Forcepoint

Présentation succincte

Forcepoint ONE : 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.
- Contrôlez l'accès au contenu Web à haut risque.
- 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 simple plateforme unifiée permet de gérer un ensemble de politiques pour toutes les applications, tournant sur console isolée ou terminal endpoint.
- 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 (voir p. 2 pour plus de détails).

Résultat

- Simplification - Regroupe la sécurité du Web, du cloud et des applications privées via un seul ensemble de politiques, une seule console et un seul agent (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.

Les solutions à fonction uniques complexes vous exposent aux risques

La sécurité devient de plus en plus complexe. Lorsque 75 % du personnel travaille à distance, la frontière entre la maison et le bureau n'existe plus. Les données sont désormais partout – sur les sites Web, dans les applications cloud et dans les applications privées.

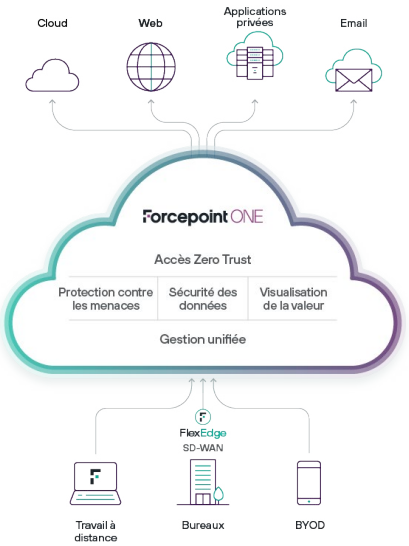
Les salariés distants, les partenaires et les sous-traitants qui utilisent des appareils non gérés et les politiques PAP vous rendent vulnérables. Les appareils se connectent en utilisant des VPN anciens et lents. Même les applications de travail que vous utilisez pour la collaboration ou la communication présentent des risques. Les cybercriminels et les États-nations s'en prennent à vos données et utilisent toutes les astuces possibles pour entrer par effraction.

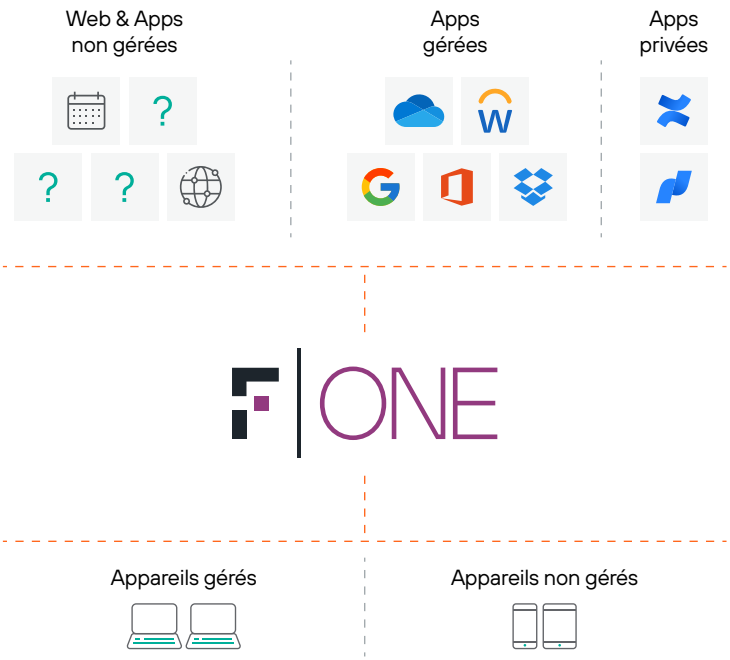
L'ancien portfolio de produits à fonctions ponctuelles n'était pas conçu pour faire face à ces situations. Il vous faut une approche beaucoup plus simple.

Forcepoint ONE simplifie la sécurité

Forcepoint ONE est une plateforme cloud tout-en-un qui simplifie la sécurité. Vous pouvez adopter rapidement Zero Trust et Security Service Edge (SSE, l'élément de sécurité de SASE), parce que nous avons unifié des services de sécurité essentiels, notamment Secure Web Gateway (SWG), Cloud Access Security Broker (CASB) et Zero Trust Network Access (ZTNA).

Vous n'aurez plus besoin de produits fragmentés. Nous vous offrons une seule plateforme, une seule console et un seul agent, avec de nombreuses solutions. Gagnez en visibilité, contrôlez l'accès et protégez vos données sur les applications gérées et non gérées et sur tous les appareils, à partir d'un seul ensemble de politiques de sécurité.





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

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

- → **Passerelles unifiées pour l'accès au web, au cloud et aux applications privées –** Contrôle d'accès aux applications d'entreprise basé sur l'identité et gestion via un seul point pour SWG, CASB et ZTNA.
- → **Sécurité BYOD sans agent pour les applications cloud et privées –** Utilisez en toute sécurité des applications web professionnelles privées à partir d'appareils personnels, tout en sécurisant les données sensibles.
- → **Protection contre les menaces avancées et sécurité des données** intégrée sur toutes les passerelles, empêchant la perte ou l'exfiltration de données et les effractions par les pirates.
- → **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.

- → **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. SWG embarqué sur appareil applique des politiques d'utilisation acceptables sur les appareils gérés situés n'importe où.
- → **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.
- → **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.

Application simplifiée à partir d'un seul ensemble de politiques

- → **Console de gestion unique** pour la configuration, la surveillance et les rapports
- → **Un ensemble unique de politiques de connexion** pour contrôler l'accès à des applications web, cloud ou privées en fonction de l'emplacement de l'utilisateur, du type d'appareil, de sa doctrine de sécurité, du comportement de l'utilisateur et du groupe d'utilisateurs. Ces paramètres aident à empêcher les prises de contrôle illégales de comptes.
- → **Un ensemble unique de politiques DLP** contrôle le téléchargement et l'envoi des données sensibles via les applications SaaS, les sites Web et les applications privées, et détecte et gère les données sensibles stockées dans les SaaS et IaaS.
- → **Un agent unifié sur appareil** pour Windows et MacOS pour la prise en charge de SWG, CASB et ZTNA pour les applications clientes hors navigateur et les applications shadow IT.
- → **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.
- → **Désarmement et reconstruction Zero Trust - Zero Trust Content Disarm and Reconstruction (CDR) :** Retire d'un document les malwares intégrés et recrée le fichier avant que l'utilisateur ne l'ouvre.

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
- → **Édition Sécurité Web** avec capacité d'ajout ultérieur de la prise en charge des applications cloud et privées.
- → **Tous les abonnements** comprennent une gestion centralisée du cloud, des politiques unifiées avec prévention des pertes de données, un accès automatisé via un agent unifié pour les terminaux endpoint et des rapports complets.

forcepoint.com/contact