Check Point
SOFTWARE TECHNOLOGIES LTD

2021 INNOVATION

Au cours des trente dernières années, Check Point est devenu une référence en matière de cybersécurité. Notre mission ? Sécuriser tout votre environnement.

Des réseaux d'entreprise au cloud, du télétravail aux infrastructures critiques — dans un monde numérique en constante évolution, nous protégeons les entreprises contre les cybermenaces imminentes grâce à une innovation continue.

Check Point
SOFTWARE TECHNOLOGIES LTD

2021 INNOVATION

CloudGuard

SÉCURISER LE CLOUD

CloudGuard Posture Management

Plateforme SaaS qui automatise la gouvernance des actifs et services multi-cloud, notamment l'évaluation et la visualisation du niveau de sécurité, la détection des erreurs de configuration, ainsi que l'application des bonnes pratiques de sécurité et de conformité.

CloudGuard Posture Management offre une approche innovante pour visualiser l'exposition aux risques à l'aide d'un langage intuitif, lisible par l'homme. La plateforme permet d'identifier et de corriger les erreurs de configuration à n'importe quelle étape du pipeline CI/CD au moyen d'outils d'analyse IaC (Infrastructure as Code), d'outils CLI, d'API ouvertes et d'intégrations.

CloudGuard Intelligence

Solution de cyberveille cloud et de traque des menaces permettant une investigation numérique des cybermenaces native au cloud. Elle fournit un contexte en temps réel des menaces et anomalies, avec remédiation automatique et prise en charge des environnements multi-cloud — dont AWS, Azure et GCP.

CloudGuard Analytics utilise du machine learning avancé pour identifier les menaces en fonction des modèles de trafic et de productivité.

CloudGuard Workload

Solution de protection automatisée des workloads applicatifs et de tous leurs composants, compatible avec n'importe quel cloud et n'importe quel environnement.

Il s'agit de la seule solution de bout en bout pour la protection des workloads entièrement axée sur les applications — depuis les applications et les API, jusqu'aux fonctions Serverless et aux conteneurs qui les constituent.

CloudGuard Workload repose sur une approche d'autoprotection, assurant une analyse approfondie du code et des applications qui automatise la configuration et le déploiement des mesures de sécurité sur le workload lui-même.

CloudGuard Network

Solution de sécurité réseau pour les clouds publics et privés, qui offre une prévention avancée des menaces grâce à une passerelle de sécurité virtuelle, automatisée et unifiée s'appliquant à tous les environnements sur site et multi-cloud.

L'accès VPN IPSec sécurisé et évolutif pour les télétravailleurs prend en charge les infrastructures Azure et permet le télétravail en toute sécurité à une époque où celui-ci se généralise, voire s'impose en raison de la conjoncture.

Les utilisateurs AWS bénéficient d'un déploiement rapide des passerelles de sécurité en mode passif, grâce à la mise en miroir du trafic qui permet la cyber-observabilité, l'inspection approfondie des paquets, ainsi que la NDR (Network Detection and Response), sans impact sur le trafic de l'entreprise.

WAF de nouvelle génération

WAF (Web Application Firewall) de nouvelle génération assurant une protection des applications Web et des API basée sur l'intelligence artificielle. Que l'application soit hébergée dans un centre de données ou sur un cloud public/privé, le moteur de décision innovant de la solution, en attente de brevet, fournit une protection contre les attaques d'API et les risques OWASP, et bloque les bots malveillants.

Grâce à une analyse contextuelle approfondie des applications, le WAF nouvelle génération de Check Point comble la principale lacune des WAF traditionnels, à savoir un juste équilibre entre niveau de sécurité et complexité de gestion.

CloudGuard Shift Left

Solution permettant une prise en compte de la sécurité très tôt dans le processus de développement (concept du « shift-left »). Elle permet notamment d'évaluer les vulnérabilités liées aux dépendances, le contenu sensible, le code sensible, les autorisations excessives, etc. CloudGuard Shift Left détecte en continu les bibliothèques, les fichiers binaires et les modules vulnérables, et applique les méthodes recommandées pour corriger le niveau de sécurité à grande échelle.

La série d'outils Shift Left permettra à l'équipe DevOps de devenir de véritables experts en sécurité cloud. Grâce à l'outil CLI compatible DevOps, les capacités de détection et de correction de CloudGuard contribuent efficacement à la sécurité du pipeline CI/CD.

Check Point
SOFTWARE TECHNOLOGIES LTD

2021 INNOVATION

Harmony

UTILISATEURS ET ACCÈS

Accès à distance sécurisé

Service cloud qui fournit à tous les utilisateurs un accès à distance Zero Trust, sécurisé mais intuitif, à toutes les applications d'entreprise internes — qu'elles résident dans le centre de données, l'IaaS, les clouds publics ou les clouds privés. La fonction d'accès à distance sécurisé de Check Point se déploie en quelques minutes et élimine les risques associés aux accès réseau. Les utilisateurs peuvent se connecter par le biais d'une application VPN légère ou en mode sans client à partir d'un appareil BYOD via un navigateur. La solution d'accès sans client est fournie pour les services Web, RDP, SSH et SQL. Une technologie de connecteur d'application masque les applications d'entreprise derrière un cloud sécurisé, et protège le centre de données contre les attaques DDoS.

Une sécurité hautes performances

Unifie 11 services de sécurité en s'intégrant avec les solutions SD-WAN leaders du marché, assurant une sécurité rapide et efficace pour les entreprises distribuées. Les paquets sont acheminés intelligemment et inspectés rapidement, indépendamment de l'emplacement de l'utilisateur ou du site. Les collaborateurs en télétravail peuvent ainsi préserver leur productivité, où qu'ils se trouvent.

Un WAF intégrant une technologie avancée de prévention des menaces garantit la protection des applications d'entreprise.

Accès simplifié au cloud

Automatise entièrement la gestion de l'accès à privilèges (PAM, Privilege Access Management) au sein des environnements cloud dynamiques, en combinant la découverte des actifs cloud à des règles déclenchées par des balises. La gestion intégrée des clés, basée sur le cloud, fournit aux équipes ingénierie et DevOps un accès transparent et immédiat aux actifs de cloud public. Les équipes DevOps peuvent utiliser un navigateur pour accéder aux services Web, RDP, SSH et SQL.

Harmony Mobile

Solution mobile qui protège les données d'entreprise en sécurisant les appareils mobiles des collaborateurs contre les cybermenaces sur tous les vecteurs d'attaque : applications, réseau et système d'exploitation. Conçue pour réduire la charge d'administration et favoriser l'adoption par les utilisateurs, elle s'adapte aux environnements mobiles existants, se déploie et monte en charge rapidement, et protège les appareils sans affecter l'expérience ou la confidentialité de l'utilisateur.

Empêche le téléchargement d'applications malveillantes, le phishing et les attaques zero-day. Détecte les techniques avancées de débridage, l'acquisition de privilèges illicites et l'exploitation de vulnérabilités des systèmes d'exploitation. Bloque les appareils infectés par des bots. Fournit un DNS protégé pour garantir la confidentialité des utilisateurs finaux, empêche les attaques MiTM et l'usurpation DNS de messages DNS en texte brut. Utilise l'intelligence partagée sur les menaces ThreatCloud ainsi que le moteur d'analyse comportementale des risques unique de Check Point.

Harmony Endpoint

Solution avancée de protection des endpoints et de prévention des menaces pour les entreprises. Permet la traque des menaces avec une visibilité à l'échelle de tout l'environnement, complétée par des renseignements sur les menaces partagés à l'échelle mondiale à partir de centaines de millions de capteurs. Disponible sous la forme de service cloud managé ou de déploiement sur site. Pris en charge par les systèmes d'exploitation Windows, macOS et Linux.

Inclut des requêtes prédéfinies qui permettent de détecter rapidement les attaques actives, les fichiers malveillants, etc. Son tableau de bord facilite les investigations des attaques en conformité avec le cadre d'analyse MITRE ATT&CK.

Check Point
SOFTWARE TECHNOLOGIES LTD

2021 INNOVATION

Harmony

UTILISATEURS ET ACCÈS

Harmony Browse

Solution de sécurité Web permettant de protéger les télétravailleurs lors de leur navigation Internet, grâce à des technologies sophistiquées de prévention des menaces.

Harmony Browse est déployé en tant que nano-agent au sein d'un navigateur, et empêche les utilisateurs d'afficher des sites de phishing, de télécharger des logiciels malveillants et de réutiliser des mots de passe d'entreprise.

La solution est basée sur une architecture hautes performances qui accélère l'implémentation et élimine la complexité, sans impact sur la confidentialité et l'expérience utilisateur, tout en évitant l'intervention SSL. Elle permet une expérience de navigation Web normale, préserve la confidentialité de l'historique de navigation et permet aux entreprises de se conformer aux réglementations sur la confidentialité des données.

Harmony Browse renforce le niveau de sécurité lorsque la situation l'impose, soit en tant que solution de sécurité Web autonome, soit en l'associant à une solution de protection des endpoints ou passerelle Web sécurisée.

Harmony Email & Office

Protection complète d'Office 365 et de Google WorkSpace, avec une attention particulière portée à la messagerie électronique, assurée par une solution unique et économique offrant un niveau de sécurité rigoureux.

Le déploiement, effectué en un seul clic, ne prend que quelques minutes. La solution bloque efficacement les attaques BEC (Business Email Compromise) sophistiquées et élimine toutes les pièces jointes malveillantes d'e-mails zero-day.

Elle offre une couche de sécurité supplémentaire, notamment en analysant les liens à chaque clic pour s'assurer qu'aucun site Web de phishing ne soit accessible, tandis qu'un processus d'authentification renforcée innovant est appliqué pour empêcher les usurpations de compte.

Check Point
SOFTWARE TECHNOLOGIES LTD

2021 INNOVATION

Quantum

SÉCURISER LE RÉSEAU

Quantum Security Gateway

La famille de passerelles Quantum offre une sécurité supérieure à celle des pare-feux nouvelle génération, avec plus de 60 services de sécurité inclus. Ces passerelles offrent un débit allant jusqu'à 1,5 Tbps en prévention des menaces et peuvent monter en charge à la demande. La série Quantum Spark, ensemble de passerelles Quantum pour PME, offre une sécurité de niveau professionnel sans frais supplémentaires, tandis qu'une gamme de passerelles à la sécurité renforcée est destinée à la protection des systèmes de contrôle industriel.

Les passerelles Quantum Security Gateway sont uniques sur le marché : elles sont prêtes à l'emploi et fournissent le plus haut niveau de prévention des menaces, couvrant à la fois les menaces connues et inconnues. Quantum prend en charge jusqu'à 16 ports 100GbE ou 40GbE fibre, 32 ports 10GbE et 64 ports 1GbE, ce qui en fait l'appareil de sécurité réseau à la densité de ports la plus élevée du secteur.

Quantum Maestro

Solution de sécurité réseau à très grande échelle, permettant de passer d'une passerelle unique à une capacité convergente de 52 passerelles, avec une vitesse de prévention des menaces allant jusqu'à 1,5 Tbps. Les nouveaux modèles haut de gamme offrent un facteur de forme 1U économe en énergie, conçu spécifiquement pour les implémentations à très grande échelle.

Basé sur la technologie brevetée HyperSync, Quantum Maestro offre le plus haut niveau de redondance et le meilleur rapport coût-performances du marché : N+1 sans aucun point de défaillance. En outre, Quantum Maestro offre une flexibilité totale avec deux couches de virtualisation, des groupes de sécurité et des systèmes virtuels, créant une abstraction complète entre l'implémentation physique et le modèle Passerelle de sécurité.

Quantum Spark

Gamme de six passerelles de sécurité qui permettent aux PME (1 à 500 utilisateurs) de protéger leurs bureaux grâce à une solution de sécurité dédiée, conçue pour répondre à leurs besoins précis. Les passerelles protègent contre toutes les menaces, sont faciles à déployer et à gérer, et fournissent à la fois des fonctions de communication et de sécurité en un seul boîtier, avec une protection pour smartphone et ordinateur portable disponible en tant que modules complémentaires.

Les passerelles Quantum Spark sont des appareils intégrés hautes performances offrant pare-feu, VPN, antivirus, visibilité et contrôle des applications, filtrage des URL, sécurité de la messagerie électronique et protection zero-day SandBlast. Le tout dans des formats compacts simples à configurer et à gérer.

Check Point
SOFTWARE TECHNOLOGIES LTD

2021 INNOVATION

Quantum

SÉCURISER LE RÉSEAU

R81 Cyber Security Platform

Logiciel de gestion de la sécurité pour les environnements de centre de données, cloud, mobile, endpoint et IoT.

Le R81 comprend un système autonome de prévention des menaces qui permet de créer des politiques et des profils de sécurité rapidement et en toute autonomie, ainsi que de les maintenir à jour. Les politiques sont installées en quelques secondes, les mises à niveau ne nécessitent qu'une seule opération et les passerelles peuvent être mises à niveau simultanément en quelques minutes.

Quantum Smart-1 Cloud

Architecture unifiée de gestion de la sécurité qui permet de gérer les passerelles de sécurité et d'autres produits directement à partir du cloud, sans aucune installation ni maintenance. La fonctionnalité Infinity Watchtower regroupe tous les journaux d'application en une vue centralisée, offrant ainsi une visibilité sur les événements qui s'étend à toutes les ressources de l'organisation.

Les experts en sécurité bénéficient désormais de la solution de gestion centralisée de pointe de Check Point sous forme de console Web, sans perte de fonctionnalités et sans nuire à l'expérience utilisateur.

Prévention autonome des menaces

Gestion intelligente des politiques de cybersécurité à partir du cloud. Aucune maintenance des politiques et des dispositifs de protection n'est nécessaire, sans compromettre la sécurité ou la connectivité.

Les moteurs de prévention des menaces pilotés par l'IA fournissent des profils automatiquement mis à jour en fonction des besoins métier, des exigences de sécurité IT et de centaines de bonnes pratiques. Les administrateurs peuvent néanmoins toujours effectuer des modifications manuelles pour remplacer les politiques et les profils recommandés.

Les configurations des politiques de sécurité sont simplifiées sur toutes les passerelles, et gérées en interne avec des niveaux de sécurité déterminés. L'entreprise dispose d'une visibilité complète sur tous les actifs protégés.

Quantum IoT Protect

Empêche les cyberattaques ciblant l'IoT, en adaptant les protections à tous les appareils IoT ou OT dans les environnements intelligents de bureaux, de bâtiments, médicaux et industriels. Fournit une politique d'accès réseau Zero Trust adaptée à chaque appareil, exploitant des renseignements en temps réel sur les menaces, plus de 3 000 protections IPS, 60 services de sécurité innovants et une protection d'exécution sur l'appareil.

Quantum IoT Protect Manager emploie une approche de la gestion des politiques de sécurité IoT centrée sur les appareils. Les bonnes pratiques en matière de sécurité sont appliquées automatiquement aux appareils IoT dès leur découverte, en fonction de leur modèle, afin que les entreprises puissent bénéficier du plus haut niveau de sécurité IoT clé en main.

Quantum IoT Protect Nano Agent

Agent léger installé sur le firmware IoT, fournissant une protection d'exécution sur l'appareil contre les attaques zero-day. En intégrant la sécurité dans les appareils et services connectés, les fabricants peuvent garantir la protection contre les failles et vulnérabilités des firmwares, appliquer les politiques au niveau des appareils et différencier leur offre.

L'agent Quantum IoT Protect Nano Agent fournit une protection contre les injections de commandes, la corruption de mémoire et le détournement de flux de contrôle. En outre, dans le cadre de la plateforme Infinity Next, les agents offrent également un contrôle d'accès et une protection basée sur les signatures, ainsi qu'une gestion centralisée et des capacités étendues de génération de rapports.

Quantum IoT Firmware Assessment

Permet d'exécuter une analyse de sécurité automatisée pour tout firmware propre à un appareil à l'aide d'un service cloud, afin de découvrir les failles de sécurité et les corriger avant la production de masse. Le rapport généré indique les principales failles de sécurité associées à l'appareil (y compris les composants de chaîne logistique externe intégrés), ainsi que des recommandations pratiques pour atténuer les risques.

En analysant le firmware sans avoir besoin d'exposer le code source, la solution découvre les vulnérabilités potentielles, les certificats non chiffrés, les identifiants faibles et les URL avec lesquelles le firmware communique. Elle résume ensuite toutes les données dans une liste d'actions classée par ordre de priorité, prête à être exécutée.

Check Point
SOFTWARE TECHNOLOGIES LTD

2021 INNOVATION

Infinity-Vision

UNE SOLUTION UNIFIÉE

Infinity Next

Architecture de sécurité innovante fournissant une plateforme de sécurité unifiée multi-pratique et multi-organisation, utilisant une technologie distribuée Nano Agent et une sécurité fournie par le cloud. Infinity Next s'exécute sur de multiples plateformes et appareils, et permet d'établir une politique complète et unifiée pour le contrôle d'accès et la prévention des menaces.

Grâce à la technologie de sécurité Nano Agent, l'utilisateur peut sécuriser les workloads cloud, les appareils IoT, les appareils utilisateur et les contrôles de sécurité natifs. Les services de sécurité unifiés fournis par le cloud permettent aux composants Nano Agent d'assurer une protection optimale.

Infinity Portal

Portail Web central pour gérer tous les produits Check Point, y compris les passerelles, Harmony Endpoint et Mobile, la famille de solutions CloudGuard, Quantum IoT Protect, SASE et Infinity Vision SOC.

Toutes les fonctions de gestion de la sécurité sont rassemblées en un portail unique, ce qui permet aux utilisateurs de réduire considérablement le temps consacré à gérer leurs différentes solutions de sécurité.

Infinity Vision SOC

Plateforme cloud qui permet aux analystes SOC d'exposer, d'investiguer et de bloquer les attaques plus rapidement, à l'intérieur et à l'extérieur du réseau d'entreprise. Expose les attaques furtives et procure des informations complémentaires sur les menaces, ainsi que des données de recherche uniques, directement issues de Check Point Research et ThreatCloud. Check Point Research utilise par ailleurs cette plateforme dans son travail quotidien.

La plateforme offre une solution révolutionnaire de détection d'incidents sans journal et basée sur l'IA, qui expose et corrige les menaces rapidement, avec une précision sans précédent, sur le réseau, le cloud, les endpoints, les appareils mobiles et l'IoT.

SandBlast

Fournit une protection de pointe contre les attaques zero-day, en associant l'émulation des menaces résistant aux tactiques de contournement, des moteurs d'IA révolutionnaires et l'extraction des menaces.

Emploie de nombreuses technologies exclusives et innovantes, y compris des mesures de protection préventives pour les utilisateurs, un vaste réseau de renseignements actualisés sur les menaces, ainsi que des moteurs révolutionnaires d'IA et non-IA. Préserve la continuité des activités tandis que l'émulation des menaces se poursuit en arrière-plan.

Extraction rapide des menaces Web

La solution permet une livraison ultra-rapide des téléchargements Web assainis. Elle protège les utilisateurs contre les logiciels malveillants zero-day, sans affecter leur productivité et sans faux positifs. L'extraction rapide des menaces Web peut être fournie en ligne à partir d'une passerelle de sécurité, ou en intégrant cette capacité à un proxy tiers.

Il s'agit de la seule extraction des menaces traitant à la fois le Web et les e-mails. Les fichiers nettoyés sont livrés en moins de 1,5 seconde, y compris l'accès autorestauré aux fichiers originaux.