CHECK POINT

Plateforme de protection des applications natives du cloud

La meilleure solution de sécurité pour le cloud devient encore plus intelligente

Le cloud a révolutionné le mode de travail des équipes de développement, et les équipes de sécurité s'efforcent de tenir la cadence en termes de rapidité et de volume. Alors que le nombre d'actifs distribués augmente de manière exponentielle, le rythme des changements, lui, ne cesse d'accélérer, et les différentes équipes ont parfois du mal à s'adapter aux consignes de sécurité requises tout au long du processus de développement. Les équipes de sécurité sont donc incapables de maitriser les risques dans leur environnement cloud et d'agir rapidement face aux alertes les plus critiques.

Les entreprises ont besoin d'informations exploitables pour corriger les problèmes de façon pragmatique. Malheureusement, la plupart des solutions CNAPP disponibles sur le marché n'offrent pas les informations nécessaires sur l'ensemble des workloads pour pouvoir mettre en œuvre les mesures de sécurité requises à la vitesse et à l'échelle du cloud.

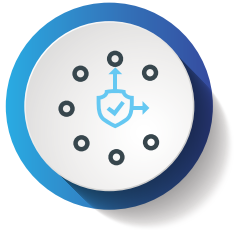
L'environnement cloud actuel a besoin de plus de contexte pour se protéger de manière plus intelligente et plus rapide.

Contexte enrichi Informations exploitables Prévention plus intelligente

Du code au cloud, la CNAPP CloudGuard de Check Point unifie la sécurité du cloud, en regroupant des données de sécurité avancées pour hiérarchiser les risques et prévenir les attaques critiques, offrant ainsi plus de contexte, des informations de sécurité réellement exploitables et une prévention plus intelligente.
CloudGuard améliore la visibilité en fournissant des informations approfondies et des recommandations utiles pour que vos équipes cloud puissent cerner et corriger plus rapidement toutes les menaces.

Contexte enrichi

Du code au cloud, bénéficiez d'une meilleure visibilité sur les configurations, les identités, les vulnérabilités et l'exposition du réseau aux menaces avec une surveillance de la sécurité en temps réel.



Informations exploitables

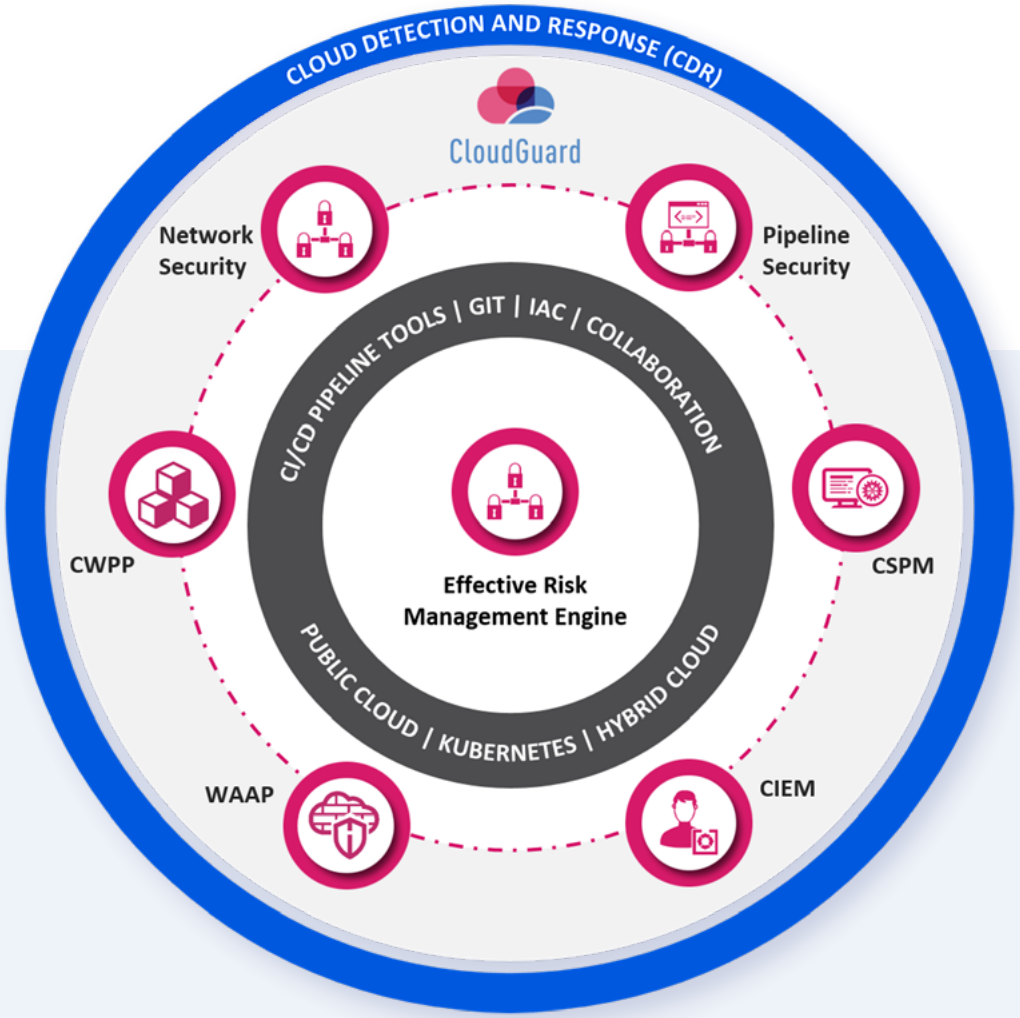
Hiérarchisez intelligemment les risques critiques en analysant le contexte de chaque élément pour vous concentrer sur les menaces réellement importantes.

Prévention plus intelligente

Prévenez les risques tôt dans le pipeline de développement ou neutralisez-les en production tout en fournissant des recommandations exploitables pour corriger les erreurs de configuration et d'autorisation.

« Check Point nous permet d'optimiser notre cybersécurité avec un niveau d'investissement fixe. Nous ajoutons simplement de nouvelles fonctionnalités quand nous en avons besoin. La flexibilité unique de Check Point nous offre l'agilité nécessaire pour développer notre activité tout en continuant d'offrir nos services à nos clients et partenaires. »

—Brian Chan, DSI, Jebsen Group



Tirez parti de nos technologies de pointe pour la sécurité du pipeline, la gestion de la posture de sécurité dans le cloud (CSPM), la gestion des identités et des droits dans le cloud (CIEM), la protection des workloads cloud (CWPP), la protection des applications Web et API (WAAP) et la détection et la réponse dans le cloud (CDR), toutes intégrées dans un moteur de gestion des risques (ERM) optimisé par IA pour créer une expérience unifiée et un centre décisionnel unique.

La CNAPP CloudGuard fournit aux clients des informations de sécurité exploitables couvrant les clouds publics, les workloads, les identités et les applications pendant l'intégralité du cycle de développement, du code jusqu'au cloud. CloudGuard fournit une expérience harmonieuse aux équipes agiles, qui peuvent compter sur des déploiements sans agent et des intégrations homogènes pour obtenir des informations de sécurité exploitables du build jusqu'au runtime.

- **Nouveau** Obtenez une visibilité totale sur la sécurité des workloads, sans agents
- **Nouveau** Comprenez vos autorisations et appliquez le principe du moindre privilège sur tous vos clouds
- **Nouveau** Utilisez votre CNAPP pour sécuriser vos applications cloud dès le départ
- **Nouveau** Focalisez-vous sur les 1 % de risques cruciaux grâce à la sécurité du cloud mise en contexte

Gestion améliorée de la posture de sécurité dans le cloud

Une meilleure compréhension grâce aux informations sur les workloads et les utilisateurs cloud

L'un des grands avantages du cloud computing est sa capacité à collecter des données télémétriques à partir de sources très variées. Le monitoring, la collecte de renseignements et d'autres sources de données fournissent une mine d'informations pour protéger vos applications. Mais le principal problème n'est plus l'extraction des données : l'enjeu est d'établir une visibilité à 100 %, de créer des synergies, de mettre fin aux problèmes de fragmentation et de comprendre la posture de sécurité dans son contexte pour prendre les bonnes décisions. Check Point CloudGuard combine le contexte des workloads et celui des activités utilisateur pour fournir des informations de sécurité plus approfondies.

Obtenez plus de visibilité et restez conforme grâce au CSPM

Tirez parti d'une plateforme unifiée pour visualiser et évaluer votre posture de sécurité, détecter les erreurs de configuration, modéliser et appliquer les meilleures politiques, vous protéger contre les attaques extérieures et les menaces internes tout en vous conformant aux exigences réglementaires et aux bonnes pratiques du secteur. Avec CloudGuard, la sécurité du cloud est plus rapide et plus efficace, la conformité et la gouvernance sont plus faciles et les opérations DevSecOps sont totalement fluides.

Visibilité complète sur la sécurité des workloads, sans agent et à n'importe quelle échelle

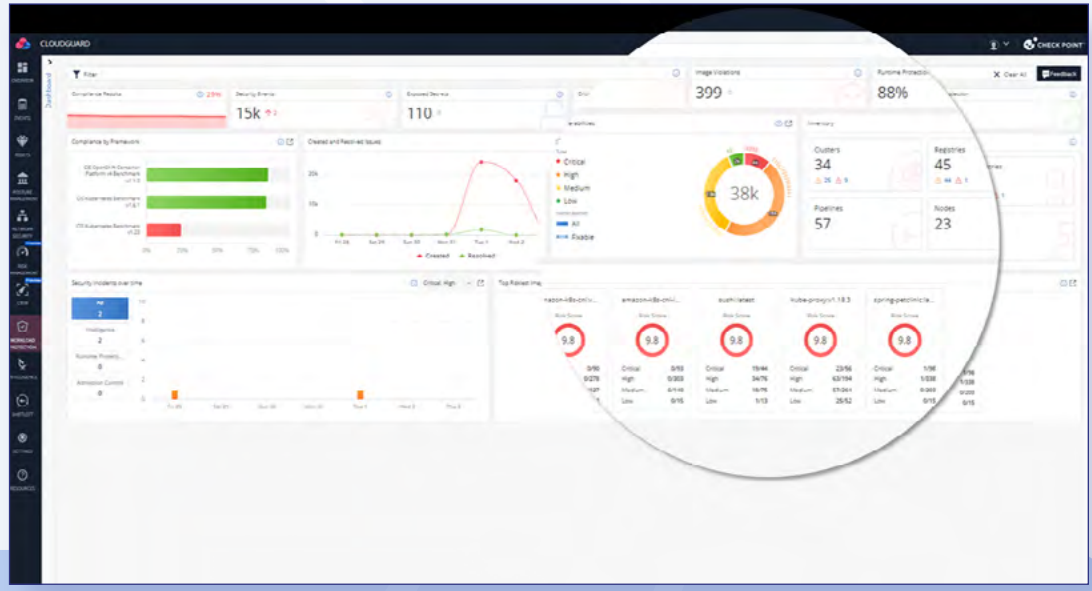
Ne comptez pas sur d'autres équipes pour déployer des services de sécurité : obtenez une visibilité totale grâce à des déploiements sans agent et comprenez ce qui passe sur vos workloads cloud.

Agentless Workload Posture (AWP) étend la visibilité sur l'infra-structure sans agent de CloudGuard sur tous les workloads. AWP scanne et identifie les risques : mauvaises configuration, détection des logiciels malveillants, vulnérabilités et secrets cachés dans tous vos workloads cloud, y compris les machines virtuelles, les conteneurs et les fonctions sans serveur :

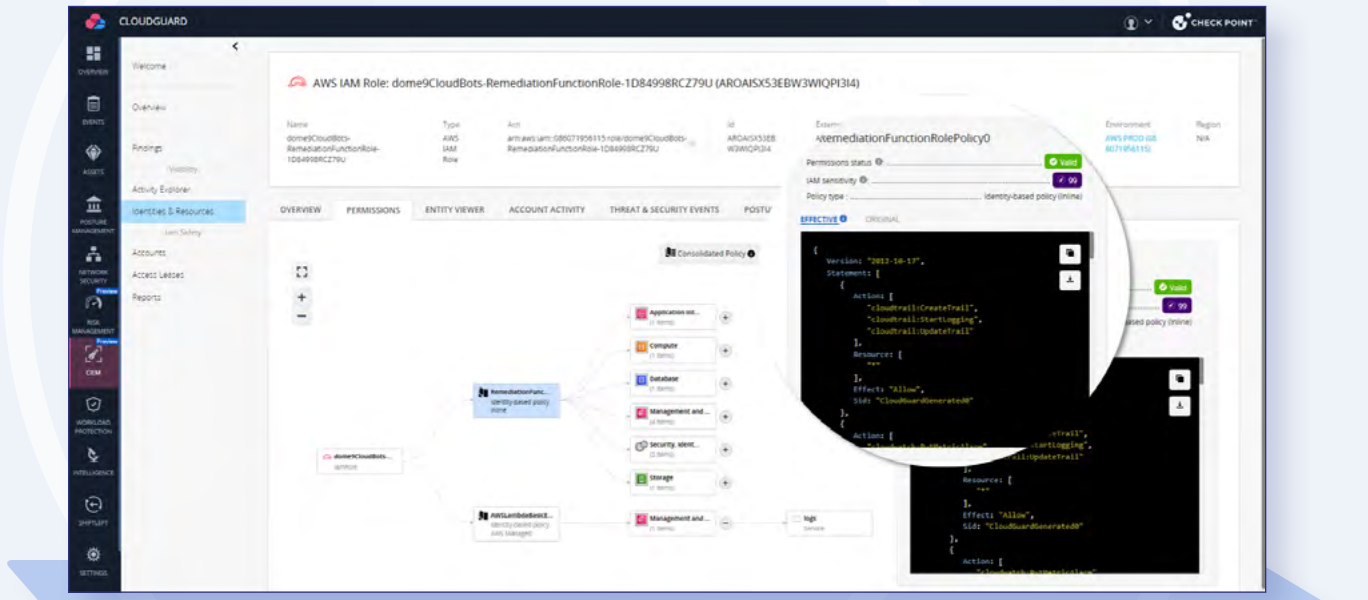
- Visibilité immédiate sur tous les workloads : VM, conteneurs, fonctions sans serveur à n'importe quelle échelle

  Détection et alertes sur les risques : erreurs de configuration, logiciels malveillants, vulnérabilités et secrets

- Les données AWP alimentent le moteur de risque contextuel (ERM) de CloudGuard et les plateformes XDR.



Comprenez vos autorisations et appliquez le principe du moindre privilège dans tous vos clouds avec Infrastructure Entitlement Management (CIEM)



Dans l'environnement cloud complexe d'aujourd'hui, vous devez vous assurer d'optimiser l'accès des utilisateurs et l'accès aux workloads en accordant uniquement les autorisations nécessaires et en rectifiant rapidement les autorisations trop laxistes.

La fonctionnalité CIEM de Check Point CloudGuard vous offre une visibilité complète sur toutes les autorisations pour identifier celles qui ne sont pas justifiées. CloudGuard identifie rapidement les risques et l'exposition pour générer automatiquement des recommandations sur les rôles nécessitant peu de privilèges pour réduire les accès et révoquer les autorisations non utilisées afin d'atteindre une sécurité zero-trust.

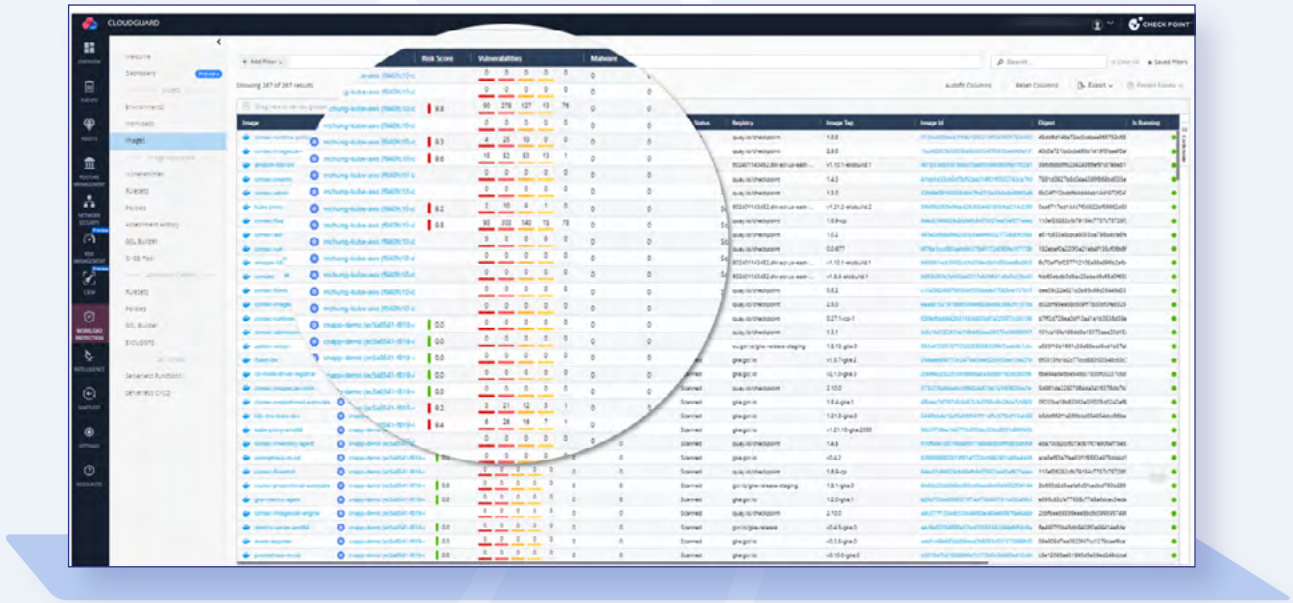
- Visualisez les autorisations accordées aux utilisateurs et aux services cloud
- Détectez les rôles inutiles, et les autorisations trop laxistes qui peuvent vous mettre en danger
- Générez automatiquement des recommandations sur les rôles nécessitant peu de privilèges en fonction de l'utilisation réelle

Protection du runtime pour vos workloads cloud (CWPP)

CloudGuard fournit une protection native du cloud et entièrement automatisée pour vos workloads. Il offre une visibilité unifiée, la conformité et la prévention des menaces pour les applications, API et microservices (conteneurs Kubernetes et fonctions sans serveur), du développement au runtime. Protégez vos workloads pendant le runtime et établissez des profils de comportement pour les fonctions, les conteneurs et les applications. Grâce à son analyse des signatures de comportement, CloudGuard vous permet de bloquer les activités malveillantes et de mettre facilement en place des politiques et mécanismes de sécurité avec contrôle des admissions sur vos clusters Kubernetes.

CloudGuard unifie la protection des workloads en fournissant une visibilité, des contrôles de sécurité et un scan complet de vos workloads cloud, de la première ligne de code jusqu'à l'environnement de production.

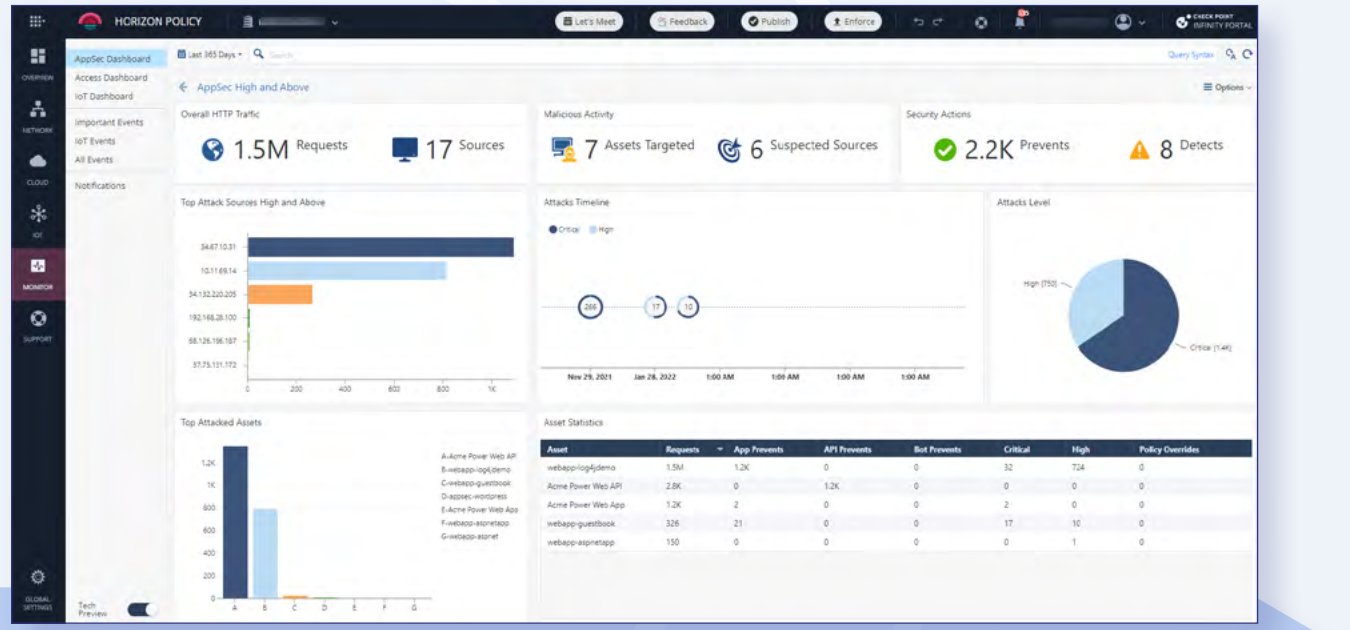
- Sécurité zero-trust pour toutes vos applications, API, Kubernetes et fonctions sans serveur
- Auto-déploiement et application des contrôles de sécurité
- Protection des déploiements hybrides et multi-clouds indépendante de l'architecture et des fournisseurs cloud



Protection des applications Web et des API (WAAP) basée sur le contexte

Paradigme révolutionnaire pour la sécurité des applications, CloudGuard remplace les pare-feu pour applications Web qui ne fonctionnent que si l'on consacre des ressources excessives pour les maintenir.

Avec CloudGuard, chaque requête entrante est analysée dans son contexte. Le moteur d'IA en attente de brevet effectue une analyse des risques en examinant le profil d'un utilisateur, les tendances repérées durant sa session, et la manière dont les autres utilisateurs interagissent avec l'application. Le score attribué à chaque requête détermine sa probabilité d'être malveillante. Le moteur s'adapte automatiquement aux changements de l'application en établissant en continu un profil de l'utilisateur, de l'application et du contenu.



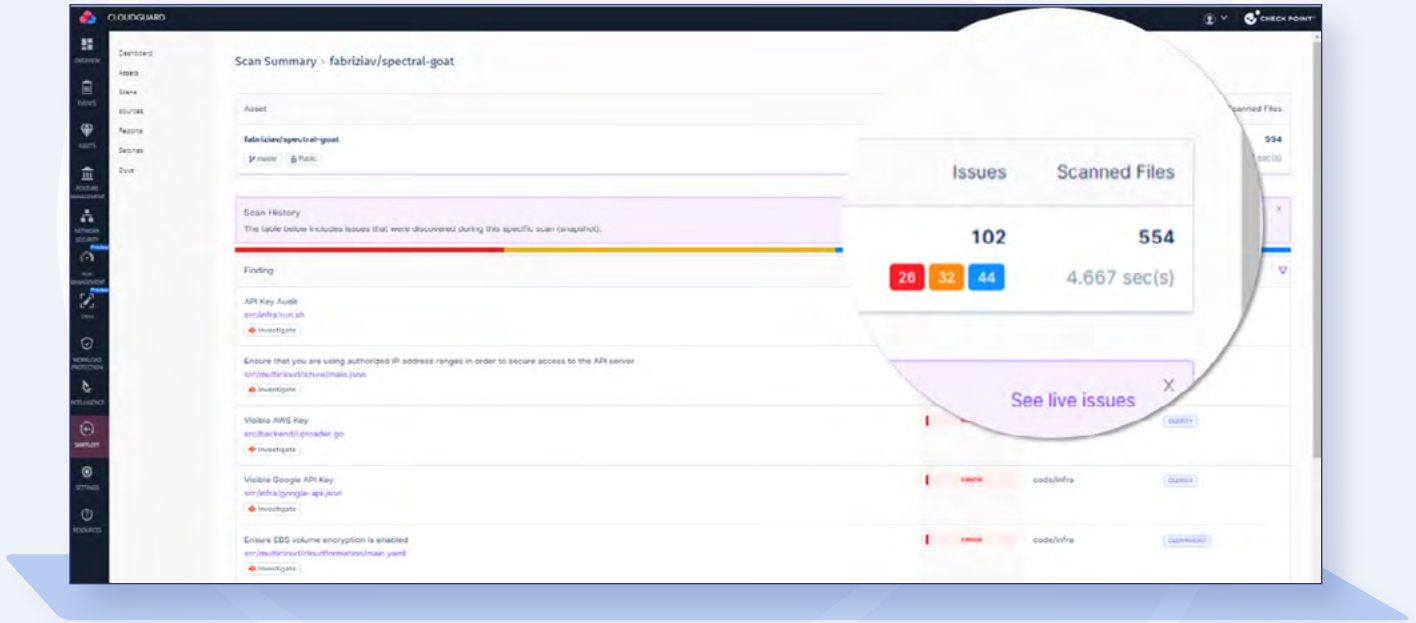
Cette approche permet d'éliminer les faux positifs tout en maintenant les normes les plus élevées en termes de sécurité des applications.

Avec un passage du déploiement à la protection en quelques heures, vous pouvez maintenir la sécurité de vos applications grâce à cette solution aussi rapide que la meilleure des équipes DevOps.

Stoppez les attaques contre vos applications : défiguration de site Web, fuite d'informations, vol numérique et piratage de session utilisateur.

Utilisez la CNAPP pour protéger vos applications dès le début de votre pipeline de développement/intégration continu(e).

Étant donné que les applications sont développées de plus en plus vite, elles contiennent souvent des secrets codés en dur ou des vulnérabilités négligées, qui se retrouvent trop souvent dans les environnements de production. CloudGuard empêche ces failles d'arriver en production et utilise la CNAPP pour optimiser la protection de votre application au moment de sa création. CloudGuard vous permet d'appliquer des politiques de sécurité durant tout le cycle du développement logiciel sans mettre de bâtons dans les roues des développeurs.



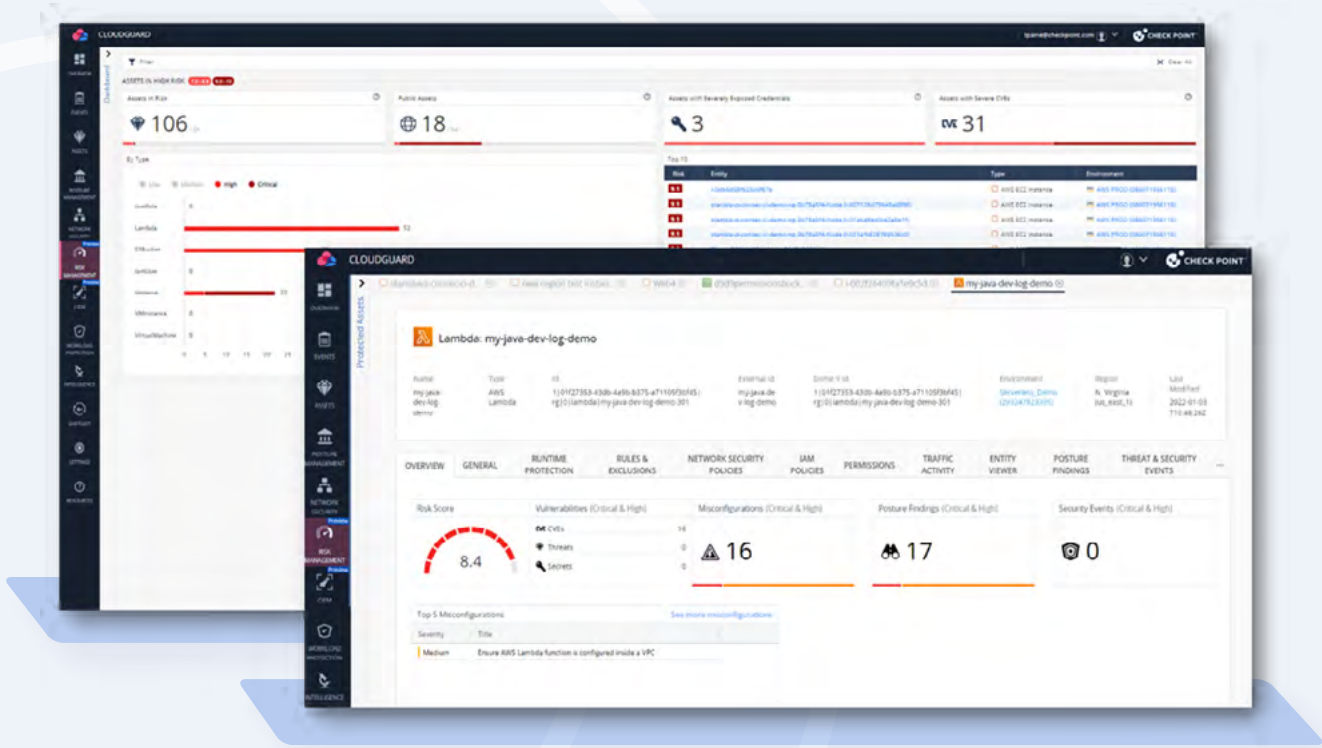
La fonctionnalité shift-left de CloudGuard s'intègre de façon fluide dans le pipeline CI/CD pour scanner le code, automatiser la protection, détecter les logiciels malveillants et éliminer les angles morts.

- Donnez à vos développeurs la possibilité de corriger les vulnérabilités, les erreurs de configuration et les secrets exposés avant le déploiement du code
- Identifiez et corrigez les risques des outils de votre pipeline de développement (Git, Jenkins et bien d'autres)
- Protégez les workloads dans l'intégralité du pipeline CI/CD pour corriger les problèmes avant la mise en production.

Concentrez-vous sur le 1 % de risques cruciaux et corrigez les problèmes plus rapidement grâce à une gestion efficace des risques (ERM).

Pour ne pas être submergé par les alertes de sécurité, il faut agir intelligemment, pas travailler plus dur. Le moteur ERM de CloudGuard hiérarchise les risques et fournit des recommandations exploitables basées sur le contexte global : posture de sécurité, exposition du réseau, autorisations et identités, analyses des chemins d'attaque et valeur commerciale de l'application.

Agissez rapidement en vous concentrant sur les 1 % de risques les plus critiques pour votre entreprise et en automatisant la sécurité dans l'ensemble de votre environnement, avec les recommandations exploitables d'un moteur contextuel qui utilise l'IA et l'évaluation des risques pour réduire la surface d'attaque.



- Hiérarchisation des risques en fonction du contexte intégral : risques de configuration, posture du workload, exposition du réseau, autorisations, chemins d'attaque, priorités commerciales
- Focalisation sur les menaces réelles pour les clouds, les workloads et le code
- Mesures correctives optimisées, basées sur la solution la plus rapide pour atténuer le risque

Prévenez les menaces de manière proactive grâce à une solution de détection et de réponse pour le cloud

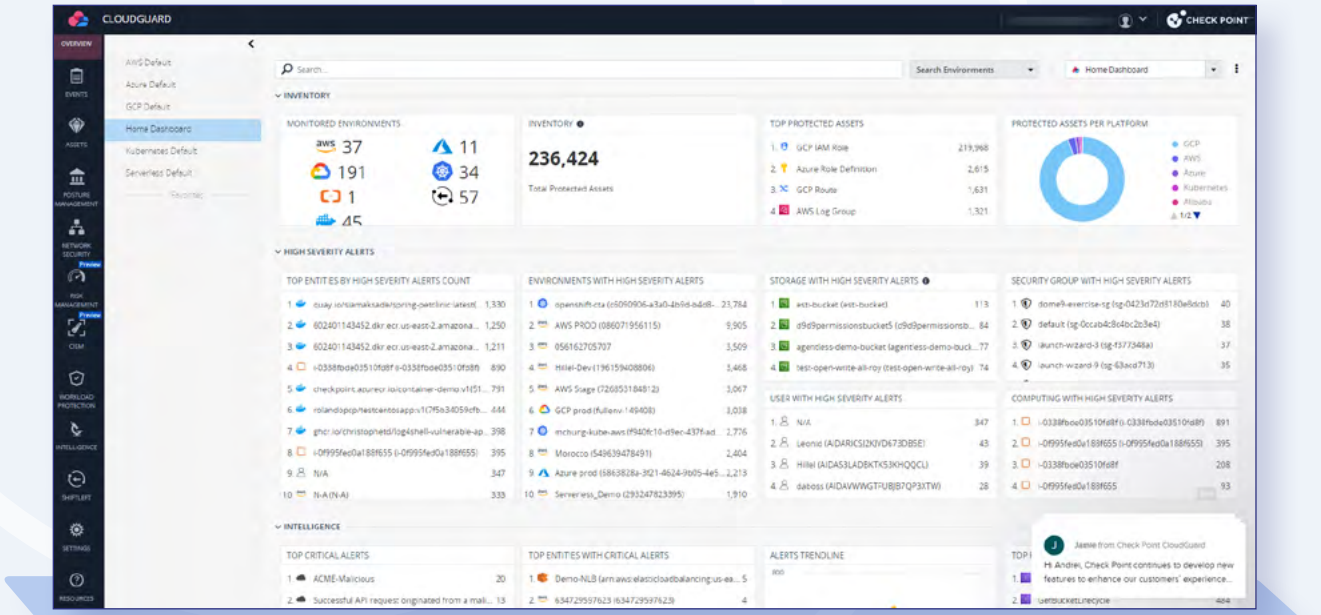
Améliorez les découvertes avec CloudGuard pour perfectionner la traque et la correction des menaces. En intégrant les informations des référentiels et configurations cloud, des activités de comptes, des journaux réseau, et des données sur les menaces telles que ThreatCloud et les bases de données sur la réputation des IP de Check Point, CloudGuard fournit un tableau exhaustif et précis pour les équipes SecOps et SOC.

Avec cette couche de renseignements supplémentaire, vous pouvez :

- Prévenir les failles de sécurité et empêcher les activités non autorisées avant que les vulnérabilités ne puissent être exploitées. Tirant parti de l'IA et de l'analyse du comportement des utilisateurs (UEBA), CloudGuard analyse en permanence l'activité des comptes et surveille le trafic réseau pour détecter les anomalies et les cybermenaces.

- Recevoir des alertes automatisées en cas de violations des règles. Les règles pré-intégrées incluent les bonnes pratiques du secteur, les dernières recherches en matière de cybersécurité, le framework MITRE ATT&CK et bien plus encore.

- Transformer ces données enrichies en informations exploitables ! Récupérez les données historiques et effectuez une analyse poussée des incidents pour prendre des décisions basées sur les données.



- Utiliser un outil d'exploration visuel qui interprète les journaux du trafic réseau et de l'activité des comptes pour fournir des informations contextuelles enrichies.

CloudGuard fournit des outils pour filtrer les faux positifs, accélérer le tri et simplifier l'analyse des incidents. L'équipe d'experts de Check Point, reconnue dans le monde entier, ne cesse d'étendre et d'améliorer les alertes. De plus, grâce à la technologie CloudBots, vous pouvez annuler automatiquement les changements de configuration risqués et créer des réponses pour n'importe alerte réseau ou élément de piste d'audit dans l'ensemble de votre environnement.

CloudGuard
CNAPP

« La CNAPP CloudGuard de Check Point fournit une **approche de pointe et très complète pour la sécurité du cloud et des DevOps**. Et surtout, nous pouvons désormais gérer tout notre environnement à partir d'un seul endroit, au lieu de jongler avec plusieurs consoles de gestion pour différents composants. »

—Mark Nix, Responsable national, Sécurité de l'information, Risques et Gouvernance

Contexte enrichi, informations exploitables et prévention plus intelligente avec CloudGuard

Du code au cloud, Check Point CloudGuard fournit une sécurité native du cloud, automatisée et unifiée pour vos applications, vos workloads et votre réseau, vous permettant de gérer les risques et prévenir les menaces en contexte, à la vitesse et à l'échelle du cloud. Axée sur la prévention, l'approche de CloudGuard protège les applications et les workloads tout au long du cycle de développement logiciel et comprend un moteur de gestion efficace des risques, avec une hiérarchisation automatisée des mesures correctives pour permettre aux utilisateurs de se concentrer sur les risques de sécurité qui comptent vraiment. Pour plus d'informations sur CloudGuard, visitezwww.checkpoint.com/cloudguard

Siège mondial
5 Shlomo Kaplan Street, Tel-Aviv 6 789 159, Israël | Tél.: +972-3-753-4599

Siège États-Unis
959 Skyway Road, Suite 300, San Carlos, CA 94 070 | Tel: 1-800-429-4391

www.checkpoint.com