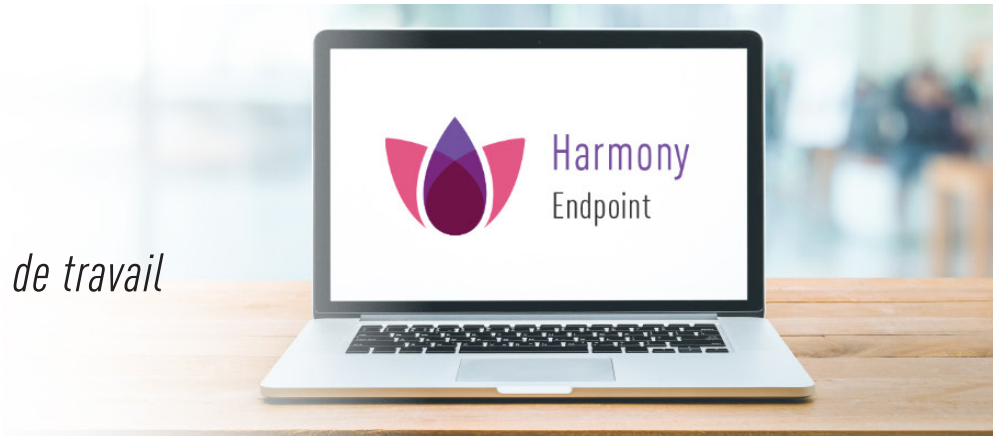
Check Point
SOFTWARE TECHNOLOGIES LTD

Harmony Endpoint

La seule protection des postes de travail dont vous avez besoin



Harmony Endpoint est une solution complète de sécurité des postes de travail conçue pour protéger votre main-d'œuvre à distance des menaces complexes d'aujourd'hui. Elle bloque les menaces les plus imminentes vers le poste de travail telles que les logiciels rançonneurs, l'hameçonnage ou les logiciels malveillants furtifs tout en réduisant rapidement l'impact des failles grâce à une détection et à une réponse autonome.

De cette façon, votre entreprise bénéficie de la seule protection des postes de travail dont elle a besoin, de la qualité qu'elle mérite, avec une solution unique, efficace et rentable.

PRINCIPAUX AVANTAGES DU PRODUIT

Protection totale des postes de travail : bloque les menaces les plus imminentes pour le poste

Restauration rapide : automatisation de 90 % des tâches de détection, d'investigation et de correction des attaques

Meilleur coût total de possession (Total Cost of Ownership ou TCO) : la seule protection des postes de travail dont vous avez besoin, avec une solution unique, efficace et rentable

CAPACITÉS UNIQUES DU PRODUIT

Les algorithmes avancés d'analyse comportementale et de machine learning bloquent les logiciels malveillants avant qu'ils n'infligent des dommages

Les taux de capture élevés et le peu de faux positifs garantissent une sécurité et une prévention efficaces

L'analyse automatisée des données post-infection fournit des informations détaillées sur les menaces

Une mise en quarantaine et une correction totales de l'attaque permettent de restaurer rapidement tout système infecté

Première solution de sécurité des postes de travail du marché

AV-TEST APPROVED CORPORATE ENDPOINT PROTECTION WINDOWS 10/2020 TOP PRODUCT
av-test.org

Harmony Endpoint est reconnue comme le meilleur produit de protection des postes de travail d'entreprise par AV-TEST

EN SAVOIR PLUS

FORRESTER®

Forrester Wave reconnaît Check Point comme un leader dans la sécurité des postes de travail

EN SAVOIR PLUS

AA
NSS Labs

Check Point Harmony Endpoint a obtenu la note AA à l'évaluation de produit de 2020 des tests de protection avancée des postes de NSS Labs

EN SAVOIR PLUS

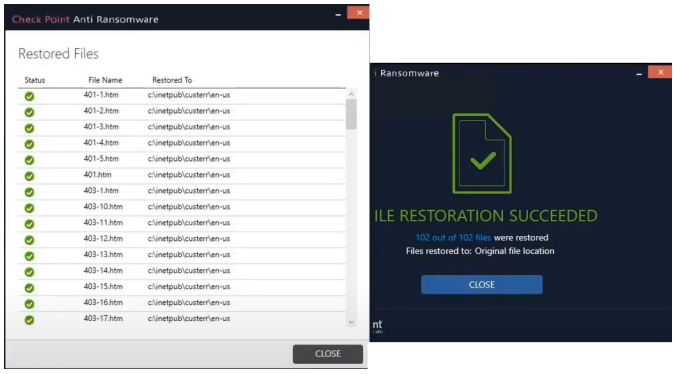
Comment ça fonctionne

Protection totale des postes de travail

Bloque les menaces les plus imminentes pour le poste de travail

- **Bloque les logiciels malveillants** provenant de votre navigation sur internet ou de pièces jointes d'emails avant qu'ils n'atteignent le poste de travail, et ce sans avoir d'impact sur la productivité des utilisateurs. Chaque fichier reçu par email ou téléchargé par un utilisateur via un navigateur Web est envoyé dans la SandBox d'émulation des menaces pour détecter d'éventuels logiciels malveillants. Les fichiers peuvent également être désinfectés à l'aide d'un processus d'extraction de menaces (technologie Content Disarm & Reconstruction) pour fournir un contenu propre et sécurisé en quelques millisecondes.

- **Bénéficiez d'une protection d'exécution contre les logiciels rançonneurs, les logiciels malveillants et les attaques sans fichiers ainsi qu'une correction instantanée et totale,** même en mode hors-ligne. Dès qu'une anomalie ou un comportement malveillant est détecté, Endpoint Behavioral Guard bloque et corrige l'ensemble de la chaîne d'attaque sans laisser de traces du logiciel malveillant. Des antiransomwares identifient les comportements de logiciels rançonneurs tels que le chiffrement de fichiers ou les tentatives de compromission des sauvegardes du système d'exploitation, et restaurent automatiquement et en toute sécurité les fichiers chiffrés par le logiciel rançonneur. Harmony Endpoint utilise un espace de stockage protégé unique directement sur la machine qui n'est accessible qu'aux processus autorisés par Check Point. Si le logiciel malveillant tente de supprimer des shadow copies, la machine ne perdra aucune donnée.



- **Protection contre le phishing** : empêche le vol d'identifiants grâce à la technologie Zero-Phishing® qui identifie et bloque l'utilisation des sites de phishing en temps réel. Les sites sont inspectés et, s'ils sont identifiés comme étant malveillants, l'utilisateur ne pourra pas entrer ses identifiants. Zero-phishing® protège même des sites d'hameçonnage inconnus et de la réutilisation d'identifiants d'entreprise.

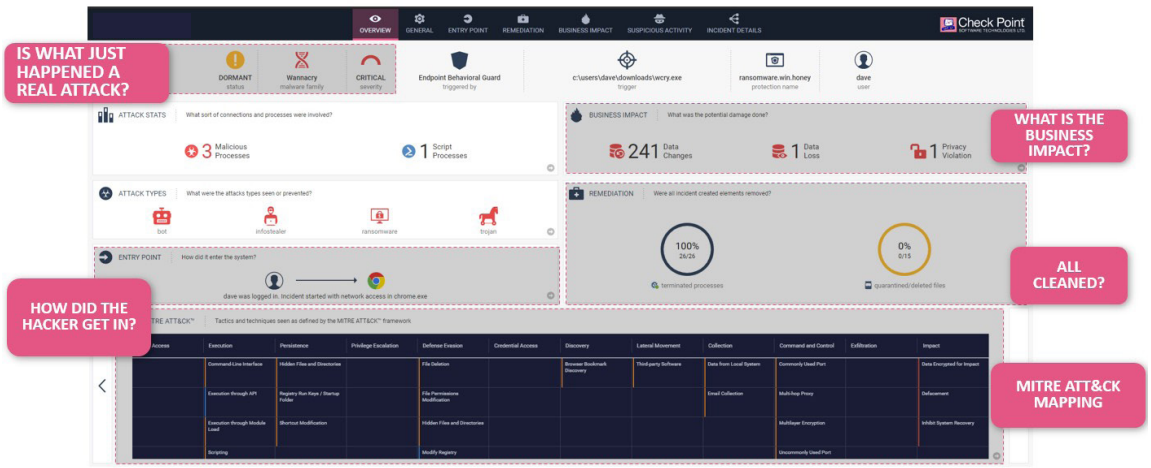
Meilleur taux de capture de logiciels malveillants connus et zero-day du secteur

Leader reconnu de l'industrie, comme l'indiquent les tests d'AV-TEST Corporate sur la protection de postes de travail et de NSS Labs sur la protection avancée de postes de 2020, Harmony Endpoint fonctionne grâce à 60 moteurs de prévention de menaces et est alimentée par Check Point ThreatCloud™, la solution de renseignements sur les menaces la plus puissante au monde offrant le plus haut taux de capture de menaces général du marché.

Restauration rapide

Automatisation de 90 % des tâches de détection, d'investigation et de correction des attaques

- **Une mise en quarantaine de l'attaque et une correction automatiques :** la seule solution de protection des postes de travail qui corrige automatiquement l'intégralité de la chaîne destructrice de la cyberattaque. Une fois qu'une attaque a été détectée, l'appareil infecté peut être automatiquement mis en quarantaine pour empêcher le mouvement latéral de l'infection et être restauré.
- **Rapports d'analyse post-infection auto-générés :** offrant une visibilité détaillée sur les actifs infectés, le flux d'attaques et la mise en corrélation avec le cadre MITRE ATT&CK™. La fonction d'analyse post-infection supervise et enregistre automatiquement les événements du poste dont les fichiers affectés, les processus lancés, les changements de la base de registre par le système et l'activité sur le réseau et crée un rapport post-infection détaillé. Des diagnostics d'attaque fiables et une bonne visibilité aident à l'effort de correction pour permettre aux administrateurs du système et aux équipes de réponse aux incidents de trier et de résoudre efficacement les attaques.

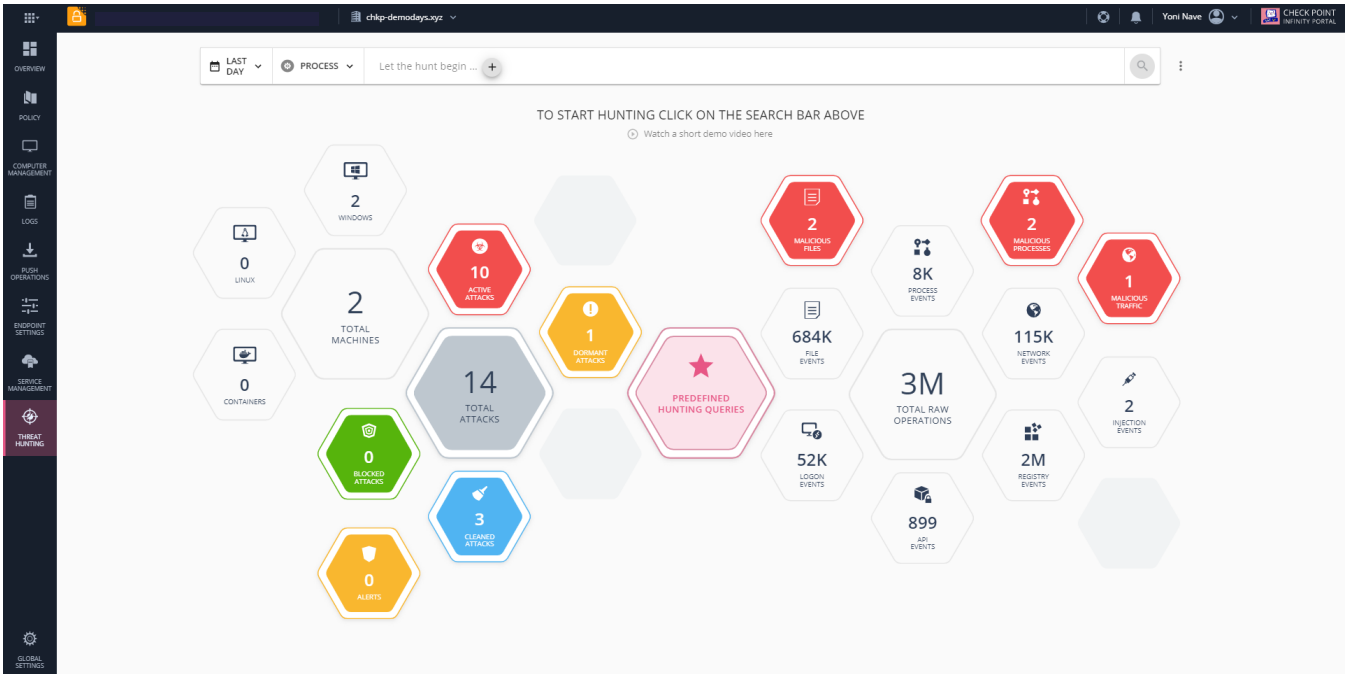


Rapport d'analyse post-infection de Harmony Endpoint

« Le plus grand avantage de l'utilisation de Check Point Harmony Endpoint est que nous n'avons pas à nous soucier des attaques de logiciels rançonneurs sur notre environnement. Elle offre une tranquillité d'esprit totale, et ça, ça n'a pas de prix. Nous savons qu'elle sera là et que nos données resteront en sécurité. »

David Ulloa, responsable de la sécurité des systèmes d'information, IMC Companies

- **Threat Hunting :** alimentée par une visibilité à l'échelle de l'entreprise et complétée par des renseignements sur les menaces partagés à l'échelle mondiale à partir de centaines de millions de capteurs collectés par ThreatCloud™. Grâce à la fonction de Threat Hunting, vous pouvez définir des requêtes ou utiliser des requêtes prédéfinies pour identifier et avoir une vision approfondie des incidents suspects et mettre en place des actions de correction manuelles.



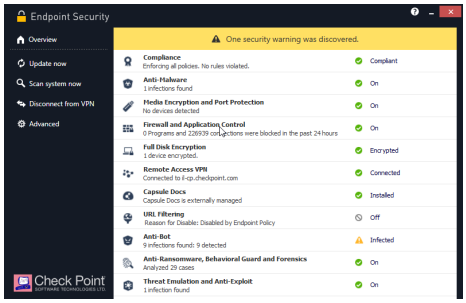
Harmony Endpoint – Traque des menaces

> *« Depuis que nous avons déployé Harmony Endpoint, nous n'avons pas eu d'incident de logiciel malveillant ou de logiciel rançonneur majeur en presque un an. »*
>
> Russell Walker, directeur technique informatique, secrétaire d'État du Mississippi

Meilleur coût total de possession

La seule protection de postes de travail dont vous avez besoin avec une solution unique, efficace et rentable

Un seul agent unifié pour une plateforme de protection de poste de travail, un EDR, un VPN, un antivirus de nouvelle génération et une protection de données et de navigation Web, afin que votre entreprise puisse faciliter les processus et réduire le coût total de possession.



Une flexibilité totale pour répondre à vos exigences spécifiques en matière de sécurité et de conformité.

- Géré soit on-premise, soit via un service cloud, Harmony Endpoint offre une fonctionnalité conviviale avec un déploiement rapide pour répondre à vos besoins
- Prend en charge les systèmes d'opération Windows, macOS et Linux
- Capacité VDI (émulation du bureau sur un serveur à distance), prend en charge VMWare Horizon, Citrix PVS/MCS
- Le Harmony Endpoint Installer récemment mis à jour permet des mises à jour transparentes et des restaurations sans redémarrage ou perturbations pour l'utilisateur final
- Aide à la protection des développeurs : pour aider à protéger les développeurs sans intégrer d'Intégration continue/Déploiement continu (CI/CD) ou d'environnement de développement intégré (IDE).

Basé sur Check Point Infinity, la première architecture de sécurité consolidée conçue pour résoudre les complexités d'une connectivité croissante et d'une sécurité inadéquate qui fournit une protection totale et des renseignements sur les menaces sur les réseaux, les clouds, les postes de travail, les appareils mobiles et l'IdO.

CHECK POINT INFINITY

> *« Check Point Harmony Endpoint : la seule et unique protection avancée des postes de travail. Harmony Endpoint était pour nous la protection avancée des postes de travail la plus adaptée. Elle a été déployée rapidement au sein de notre entreprise mondiale. La console d'administration dispose d'une interface utilisateur intuitive et conviviale. »*
>
> Analyste principal de sécurité d'une grande entreprise d'infrastructure

Caractéristiques techniques

Forfaits Harmony Endpoint	
Forfaits	• **Protection des données** : comprend le chiffrement de disque total et le chiffrement des supports amovibles, y compris le contrôle d'accès et la protection des ports • **Harmony Endpoint Basic** : comprend un anti-logiciel malveillant, des antiransomwares, un anti-phishing zero-day, une prévention des menaces avancée et un logiciel Endpoint Detection and Response (EDR) • **Harmony Endpoint Advanced** : comprend Harmony Endpoint Basic, plus l'émulation et l'extraction des menaces • **Harmony Endpoint Complete** : comprend Harmony Endpoint Advanced plus la sécurité des données (chiffrement total du disque et des supports) **Remarque : Endpoint Compliance** est fourni avec tous les forfaits
Systèmes D'exploitation	
Système d'exploitation	• Station de travail Windows 7, 8 et 10 • Windows Server 2008 R2, 2012, 2012 R2, 2016 • MacOS Sierra 10.12.6, MacOS High Sierra 10.13.4 (émulation des menaces, extraction des menaces, antiransomware, extension de navigateur Chrome pour Mac)
Content Disarm & Reconstruction (CDR) dans la boîte mail et sur le Web	
Extraction des menaces	Supprime tout contenu exploitable, reconstruit les fichiers pour éliminer les menaces potentielles et fournit en quelques secondes un contenu désinfecté aux utilisateurs
Émulation des menaces	• Capacité de SandBoxing pour détecter et bloquer tout nouveau logiciel malveillant inconnu et les attaques ciblées trouvés dans les pièces jointes d'emails, les fichiers téléchargés et les URL vers des fichiers dans des emails. • Fournit une protection pour un large éventail de types de fichiers, notamment MS Office, Adobe PDF, Java, Flash, les fichiers exécutables et les archives, ainsi que plusieurs environnements de système d'exploitation Windows. • Détecte des menaces cachées dans les communications chiffrées SSL et TLS.
Gestion centralisée	
Gestion sur cloud et sur site	• Harmony Service (hébergé sur le cloud de Check Point) • Harmony Appliance (hébergé sur place)
Antivirus de nouvelle génération : détection et protection d'exécution	
Antiransomwares	• Prévention des menaces : surveillent constamment d'éventuels comportements caractéristiques des logiciels rançonneurs et identifient tout chiffrement de fichiers illégitimes sans signatures. • Détectent et mettent en quarantaine : tous les éléments d'une attaque de logiciels rançonneurs sont identifiés par une analyse post-infection, puis mis en quarantaine. • Restauration des données : les fichiers chiffrés sont automatiquement restaurés à partir d'un snapshot pour assurer la pérennité totale de votre entreprise.
Anti-exploitation de vulnérabilité	• Fournit une protection contre les attaques exploitant les vulnérabilités pour compromettre des applications légitimes, afin de garantir que ces vulnérabilités ne pourront pas être exploitées. • Détecte les exploitations de vulnérabilité en identifiant des manipulations de mémoire suspectes pendant l'exécution. • Arrête tout processus victime d'exploitation de vulnérabilité dès la détection et corrige l'ensemble de la chaîne d'attaque.
Behavioral Guard	• S'adapte pour détecter et bloquer les mutations de logiciels malveillants en fonction de leur comportement en temps réel. • Identifie, classe et bloque les mutations de logiciels malveillants en temps réel en fonction des similitudes minimales de l'arbre d'exécution des processus.
Protection en ligne	
Zéro-Phishing	• Protection en temps réel contre les sites de phishing inconnus. • Détection statique et heuristique des éléments suspects sur les sites Web demandant des données confidentielles.
Protection des identifiants de l'entreprise	Détection de la réutilisation d'identifiants d'entreprise sur les sites externes.
Filtrage des URL	• Plug-in de navigateur léger, autorise/interdit l'accès aux sites Web en temps réel. • Applique la politique de l'entreprise pour un Internet sécurisé pour les utilisateurs dans/hors des locaux de l'entreprise, assure la conformité à la réglementation, améliore la productivité de l'entreprise. • Une visibilité totale du trafic HTTPS.
LA TRAQUE DES MENACES	
La traque des menaces	Collecte de tous les événements bruts et détectés sur le poste, permettant des requêtes avancées, une exploration approfondie et le déplacement latéral pour une traque proactive des menaces et une enquête approfondie des incidents.

Pourquoi Harmony Endpoint ?

Aujourd'hui plus que jamais, la sécurité des postes de travail joue un rôle essentiel dans la mise en place de votre main-d'œuvre à distance. Avec 70 % des cyberattaques lancées sur les postes de travail, une protection totale des postes au plus haut niveau de sécurité est essentielle pour éviter les violations de sécurité et la compromission des données.

Harmony Endpoint est une solution complète de sécurité des postes de travail conçue pour protéger votre main-d'œuvre à distance des menaces complexes d'aujourd'hui. Elle bloque les menaces les plus imminentes pour les postes de travail telles que les logiciels rançonneurs, le phishing ou les logiciels malveillants furtifs tout en minimisant rapidement l'impact des violations grâce à une détection et à une réponse autonome.

De cette façon, votre entreprise bénéficie de la seule protection des postes de travail dont elle a besoin, de la qualité qu'elle mérite, avec une solution unique, efficace et rentable.

Harmony Endpoint fait partie de la suite de produits Check Point Harmony, la première solution de sécurité unifiée du secteur pour les utilisateurs, les appareils et l'accès. Harmony regroupe six produits pour offrir un service simple et une sécurité infaillible à tous. Elle protège les appareils et les connexions Internet contre les attaques les plus sophistiquées tout en garantissant un accès zero-trust aux applications d'entreprise, le tout en une solution unique facile à utiliser, à gérer et à acheter.

En savoir plus : https ://www.checkpoint.com/products/advanced-endpoint-protection/

Siège social mondial
5 Ha'Solelim Street, Tel Aviv 67897, Israël | Tél. : 972-3-753-4555 | Fax : 972-3-624-1100 | Email : info@checkpoint.com

Siège social aux États-Unis
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tél. : 800-429-4391 ; 650-628-2000 | Fax : 650-654-4233

www.checkpoint.com