HP WOLF SECURITY

HP WOLF ENTERPRISE SECURITY

HP SURE CLICK ENTERPRISE

OPTIMISÉ PAR Bromium

ISOLER ET PRÉVENIR LES ATTAQUES INDÉTECTABLES

HP Sure Click Enterprise[1] fournit un filet de sécurité virtuel aux utilisateurs de PC, même lorsque des menaces inconnues échappent aux autres défenses. La virtualisation renforcée par le matériel isole le contenu à haut risque pour protéger les PC, 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 l'attitude de sécurité de l'organisation.

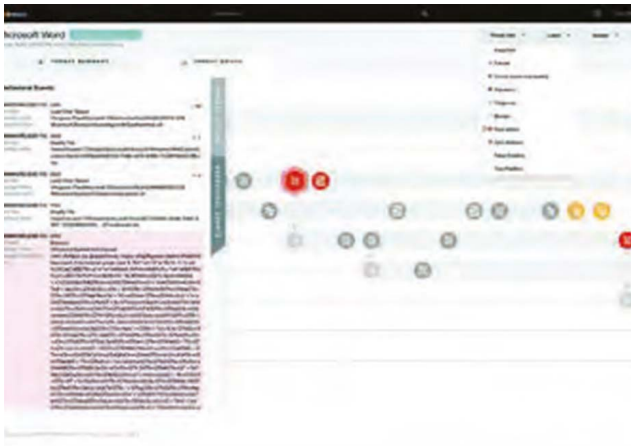
HP Sure Click Enterprise[1] bloque les attaques des terminaux en créant des micro-machines virtuelles (microVM) qui sécurisent chaque tâche de l'utilisateur, de la navigation sur le Web à l'ouverture des e-mails et au téléchargement des pièces jointes. Chaque tâche est complètement isolée à l'intérieur de la microVM. Lorsqu'une tâche est fermée, la microVM et toute menace qu'elle contenait sont éliminées sans aucune violation.

HP Sure Click Enterprise[1] est doté d'une technologie unique d'isolement renforcé par le matériel qui utilise la sécurité basée sur la virtualisation sur l'hôte pour contenir les menaces à l'intérieur de micro-machines virtuelles individuelles et à usage unique. Cette approche réduit considérablement les surfaces d'attaque, sans modifier la façon dont les utilisateurs finaux accèdent à leur e-mail, à leurs navigateurs ou à leurs données.

LES CONTRÔLES D'ACCÈS BASÉS SUR DES POLITIQUES PERMETTENT D'AFFINER LA SÉCURITÉ

HP Sure Click Enterprise[1] dispose d'un moteur de politique robuste. Les administrateurs peuvent configurer un accès sécurisé au Web et aux fichiers par groupes d'utilisateurs, avec des contrôles granulaires et des politiques par défaut pour les cas d'utilisation courants tels que les pièces jointes aux e-mails, les liens d'hameçonnage et les téléchargements de fichiers Web. Ces politiques sont simples à définir, elles sont hiérarchisées et peuvent être affinées pour répondre à vos préoccupations spécifiques en matière de sécurité et à vos profils de risque.

PRINCIPAUX AVANTAGES



ACCÉDER EN TOUTE SÉCURITÉ AUX FICHIERS PROVENANT DE SOURCES ENTRANTES

Ouvrez n'importe quel fichier ou document sans risque d'infection, qu'il soit téléchargé sur le Web, reçu par e-mail ou enregistré sur des clés USB.

BLOQUER LES LOGICIELS MALVEILLANTS

Les microVM isolent et contiennent l'activité malveillante, alors que les logiciels malveillants disparaissent à la fermeture du fichier ou du document.

PROTÉGER LES INFORMATIONS D'IDENTIFICATION CONTRE L'HAMEÇONNAGE

HP Sure Click Enterprise empêche les utilisateurs de saisir leurs données de connexion sur les sites Web malveillants connus et les avertit d'un comportement potentiellement risqué sur tous les sites de faible réputation.

DURCIR TOUTE VOTRE INFRASTRUCTURE DÉFENSIVE

Utilisez les indicateurs d'attaque et les indicateurs de compromission de HP Sure Click pour mettre en quarantaine les fichiers et rechercher les logiciels malveillants qui se cachent sur les serveurs et les appareils non protégés par HP Sure Click en utilisant des outils tiers.

RENSEIGNEMENTS SUR LES MENACES

Chaque terminal et serveur HP Sure Click fait partie d'un réseau de capteurs qui s'adapte en permanence et qui peut être utilisé pour l'analyse des logiciels malveillants et le partage instantané d'indicateurs de menaces. Les équipes de sécurité reçoivent des renseignements sur les menaces et des analyses complètes de la chaîne d'élimination, ce qui les aide à traquer les menaces, à partager les informations dans toute l'entreprise et à résoudre rapidement les problèmes.

FONCTIONNALITÉS PRINCIPALES

UNE PROTECTION INÉBRANLABLE CONTRE LES LOGICIELS MALVEILLANTS GRÂCE À UN ISOLEMENT RENFORCÉ PAR LE MATÉRIEL

Isolez les fichiers entrants et le contenu Web du PC hôte et du réseau interne en utilisant des techniques d'analyse comportementale évoluées pour identifier les activités malveillantes.

RENSEIGNEMENTS SUR LES MENACES

L'isolement d'un logiciel malveillant génère des alertes de menace destinées aux analystes du centre de gestion de la sécurité (SOC), et envoie des flux de menaces à des systèmes tiers pour renforcer les infrastructures défensives.

BLOQUER RAPIDEMENT LES VECTEURS D'ATTAQUE

Une protection prête à l'emploi contre les principaux vecteurs d'attaque tels que les pièces jointes des e-mails, les liens d'hameçonnage et les téléchargements de fichiers, sans avoir à passer par des paramètres de configuration complexes.

CLASSIFICATION DES MENACES GRÂCE À L'INTELLIGENCE CONTEXTUELLE

La classification des menaces basée sur les flux de travail, avec des renseignements augmentés sur les menaces, accélère l'identification analytique des faux positifs à des fins de résolution et de correction proactives sur les systèmes protégés par HP Sure Click et les autres.

TABLEAUX DE BORD, RAPPORTS ET ANALYSES DÉTAILLÉS EXPLOITABLES

Constatez et partagez facilement la valeur ajoutée offerte par HP Sure Click grâce à des notes de synthèse administratives (rapports de RSSI/DSI, tableau de bord opérationnel pour l'équipe chargée des terminaux), et à un tableau de bord des menaces pour votre équipe de sécurité.

HP SURE CLICK ENTERPRISE[1] OFFRE LES SERVICES SUIVANTS :

NAVIGATION SÉCURISÉE, FICHIERS SÉCURISÉS, PROTECTION DES INFORMATIONS D'IDENTIFICATION, RENSEIGNEMENTS SUR LES MENACES ET RAPPORTS

NAVIGATION SÉCURISÉE

NAVIGATION WEB SÉCURISÉE ORIENTÉE UTILISATEUR

La navigation sécurisée isole les menaces véhiculées par le Web et l'exploitation du navigateur à l'aide de microVM renforcées par le matériel, de sorte que vous ne dépendez pas de la détection ni des listes noires restrictives de sites Web.

Chaque onglet du navigateur est complètement isolé de tous les autres onglets, du PC hôte et du réseau interne. La navigation sécurisée s'effectue au sein d'une microVM protégée, ce qui permet de mener à bien les tâches sans entrave et en étant isolé des fichiers et processus sensibles. Les utilisateurs bénéficient d'une navigation native pour les sites sûrs dans Chrome, Firefox ou Edge, avec un routage automatique vers une navigation isolée pour les sites à risque dans le navigateur sécurisé HP Sure Click, y compris les liens d'hameçonnage présumés et les sites Web non classés.

MENACES WEB : NEUTRALISÉES

Toute l'activité du site Web est séquestrée dans le conteneur microVM sécurisé. La microVM et toutes les menaces sont détruites dès la fermeture de l'onglet du navigateur, en laissant derrière elle un rapport enrichi sur les menaces, qui sert de trace criminalistique de toute activité malveillante. La protection Web s'étend aux vulnérabilités connues et inconnues, notamment l'exploitation du navigateur de type « zero-day », les scripts intersites malveillants et les logiciels malveillants sans fichier qui exploitent les failles de mémoire ou d'autres faiblesses de Windows. L'application de correctifs et la vérification des versions deviennent moins urgentes, car la navigation sécurisée rend les systèmes non corrigés sûrs pour tous les utilisateurs.

SECURE FILES

TÉLÉCHARGEMENT ET ACCÈS SÉCURISÉS DES FICHIERS ENTRANTS

Secure Files utilise la micro-virtualisation renforcée par le matériel pour isoler les menaces malveillantes cachées dans les fichiers et documents entrants, y compris les pièces jointes des e-mails, les téléchargements Web et les fichiers sur clés USB.

Chaque fichier est ouvert de manière transparente à l'intérieur d'une microVM protégée. Ce processus est transparent pour l'utilisateur, les fichiers étant complètement contenus et isolés des autres fichiers et processus. Secure Files fonctionne en ligne et hors ligne, ce qui permet aux utilisateurs d'imprimer, d'enregistrer, de modifier et de renommer leurs documents et fichiers en toute sécurité.

LES MENACES SUR LES DOSSIERS ET LES DOCUMENTS SONT SÉQUESTRÉES

Si un fichier est malveillant, toute activité reste isolée dans le conteneur sécurisé, et toute menace est éliminée lorsque le fichier est fermé. Cette protection s'étend aux vulnérabilités connues et inconnues, notamment les exploitations de type « zero-day », les macros malveillantes, les scripts et les techniques d'attaque évoluées qui tirent parti des bogues du noyau de la mémoire ou d'autres faiblesses de Windows.

PROTECTION DES IDENTIFIANTS

ALERTER ET EMPÊCHER LES UTILISATEURS DE RÉVÉLER LEURS INFORMATIONS D'IDENTIFICATION

Lorsqu'un utilisateur visite un site Web et est invité à saisir ses identifiants de connexion, l'agent HP Sure Click Enterprise utilise le service HP de renseignement sur les menaces afin de mener (en arrière-plan) une analyse de la réputation et du domaine, de façon à déterminer la sécurité du site. Pour les sites légitimes et connus comme étant sûrs, aucune mesure n'est prise, tandis que les utilisateurs sont empêchés de saisir leur mot de passe sur les sites malveillants connus, et reçoivent un message d'avertissement pour les sites de faible réputation.

LAISSER LES UTILISATEURS NAVIGUER EN TOUTE TRANQUILLITÉ

Pour les sites de faible réputation, les administrateurs peuvent laisser aux utilisateurs la liberté de poursuivre, ce qui permettra d'inscrire le site sur la liste blanche du PC de l'utilisateur et d'éviter des restrictions inutiles de productivité lors de visites ultérieures. Pour les sites malveillants, le logiciel peut être configuré pour permettre à l'utilisateur de consulter le site avec tous les champs de capture de données désactivés. Toutes les actions sur les sites connus pour être malveillants ou de faible réputation sont enregistrées et signalées au contrôleur Sure Click afin que le service informatique puisse vérifier l'état des menaces et du comportement des utilisateurs.

L'ACTIVITÉ À RISQUE DE L'UTILISATEUR EST ISOLÉE DANS UNE MICROVM

LES MICROVM N'ONT ACCÈS NI À L'HÔTE, NI AUX PARAMÈTRES, NI À INTERNET

LES MICROVM NE CONTIENNENT AUCUNE INFORMATION PERSONNELLE

RENSEIGNEMENTS ET RAPPORTS SUR LES MENACES

RAPPORTS ET ANALYSES INTELLIGENTS

HP Sure Click Enterprise[1] émet des alertes en temps réel avec des informations criminalistiques complètes sur chaque attaque, offrant ainsi une visibilité en temps réel des terminaux aux équipes de sécurité.

L'application HP Sure Click Enterprise[1] pour les terminaux et le contrôleur central forment un réseau de capteurs qui s'adapte en permanence pour l'analyse des logiciels malveillants et le partage instantané des indicateurs de menace. Le contrôleur central HP Sure Click Enterprise gère les politiques à l'échelle de l'entreprise et collecte les données d'attaque en temps réel à partir des terminaux pour fournir une analyse criminalistique et des données télémétriques complètes sur les menaces. Les équipes de sécurité reçoivent des alertes en temps réel et des rapports complets d'analyse sur la chaîne d'élimination pour trouver les menaces plus rapidement, ce qui garantit une visibilité et un contrôle à l'échelle de l'entreprise.

Les équipes du centre de gestion de la sécurité obtiennent une visibilité complète de la sécurité lorsque Sure Click Enterprise est déployé sur les terminaux et serveurs Windows dans toute l'entreprise. La lecture continue en temps réel des données d'attaque avec l'analyse du flux d'applications fournit une vue complète et intégrée de l'attaque aux analystes du centre de gestion de la sécurité. Des milliers d'événements de surveillance de bas niveau sont corrélés en temps réel au niveau du terminal ou du serveur, ce qui élimine le besoin d'une analyse manuelle fastidieuse ou de datacenter coûteux.

Les données brutes sont transformées en renseignements de plus haut niveau, ce qui permet aux équipes de sécurité d'avoir à tout moment une connaissance en temps réel de l'état général des menaces. Vous n'aurez plus besoin de consacrer un budget et des ressources à la chasse aux faux positifs et aux mesures correctives, aux reconstructions ou aux correctifs d'urgence.

UTILISER HP SURE CLICK ENTERPRISE[1] POUR SÉCURISER VOS VECTEURS D'ATTAQUE LES PLUS VULNÉRABLES

PIÈCES JOINTES D'E-MAIL
• Rançongiciels • Macros à cheval de Troie • Logiciels malveillants sans fichier • Liens malveillants

LIENS D'HAMEÇONNAGE
• Liens malveillants dans le corps du message et les pièces jointes • Exploitation des navigateurs
• Fausses mises à jour de Flash/Java • Téléchargements furtifs (« drive by »)
• Attaques de type « point d'eau » • Publicité malveillante • Liens dans les programmes de discussion instantanée

TÉLÉCHARGEMENTS ET EXÉCUTABLES
• Téléchargements délibérés • Fausses mises à jour d'exécutables • Liens vers des documents
• DNS malveillant/redirections d'URL • Pilotes et utilitaires corrompus • Attaques de type « point d'eau »

LA PROTECTION DE L'IDENTITÉ
• Hameçonnage d'identifiants • Extraction d'informations d'identification locales et de domaine
• Réutilisation non autorisée d'informations d'identification

RÉSEAUX NON PROTÉGÉS
• Exploitation des navigateurs • Logiciels malveillants sans fichier • Téléchargements furtifs (« drive-by »)
• DNS malveillant/redirections d'URL • Fausses mises à jour (Reader, Flash, Java, etc.)

SITES WEB NON CATÉGORISÉS
• Exploitation des navigateurs • Logiciels malveillants sans fichier
• Téléchargements cryptés échappant à la détection

CONTENU MULTIMÉDIA SUR CLÉ USB
• Fichiers de productivité au bureau • Fichiers multimédia
• Fichiers exécutables • Liens vers des documents • Signets Web

AUCUNE INTRUSION PAR MICROVM
(selon nos clients)

Déployez la plate-forme HP Sure Click Enterprise Secure Platform pour protéger les vecteurs d'attaque des utilisateurs ciblés ou activez toutes les capacités pour une véritable sécurité d'une qualité similaire à celle adoptée par la « défense ».

Pour en savoir plus, consultez **https://www.hp.com/enterprisesecurity**

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.

4AA7-7470FRE, avril 2021, rév. 2

HP WOLF SECURITY