CHECK POINT
MOBILE THREAT PREVENTION

AVANTAGES

- Déployez tout appareil mobile iOS ou Android dans le réseau de votre entreprise en toute confiance.
- Protégez les données confidentielles sur les appareils mobiles contre le cyberespionnage
- Améliorez la visibilité et la protection contre les toutes dernières menaces mobiles grâce à la sécurité mobile qui s'intègre facilement dans vos infrastructures existantes de mobilité et de sécurité (MDM, MAM, NAC, SIEM, etc.)
- Renforcez les mesures de sécurité de Microsoft Exchange et des solutions de conteneurs/enveloppes
- Réagissez rapidement aux attaques persistantes avancées multiplateformes
- Donnez accès aux données de l'entreprise en toute sécurité à vos sous-traitants à partir d'appareils non gérés
- Préservez l'expérience utilisateur et la confidentialité, tout en ajoutant le niveau de protection requis par l'entreprise ou la réglementation.

DÉTECTEZ ET STOPPEZ LES ATTAQUES AVANT QU'ELLES NE SE CONCRÉTISENT

Les smartphones et les tablettes nous donnent un accès sans précédent aux données critiques de l'entreprise dont nous avons besoin pour travailler plus rapidement et plus efficacement. Fournir à vos employés un accès aux données sur les appareils mobiles de leur choix comporte de nombreux avantages, mais augmente également le risque d'exposition de votre entreprise.

Check Point Mobile Threat Prevention est une approche novatrice de la sécurité mobile pour les appareils iOS et Android, qui détecte et bloque les menaces mobiles avant qu'elles ne se concrétisent. Que vos données soient stockées sur un appareil ou utilisées dans le Cloud, Mobile Threat Prevention vous protège contre les vulnérabilités et les attaques qui mettent les données en danger.

LE PLUS HAUT NIVEAU DE SÉCURITÉ MOBILE POUR L'ENTREPRISE

Seul Check Point fournit une solution de sécurité mobile complète qui protège les appareils contre les menaces au niveau de l'appareil (système d'exploitation), des applications et du réseau, et qui offre le taux de blocage le plus élevé du marché pour iOS et Android. Mobile Threat Prevention détecte les applications malveillante pour trouver les menaces connues et inconnues à l'aide d'une technologie d'émulation des menaces, de l'analyse avancée du code statique, de la réputation des applications et d'apprentissage machine.

Il protège les appareils des réseaux Wi-Fi® non protégés et des attaques de type homme-du-milieu, et empêche l'accès au réseau d'entreprise lorsqu'une menace est détectée. Il évalue les risques en temps réel au niveau de l'appareil (système d'exploitation) afin de réduire la surface d'attaque en détectant les attaques, les vulnérabilités, les changements de configuration, le rootage et le jailbreaking. Une réponse dynamique aux menaces empêche les appareils compromis d'accéder à votre réseau et permet aux entreprises d'implémenter des contrôles adaptatifs à partir de seuils uniques pour atténuer et éliminer les menaces sur les appareils.

Analyse avancée des applications

Vous pouvez faire confiance à vos employés pour accéder à vos actifs professionnels confidentiels, mais pouvez-vous faire confiance à leurs applications ? Notre solution détecte les applications lorsqu'elles sont téléchargées dans les appareils, et les exécute dans un environnement virtuel basé sur le Cloud pour analyser leur comportement avant de les approuver ou les signaler comme étant malveillantes. Nos rapports d'analyse exportables et faciles à comprendre aident vos équipes de sécurité à garantir que les applications utilisées sont sans danger.

18 août 2015

Attaques réseau

Les lieux publics sont remplis de réseaux Wi-Fi ouverts, ce qui rend difficile la tâche de savoir lesquels sont sûrs de ceux qui ne le sont pas. Les cybercriminels peuvent utiliser ces réseaux pour détourner les smartphones et les tablettes, et prendre le contrôle des appareils et des données précieuses telles que messages, fichiers et identifiants réseau. Notre solution détecte les conditions et les comportements réseau malveillants, et désactive automatiquement les réseaux suspects pour protéger les appareils et vos données.

Évaluations de la vulnérabilité des appareils

La force des cybercriminels est de connaître le maillon faible de votre sécurité avant vous. Cela inclut souvent des vulnérabilités dans les systèmes d'exploitation et les applications que d'autres solutions de sécurité peuvent ne pas détecter. Notre solution analyse en permanence les appareils pour découvrir les vulnérabilités et les comportements que les cybercriminels utilisent pour attaquer les appareils et dérober des données. Avec une meilleure visibilité sur les menaces auxquelles les appareils mobiles font face, vous pouvez réduire votre surface d'attaque globale et les risques.

VISIBILITÉ COMPLÈTE SUR LES MENACE MOBILES GRÂCE AUX RENSEIGNEMENTS SUR LES MENACES

Un tableau de bord dans le Cloud facilite et accélère l'administration des appareils et le contrôle des menaces mobiles. Il fournit aux équipes de sécurité et de mobilité des renseignements en temps réel sur les menaces et une visibilité quant à la quantité et les types de menaces mobiles qui pourraient avoir un impact sur leur entreprise ou leurs utilisateurs.

Intégration des renseignements dans les systèmes existants

Le flux de renseignements en temps réel sur les menaces de Mobile Threat Prevention est automatiquement fourni à Check Point SmartEvent pour surveillance des événements de sécurité et corrélation avec les attaques sur les réseaux internes. Cette information est ensuite partagée et corrélée dans Check Point Threat Cloud pour constituer la plus grande base de données de renseignements sur les menaces pouvant être utilisée dans les environnements réseau pour empêcher les cyberattaques de se produire. Les renseignements sur les menaces peuvent également être introduits dans des systèmes d'entreprise existants tels que vos plates-formes de gestion des informations de sécurité et d'événements (SIEM). Cela inclut des journaux détaillés et autres indicateurs qui peuvent être filtrés pour déclencher des interventions qui aident votre équipe de sécurité à prendre rapidement des mesures pour contrôler et éliminer les risques.

LE DÉPLOIEMENT DE LA SÉCURITÉ MOBILE N'A JAMAIS ÉTÉ AUSSI FACILE

Les équipes de sécurité et de mobilité ont déjà assez de soucis. C'est pourquoi Mobile Threat Prevention est conçu pour les aider à protéger les appareils mobiles rapidement et en toute confiance grâce à l'intégration et à la coopération avec des solutions de MDM ou d'EMM. La solution est hautement évolutive et capable de gérer la sécurité mobile au sein d'une infrastructure de sécurité plus large.

Déploiement facile d'une sécurité mobile avancée

Que vous preniez en charge 300 ou 300 000 appareils, l'intégration de notre solution avec votre solution de MDM est rapide et facile. Le déploiement et l'administration peuvent être effectués automatiquement par votre solution de MDM, pour accélérer l'adoption et réduire les coûts globaux d'exploitation. Notre solution évolue avec votre solution de MDM, protégeant parfaitement les appareils mobiles que vous ajoutez et supprimant les fonctionnalités de ceux que vous retirez. Par conséquent, vous disposez des couches de sécurité dont vous avez besoin à la fois pour gérer et protéger les appareils mobiles, même dans un environnement très dynamique.

Atténuation et élimination des menaces directement sur les appareils

Lorsqu'une menace est identifiée, notre solution atténue automatiquement tout risque jusqu'à ce que la menace soit éliminée. Si une menace peut être immédiatement éliminée sur un appareil, les utilisateurs sont informés et invités à prendre des mesures, telles que la suppression des applications malveillantes ou la déconnexion des réseaux hostiles. L'intégration avec votre solution de MDM permet à la solution de restreindre l'accès au conteneur sécurisé, ou d'effectuer des ajustements en temps réel de la politique de sécurité sur les appareils compromis, que la solution de MDM ne peut effectuer. Notre solution peut également activer un VPN à la demande pour acheminer le trafic de données hors de portée des cybercriminels, pour éviter les exfiltrations de données tout en gardant les utilisateurs connectés.

18 août 2015

Respect de la confidentialité des utilisateurs et performance des appareils

La confidentialité des utilisateurs finaux est essentielle. Nous n'analysons jamais les fichiers, les historiques des navigateurs ni les données des applications. Notre solution utilise des états et des métadonnées de contexte des systèmes d'exploitation, des applications et des réseaux afin de déterminer si un appareil est compromis. Les données utilisées sont anonymisées pendant les analyses et les renseignements de sécurité tirés sont séparés. Nos analyses sont effectuées dans le Cloud pour éviter la dégradation des performances des appareils, et la protection fonctionne en arrière-plan pour que les utilisateurs restent protégés sans avoir à apprendre quoi que ce soit de nouveau.

Pour plus d'informations, rendez-vous sur checkpoint.com/mobilesecurity.

CONTACTEZ-NOUS

Siège mondial | 5 Ha'Solelim Street, Tel Aviv 67897, Israël | Tél. : +972 3 753 4555 | Fax : +972 3 624 1100
Email : info@checkpoint.com
Siège français | 120 avenue Charles de Gaulle, 92200 Neuilly sur Seine | Tél. : +33 (0)1 55 49 12 00
Email : info_fr@checkpoint.com | www.checkpoint.com

18 août 2015