Forcepoint Cloud Security Gateway

Assurer la sécurité des nouvelles méthodes de télétravail

Convergence

› Ce qui était autrefois un produit individuel est devenu une fonctionnalité intégrée : pour nous, Convergence signifie Fusion. Entre la sécurité web, la sécurité réseau et la sécurité des applications dans le cloud, le tout en un seul service facile à utiliser.

Sécurité en tant que Service

› Secure Access Service Edge (SASE, ou Service d'Accès Sécurisé vers l'Extérieur) demande que les entreprises sécurisent le cloud depuis le cloud. Pour cela, il faut passer d'une approche centrée sur l'infrastructure à une approche centrée sur l'utilisateur et les données, ce qui permet un contrôle granulaire des politiques d'accès au Web, où que vous soyez.

› Le but ultime est d'unifier la gestion du niveau de sécurité requis avec des Politiques de sécurité complexes, et d'effectuer des rapports depuis le cloud, là où se trouve l'appareil d'application des règles, ou depuis n'importe quel terminal, où qu'il se trouve.

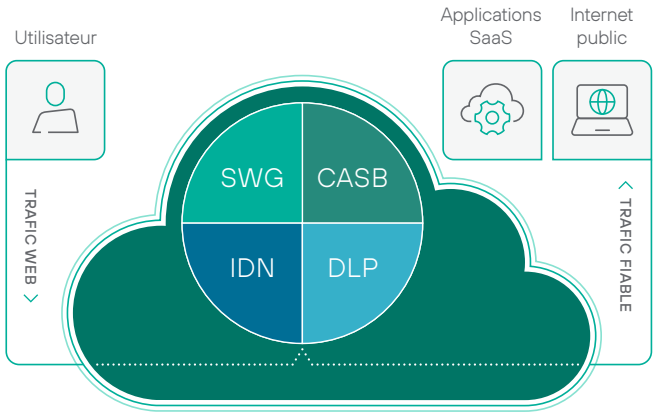
Déploiement hybride souple

› Une grande partie de la livraison des applications se fait encore sur site, que ce soit sur celui de l'entreprise ou dans un autre lieu. Une posture de sécurité efficace et pragmatique gèrera les applications, les données et les utilisateurs, où qu'ils soient. Ceci est essentiel, car la transition sera différente pour chaque secteur, activité et entreprise.

Forcepoint CSG est un service de sécurité cloud convergent qui offre aux utilisateurs et aux données, où qu'ils se trouvent, visibilité, contrôle et protection contre les menaces. Les fonctionnalités intégrées réduisent le délai de rentabilité et garantissent la disponibilité d'un maximum de capacités. L'élimination des produits à usage unique permet aux entreprises de réduire les coûts, la complexité et les frais généraux opérationnels tout en éliminant le chevauchement entre les responsabilités des équipes en charge des produits et celles des équipes de sécurité.

La sécurité des entreprises s'est transformée – chacun des membres de son personnel en constituent le nouveau périmètre. Au début des années 2000, les solutions de sécurité étaient toujours orientées sur la construction de pare-feux. Au cours des 10 dernières années, la virtualisation a donné naissance à l'industrie du cloud public et a généré de grandes quantités de données. Allant au-delà de l'introduction de capacités cloud computing dans les entreprises, ce changement a mis en évidence l'importance de la protection des données numériques critiques. Comme aujourd'hui les utilisateurs et les données sont répartis partout, cela a créé pour les RSSI un problème difficile à résoudre : Sécuriser utilisateurs et données, où qu'ils se trouvent, à tout moment, et sur n'importe quel appareil.

Passerelle Sécurité Cloud



Le concept qui considère les individus comme le nouveau périmètre à sécuriser devenant la réalité normative, il s'agit de protéger les utilisateurs et les données dans un environnement distribué et diversifié, faisant la liaison entre les infrastructures traditionnelles sur site, y compris le travail à domicile, les environnements multi-cloud et multi-SaaS. La situation actuelle a imposé un changement rapide vers la prise en charge de grands volumes de travailleurs à distance. C'est un changement qui a initié une nouvelle méthode de travail. Cela a aussi mis l'accent sur la protection des utilisateurs et des données dans des environnements informatiques hybrides.

Découvrez les avantages de Forcepoint Cloud Security Gateway

→ **Uniformisez la protection et les politiques web partout, pour tous les utilisateurs**

- Étendez la protection aux utilisateurs se trouvant sur le réseau de l'entreprise et en dehors de celui-ci - au bureau, à la maison, en déplacement.
- Appliquez des politiques cohérentes dans l'ensemble de votre organisation – pour un accès sécurisé au contenu web et aux applications cloud, tout en protégeant vos données critiques.

→ **Protégez les utilisateurs contre les menaces avancées sur le web et dans le cloud**

- Sécurisez tout le trafic Internet pour vos utilisateurs, où qu'ils aillent.
- Prévenez et arrêtez les menaces tout au long de leur chaîne de frappe, même celles que vous ne pouvez pas voir, par exemple les menaces Zero day.

→ **Découvrez la Shadow IT et sécurisez l'accès au cloud dans toute votre entreprise**

- Découvrez les applications cloud dont l'utilisation pose des risques.
- Activez des politiques protégeant les données, sans entraver la productivité

→ **Optimisez la gestion opérationnelle et les dépenses de la sécurité cloud**

- Diminuez les coûts et les empreintes matérielles.
- Éliminez les lacunes dans les opérations de sécurité et rationalisez la gestion informatique et du flux de travail

→ **Réduisez le nombre de prestataires et la surcharge de produits**

- Gérez une relation et une source de soutien uniques
- Tirez parti de logiciels qui ont été conçus dès le départ pour fonctionner ensemble

→ **Simplifiez la mise en conformité réglementaire**

- Utilisez des modèles de politiques réglementaires prédéfinis pour éliminer les conjectures et réduire le travail.
- Utilisez une solution unique qui unifie

→ **Garantissez la productivité des employés**

- Alignez le SaaS et l'utilisation du web avec des politiques d'entreprise acceptables
- Arrêtez les données fantôme en bloquant les applications non autorisées

→ **Sécurisez votre main-d'œuvre locale, distante et mondiale**

- Travaillez n'importe où, sur n'importe quel appareil, sachant que votre personnel et vos données sont protégés.
- Fournissez du contenu localisé à l'échelle mondiale pour permettre à votre force de travail multinationale de s'épanouir pleinement.

POINTS SAILLANTS DU PRODUIT	DESCRIPTION
Une expérience utilisateur supérieure	› Un seul SKU à acheter › Un seul accès pour toutes les fonctionnalités › Une seule page de statut › Un seul numéro de téléphone pour l'assistance
Protection contre les menaces avancées	› Anti-virus, anti-malware, cryptodevises et ransomware › Filtrage et catégorisation des URL et du contenu › Inspection du SSL › API d'ingestion des menaces › Moteur de classification avancé (ACE) › Partage de renseignements sur les menaces & ThreatSeeker › Sandboxing cloud avec apprentissage machine › Protection des données entrantes et sortantes › Blocage des fichiers
Facilité d'accès et d'administration	› Politiques et contrôles d'utilisation acceptables › Rapports – (Interface glisser-déposer) › Application de Quotas › Application de politiques basées sur des règles (adaptative) › Intégration SIEM & AD › Application de politiques universelles › Vue personnalisée du tableau de bord : utilisateur final vs. auditeur
Infrastructure cloud mondiale	› ISO 27001, IS27018, CSA STAR, SOC 1 & 2. Certifications dans chaque data center pour couvrir le cycle de vie entier des opérations › Mises à jour en temps réel › Tolérance aux pannes, haute disponibilité et haute performance › Plus de 160 Points de Présence (PoPs) avec une couverture sur 145 pays › Localisation de contenu › SLA
La sécurité des applications cloud, simplifiée	› Découverte Shadow IT › Contrôle des applications Cloud › Proxy transparent et inversé, mode API › Analyses comportementales › Détection des anomalies
Conformité prouvée & Prévention de la perte de données	› Classement des risques d'incidents › PCI, HIPPA › Mise en place d'empreintes › Détection des microfuites › Phishing

Vous souhaitez en savoir plus sur Cloud Security Gateway et comment cette solution peut vous offrir une expérience cloud sans nuages ? Prenez contact avec un expert.

forcepoint.com/contact