Forcepoint

Présentation succincte

Forcepoint Next Generation Firewall avec Amazon Web Services

Le firewall d'entreprise le plus sécurisé et le plus efficace du marché – géré de manière centralisée, toujours actif et inlassable.

Le défi

- Les entreprises et les organisations doivent maintenir le même niveau de sécurité sur leurs environnements cloud et hybrides qu'avec leurs infrastructures traditionnelles sur site.
- Construire et maintenir une infrastructure hybride ou cloud sécurisée peut s'avérer coûteux et pose un défi technique.
- Le respect de la conformité réglementaire peut être difficile à gérer et prendre du temps.

La Solution

- Les solutions logicielles Firewall nouvelle génération (NGFW) de Forcepoint sont conçues pour offrir une sécurité maximale pour un coût et une complexité minimes.
- Le Centre de gestion de la sécurité Forcepoint NGFW (SMC) est une plateforme unifiée qui rationalise les processus et offre visibilité et contrôle.
- Forcepoint NGFW SMC permet aux administrateurs TI de rationaliser les efforts de conformité sur les réseaux virtuels et physiques, notamment en facilitant l'accès pour les rapports d'audit.

Résultat

- Une sécurité maximale dans les systèmes cloud et hybrides avec un minimum de complexité.
- Intervention plus rapide en cas d'incident
- Simplification de la conformité, de la mise en œuvre et de la gestion de la conformité aux réglementations
- Réduction des coûts d'infrastructure et de sécurisation du réseau.

Forcepoint Next Generation Firewall (NGFW) connecte et protège les personnes, et les données qu'elles utilisent, sur l'ensemble du réseau d'entreprise hybride ou cloud – avec un maximum d'efficacité, de disponibilité et de sécurité. Après avoir gagné la confiance de milliers de clients dans le monde entier, les solutions de sécurité réseau de Forcepoint sont maintenant disponibles sur le marketplace AWS. Ces solutions permettent aux entreprises et aux organisations d'aborder les problèmes critiques de manière efficace et économique.

Forcepoint Security pour les environnements de cloud public

Les services basés dans le cloud et les déploiements virtuels transforment les entreprises de toutes les formes et de toutes les tailles. Le matériel traditionnel sur site disparaît rapidement, parce que les entreprises ont besoin d'une plus grande efficacité, d'une plus grande souplesse et d'un meilleur contrôle des coûts sans avoir de contraintes de maintenance ou de frais généraux, afin de garder leur compétitivité. L'adoption généralisée des architectures infonuagiques impose aux professionnels de la sécurité et aux responsables informatiques la pression de s'assurer que ces nouveaux environnements soient tout aussi sécurisés que leurs prédécesseurs physiques.

Les solutions logicielles Firewall nouvelle génération (NGFW) de Forcepoint sont conçues pour offrir une sécurité maximale pour un coût et une complexité réduits. Le centre de gestion de la sécurité (SMC) Forcepoint NGFW est une plateforme unifiée qui vous offre une visibilité et un contrôle inégalés, ainsi qu'une application cohérente des politiques, afin de garantir la conformité réglementaire dans les infrastructures physiques comme dans les environnements virtuels et cloud.

AWS Sécurité Cloud

Pour sécuriser les environnements cloud, Forcepoint apporte à AWS une technologie firewall de pointe, nouvelle génération, avec une évolutivité, une efficacité opérationnelle et une sécurité très robustes. Étendez facilement et en toute sécurité le réseau de votre entreprise – des centres de données et de la périphérie du réseau à vos succursales et sites distants - à votre environnement de cloud AWS via une passerelle VPN (Virtual Private Network) sécurisée. Notre gestion centralisée vous permet de créer et de déployer des politiques rapidement et de manière cohérente sur l'ensemble de vos systèmes. Vous pouvez rapidement et précisément repérer ce qui se passe à la fois dans votre environnement AWS et dans votre réseau physique.

Les clients qui passent à Forcepoint NGFW font état d'une baisse de 86 % des cyberattaques, d'une diminution de 53 % du temps de travail de l'équipe TI et d'une diminution de 70 % de la maintenance planifiée.

Sécurité maximum – Complexité minimum

L'architecture logicielle des solutions de sécurité de Forcepoint, telles que la protection contre les menaces avancées, l'inspection approfondie des paquets et le contrôle au niveau des applications, est conçue pour être déployée facilement, afin de garantir une sécurité maximale sans toute la complexité et les coûts supplémentaires. La plateforme de sécurité logicielle de Forcepoint offre une protection complète et intégrée, avec une défense en profondeur qui peut être adaptée aux besoins spécifiques de chaque personne, lieu ou bien, incluant un firewall, un VPN, un IPS et une protection par filtrage d'URL. Cette plateforme logicielle offre toutes les fonctionnalités existantes des appareils matériels, notamment l'inspection dynamique, la politique granulaire et le contrôle d'accès, ainsi que les connexions ISP redondantes, mais sans nécessiter de boîtier.

Une visibilité et un contrôle en temps réel

Forcepoint NGFW offre une visibilité et un contrôle complets sur le flux de trafic au sein de l'environnement virtuel, ainsi que dans l'environnement cloud – ce que les consoles de gestion traditionnelles ne peuvent pas faire. Le SMC fournit des rapports immédiats sur la quantité de trafic passant entre les systèmes virtuels et alerte les administrateurs si un système est sur le point de tomber en panne. Gérez n'importe quel nombre ou combinaison d'appareils ou de clusters Forcepoint physiques ou virtuels, ainsi que des versions logicielles exécutées selon du matériel x86 standard. Le SMC renforce également la sécurité des systèmes virtuels grâce à un tableau de bord holistique de surveillance, qui offre une visibilité complète des applications et un contrôle granulaire.

Simplifiez la mise en conformité réglementaire

Il est difficile de se conformer aux dernières exigences réglementaires telles que PCI DSS, HIPAA, Sarbanes-Oxley et FISMA dans le monde physique, mais il est encore plus difficile de le faire dans l'espace virtuel. Les contrôles traditionnels autour de chaque application ne sont pas présents dans un environnement virtuel. Il est donc pratiquement impossible de déterminer quelles informations ont été consultées, qui les a lues, et à quel moment, et cela risque d'alerter les auditeurs. Le SMC vous offre le niveau de surveillance, d'analyse et de rapport dont vous avez besoin pour garantir la conformité des réseaux virtuels et physiques. Il recueille des données complètes sur tous les événements du réseau et les présente dans des journaux d'audit clairs et faciles à lire. Le SMC répertorie également les paramètres de sécurité, signale les modifications apportées au système et fournit les rapports d'audit précis dont vous avez besoin, sur simple appui d'un bouton.

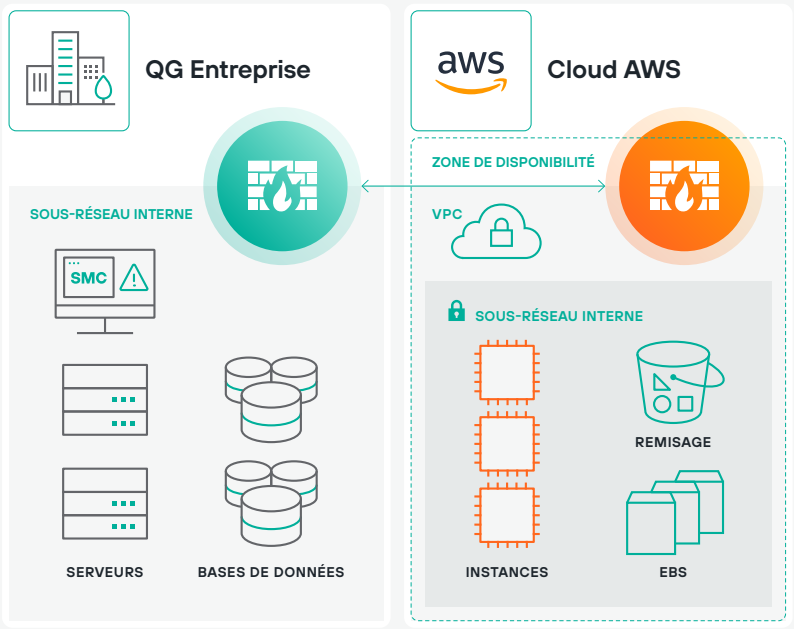
Déploiement rapide et élastique

Pour déployer rapidement la sécurité logicielle d'architecture Forcepoint dans votre environnement AWS, il suffit de choisir l'une des options disponibles sur le marketplace AWS.

→ Aller sur le Marketplace

Solutions Forcepoint NGFW + AWS

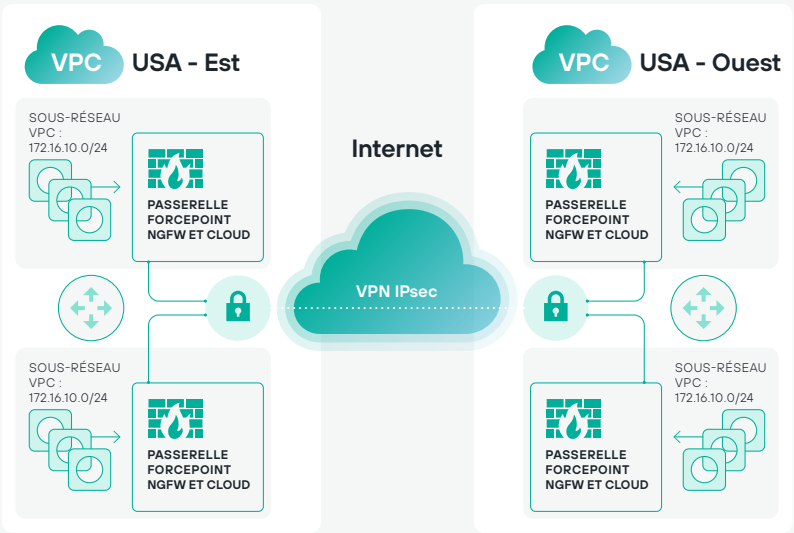
Sécurisez les réseaux d'entreprise et exploitez la puissance d'AWS avec Forcepoint NGFW.



Étendez les réseaux d'entreprise vers les environnements AWS

Forcepoint NGFW applique des politiques de prévention des menaces spécifiques aux applications pour stopper les failles de sécurité, les malwares et les vulnérabilités de type « zero-day » qui tentent d'exfiltrer des données à partir des environnements AWS d'une entreprise. AWS Security Hub vous donne une visibilité centralisée de toutes les actions et conditions qui ont déclenché les alertes d'application de politique.

- → Étendre le réseau de votre entreprise vers AWS
- → Déployez efficacement l'informatique hybride et simplifiez le transfert de données vers et depuis AWS.
- → Gérez facilement les deux extrémités de plusieurs connexions VPN depuis un seul endroit.



Redirection Inter-régions VPC-to-VPC

Connectez les VPC entre plusieurs régions AWS en toute sécurité. Vous pouvez gérer, contrôler et appliquer des politiques de sécurité à l'aide de la technologie de sécurité réseau leader de sa catégorie de Forcepoint.

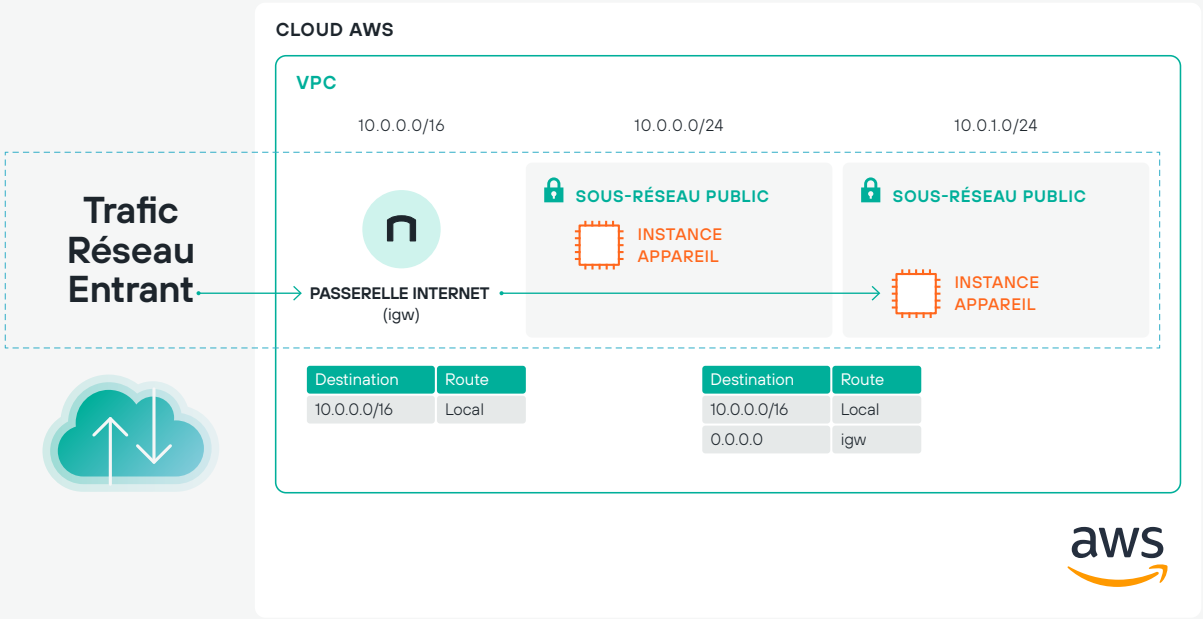
- → Sécurisez les informations qui circulent entre les régions.
- → Appliquez des politiques de sécurité cohérentes dans toutes les régions.

Une société d'énergie a économisé 90 % de ses coûts de réseau étendu WAN en déployant NGFW avec SD-WAN de Forcepoint et en migrant vers le cloud – le tout grâce à un déploiement sans contact.

Amazon VPC Ingress Routing

La redirection basée sur le système Amazon VPC Ingress Routing simplifie l'intégration de la sécurité réseau à votre infrastructure Amazon Virtual Private Cloud (VPC), ce qui vous permet d'appliquer plus facilement des politiques de sécurité de manière uniforme sur l'ensemble de votre réseau d'entreprise (dans le cloud et sur site) afin de protéger efficacement vos charges de travail AWS.

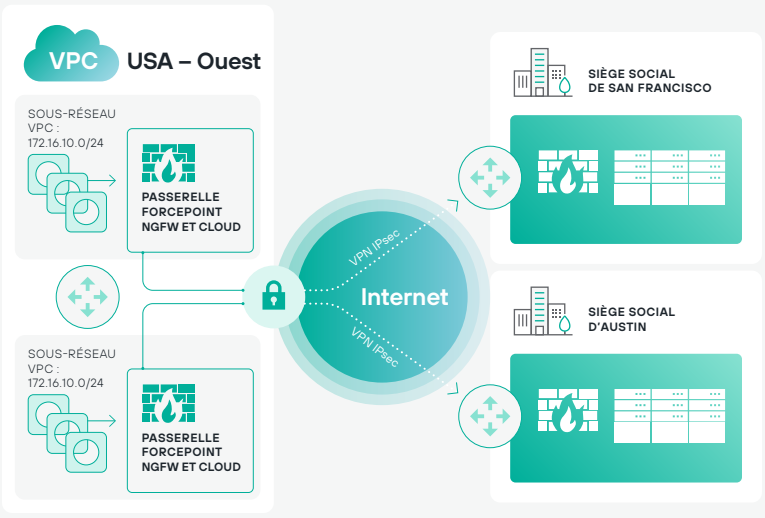
- → Profitez de plus de flexibilité pour traiter tout trafic destiné à Amazon VPC avec le même niveau d'examen que celui utilisé pour accéder au réseau de l'entreprise.
- → Appliquez des politiques de sécurité réseau de manière uniforme sur l'ensemble de l'entreprise, sans ajouter de latence
- → Obtenez une sécurité maximale pour un coût et une complexité minimaux.



AWS VPN CloudHub

Connectez les VPC entre plusieurs régions AWS en toute sécurité. Vous pouvez gérer, contrôler et appliquer des politiques de sécurité à l'aide de la technologie de sécurité réseau de Forcepoint, leader du marché.

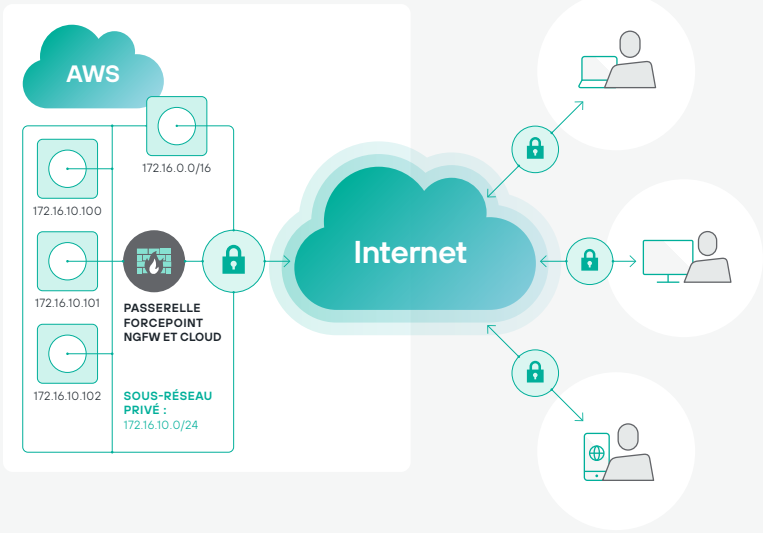
- → Sécurisez les informations qui circulent entre les régions.
- → Appliquez des politiques de sécurité cohérentes dans toutes les régions.



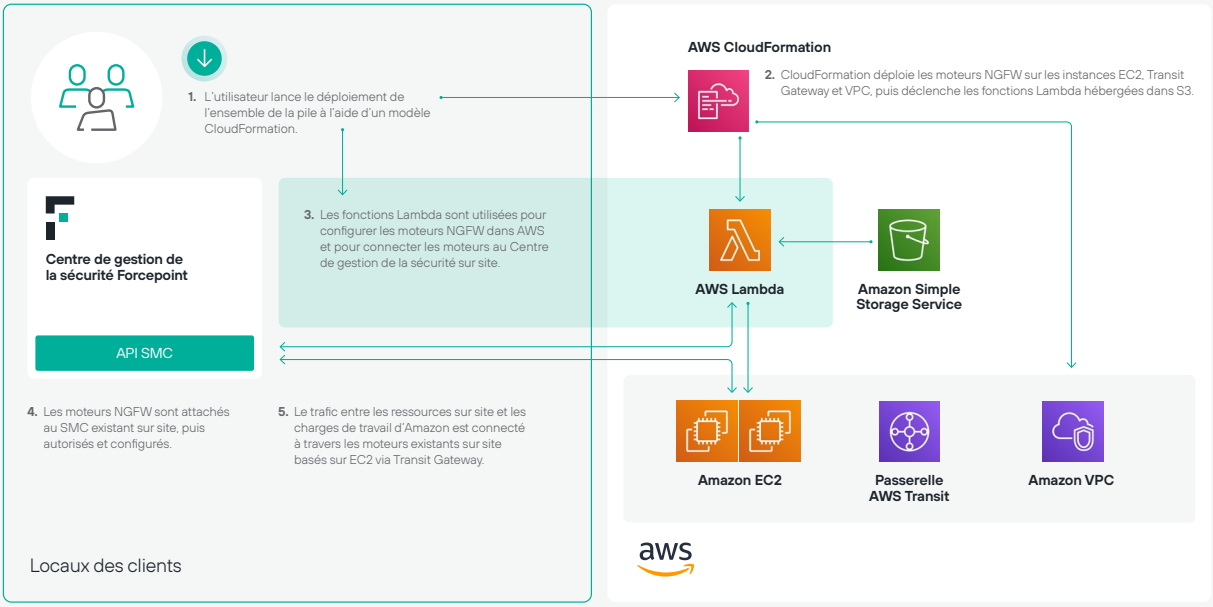
Connectivité pour Accès à distance

Forcepoint NGFW peut être utilisé comme une passerelle de périphérie cloud pour connecter vos utilisateurs distants au Virtual Private Cloud (VPC) d'Amazon. La passerelle cloud de Forcepoint NGFW peut être déployée dans une instance Amazon Elastic Compute Cloud (EC2), offrant des fonctionnalités de firewall avancées pour protéger vos instances EC2 pour tous les accès entrants et sortants, comme :

- → Conscience situationnelle des applications
- → Capacités d'identification des utilisateurs



Intégration des services Forcepoint NGFW + AWS

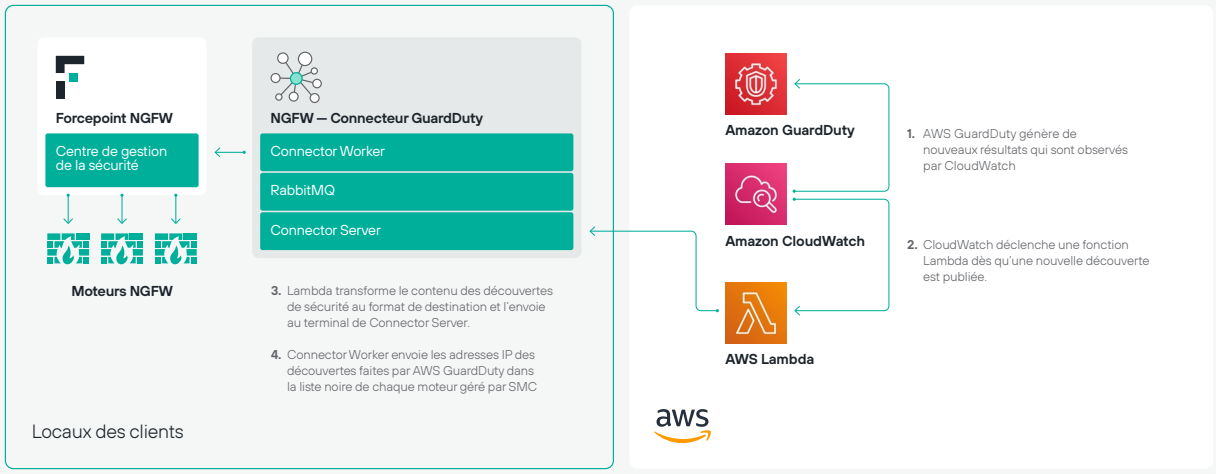


Intégration d'une Passerelle de transit

Déploiement d'un ensemble redondant de firewalls nouvelle génération Forcepoint en tant qu'instances EC2, ainsi qu'une passerelle de transit AWS, et connexion des moteurs NGFW au Centre de Gestion de Sécurité Forcepoint existant à l'aide des fonctions Lambda AWS. Des tunnels IPSEC redondants sont configurés entre les moteurs NGFW dans le cloud et la passerelle de transit, et les politiques de sécurité gérées par le Centre de Gestion de Sécurité Forcepoint peuvent être appliquées aux moteurs NGFW situés dans AWS pour sécuriser le trafic en provenance et à destination de la passerelle de transit.

- → Active l'application cohérente des politiques de sécurité sur site et sur AWS.
- → Automatise le déploiement de l'ensemble de la pile technologique à l'aide d'un seul modèle AWS CloudFormation, avec des paramètres personnalisables pour permettre des déploiements sur mesure.

Obtenez le guide

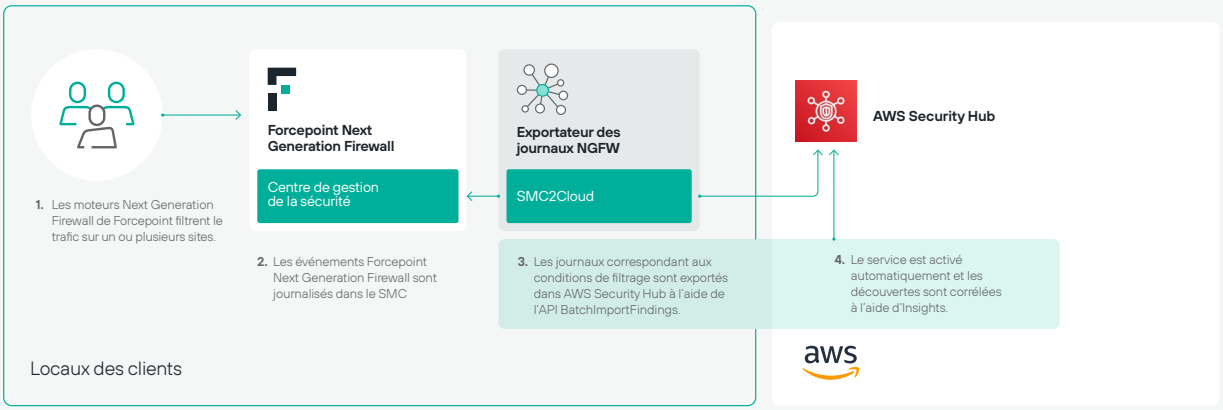


Intégration Amazon GuardDuty

GuardDuty offre aux clients AWS une option intelligente et rentable pour la détection continue des menaces dans le cloud AWS. Le service utilise l'apprentissage automatique, la détection des anomalies et les informations intégrées sur les menaces pour identifier et hiérarchiser les menaces potentielles. L'intégration de Forcepoint NGFW automatise l'importation en temps réel des résultats de sécurité d'Amazon GuardDuty.

- → Les utilisateurs, les applications et les services hébergés sur site et protégés par NGFW bénéficient d'une visibilité accrue des acteurs de la menace qui ciblent l'empreinte AWS d'une entreprise.
- → Les adresses IP émanant de sources malveillantes identifiées par Amazon GuardDuty sont ensuite placées sur une liste noire, distribuée dans toute la flotte de moteurs NGFW déployés sur les sites de l'entreprise.
- → Assurez efficacement une protection accrue grâce au partage des renseignements.

Obtenez le guide



Interopérabilité avec AWS Security Hub

AWS Security Hub fournit une vue consolidée de votre statut de sécurité sur l'ensemble des comptes AWS. L'intégration de Forcepoint avec AWS Security Hub offre une visibilité sur la façon dont les utilisateurs interagissent avec vos données les plus sensibles, où qu'elles se trouvent.

- → Exportez automatiquement et en temps réel les événements des journaux de Forcepoint NGFW vers AWS Security Hub pour accélérer le temps de réponse.
- → Mettez en corrélation les résultats de sécurité avec d'autres sources pour améliorer la visibilité sur tous les sites protégés par NGFW.
- → Gérez facilement les données en les regroupant selon divers champs, tels que la gravité et le type, afin de donner la priorité à ce qui compte le plus pour votre entreprise.

Obtenez le guide | Demandez une démonstration

© 2021 Forcepoint. Forcepoint et le logo FORCEPOINT sont des marques déposées par Forcepoint. Toutes les autres marques citées dans ce document appartiennent à leurs propriétaires respectifs
[Forcepoint Next Generation Firewall with Amazon Web Services Solution-Brief-FR] 21 mai 2021