Forcepoint

Présentation succincte

Forcepoint ONE : est une plateforme cloud tout-en-un qui simplifie la sécurité des équipes alternant télétravail et présentiel

Études de cas

- Obtenez visibilité et contrôle sur les interactions du personnel hybride avec les données se trouvant sur le web, le cloud et les apps privées.
- Empêchez l'utilisation abusive de données sensibles lors de leur accès par des appareils gérés ou non gérés.
- Contrôler l'accès aux contenus Web à haut risque et aux différents types de sites IAg.
- Fournissez un accès sécurisé rapide et à distance aux ressources de l'entreprise et aux applications privées en évitant la complexité des VPN.

La Solution

- Une plateforme unique et unifiée permet de gérer des politiques de sécurité cohérentes pour toutes les applications de l'entreprise.
- Un service cloud intégral sécurise l'accès et les données, combinant Secure Web Gateway (SWG), Cloud Access Broker (CASB) et Zero Trust Network Access (ZTNA).
- Protection avancée intégrée contre les menaces et sécurisation des données, pour éloigner les assaillants et empêcher la fuite des données sensibles.
- Capacités RBI et CSPM supplémentaires pour examiner les locataires de clouds publics dans les configurations à risque, fonctions CDR pour la suppression des menaces de contenu, et autres fonctions.
- Classification Forcepoint pour le marquage des données.

Résultat

- Simplifié - réunit la sécurité des applications web, cloud et privées dans une plateforme unifiée (avec prise en charge sans agent).
- Modernisation - Combine les principes de Zero Trust avec une architecture SASE et une sécurité avancée comme la RBI (Remote Browser Isolation, ou isolation à distance du navigateur) et la désinfection des fichiers téléchargés.
- Ubiquité - Disponible dans le monde entier, avec plus de 300 Points de Présence (PoP).
- Fiabilité - Disponibilité de 99,99 % depuis 2015.
- Rapidité - Utilise une application distribuée et un échelonnement automatique pour éliminer les points de congestion.

Sécurité « Data-first »

La sécurité devient de plus en plus complexe, mais il existe une alternative à la complexité. Les utilisateurs travaillent désormais de n'importe où, avec des données qui sont diffusées partout, sur les sites Web, les applications cloud et les applications privées.

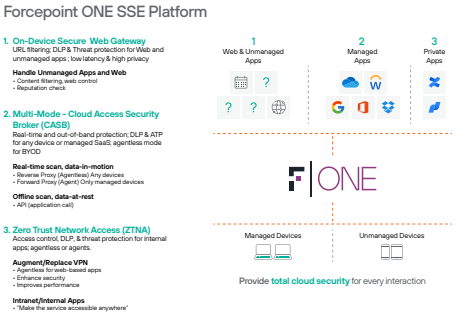
Afin de prendre en charge les initiatives de retour au bureau et le travail hybride, les équipes de sécurité ont besoin d'une plateforme de sécurité convergée qui place les données au centre de l'image. Les contrôles de sécurité doivent pouvoir s'étendre au Web, au cloud et aux applications privées avec une visibilité et une gestion cohérentes afin que les entreprises puissent arrêter la perte de données avant qu'elle ne se produise.

Avec une solution axée sur les données, les données d'entreprise peuvent être sécurisées partout pour les personnes travaillant n'importe où.

Forcepoint ONE simplifie la sécurité

Forcepoint ONE est une plateforme cloud intégrée qui simplifie la sécurité. Vous pouvez facilement adopter Zero Trust et Security Service Edge (SSE, le composant de sécurité de SASE) parce que nous avons rassemblé des services de sécurité fondamentaux, y compris SWG, CASB et ZTNA.

Décuplez votre productivité en adoptant en toute sécurité de nouvelles technologies telles que l'IAg, en contrôlant l'accès aux différents types de sites IAg et en renforçant systématiquement la protection des données sensibles et en évitant l'exposition aux logiciels malveillants.



Les capacités Zero Trust de Forcepoint ONE, natives du cloud, comprennent:

- **Sécurité DLP sans agent pour les applications cloud et privées.** Utilisez en toute sécurité des applications Web professionnelles privées à partir d'appareils personnels, tout en protégeant les données sensibles.
- **Protection avancée contre les menaces et sécurité des données intégrées.** Prévenez la perte ou l'exfiltration de données et empêchez les pirates d'y accéder grâce à des commandes régulières et omniprésentes.
- **Passerelles unifiées pour l'accès au cloud, au Web et aux applications privées.** Contrôle basé sur l'identification pour l'accès aux applications d'entreprise et géré en un seul endroit pour SWG, CASB et ZTNA.
- **Modularité dynamique avec accès mondial –** 300 Points de Présence répartis dans AWS offrent une connectivité rapide, à faible latence et un temps de disponibilité de 99,99 %, quel que soit l'endroit où les gens travaillent.

Sécurité unifiée pour le web, le cloud et les applications privées.

- **Cloud:** CASB applique un accès granulaire aux applications et données SaaS de l'entreprise depuis n'importe quel appareil. CASB bloque le téléchargement des données sensibles et bloque le chargement des malwares en temps réel. Il analyse les données statiques dans les SaaS et IaaS populaires pour y rechercher les malwares et les données sensibles, et prend les mesures correctives nécessaires. CASB détecte les applications de shadow IT et contrôle l'accès depuis n'importe quel appareil géré.
- **Web:** SWG supervise et contrôle les interactions avec tout site Web en fonction du risque et de la catégorie, bloquant le téléchargement de logiciels malveillants ou le téléversement de données sensibles vers des comptes personnels de partage de fichiers et d'e-mail. Notre sécurité web sur les dispositifs applique les politiques d'utilisationmacceptable sur les dispositifs gérés, où qu'ils se trouvent.
- **Applications privées:** ZTNA sécurise et simplifie l'accès aux applications privées sans la complication ou le risque associés aux VPN.

Protection intégrée contre les menaces avancées et sécurité des données

- **Prévention de la perte des données - Data Loss Prevention (DLP):** Les fichiers et le contenu textuel sont analysés au moment de l'envoi et du téléchargement pour détecter les données sensibles et sont bloqués, suivis, cryptés ou expurgés selon le cas.
- **Analyse des malwares:** Les fichiers sont analysés au moment de l'envoi et du téléchargement pour détecter et bloquer les malwares à l'utilisation.

Visibilité et commande intégrées

- **Suite de gestion intégrée** pour la configuration, la surveillance et l'établissement de rapports sur l'ensemble des canaux SSE.
- **Politiques de connexion** pour contrôler l'accès aux applications web, cloud ou privées en fonction de l'emplacement de l'utilisateur, du type de dispositif, de la posture du dispositif, du comportement de l'utilisateur et du groupe d'utilisateurs. Ces paramètres permettent d'éviter les reprises de compte.
- **Politiques DLP faciles** à utiliser pour contrôler le téléchargement et le téléversement de données sensibles et de logiciels malveillants pour les applications SaaS administrées, les applications privées et les sites Web, ainsi que pour les données stockées dans les applications SaaS et IaaS administrées.
- **Agent sur dispositif** pour Windows et MacOS permettant de prendre en charge SWG, CASB ou ZTNA pour les applications hors navigateur et le contrôle d'informatique fantôme.
- **Des analyses unifiées et une visualisation de la valeur** vous donnent un aperçu rapide des risques de sécurité, vous informent de l'utilisation globale et de l'impact sur votre entreprise de la plateforme intégrée de sécurité cloud.

Capacités supplémentaires disponibles selon les besoins

- **Doctrine de sécurité cloud - Cloud Security Posture Management (CSPM):** Analyse les paramètres des locataires AWS, Azure et GCP à la recherche de configurations à risque, et fournit une remédiation manuelle et automatisée.
- **Doctrine de sécurité SaaS - SaaS Security Posture Management (SSPM):** Analyse les paramètres des locataires Salesforce, ServiceNow et Office 365 à la recherche de configurations à risque et fournit une remédiation manuelle et automatisée.
- **Isolation à distance du navigateur - Remote browser isolation (RBI):** Protège un utilisateur contre les malwares transmis par le web sur son appareil local en exécutant un navigateur dans une machine virtuelle hébergée dans le cloud.
- **Forcepoint Classification:** la Data Classification fonctionne avec des suggestions basées sur l'IA pour améliorer la précision du marquage.
- **AMDP :** Analyse le comportement des fichiers dans un bac à sable contrôlé pour identifier les contenus cachés et malveillants.

Des abonnements qui libèrent la simplicité

Des abonnements annuels par utilisateur individuel sont disponibles :

- **Édition tout-en-un** pour la sécurité du web, du cloud et des apps privées
- **La version Web-security** comprend la passerelle Web et le CASB en ligne pour un nombre illimité d'applications cloud, ainsi que les éléments essentiels de RBI pour les sites non classés et nouvellement enregistrés, afin d'ajouter ultérieurement la prise en charge des API pour les applications cloud et la prise en charge des applications privées.
- **L'édition ZTNA** protège un nombre illimité d'applications privées.
- **L'édition CASB** protège un nombre illimité d'applications cloud en ligne et comprend des API pour 3 applications avec la possibilité d'ajouter des packs d'applications supplémentaires ou des nœuds d'interrogation d'API dédiés.
- **Toutes les souscriptions** comprennent la gestion centralisée du cloud, des politiques avec prévention de perte de données, l'accès automatisé via un agent de point de terminaison, et des rapports complets.

forcepoint.com/contact