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
- Détectez et maîtrisez la Shadow IT

La Solution

- Sécurité des applications SaaS avec DLP intégré et protection contre les menaces avancées
- 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 modèles actuels de ressources humaines nécessitent que les utilisateurs aient un accès rapide, mais restreint aux données d'entreprise où qu'ils soient. Cela signifie que les utilisateurs ont besoin d'accéder aux données depuis des applications SaaS telles que Microsoft 365, Google Workspace, Slack, Jira et Salesforce sur n'importe quel type d'appareil et de n'importe quel emplacement. Il existe plus de 250 applications SaaS pour l'entreprise de taille moyenne, la visibilité et le contrôle peuvent donc rapidement devenir ingérables.

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

Forcepoint simplifie la sécurité cloud. Le service de sécurité CASB de Forcepoint ONE gère un accès Zero Trust permettant aux applications SaaS 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 plusieurs anti-programmes malveillants tiers. Il peut également détecter les programmes malveillants dans les fichiers de stockage SaaS et IaaS populaires, et mettre ces fichiers en quarantaine.

Détectez et maîtrisez la Shadow IT

Forcepoint ONE CASB met en lumière la 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 des pare-feux et proxies des entreprises 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.

Solution de sécurité SaaS qui maximise la disponibilité, la disponibilité et la productivité

Notre CASB est construit sur une architecture native du cloud et basée sur une infrastructure hyperscale avec plus de 300 points de présence (PoP), une accessibilité globale et une disponibilité éprouvée de 99,99 % pour sécuriser les applications SaaS de manière transparente et préserver la productivité des utilisateurs. D'autres solutions détournent le trafic réseau à destination et en provenance des applications SaaS vers des centres de données privés plutôt que vers des emplacements 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

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 téléversés dans les applications SaaS. Le CASB peut bloquer automatiquement le téléversement. Il peut même bloquer le téléversement de fichiers dans des applications non autorisées en utilisant l'agent unifié sur l'appareil.

Une partie de la stratégie Data Security Everywhere de Forcepoint

La mission Data Security Everywhere de Forcepoint permet aux organisations de protéger les données sur les SaaS, le Web, les e-mails, le réseau et les terminaux, afin que les utilisateurs puissent travailler en toute sécurité n'importe où avec des données disponibles partout.

Étendre les capacités DLP de pointe aux applications SaaS

Avec Forcepoint, les organisations peuvent utiliser leurs politiques Forcepoint DLP existantes pour sécuriser les données dans les applications SaaS, étendant cette même sécurité des données de pointe au cloud en quelques clics seulement. Les politiques DLP unifiées appliquées à partir d'une seule console aident à fournir une sécurité des données cohérente et de classe entreprise aux applications SaaS, en simplifiant la gestion de la sécurité des données, en minimisant les violations tout en rationalisant la conformité. Les clients bénéficient des avantages suivants grâce à cette intégration :

- → Sécurité des données simplifiée dans le cloud avec des politiques et une console unifiées.
- → 1 700 classificateurs et modèles de politiques prêts à l'emploi pour une couverture complète et un support à la conformité pour plus de 150 régions.
- → Configuration et délai de rentabilité en quelques minutes, améliorant la productivité des équipes informatiques et de sécurité.
- → Éliminer les produits de sécurité redondants et fragmentés permet de réaliser des économies significatives.

Lire la brochure Forcepoint DLP pour plus de détails.

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

Commençons par une démonstration.

forcepoint.com/contact