Forcepoint

Présentation succincte

Cloud Access Security Broker

Sécurisez vos données facilement 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
- Stoppez les malwares cachés dans les fichiers de données d'entreprise
- Détectez et maîtrisez la 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

L'accès aux applications et aux données du cloud à partir d'appareils mobiles est une évidence pour la main-d'œuvre hybride d'aujourd'hui. Une entreprise déploie en moyenne plus de 280 applications SaaS, y compris des outils de collaboration comme Microsoft 365, Google Workplace, Slack ou Jira, indispensables aux employés et prestataires distants. Utiliser ces services sans pouvoir gérer l'accès depuis les appareils mobiles ou sans établir la confiance dans les appareils (doctrine des appareils) ajoute de la complexité et des risques.

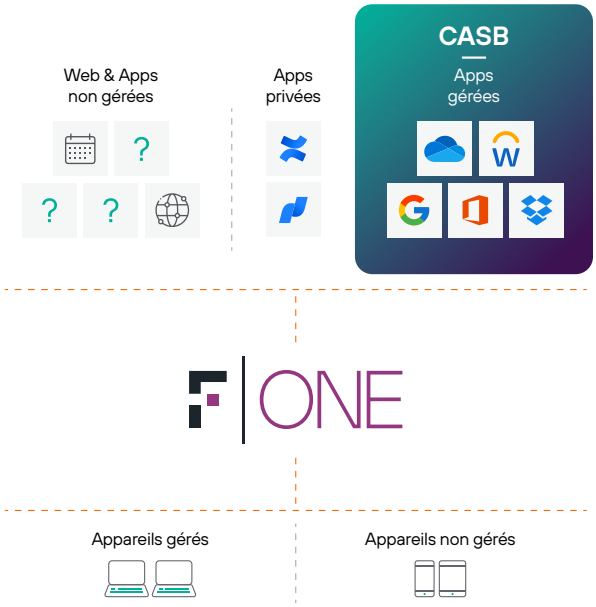
Protégez l'accès aux applications d'entreprise depuis les appareils PAP et non gérés.
Forcepoint simplifie la sécurité dans le cloud. Le service de sécurité CASB de Forcepoint ONE active un accès Zero Trust permettant aux applications cloud critiques de l'entreprise d'être utilisées en toute sécurité 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 depuis des appareils mobiles facilite l'adoption et la productivité, tandis que la mise en place de politiques variables selon la position et l'emplacement de l'appareil permet un contrôle Zero Trust granulaire garantissant la sécurité des données. Vous avez plus d'assurance sur la façon dont les données confidentielles sont partagées dans les applications de l'entreprise sur n'importe quel appareil, même sur un appareil personnel. Data loss prevention (DLP) est intégrée, vous n'avez donc pas besoin de produits individuels pour mettre fin aux violations.

Stoppez les malwares cachés dans les fichiers de données d'entreprise
Notre CASB peut détecter et bloquer les malwares dans les données en transit entre les utilisateurs et l'application SaaS en utilisant les moteurs de malware Bitdefender et CrowdStrike. Il peut également détecter les malwares dans les fichiers de stockage SaaS et IaaS populaires, et mettre ces fichiers en quarantaine.

Détectez et maîtrisez la Shadow IT
Le CASB ne se contente pas de mettre en lumière l'informatique de l'ombre, il permet également de contrôler et d'encadrer l'utilisation sûre et les meilleures alternatives. Le CASB détecte et répertorie les applications SaaS non gérées mais cependant utilisées, ce qui permet aux administrateurs de concevoir des politiques pour les appareils de l'entreprise, en bloquant l'accès ou en affichant un message à l'utilisateur pour le guider vers des applications SaaS approuvées.

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 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 sur des centres de données privés, plutôt que vers des sites proches des utilisateurs. 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.



Fournit une **sécurité totale dans le cloud** pour chaque interaction.

Faciliter la sécurité cloud pour une utilisation réaliste

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

À partir d'une console unique, les administrateurs peuvent gérer l'accès et contrôler la réception et l'envoi de fichiers pour les utilisateurs d'appareils gérés et non gérés (tels que les ordinateurs PAP et ceux des entrepreneurs 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 doctrine de sécurité. Sur la base de politiques de sécurité prédéfinies, le CASB confirme l'identité de Kris grâce à des applications d'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).
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 malwares et de données sensibles. En fonction du résultat et de la politique, il peut bloquer les fichiers de malware et bloquer, suivre ou chiffrer les données sensibles. Si une politique restreint le téléchargement de données sensibles uniquement sur les appareils gérés, le téléchargement sera autorisé puisque Kris utilise un ordinateur portable de l'entreprise.
Kris tente de transférer des données sensibles ou un fichier contaminé par un malware via Slack ou de télécharger les données sur son stockage personnel Dropbox.	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** telles que l'isolation à distance du navigateur ou l'analyse des prestataires cloud pour détecter les configurations à risque (CSPM), selon les 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.