Forcepoint

Présentation succincte

Secure Web Gateway

Arrêtez les pertes de données et les attaques de malware, pas la productivité.

Études de cas

- Offrez aux employés un accès rapide et sûr au Web
- Mettez en place des politiques d'utilisation acceptable
- Bloquez le téléchargement de données sensibles vers des sites web non sanctionnés
- Empêchez les malwares de pénétrer sur les appareils des utilisateurs sans entraver l'expérience de l'utilisateur.
- Détectez et contrôlez la Shadow IT
- Empêchez que les entreprises exposent par accident

La Solution

- Sécurité web rapide avec DLP intégré et protection avancée contre les menaces
- Contrôles Zero Trust granulaires d'accès et de données basés sur le groupe d'utilisateurs, le type d'appareil, l'emplacement de l'utilisateur, la catégorie de site Web, le score de risque du site Web et bien plus
- L'architecture distribuée élimine les points d'étranglement via la plateforme AWS à haute disponibilité et hyperscaling
- Une Remote Browser Isolation (RBI) en option pour une navigation et des téléchargements sécurisés

Résultats

- Augmentez la productivité, en permettant à vos utilisateurs de naviguer sur le Web depuis n'importe où, de manière transparente et en toute sécurité
- Réduisez les risques en contrôlant les données sensibles dans le cloud et en stoppant les malwares
- Réduisez les coûts en simplifiant les activités de sécurité, configurez toutes vos politiques depuis un seul endroit

Le web est perçu tantôt comme un bienfait, tantôt comme un fléau. La plupart des gens en dépendent pour obtenir des informations afin de faire leur travail, mais le web génère également des risques d'exfiltration de données, de violations des politique RH, de perte de productivité et d'infection par des malwares. Et quand les conséquences du nonrespect de la sécurité des données et des personnes deviennent chaque jour plus lourdes, sécuriser les interactions web est une exigence stratégique pour les entreprises modernes.

Offrez aux employés un accès rapide et sûr au Web

La plupart des SWG redirigent de force tout le trafic Web à transiter par un centre de données centralisé – qu'il soit sur site ou dans le cloud – ce qui ajoute une latence qui peut nuire considérablement aux applications Web modernes. En revanche, Secure Web Gateway de Forcepoint ONE possède une architecture distribuée qui élimine ces points d'étranglement, et peut offrir un débit jusqu'à deux fois supérieur pour les contenus et les applications Web sensibles aux performances. Nous rendons cela possible en appliquant des politiques de sécurité localement sur l'appareil de l'utilisateur, afin que le trafic puisse être échangé directement entre l'utilisateur et le site Web.

Mettez en place des politiques d'utilisation acceptable (PUA) pour les sites à risque

Le web peut être un lieu de distraction qui n'est pas toujours utilisé pour les activités de l'entreprise. Secure Web Gateway de Forcepoint ONE vous permet de bloquer ou d'autoriser les visiteurs de sites Web non productifs ou inappropriés avec un contrôle total du chemin d'accès. Par exemple, vous pouvez bloquer certains subreddits de Reddit, tout en autorisant d'autres. Vous pouvez gérer l'accès en fonction du groupe d'utilisateurs, de la doctrine de l'appareil, de l'emplacement, de la catégorie d'URL (prédéfinie ou personnalisée), du score de réputation et du score de risque des applications d'entreprise. Les catégories d'URL personnalisées peuvent inclure des chemins d'accès complets aux répertoires d'URL, ce qui permet aux administrateurs d'appliquer des politiques différentes selon les répertoires.

Bloquez le téléchargement de données sensibles vers des sites web non sanctionnés

Grâce à notre SWG, vous pouvez empêcher que des données réglementées ou des propriétés intellectuelles soient envoyées vers des espaces personnels de stockage de fichiers, vers les réseaux sociaux ou vers des comptes de courriel personnels. Vous pouvez analyser et bloquer les téléchargements de fichiers et les méthodes de postage HTTPS pour les données sensibles, avec les mêmes modèles DLP prédéfinis et personnalisés utilisés par les services CASB et ZTNA dans Forcepoint ONE.

Empêchez les malwares de pénétrer sur les appareils des utilisateurs sans entraver l'expérience de l'utilisateur.

Notre SWG offre plusieurs formes de protection contre les malwares transmis par le Web, notamment le blocage par catégorie des sites Web, l'analyse en ligne des fichiers téléchargés et la protection Zero Trust contre les menaces avancées, comme l'isolation à distance du navigateur (RBI). Avec RBI, même les sites ou les fichiers téléchargés qui sont infectés peuvent être utilisés de manière sûre et efficace.

Détectez et contrôlez la Shadow IT

Le service de Secure Web Gateway travaille de concert avec notre CASB pour identifier les sites Web qui sont utilisés à la place des applications d'entreprise préférées. Ces sites « shadow IT » sont automatiquement collectés et affichés dans la console.

Empêchez que les entreprises exposent par accident les données privées de leurs clients

Pour protéger la confidentialité des employés, les organisations peuvent empêcher le décryptage et l'inspection du trafic en provenance et à destination de catégories spécifiques de sites Web qui sont généralement utilisés avec des informations personnelles identifiables (IPI), comme les données bancaires, de santé et d'assurance.

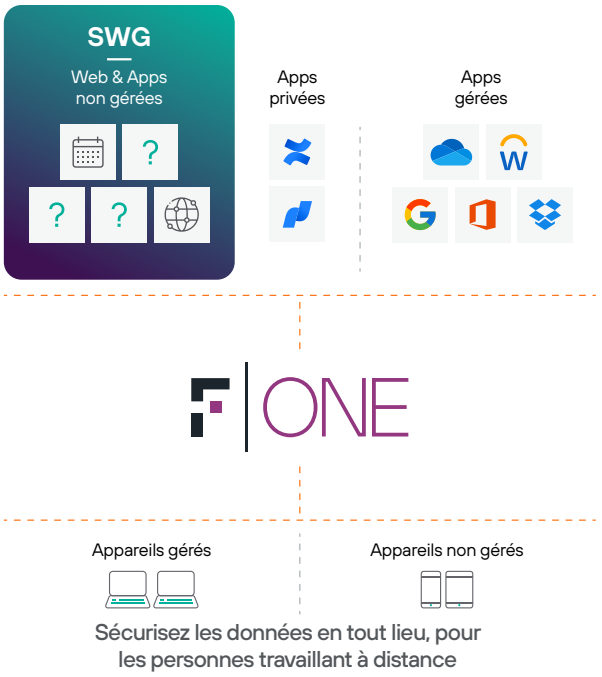
Secure Web Gateway de Forcepoint ONE maximise le temps de fonctionnement, la productivité et les performances

SWG fait partie de Forcepoint ONE, notre plateforme cloud basée sur un hyperscaler ayant plus de 300 points de présence (PoP), une accessibilité mondiale et un temps de disponibilité éprouvé de 99,99 % pour sécuriser l'accès au Web et préserver la productivité des utilisateurs. Forcepoint ONE unifie CASB, SWG et ZTNA pour sécuriser l'accès aux applications SaaS, Web et privées de l'entreprise, ce qui simplifie la sécurité.

Simplifier la sécurité Web dans le monde réel

La plateforme cloud Forcepoint ONE offre un simple « bouton poussoir » pour mettre en oeuvre la sécurité dans le cloud.

Depuis une même console, les administrateurs peuvent gérer l'accès et contrôler les téléchargements et les envois de fichiers entre un appareil géré et n'importe quel site Web.



Voyons comment SWG simplifie la sécurité du Web lorsque Kris, analyste travaillant à domicile, commence sa journée de travail.

Kris se rend sur reddit.com pour des recherches liées à l'entreprise.	Kris se rend sur reddit.com/r/technology pour rechercher des messages récents sur les malwares. Les politiques de contenu SWG autorisent une granularité au niveau du répertoire. Ce subreddit est considéré comme lié au travail, donc Kris peut y accéder.
Dans le subreddit r/technologie, Kris clique accidentellement sur un lien vers une page inappropriée.	L'administrateur Forcepoint ONE de Kris a créé des politiques de contenu SWG qui autorisent l'accès à des répertoires tels que r/technologie, mais bloquent l'accès aux subreddits et aux pages inappropriées. La SWG remarque l'erreur de Kris et bloque la nouvelle page.
Kris commence une feuille de calcul confidentielle sur son ordinateur portable de l'entreprise, qui comprend des IPI de clients, et veut continuer à travailler sur son ordinateur portable personnel. Krys essaie de télécharger le fichier sur son stockage cloud personnel puis de le télécharger sur son ordinateur portable personnel.	Pour empêcher la perte de données commerciales, l'administrateur Forcepoint ONE de l'entreprise a créé une politique de contenu SWG qui bloque le téléchargement des informations personnelles identifiables des clients (PII) sur tout site Web de partage de fichiers personnels. Lorsque Kris tente le téléchargement, il est bloqué et un message s'affiche pour expliquer pourquoi le téléchargement a été bloqué.

Élément d'une solution de sécurité unifiée pour le Web, le cloud et les applications privées.

En plus de la SWG, la plateforme tout-en-un Forcepoint ONE sécurise l'accès aux informations commerciales sur n'importe quel locataire SaaS d'entreprise et sur les applications privées :

- **Cloud (SaaS et IaaS) :** CASB applique un contrôle d'accès contextuel, une prévention des pertes de données (DLP) et une protection contre les malwares à toute application Web publique prenant en charge l'intégration SAML 2 avec des prestataires d'identité tiers, depuis n'importe quel navigateur moderne sur n'importe quel appareil pris en charge par Internet. Les données au repos dans les IaaS et SaaS populaires peuvent également être analysées pour détecter les données sensibles et les malwares, puis désinfectées. Utilise les mêmes modèles de correspondance DLP disponibles pour SWG et ZTNA pour les applications Web privées.
- **Applications privées :** ZTNA sécurise et simplifie l'accès aux applications privées sans la complication ou le risque associés aux VPN. Comme les autres solutions Forcepoint ONE, ZTNA applique également le contrôle d'accès contextuel, la DLP et la protection contre les malwares à toute application Web privée.
- **Capacités supplémentaires :** RBI pour la forme ultime de protection des menaces Web, ou le Cloud Security Posture Management (CSPM) pour analyser les fournisseurs de cloud à la recherche de conformes à risque.
- **Cloud Firewall :** modèle complémentaire à SWG pour sécuriser tout le trafic Internet et se protéger des attaques destinées à exploiter les sites de succursales vulnérables.

Lisez la synthèse sur la solution Forcepoint ONE pour plus de détails.

Prêt à sécuriser les données dans les applications cloud à partir de n'importe quel appareil ?

Commençons par une démonstration.

forcepoint.com/contact