Forcepoint

Présentation succincte

Cloud Access Security Broker

Sécurisez vos données dans n'importe quelle application cloud, accessible depuis n'importe quel appareil

Le Défi

- Protégez et contrôlez l'accès aux applications gérées via vos politiques PAP
- Contrôlez l'envoi et le téléchargement de données sensibles dans toute application SaaS gérée
- Détecter shadow IT

La Solution

- Sécurité des applications cloud avec DLP intégré et protection avancée contre les menaces
- Contrôles granulaires Zero Trust d'accès aux données en fonction de l'utilisateur, de l'appareil ou du lieu
- La plateforme AWS hyperévolutive maximise la disponibilité et minimise la latence
- Application de stratégies DLP sur les appareils gérés et non gérés

Résultat

- Augmentez la productivité en permettant aux salariés d'utiliser les informations n'importe où, sans contraintes 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 en configurant les politiques en un seul endroit
- Uniformisation de la conformité avec des processus démontrables pour contrôler le flux d'information

Les nouveaux modèles de travail d'aujourd'hui exigent que les utilisateurs, où qu'ils se trouvent, aient un accès rapide, mais contrôlé aux données d'entreprise. Cela signifie que les utilisateurs doivent accéder aux données dans des applications cloud comme Microsoft 365, Google Workspace, Slack, Jira et Salesforce depuis n'importe quel type d'appareil ou emplacement. Avec plus de 250 applications SaaS pour la visibilité et la gestion moyennes de l'entreprise, vous pouvez facilement devenir ingérable.

Protégez l'accès aux applications d'entreprise depuis les appareils PAP et non gérés.

Forcepoint simplifie la sécurité dans le cloud. Le service de sécurité CASB de Forcepoint ONE active un accès Zero Trust permettant aux applications cloud critiques de l'entreprise d'être utilisées en toute sécurité sur les appareils personnels des employés (PAP), ainsi que sur les appareils non gérés des partenaires et des prestataires.

Contrôlez l'envoi et le téléchargement de données sensibles dans toute application SaaS gérée

Vous disposez d'un jeu unique de politiques de sécurité à performances inégalées pour contrôler les données sensibles, quels que soient l'endroit et la façon dont les salariés et les prestataires se connectent à Internet. La gestion de l'accès à ces applications à partir d'appareils mobiles facilite l'adoption et la productivité, tandis que des politiques différentes basées sur l'identification et l'emplacement fournissent des contrôles Zero Trust granulaires. L'analyse en ligne des données sensibles et des programmes malveillants protège les données de toutes les applications SaaS. Vous gagnez plus de certitude sur la façon dont les données privées sont partagées dans les applications de l'entreprise et, avec Data Loss Prevention (DLP) intégrée, vous n'avez pas besoin de produits ponctuels pour arrêter les violations de données.

Stoppez les malwares cachés dans les fichiers de données d'entreprise

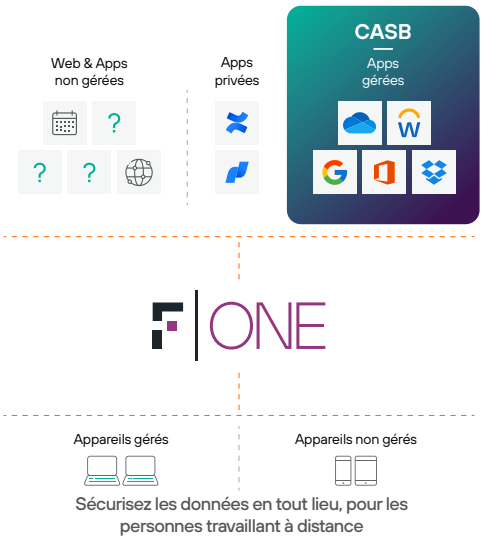
Forcepoint ONE CASB peut détecter et bloquer les programmes malveillants dans les données en transit entre les utilisateurs et l'application SaaS en utilisant les moteurs de programmes malveillants de Bitdefender et Trellix. Il peut également détecter les programmes malveillants dans les fichiers de stockage SaaS et IaaS populaires, et mettre ces fichiers en quarantaine.

Détecter shadow IT

Forcepoint ONE CASB fait ressortir le shadow IT et génère un score de risque pour les applications non approuvées en analysant plusieurs attributs. Cela permet aux équipes informatiques d'avoir une meilleure compréhension de l'utilisation des SaaS au sein de leur entreprise et d'appliquer les contrôles de sécurité nécessaires. Le CASB détecte les applications SaaS non gérées en cours d'utilisation à l'aide des journaux de réseau ou de la télémétrie de la passerelle web sécurisée Forcepoint ONE pour permettre l'application de politiques de sécurité cohérentes aux applications SaaS approuvées et non approuvées afin que les données de l'entreprise restent sécurisées où qu'elles soient utilisées.

Le CASB intégré dans Forcepoint ONE maximise le temps de fonctionnement, la disponibilité et la productivité

Notre CASB fait partie de Forcepoint ONE, notre plateforme cloud basée sur un hyperscaler disposant de plus de 300 points de présence (PoP), un accès mondial et une disponibilité prouvée de 99,99 %. Il sécurise les applications cloud sans entrave et préserve la productivité des utilisateurs. D'autres solutions détournent le trafic réseau vers et depuis les applications cloud vers des centres de données privés plutôt que vers des sites plus proches des utilisateurs et des applications auxquelles ils accèdent. Cela se traduit par des performances médiocres, causant des dysfonctionnements dans des applications sensibles à la latence comme Slack, et par la tentation des employés de rechercher des solutions de contournement à haut risque.



Making Cloud Security Simple in the Real World

La plateforme cloud Forcepoint ONE dispose d'un « bouton magique » pour mettre en oeuvre la sécurité dans le cloud.

À partir d'une seule console, les administrateurs peuvent gérer les données d'accès et de gestion pour les utilisateurs d'appareils gérés et non gérés (comme PAP et les ordinateurs des sous-traitants ou des partenaires).

Regardez comment CASB simplifie la sécurité dans le cloud lors de la journée de travail de Kris, analyste travaillant à domicile.

Kris se connecte à son compte Salesforce à partir de son ordinateur portable fourni par l'entreprise.	Le CASB de Forcepoint ONE gère les connexions aux applications de l'entreprise, en permettant aux utilisateurs de se connecter de manière transparente et sûre.
Kris navigue directement sur salesforce.com ou via un portail d'applications d'entreprise.	Salesforce redirige la session vers le CASB (via SAML), qui analyse si l'appareil est géré, son emplacement et sa posture de sécurité. Sur la base de politiques de sécurité prédéfinies, le CASB confirme l'identité de Kris grâce à l'authentification à plusieurs facteurs.
Kris se voit accorder l'accès aux applications gérées.	Les politiques d'administration contrôlent également l'accès direct à l'application, l'accès contrôlé ou même l'absence d'accès. Cela se passe en quelques millisecondes, sans affecter la productivité des employés. Tout le trafic entre l'appareil de Kris et l'application passe par le CASB (en utilisant un proxy inversé ou de transfert).
Kris décide de télécharger une prévision de revenus à partir de Salesforce.	Le CASB analyse tout fichier téléchargé depuis l'application à la recherche de programmes malveillants et de données sensibles. En fonction du résultat et de la politique, il peut bloquer les fichiers de programme malveillant et bloquer, suivre ou chiffrer les données sensibles. Si une politique restreint le téléchargement de données sensibles uniquement sur les appareils non gérés, le téléchargement sera autorisé puisque Kris utilise un ordinateur portable de l'entreprise.
Kris tente de transférer des données sensibles ou un fichier infecté par un programme malveillant via Slack.	Le CASB peut également vérifier les fichiers téléchargés dans les applications cloud. Le CASB peut bloquer automatiquement le téléchargement. Il peut même bloquer le téléchargement de fichiers dans des applications non autorisées en utilisant l'agent unifié sur l'appareil.

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

Outre le CASB, la plateforme tout-en-un Forcepoint ONE sécurise l'accès aux informations commerciales sur tout site Web et application privée :

- **Web :** Notre solution SWG (Passerelle Web Sécurisée) surveille et contrôle les interactions avec n'importe quel site Web en fonction du risque et de la catégorie, bloquant le téléchargement de malware ou le chargement de données sensibles sur des comptes personnels de partage de fichiers et de courriel. Notre SWG embarqué sur appareil applique des politiques d'utilisation acceptables sur les appareils gérés situés n'importe où.
- **Applications privées :** ZTNA sécurise et simplifie l'accès aux applications privées sans la complication ou le risque associés aux VPN.
- **Des capacités supplémentaires** comme l'analyse des fournisseurs de cloud pour les paramétrages à risque de la gestion de la posture de sécurité cloud (CSPM) et de la gestion de la posture de sécurité SaaS (SSPM), en fonction des besoins.

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

Prêt à sécuriser les données des applications cloud depuis n'importe quel appareil ?

Commençons par une démonstration.

forcepoint.com/contact