CHECK POINT

CloudGuard™ SaaS

MEILLEURE PRÉVENTION DES MENACES CIBLANT LES APPLICATIONS SaaS

Office 365 · G Suite · box · salesforce

Dropbox · servicenow · slack · EGNYTE

LE DÉFI DE LA SÉCURITÉ SaaS – LE CONTRAIRE DE CE QUE VOUS ATTENDIEZ

Les entreprises cherchant à optimiser leurs activités et réduire leurs coûts se tournent de plus en plus vers des applications dans le Cloud et des produits SaaS. Gartner affirme notamment que plus de 70 % des entreprises utilisent déjà des applications dans le Cloud.

Si les applications SaaS améliorent toutefois l'agilité des entreprises, elles les exposent également à des risques. Les applications SaaS d'entreprise sont très exposées car elles ne nécessitent qu'une connexion Internet, et sont accessibles à tous, en tout lieu. De plus, elles ne sont fournies qu'avec une sécurité par défaut insuffisante, qui permet le partage de fichiers sans restriction et la diffusion de programmes malveillants.

90 %
DES FAILLES DE SÉCURITÉ DANS LE CLOUD SONT CAUSÉES PAR DES PIRATES

Le plus gros risque lié à l'utilisation du Cloud en entreprise ne provient étonnamment pas d'un partage aveugle de données, mais de menaces externes. Celles-ci se présentent principalement sous la forme d'un accès non autorisé à des comptes d'entreprise dans le Cloud. En effet, l'équipe d'intervention de Check Point a constaté que 90 % des failles de sécurité dans le Cloud sont causées par des pirates. Plus précisément, 50 % de ces failles résultent de la prise de contrôle du compte d'un collaborateur dans le Cloud.*

* Statistiques d'interventions de Check Point en 2017

Check Point CloudGuard SaaS
MEILLEURE PRÉVENTION DES MENACES CIBLANT LES APPLICATIONS SaaS

AVANTAGES

- Bloque la diffusion des logiciels malveillants et les menaces zero-day
- Empêche la prise de contrôle des comptes dans le Cloud
- Protège le partage de fichiers et les données sensibles
- Administré depuis une console unifiée
- Assure une couverture de sécurité complète
- Visibilité totale sur les applications non sanctionnées

FONCTIONS

- Prévention des menaces zero-day
- Renseignements complets sur les menaces
- Prévention des fuites de données
- Protection des identités
- Administration simplifiée
- Recherche des applications SaaS non sanctionnées

POINTS FORTS

- Prévention primée des menaces zero-day
- Technologie unique empêchant la prise de contrôle des comptes dans le Cloud
- Architecture de sécurité Check Point Infinity

ÉLIMINATION DES MENACES DU CLOUD

Office 365 G Suite box salesforce

Dropbox servicenow slack EGNYTE

Check Point CloudGuard SaaS stoppe les attaques sur les applications SaaS d'entreprise.

Alors que la plupart des solutions de sécurité pour le Cloud se concentrent uniquement sur le contrôle des applications et les fuites de données, CloudGuard SaaS fournit une protection complète contre le détournement des comptes des collaborateurs dans le Cloud, les logiciels malveillants sophistiqués et les menaces zero-day, ainsi que le partage de données sensibles.

CloudGuard SaaS est la seule solution de sécurité adaptée aux menaces du Cloud.

CAS D'UTILISATION

- Blocage des logiciels malveillants et des menaces zero-day
- Blocage des emails de phishing dans Office365 et G Suite
- Blocage des accès non autorisés depuis des PC et des mobiles
- Blocage du partage de données sensibles
- Détection et contrôle des applications non sanctionnées
- Administration de la totalité de la sécurité via une seule console

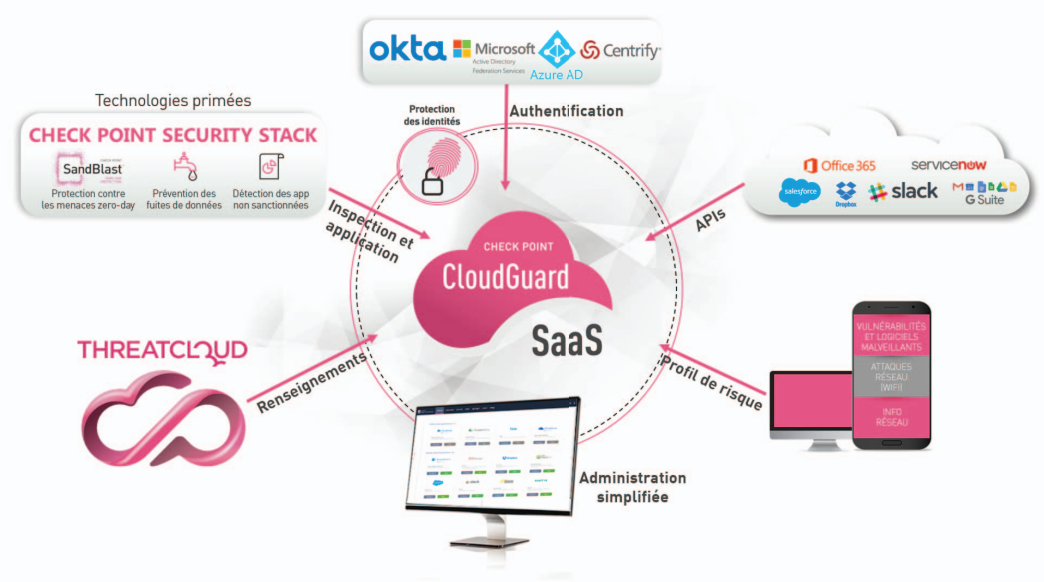
FONCTIONNEMENT DE CLOUDGUARD SAAS

Check Point CloudGuard SaaS est proposé sous forme de service dans le Cloud, qui protège les applications SaaS d'entreprise dès que son déploiement est terminé. Installé dans le Cloud, il s'intègre à différents prestataires de SaaS via des API.

Lorsqu'un utilisateur transmet un email/un fichier via une application SaaS, CloudGuard SaaS en est averti via une API. Son moteur de sécurité analyse les données à la recherche de menaces et de contenus malveillants, et détermine si elles doivent être mises en quarantaine, nettoyées, supprimées, etc.

CloudGuard SaaS utilise la totalité de la pile de sécurité de Check Point pour l'analyse des données : SandBlast pour une protection contre les menaces zero-day et la prévention des logiciels malveillants, moteur de prévention des fuites de données, détection des applications non sanctionnées. Conçu pour protéger contre les menaces réelles dans le Cloud, CloudGuard SaaS protège également les identités avec ID-GuardTM, une technologie en attente de brevet qui empêche la prise de contrôle des comptes dans le Cloud.

Les activités sont journalisées et peuvent être supervisées via une console d'administration web ou via Check Point SmartConsole. S'appuyant sur l'architecture Check Point Infinity, CloudGuard SaaS journalise les activités et consolide l'administration des politiques de sécurité pour le Cloud et sur site, et fournit une base d'informations enrichie sur les menaces pour étendre la couverture de sécurité.



EMPÊCHE LA PRISE DE CONTRÔLE DES COMPTES AVEC LA TECHNOLOGIE ID-GUARD

La **prise de contrôle des comptes** est une forme de vol d'identité dans laquelle les identifiants légitimes d'un collaborateur sont dérobés et utilisés illégalement par un cybercriminel. En usant de l'identité de l'utilisateur, le criminel est alors en mesure de mener des activités et des transactions au nom de la victime.

CloudGuard SaaS utilise la technologie ID-Guard en attente de brevet pour empêcher les utilisateurs non autorisés et les appareils compromis d'accéder à vos applications SaaS, les empêchant ainsi de s'approprier des comptes d'utilisateurs dans le Cloud. Il les intercepte à l'aide d'algorithmes d'apprentissage machine qui analysent le comportement des utilisateurs et qui sont renseignés par des sources telles que : la technologie de détection des exploitations des vulnérabilités des systèmes d'exploitation sur mobiles et PC, les attaques de logiciels malveillants et réseau, les API SaaS natives et Check Point Threat Cloud.

Protection des identités avec la technologie ID-Guard : CloudGuard SaaS Identity Protection utilise la technologie ID-Guard pour garantir un accès légitime aux applications SaaS, et empêcher la prise de contrôle des comptes des collaborateurs dans le Cloud. CloudGuard SaaS s'intègre à différents gestionnaires d'identités, tels que

Okta, Microsoft Active Directory, Azure Active Directory, etc., et ajoute une couche de sécurité à leur processus d'authentification. Chaque fois qu'un utilisateur tente d'accéder à un compte dans le Cloud, via un téléphone mobile ou un PC, CloudGuard SaaS vérifie son identité à l'aide de techniques d'analyse de l'appareil, de vérification de la connexion, de validation de la localisation de la connexion et des emails, etc. En intégrant des informations provenant de CloudGuard SaaS dans le processus d'authentification du gestionnaire d'identités, les connexions suspectes (par ex. effectuées depuis deux localisations très différentes dans un court laps de temps, mauvaise réputation IP) sont immédiatement refusées et bloquées. CloudGuard SaaS Identity Protection est transparent pour les utilisateurs et ne nécessite pas leur intervention.

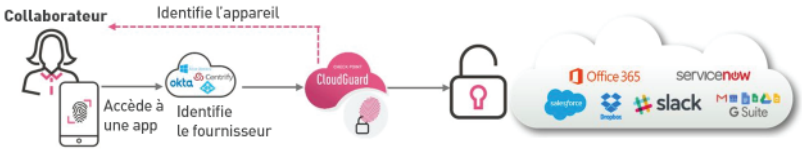
CloudGuard SaaS Identity Protection fonctionne en deux modes

1. Mode agent

ID-Guard en mode agent offre une protection robuste des identités pour toutes les applications SaaS, notamment les consoles d'administration Office365, Google Suite, Salesforce, Microsoft Azure et Amazon AWS. Il comprend un agent installé sur les postes professionnels et personnels, tels que les ordinateurs de bureau, les ordinateurs portables et les appareils mobiles, qui sécurise les connexions SaaS de manière déterministe.

Comment ? Lorsqu'un collaborateur tente d'accéder à un compte dans le Cloud, son accès est authentifié par un gestionnaire d'identités. CloudGuard SaaS évalue alors son identité : il envoie une requête à l'appareil du collaborateur pour vérifier si un agent ID-Guard est installé. Lorsqu'ID-Guard est présent, l'utilisateur et l'appareil sont autorisés à se connecter à l'application SaaS.

CloudGuard SaaS Identity Protection avec la technologie ID-Guard est transparent pour les utilisateurs et ne nécessite pas leur intervention.

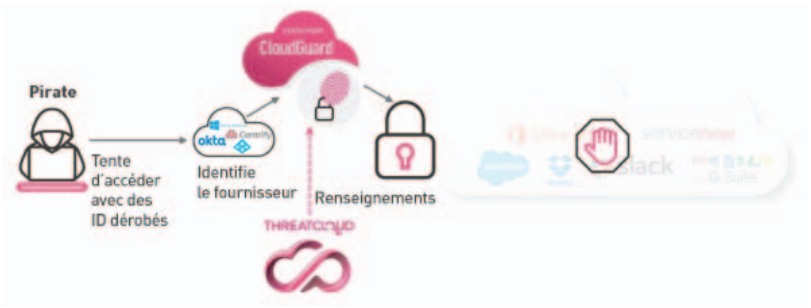


Au cas où un pirate informatique tenterait d'accéder à une application SaaS avec une identité dérobée, CloudGuard SaaS compare son identité à des connexions effectuées depuis un appareil équipé de l'agent. Si l'agent ID-Guard est absent de l'appareil, l'utilisateur n'est pas autorisé à accéder à l'application, même s'il dispose des identifiants.

2. Mode sans agent

Un mode sans agent permet à ID-Guard de fonctionner instantanément dans toute l'entreprise, sans qu'il soit nécessaire de déployer des agents sur les appareils. En plus de fournir un mécanisme d'authentification à deux facteurs par SMS, le réseau, la localisation et le type d'appareil peuvent être utilisés comme contrôles de base.

Ce mode s'appuie sur les renseignements enrichis de Check Point sur les menaces, provenant de sa base de passerelles de sécurité installées sur site, pour prendre des décisions concernant les connexions des utilisateurs aux applications SaaS. Ainsi, les « mauvais » scénarios tels que des tentatives de connexion depuis des localisations suspectes, des anomalies dans les actions des utilisateurs et une adresse IP source de mauvaise réputation, sont identifiés et les pirates ne peuvent accéder au compte dans le Cloud.



STOPPEZ LES MENACES ZERO-DAY GRÂCE À LA MEILLEURE TECHNOLOGIE

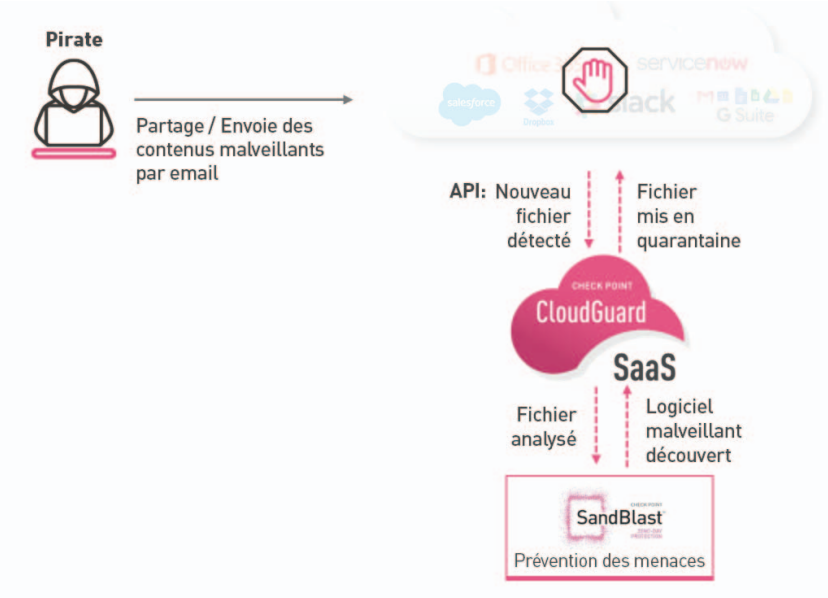
CloudGuard SaaS empêche les logiciels malveillants et les menaces zero-day d'accéder aux applications SaaS. Grâce à un simple déploiement complémentaire, CloudGuard SaaS Threat Prevention stoppe le phishing et les attaques de logiciels malveillants zero-day, protège le partage de fichiers intra-applications, met en quarantaine les emails et les fichiers malveillants, et fournit une protection multicouches.

Sa suite complète de protections pour messagerie Office365 et Gmail comprend des technologies de prévention du phishing et des logiciels malveillants qui, contrairement aux passerelles MTA et SMTP traditionnelles, utilisent des API pour s'intégrer aux fournisseurs de messagerie. Cela signifie :

1. Aucune modification du réseau n'est nécessaire
2. Les correspondances internes sont analysées pour empêcher le mouvement latéral des menaces

CloudGuard SaaS utilise la technologie primée Check Point SandBlast, qui comprend :

- L'émulation des menaces au niveau du processeur, résistante à toute tentative d'évasion, bloque les logiciels malveillants dès leur première apparition et vous protège des cybermenaces les plus avancées
- L'extraction proactive des menaces assainit les fichiers et élimine les menaces potentielles pour fournir rapidement aux utilisateurs une version saine des fichiers
- L'antivirus bloque les logiciels malveillants connus



- L'antiphishing pour les messageries dans le Cloud offre une protection avancée des emails des utilisateurs via le filtrage des URL et l'analyse des contenus

CloudGuard SaaS empêche la diffusion de logiciels malveillants, même sur des appareils non gérés, quel que soit le lieu où vos applications SaaS sont utilisées

EMPÊCHEZ LES FUITES DE DONNÉES AVEC LA PROTECTION CLOUDGUARD SAAS

CloudGuard SaaS détecte le partage de données sensibles dans le Cloud et limite immédiatement l'exposition des données. Il vous permet de rendre obligatoire l'application d'une politique de chiffrement des données, en fonction des besoins de votre entreprise.

Comment ? Lorsqu'un collaborateur partage des données via une application SaaS, CloudGuard SaaS en est informé via une API. Le fichier est analysé, et en cas de partage de données sensibles telles que des informations de carte bancaire ou des informations sur la concurrence, le partage de fichiers est bloqué ou « annulé » (par ex. dans Box, Dropbox) pour éviter les fuites de données.

Détection des applications non sanctionnées

CloudGuard SaaS étend les capacités de Check Point en matière de détection et de contrôle des applications non sanctionnées. Il détecte les applications SaaS non sanctionnées et les ajoute aux passerelles de sécurité Check Point, qui fournissent un contrôle granulaire sur les applications dans le Cloud, ainsi qu'une évaluation des risques et un contrôle sur les nouvelles applications et les applications traditionnelles.

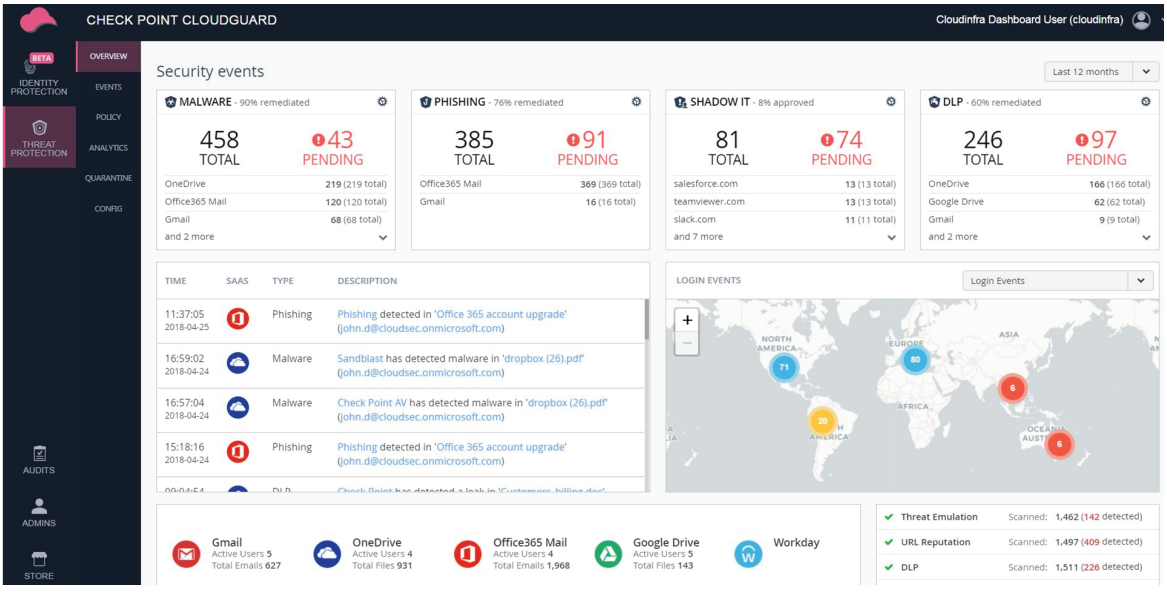
CloudGuard SaaS traite les notifications par email (par ex. « Vous avez un nouveau message de la part de Slack ») et les utilise comme validateurs supplémentaires pour détecter les applications non sanctionnées. Cette détection est disponible via l'interface utilisateur web de CloudGuard, et sera bientôt intégrée à Check Point SmartEvent.

Check Point permet ainsi aux entreprises de détecter et d'empêcher l'utilisation d'applications risquées, et de contrôler l'utilisation d'applications non sanctionnées via une politique de sécurité granulaire.

Consultez https://appwiki.checkpoint.com pour obtenir la liste complète des applications prises en charge.

COUVERTURE DE SÉCURITÉ ET ADMINISTRATION UNIFIÉE DE BOUT EN BOUT

CloudGuard SaaS fournit une couverture de sécurité complète sur l'ensemble de l'entreprise. Il s'appuie sur l'architecture Check Point Infinity et permet l'implémentation de politiques de sécurité cohérentes, et le partage de renseignements sur les menaces entre les appareils réseau, le Cloud et les mobiles. Déployé en quelques minutes, il fournit également une plate-forme d'administration simplifiée qui recherche instantanément les menaces.



CloudGuard SaaS offre à la fois une interface utilisateur web autonome et une option d'administration consolidée via Check Point SmartConsole.

Check Point SmartConsole simplifie l'administration de la sécurité avec supervision centralisée de CloudGuard SaaS :

- Le trafic est journalisé et peut être facilement visualisé dans le même tableau de bord que les passerelles de sécurité Check Point.
- Des rapports de sécurité peuvent être générés pour mesurer la conformité de la sécurité du réseau.

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