
- Protection de l'hôte contre les réseaux inconnus et non sécurisés (Wi-Fi gratuit) et les portails captifs malveillants

PROTECTION DES APPAREILS TACTIQUES

Le gouvernement américain prend en charge de nombreux types d'utilisateurs à travers son infrastructure mondiale. Les exigences comprennent les utilisateurs professionnels standard avec des appareils connectés aux réseaux gouvernementaux à partir d'une installation et infrastructure de cyberrésilience dédiée. Cependant, il comprend également de nombreux dispositifs connectés à des réseaux tactiques ou de partenaires, ou à des réseaux prenant en charge des utilisateurs tactiques connectés à des réseaux à faible bande passante et à forte latence ou potentiellement hostiles.

La protection des appareils connectés à des réseaux distants est un défi majeur en raison des latences du réseau et d'autres limitations. Souvent, ces appareils ne sont pas en mesure de se connecter facilement à des services de sécurité gérés et contrôlés de manière centralisée, à des proxys de réseau ou à des solutions de protection des navigateurs basées sur le cloud.

HP Sure Click Enterprise parvient à protéger les appareils tactiques ou à connectivité limitée sur des réseaux non gérés. Comme les microVM HP Sure Click Enterprise ne nécessitent aucune connexion réseau pour assurer leur protection, les appareils utilisant le confinement HP peuvent être déconnectés de la gestion centrale et fonctionner pendant des semaines ou des mois dans un environnement hostile sans avoir à se reconnecter pour être protégés.

Les utilisateurs des appareils tactiques restent entièrement protégés grâce à la technologie de confinement HP lorsqu'ils sont connectés à n'importe quel réseau, y compris les réseaux malveillants. Les activités suivantes sont totalement isolées lorsqu'elles sont exécutées dans n'importe quelle condition de réseau sur l'appareil :

- Toutes les sessions de navigation Web sont isolées dans la microVM.
- Tous les fichiers téléchargés sur l'appareil ou consultés par courrier électronique sont isolés dans la microVM.
- Tous les fichiers ouverts à partir d'un support USB ou amovible sont isolés dans la microVM.

Un avantage supplémentaire de HP Sure Click Enterprise est que les appareils restent protégés même lorsqu'ils ne peuvent pas être immédiatement corrigés ou mis à jour. Par exemple, si une nouvelle vulnérabilité du noyau du système d'exploitation Windows est découverte et que l'appareil n'est pas corrigé ou que son antivirus n'est pas mis à jour pour détecter la vulnérabilité, les conteneurs HP continueront à protéger entièrement l'appareil. Les exploitations du noyau ou autres qui s'exécutent dans la microVM ne pourront pas infecter l'hôte, même si celui-ci n'est pas corrigé et reste vulnérable. HP Sure Click Enterprise est notre solution d'isolement et de confinement des applications de terminaux la plus avancée au monde pour protéger les appareils et les utilisateurs sur les appareils et les réseaux tactiques, indépendamment de leur connectivité ou de l'état des correctifs[7].

PROTECTION CONTRE LES ATTAQUES CONNUES ET INCONNUES SANS SIGNATURE

HP Sure Click Enterprise est une solution offrant une protection intégrée au matériel qui repose sur l'isolation des menaces : elle bloque les attaques de type zero-day, sans fichier et en mémoire, ainsi que les menaces connues et inconnues sans signature. Avec plus de 8 milliards de pièces jointes de courrier électronique, de pages Web et de téléchargements ouverts sans qu'aucune violation ne soit signalée[4], aucune autre cyber-solution n'a prouvé qu'elle pouvait isoler les attaques aussi efficacement que cette solution de confinement professionnelle proposée par HP .

VECTEURS DE MENACE

RÉSULTATS MALVEILLANTS

- Logiciel de rançon
- Harponnage
- Chevaux de Troie basés sur des macros
- Liens malveillants
- Exploitation des navigateurs
- Logiciels malveillants sans fichier
- Téléchargements cryptés échappant à la détection
- Fichiers de productivité bureautique
- Fichiers multimédias
- Fichiers exécutables
- Liens des documents
- Fausses mises à jour de Flash/Java
- Téléchargements furtifs
- Attaques de type « point d'eau »
- Placement de publicité malveillante
- Liens dans les programmes de discussion
- DNS malveillant/redirections d'URL
- Téléchargements intentionnels
- Pilotes et utilitaires corrompus
- Hameçonnage d'informations d'identification
- Extraction d'informations d'identification locales et de domaine
- Points d'accès Wi-Fi malveillants

AVANTAGES SUPPLÉMENTAIRES : RÉDUCTION DE LA COMPLEXITÉ — ANALYSE DES MENACES SUR LES TERMINAUX

Le gouvernement américain gère et exploite des centaines de produits de cybersécurité pour répondre à ses besoins cybernétiques sur la plus grande infrastructure informatique et de soutien aux missions de ce type. Chaque solution est destinée à fournir une visibilité et des alertes à travers chaque agence, signalant les attaques à leurs équipes cybernétiques respectives, agissant comme un tissu de capteurs de menaces. Pour pouvoir traiter le volume considérable d'alertes, il faut disposer d'outils instrumentés d'agrégation et de corrélation des menaces, chacun d'entre eux devant ensuite réagir pour corriger une attaque identifiée, à grande échelle.

Imaginez l'impact du traitement d'un tel volume d'alertes, pouvant laisser passer de vrais positifs en raison de l'effort consacré au traitement de cet immense volume de faux positifs ou, pire encore, de l'inefficacité des efforts déployés pour résoudre des vulnérabilités qui n'ont pas encore été identifiées ou pour lesquelles aucun correctif n'est disponible.

Ces réalités ont créé un environnement caractérisé par des volumes ingérables de données qui sont stockées pour être analysées après une attaque, ainsi que par des efforts exhaustifs de chasse aux menaces et de correction, et des frais généraux élevés pour les équipes qui réagissent aux incidents avec des outils de détection redondants, dans l'espoir que l'un d'entre eux arrête ou signale ce que l'autre a manqué. L'entreprise se retrouve souvent à travailler sans relâche pour déterminer l'ampleur d'une attaque, après coup, le réseau de capteurs devenant un mécanisme d'alerte complexe plutôt qu'un tissu de capteurs de menaces agiles, capables de se rétablir et de se défendre. La destruction, l'exfiltration et la manipulation des données sont d'abord identifiées, puis les alertes prennent tout leur sens. Mais il existe un moyen moins complexe.

HP Sure Click Enterprise simplifie les renseignements sur les menaces provenant des terminaux en isolant d'abord une attaque potentielle, en exécutant l'intégralité de l'attaque de manière isolée, en détruisant le logiciel malveillant, puis en communiquant la télémétrie complète de la menace en temps réel directement au gouvernement américain. La solution HP Sure Click Enterprise forme un réseau de capteurs d'attaques en direct sur l'ensemble des terminaux de l'entreprise, avec des informations en temps réel sur les attaques malveillantes. Cela permet de réduire les rapports faussement positifs, de localiser l'attaque exacte et de permettre aux cyberanalystes et aux outils de se concentrer sur les vraies attaques.

Grâce à la technologie de confinement HP, le gouvernement américain dispose d'une preuve criminalistique de ce qui aurait été une violation réussie et des binaires pour une analyse plus approfondie afin de déterminer la source et l'intention, ainsi que la possibilité d'automatiser l'analyse et la mise en quarantaine de cette chaîne d'élimination exacte pour ce département ou pour l'ensemble du gouvernement américain. Il s'agit d'une réduction globale de la complexité, du terminal jusqu'au cyberanalyste.

Plutôt que d'obliger les professionnels de la cybersécurité à parcourir des volumes d'alertes, une seule alerte HP Sure Click Enterprise peut permettre au gouvernement américain d'être informé d'une attaque, sans violation, sans que l'adversaire sache qu'il se trouve dans un environnement gouvernemental américain, avec un enregistrement en direct de toute la chaîne d'élimination. Le gouvernement américain a accès aux renseignements sur les menaces avant les fournisseurs de systèmes d'exploitation et d'applications et les référentiels de menaces, et avant qu'il n'y ait un correctif. Le gouvernement peut continuer à répondre à ses besoins et se défendre contre les attaques les plus évoluées. HP Sure Click Enterprise est efficace pour réduire la complexité au niveau du terminal, de la cybernétique, ainsi que pour les équipes de gestion des postes de travail et des applications.

VISIBILITÉ ET GESTION

La clé d'une architecture cybernétique moderne et d'un tissu de résilience est la capacité de réduire la complexité, d'augmenter la protection et de créer un tissu intégré de cyberconscience et de capacité de survie. Alors que le gouvernement cherche à moderniser sa stratégie de cybersécurité, HP Sure Click Enterprise peut s'intégrer de manière transparente dans l'infrastructure de visibilité et de gestion des actifs. Une fois qu'une attaque a été isolée, l'alerte de menace est envoyée au contrôleur HP géré sur place par l'agence ou le service. Là, par politique, les artefacts des menaces, les hachages et autres particularités peuvent être envoyés automatiquement ou manuellement aux systèmes existants. La télémétrie des menaces peut être envoyée à un SIEM, à un outil de visibilité et de gestion des actifs (par exemple, Tanium), à une structure gouvernementale d'analyse et de diffusion des menaces (par exemple, Phantom, McAfee), etc. via SYSLOG ou STIX. Après avoir reçu les données sur les menaces, le gouvernement américain peut les utiliser efficacement pour agir.

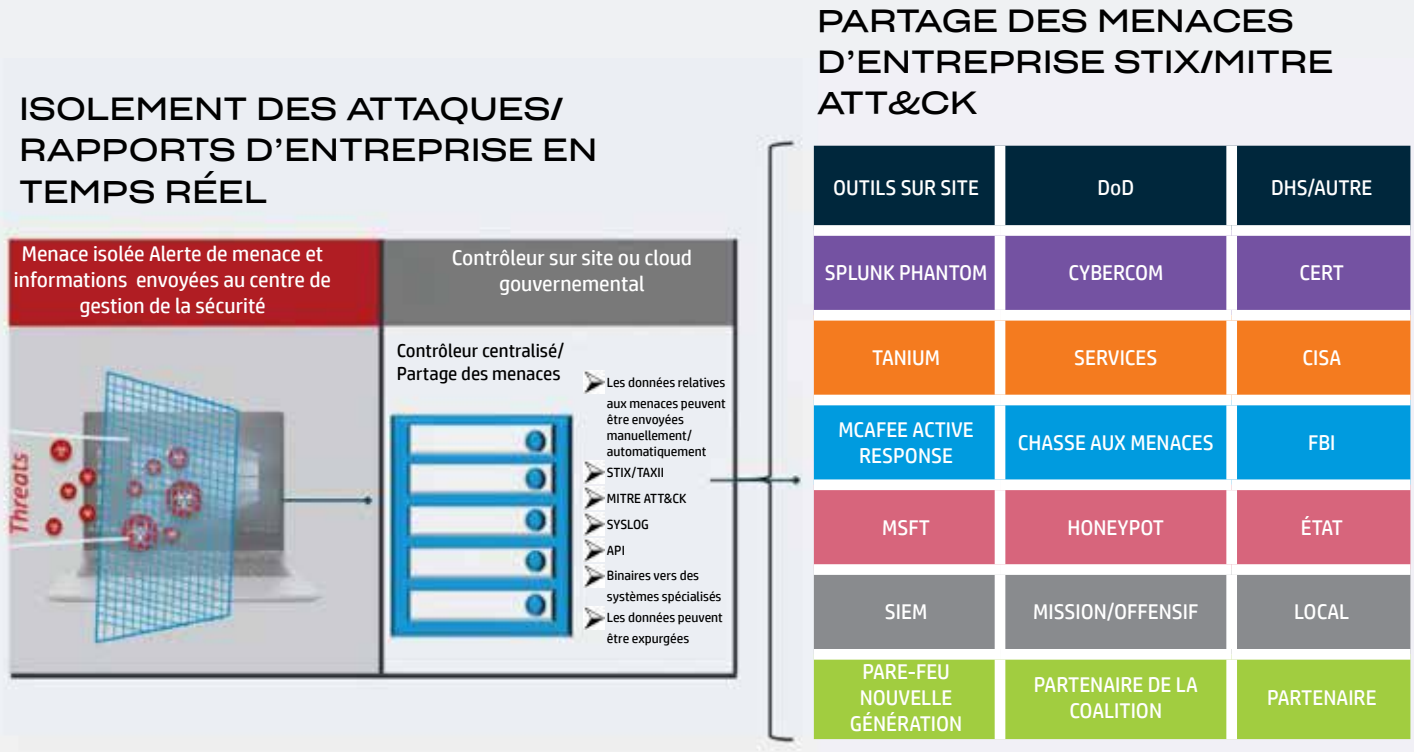
ANALYSE DES MENACES

Lorsqu'une attaque est isolée, HP Sure Click Enterprise fournit une trace criminalistique détaillée de l'exécution malveillante en temps réel, ce qui lui permet de fournir la charge utile complète du logiciel malveillant ainsi qu'une analyse criminalistique complète de la chaîne d'élimination. Il n'est pas nécessaire d'examiner plusieurs capteurs d'entreprise pour réagréger les logiciels malveillants après un fait, une violation ou une exfiltration de données. L'entreprise est protégée en temps réel tout en fournissant des renseignements exploitables sur les menaces afin d'étudier l'intention du pirate et de répondre aux exigences de cyberprotection des commandements et services interarmées.

RECHERCHE D'ENTREPRISE ET MISE EN QUARANTAINE – PARTAGE DES CONNAISSANCES SUR LES MENACES

Le système HP Sure Click Enterprise fournit immédiatement des informations sur les menaces d'attaque directement au serveur contrôleur centralisé HP attribué et autorisé par le gouvernement américain. Chaque chaîne d'élimination des attaques et les données de télémétrie peuvent être attribuées, par le biais d'une politique, automatiquement ou manuellement à un SIEM désigné, à un outil de gestion et de visibilité des actifs (par exemple, Tanium), au cloud des menaces du gouvernement américain ou à tout autre composant de l'infrastructure de sécurité nécessitant des données sur les menaces en temps réel. Ces outils existants, intégrés dans le tissu cybernétique, peuvent ensuite analyser et mettre en quarantaine d'autres infections identifiées, mettre à jour l'infrastructure du réseau et ses tables, ou déplacer les binaires et l'analyse vers d'autres systèmes du gouvernement américain nécessitant une cyberanalyse ou des mesures plus approfondies.

Avec HP Sure Click Enterprise, le confinement offre une visibilité en temps réel des attaques et une intégration complète dans les systèmes de gestion des menaces existants, les SIEM, les plateformes de partage des menaces, les outils de conformité et de visibilité du réseau/périmètre, les plateformes de gestion et d'orchestration des systèmes, les analyses de cybersécurité du réseau et d'autres solutions avec des API simples telles que STIX/TAXII. Le moteur de menaces HP conçu par Bromium met également en correspondance les tactiques et techniques d'attaque évitées avec le cadre ATT&CK de MITRE.



AMÉLIORATION DE L'ISOLEMENT D'INTERNET, BASÉE SUR LE CLOUD

L'isolement d'Internet basé sur le cloud (CBII) est une technologie qui permet d'acheminer le trafic Internet du navigateur de l'utilisateur final vers un serveur proxy basé sur le cloud. Ce serveur proxy affiche la page Web dans un conteneur infonuagique qui est isolé de l'appareil et du réseau de l'utilisateur. La sortie graphique (les pixels) du conteneur distant est la seule chose transmise en retour au navigateur de l'utilisateur. Cette architecture protège le dispositif contre les exploitations basées sur le navigateur.

Cinq caractéristiques assurent la compatibilité de HP Sure Click Enterprise avec les solutions CBII et leur amélioration :

- **Les navigateurs HP Sure Click Enterprise peuvent se connecter aux solutions CBII.** Comme couche supplémentaire de protection, HP Sure Click Enterprise peut se connecter aux solutions CBII et rendre les pages Web dans une microVM, fournissant une couche supplémentaire d'isolement et de protection.

- **HP Sure Click Enterprise peut isoler bien plus que des connexions Internet.** Une des limites des solutions CBII est qu'elles ne peuvent pas isoler le trafic non Internet (par exemple, le trafic des partenaires, le trafic des autres agences gouvernementales, ou le trafic des parties internes de l'Intranet). HP Sure Click Enterprise peut exécuter n'importe quel site Web dans une microVM et ainsi protéger des sites que le CBII ne peut pas protéger.

- **HP Sure Click Enterprise peut isoler les fichiers introduits sur l'hôte à partir de supports USB et amovibles.** Les fichiers malveillants PDF, Word, Excel, PowerPoint, EXE, images, scripts et bien d'autres peuvent être introduits sur l'hôte à partir de sources autres que les navigateurs connectés à Internet. HP Sure Click Enterprise offre la possibilité de protéger l'appareil contre ces sources potentiellement malveillantes.

- **Les solutions CBII doivent souvent établir une liste blanche ou faire confiance à certains sites Web de collaboration et de partage de fichiers bien connus.** Il peut s'agir de sites avec des outils de réunion tels que WebEx, Skype, Zoom, Adobe Connect, etc. Pour que ces sites et outils fonctionnent à des fins de collaboration et de partage, ils doivent souvent contourner le CBII. HP Sure Click Enterprise peut être configuré pour protéger ces types de sites et d'outils en isolant et en contenant tous les fichiers téléchargés ou créés par ces outils ou sites Web.

- **Les solutions CBII offrent plusieurs options pour le téléchargement de fichiers, telles que l'aplatissement du contenu du fichier ou la visualisation à distance du contenu du fichier.** Cependant, il arrive que le format de fichier brut doive être téléchargé du navigateur CBII vers le bureau. HP Sure Click Enterprise peut protéger tous les téléchargements de fichiers qui proviennent de CBII. Cela constitue une couche supplémentaire de protection. Si un fichier ou un document malveillant contourne les algorithmes de détection CBII et est autorisé à atteindre l'hôte, HP Sure Click Enterprise peut toujours isoler et contenir ce fichier.

SUPPRESSION DE L'ACCÈS DE L'HÔTE À INTERNET

L'une des configurations attrayantes souvent associées à CBII est la possibilité de bloquer les connexions directes du dispositif hôte à la plupart des sites Internet. En empêchant l'hôte de communiquer avec l'Internet, les logiciels malveillants peuvent avoir plus de mal à atteindre les serveurs de commande et de contrôle (C&C).

HP Sure Click Enterprise a la capacité intégrée d'isoler l'hôte d'Internet, comme CBII. Avec HP, les pare-feu d'hôte et de réseau peuvent être configurés pour empêcher l'appareil et toutes les applications fonctionnant sur l'appareil de communiquer avec Internet. HP Sure Click Enterprise peut être configuré pour utiliser un proxy séparé et dédié qui est inconnu du système d'exploitation hôte et des applications qui y sont exécutées. En effet, un appareil peut être configuré de manière à ce que seules les microVM HP Sure Click Enterprise soient autorisées à se connecter à Internet.

Dans un environnement sécurisé, il est hautement souhaitable de surveiller et de contrôler les connexions réseau des terminaux afin d'identifier ou d'inhiber les flux réseau inattendus qui peuvent être utilisés pour le C&C ou l'exfiltration par les logiciels malveillants fonctionnant sur l'hôte infecté. Cette tâche est difficile pour les terminaux typiques, car lorsqu'on les regarde au niveau du réseau, on observe le trafic global de toutes les applications fonctionnant sur le système, en particulier les navigateurs Web, dont on peut raisonnablement s'attendre à ce qu'ils établissent des connexions avec un grand nombre de serveurs Internet. HP Sure Click Enterprise met en œuvre un certain nombre de fonctionnalités pour aider les entreprises à mieux segmenter leur réseau et ainsi identifier les flux anormaux.

Comme décrit précédemment, les sites Web et les documents non fiables sont ouverts et affichés dans des machines virtuelles isolées fonctionnant sur le terminal. HP Sure Click Enterprise permet d'identifier et d'acheminer tout le trafic provenant de ces VM non fiables, indépendamment de tout autre trafic provenant de l'hôte. Ainsi, il est possible d'empêcher les VM non fiables de communiquer avec des hôtes sur l'Intranet (ce qui empêche les mouvements latéraux). Étant donné que la navigation sur Internet et les documents non fiables isolés dans les machines virtuelles représentent probablement la majeure partie du trafic Internet, il devient alors possible de commencer à surveiller de plus près le trafic d'autres applications sur l'hôte. Dans certains déploiements, les clients ont déterminé que toutes les autres applications sur le terminal ne sont pas censées communiquer avec des hôtes en dehors de l'Intranet. En effet, toute tentative de la part du terminal de le faire est une indication d'un potentiel trafic C&C ou d'exfiltration et sera bloquée et examinée. Cette méthode s'est avérée extrêmement efficace pour identifier les hôtes compromis et empêcher toute exfiltration.

Une configuration typique employée par les clients de HP Sure Click Enterprise pour mettre en œuvre la ségrégation du réseau consiste à déployer un proxy http/https spécial pour acheminer tout le trafic provenant des VM non fiables, les applications exécutées sur ces dernières pouvant communiquer avec l'Internet mais pas avec l'Intranet. Ce proxy spécial serait inconnu des autres applications sur l'hôte, et celles-ci ne pourraient pas s'authentifier auprès de lui. Ainsi, une application hôte compromise qui tenterait de communiquer avec Internet suivrait la configuration de routage de l'hôte et déclencherait une alerte du pare-feu réseau, offrant à l'entreprise une visibilité immédiate de l'hôte potentiellement compromis, tout en empêchant l'hôte de communiquer avec le serveur C&C d'un pirate.

SÉCURISATION DES APPLICATIONS ET DES SYSTÈMES D'EXPLOITATION HÉRITÉS

Le gouvernement américain est fortement tributaire des applications modernes et anciennes pour soutenir les systèmes d'entreprise et stratégiques. Dans le cas des applications héritées, leur mise à niveau est longue et coûteuse, elles restent donc en place. Toutefois, les pratiques de fin de vie des fournisseurs de systèmes d'exploitation et d'applications ont entravé la capacité du gouvernement à prendre en charge les applications héritées, car leurs fournisseurs ne prennent plus en charge la correction des vulnérabilités identifiées dans ces systèmes. HP Sure Click Enterprise protège les applications héritées dont dépendent les agences gouvernementales, notamment (mais pas exclusivement) Internet Explorer, JAVA 1.6, JAVA 1.7 et Flash, ainsi que Windows 10. Grâce à l'utilisation d'un hyperviseur par la technologie HP Sure Click Enterprise, les vulnérabilités connues et inconnues de ces applications patrimoniales ne sont plus pertinentes, et l'entreprise peut sécuriser ces applications tout au long de la période d'utilisation continue et lors de la migration vers des plateformes et des applications plus récentes.

ARCHITECTURE DIFFÉRENTE DES AUTRES SOLUTIONS DE CONFINEMENT

Un certain nombre de solutions prétendent assurer le confinement aujourd'hui, ou le feront à l'avenir. Les principaux différenciateurs architecturaux entre HP Sure Click Enterprise et ces autres solutions sont les suivants.

Les bacs à sable d'applications, qui s'exécutent dans le système d'exploitation ou la couche d'applications :

- Les vulnérabilités du mode noyau et les vulnérabilités des services privilégiés peuvent être utilisées pour contourner directement les bacs à sable des applications.
- HP Sure Click Enterprise isole au niveau de la VM, chaque VM ayant son propre noyau et ses propres services.

Certaines solutions conteneurisées s'exécutent sur des serveurs distincts sur le réseau, comme les solutions de navigation Web non fiables basées sur le cloud :

- Elles fournissent une abstraction Internet de l'hôte d'entreprise.
- Pas d'intégration de l'entreprise avec les ressources de l'Intranet. Le trafic Internet peut être nécessaire à l'entreprise, par exemple la recherche, les comptes fournisseurs, les réseaux sociaux, les missions, etc.
- Aucune intégration avec les outils de messagerie, de stockage ou de collaboration de l'entreprise.
- Aucune intégration avec l'infrastructure de sécurité de l'entreprise.
- Possibilité limitée, voire inexistante, de renseignement sur les menaces, ce qui entraîne une perte potentielle de preuves et de renseignements sur les menaces pour les entreprises.
- La configuration du réseau des ressources internes pour prendre en charge la segmentation du réseau vers un Internet non fiable peut être complexe.
- HP Sure Click Enterprise isole l'utilisation d'Internet par l'entreprise et est plus facile à configurer que les navigateurs basés sur le cloud, tout en prenant en charge la protection des ressources Intranet

Sécurité basée sur l'hôte de l'hyperviseur : machine virtuelle persistante unique telle que WDAG :

- Une seule grande machine virtuelle partagée pour toute la navigation non fiable pour le navigateur Microsoft Edge (Chromium), Word, Excel et PowerPoint uniquement.
- Une seule VM persistante est arrêtée et réinitialisée qu'en cas de déconnexion ou de mise hors tension.
- De par son architecture de VM persistante, une VM compromise ne sera pas détectée, ce qui permettra au logiciel malveillant de se propager aux autres applications exécutées dans la VM.
- Lié à un accord de licence d'entreprise qui peut être coûteux pour le gouvernement américain.
- Peu ou pas de renseignements sur les menaces qui puissent être partagés directement avec le gouvernement américain sans être d'abord envoyés à un fournisseur externe de solutions infonuagiques pour analyse.
- Analyse de la menace uniquement si l'utilisateur veut faire confiance au document via un outil de détection et réponse aux points d'accès (EDR) qui vérifie les attaques connues en s'appuyant sur sa solution d'analyse en cloud. Pas d'analyse directe du gouvernement américain ou d'analyse de type zero-day.
- La télémétrie des terminaux et des utilisateurs de l'entreprise peut être partagée avec le fournisseur de la solution.
- Pas de prise en charge de Windows 7 ou 8.1.
- Pas de prise en charge des navigateurs du gouvernement américain : IE, Chrome, Mozilla Firefox
- Pas de prise en charge des applications héritées.
- Pas de prise en charge des applications ou des systèmes d'exploitation non corrigés.
- Pas de serveur de gestion centralisé ou de moteur de rapports.
- S'appuie sur la politique de groupe Active Directory pour la configuration.
- Pas de stockage local pour les alertes mises en cache, si de collecte de renseignements sur les menaces.
- Les environnements tactiques hors ligne et à faible bande passante peuvent ne pas être protégés sans connexion au cloud.

EXÉCUTION COMPLÈTE D'UNE ATTAQUE DANS UN ENVIRONNEMENT ISOLÉ

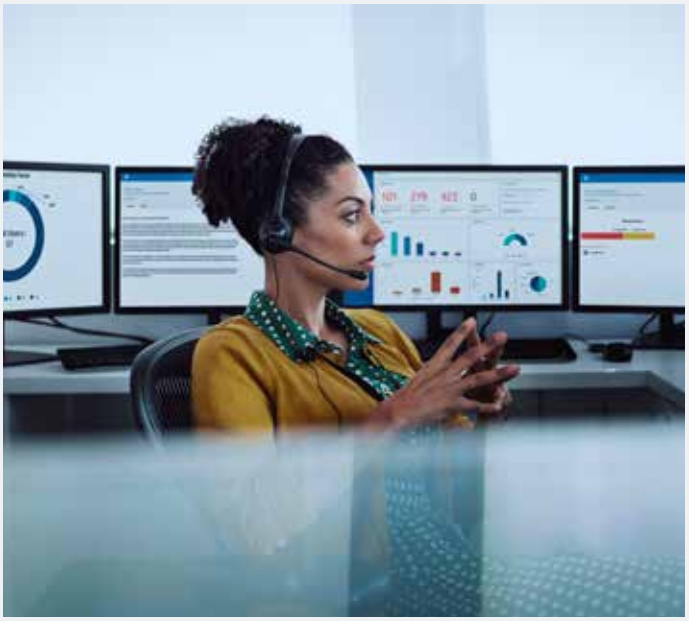
Avec HP Sure Click Enterprise, les menaces sont complètement isolées et, en fonction de la politique gouvernementale mise en œuvre, elles peuvent être autorisées à s'exécuter pleinement et sans interruption, de sorte que le gouvernement puisse retracer entièrement la chaîne d'élimination, en limitant les faux positifs, en augmentant les renseignements sur les menaces collectés par attaque et en autorisant des modèles personnalisés avec un piège à pirates personnalisé dans le contenu à l'intérieur de la VM pour répondre à d'autres exigences du gouvernement américain. Lorsque la tâche est terminée, la microVM est détruite, ainsi que la menace.

La solution est amortie dès la première attaque isolée. Il n'est plus nécessaire de corriger les erreurs sur l'appareil, de recréer l'image ou de le retirer du réseau ou d'expulser une intrusion réussie, car HP Sure Click Enterprise constitue la dernière ligne de défense de la pile de cyberrésilience, en isolant les attaques qui contournent toutes les autres défenses.

SÉCURITÉ SANS DÉPENDANCE VIS-À-VIS DES CORRECTIFS DE SYSTÈMES

L'application de correctifs reste une exigence pour le gouvernement américain ; cependant, HP Sure Click Enterprise protège contre les attaques des vulnérabilités des systèmes d'exploitation et des applications non corrigés (y compris les exploitations de type zero-day), ainsi que contre les applications anciennes pour lesquelles l'application de correctifs est devenue impossible. L'entreprise n'a plus besoin d'appliquer des correctifs d'urgence, un exercice qui conduit souvent à la rupture de systèmes stratégiques.

HP Sure Click Enterprise assure une isolement contre de grandes catégories de vulnérabilités non corrigées, offrant ainsi au gouvernement américain une protection et une visibilité sur les menaces, les vecteurs et les logiciels malveillants inconnus qui ne disposent pas encore d'un correctif du fournisseur du système d'exploitation ou des applications. Les renseignements sur les menaces peuvent être exploités et des protections mises en place avant la réception ou le déploiement d'un correctif. En outre, le gouvernement dispose d'un aperçu immédiat d'un nouveau vecteur de menace, peut-être avant la communauté des fournisseurs et des responsables de la sécurité, ce qui lui donne un avantage concurrentiel sur ses adversaires.



SÉCURITÉ À L'INTÉRIEUR ET À L'EXTÉRIEUR DU RÉSEAU

Les terminaux exécutant HP Sure Click Enterprise isolent les tâches et assurent la protection, indépendamment de l'emplacement ou de la proximité du système administratif de gestion. Que ce soit sur site ou hors réseau, le contenu non fiable est isolé de l'hôte et la politique permanente est appliquée comme prévu ; aucune connexion en temps réel au serveur de gestion n'est nécessaire pour assurer le confinement. Si un événement de sécurité se produit hors réseau, tous les détails criminalistiques seront stockés localement et transmis une fois que le terminal aura rétabli la connectivité réseau avec le serveur de gestion. Le logiciel malveillant est isolé et le transfert du fichier malveillant à partir de l'appareil est empêché, ce qui constitue une mesure de protection supplémentaire pour les utilisateurs à faible bande passante ou déconnectés.

SYNTHÈSE

Les cybercriminels sont plus expérimentés, organisés et déterminés que jamais. Ils exploitent de plus en plus les vulnérabilités du lieu de travail en mutation et ciblent un nombre toujours plus grand de terminaux et de dispositifs IoT . Alors que les équipes informatiques surchargées s'efforcent de suivre le rythme, la sécurité des terminaux est devenue de plus en plus critique en tant que première ligne de défense.

Les agences civiles et de défense du gouvernement américain ont besoin de pouvoir isoler les attaques ciblées de type zero-day et de disposer d'un aperçu criminalistique en temps réel de l'attaque et de l'intention, avec des renseignements complets sur les menaces pour protéger le gouvernement, les commandements interarmées et les services contre une telle attaque.

Grâce à HP Wolf Enterprise Security[5], le tissu de capteurs de menaces du gouvernement américain peut isoler l'attaque inconnue, recevoir des informations en temps réel sur l'attaque, les injecteurs, les charges utiles et l'intention, puis partager ces renseignements avec ses partenaires. Notre portefeuille de matériel à sécurité renforcée et nos services de sécurité axés sur les terminaux sont conçus pour aider les organisations à protéger leurs ordinateurs, imprimantes et employés des cyberprédateurs.

HP Sure Click Enterprise fournit un filet de sécurité virtuel aux utilisateurs d'ordinateurs, même lorsque des menaces inconnues échappent aux autres défenses. La virtualisation renforcée par une protection matérielle isole le contenu à haut risque pour protéger les ordinateurs, les données et les informations d'identification des utilisateurs, en rendant les logiciels malveillants inoffensifs, alors que les services informatiques obtiennent des renseignements exploitables sur les menaces pour renforcer la stratégie de sécurité de l'organisation.

Nous proposons un nouveau type de sécurité des terminaux[6], ancré dans les principes du Zéro Trust, qui évolue en permanence pour aider le gouvernement américain à garder une longueur d'avance sur les menaces modernes. Découvrez pourquoi les organisations les plus soucieuses de la sécurité au monde utilisent HP Wolf Enterprise Security[7] pour éliminer les vecteurs de menaces bruyants et à haut risque, afin que leurs équipes puissent se concentrer sur ce qui compte vraiment.

[1] HP Sure Click Enterprise exige Windows 8 ou 10. Microsoft Internet Explorer, Google Chrome, Chromium et Firefox sont pris en charge. 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.

[2] HP Sure Recover est disponible sur certains ordinateurs HP et nécessite une connexion réseau ouverte. Les fichiers, données, photos, vidéos et tout autre élément important doivent être sauvegardés avant d'utiliser HP Sure Recover afin d'éviter toute perte de données.

[3] HP Sure Admin est disponible sur certains ordinateurs HP et nécessite le module de gestion intégrée HP Manageability Integration Kit disponible sur http://www.hp.com/go/clientmanagement et l'application pour smartphone HP Sure Admin Local Access Authenticator disponible sur Google Play ou l'Apple Store.

[4] D'après les utilisateurs actifs de HP Sure Click et les comportements moyens d'utilisation des applications.

[5] HP Security est désormais HP Wolf Security. Les fonctions de sécurité varient selon la plateforme, veuillez consulter la fiche technique du produit pour plus de détails.

[6] Sur la base d'une analyse interne HP de fonctionnalités uniques et complètes, parmi les solutions de sécurité par isolement et confinement des applications. Nécessite Microsoft Windows 10. La protection de Microsoft Word, Excel ou PowerPoint nécessite une licence Office.

[7] HP Wolf Enterprise Security est un service en option qui peut inclure des offres telles que HP Sure Click Enterprise et HP Sure Access Enterprise. HP Sure Click Enterprise nécessite Windows 8 ou 10. Microsoft Internet Explorer, Google Chrome, Chromium et Firefox sont pris en charge. 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. HP Sure Access Enterprise nécessite Windows 10 Professionnel ou Entreprise. Les services HP sont régis par les conditions générales HP applicables au service considéré ou indiquées au client au moment de l'achat. La législation locale en vigueur peut octroyer des droits statutaires au client. Ces droits ne sont en aucune façon affectés par les conditions générales de service HP ni par la garantie limitée HP fournie avec les produits HP. Pour tous les détails sur la configuration requise du système, rendez-vous sur www.hpdaas.com/requirements.

4AA8-0128FRE, juin 2021