Forcepoint

Fiche technique

# Forcepoint ONE

## Principaux avantages :

- Disponibilité vérifiée de 99,99 % depuis 2015
- Latence minimale et débit maximisé avec l'a mise à échelle automatique
- Intégration flexible dans n'importe quel IdP compatible avec SAML
- Console d'administration unifiée
- L'agent de synchronisation AD ou l'approvisionnement SCIM accélèrent l'intégration des utilisateurs
- Le proxy inverse avec AJAX-VM permet de protéger toutes les applications Web gérées sans agent sur l'appareil
- L'analyse des données en mouvement bloque les programmes malveillants et l'exfiltration des données entre les utilisateurs et toute application Web
- L'analyse des données au repos met en quarantaine les programmes malveillants et contrôle le partage de données à risque pour de nombreuses offres de stockage SaaS et IaaS populaires
- Le chiffrement des données structurées et non structurées dans le SaaS et IaaS garantit la protection des données
- Possibilité de bloquer des méthodes de requête HTTP/S spécifiques, ce qui permet un contrôle granulaire des interactions des utilisateurs avec n'importe quelle application Web SaaS ou privée

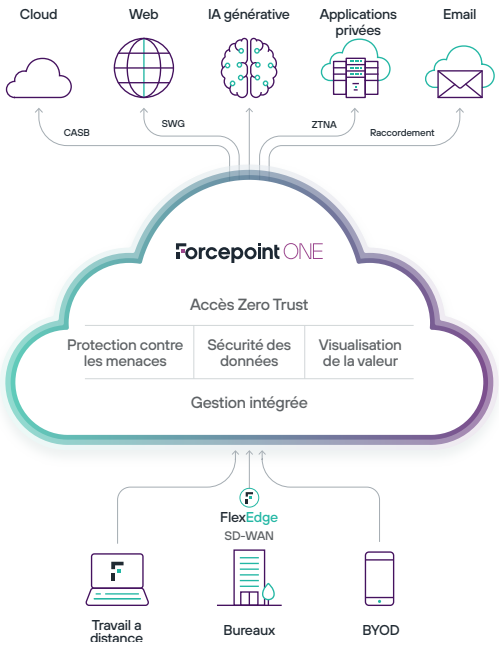
Forcepoint ONE est un service cloud qui sécurise les données en tout lieu pour les entreprises distribuées et les agences gouvernementales qui doivent s'adapter rapidement à l'évolution du travail à distance et hybride. Il fournit aux employés, aux sous-traitants et aux autres utilisateurs un accès sécurisé et contrôlé aux informations de l'entreprise sur le Web, dans le cloud (SaaS et IaaS) et dans les applications privées, tout en empêchant les intrusions et la fuite de données sensibles. Forcepoint ONE augmente la productivité des utilisateurs, que ce soit à distance ou au bureau, et l'efficacité des entreprises.

Forcepoint ONE combine les technologies de sécurité Zero Trust et SASE, y compris trois passerelles d'accès sécurisées et une variété de services de protection des menaces et de sécurité des données partagés, le tout basé sur une plateforme cloud native. Cette approche permet aux organisations de gérer des politiques unifiées, sur tous les canaux, afin d'éviter les menaces et de conserver les données sensibles.

→ **Sécurité Web.** Surveille et contrôle toute interaction avec n'importe quel site Web, y compris le blocage de l'accès aux sites Web en fonction de la catégorie et du score de risque, le blocage du téléchargement de logiciels malveillants, le blocage du téléversement de données sensibles et la détection et le contrôle des systèmes informatiques fantômes.

→ **Cloud Access Security Broker (CASB).** Solution avec ou sans agent qui permet d'appliquer des contrôles d'accès granulaire aux applications SaaS de l'entreprise en fonction de l'identité, de l'emplacement, de l'appareil et du groupe, qui permet d'appliquer contrôles d'accès granulaire en temps réel pour les applications privées. Il analyse les données statiques dans les SaaS et IaaS populaires pour y rechercher les programmes malveillants et les données sensibles, et prend les mesures correctives nécessaires. L'option sans agent facilite l'accès au BYOD et aux sous-traitants.

→ **Zero Trust Network Access (ZTNA).** Solution avec ou sans agent qui permet un accès granulaire aux applications privées sans nécessiter de VPN. Solution avec agent nécessaire pour les applications non-HTTP/S.




## Les fonctionnalités communes aux trois passerelles comprennent :

- **Contrôle d'accès contextuel.** L'accès aux applications Web, cloud ou privées est contrôlé en fonction du type de dispositif, de la posture de l'appareil, du comportement des utilisateurs et du groupe d'utilisateurs.
- **Data Loss Prevention (DLP).** Les fichiers et le texte sont scannés lors du téléversement et du téléchargement pour les données sensibles et bloqués, suivis, chiffrés ou expurgés le cas échéant. Plus de 190 règles DLP prédéfinies aident à simplifier le respect de la réglementation et à fournir une rentabilisation rapide. Intégration facile avec Forcepoint Enterprise DLP permet de sécuriser les données partout – sur le point de terminaison, dans le réseau, sur le Web et dans les services cloud.
- **Analyse des programmes malveillants.** Les fichiers sont analysés au moment de l'envoi et du téléchargement pour détecter et bloquer les malwares à l'utilisation.
- **Console de gestion intégrée.** Pour la configuration, la surveillance et le reporting.
- **Insights.** Tableaux de bord d'analyses sécurité avec des widgets et des visualisations personnalisables montrant l'impact de votre posture de sécurité au fil du temps, y compris les évaluations de valeur financière.
- **Agent sur l'appareil.** Pour Windows et macOS.
- **Disponibilité de 99,99 %.**

## Forcepoint ONE inclut également ces capacités complémentaires :

- **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.
- **SaaS Security Posture Management (SSPM).** Analyse les paramètres des clients Salesforce, ServiceNow et Office 365 à la recherche de configurations à risque et fournit une remédiation manuelle et automatisée.
- **Remote Browser Isolation (RBI) avec Content Disarm Reconstruction (CDR).** intégré Les utilisateurs sont protégés des logiciels malveillants Web sur leur appareil local en exécutant un navigateur dans une machine virtuelle hébergée dans le cloud. Avec le CDR, les téléchargements de documents et d'images peuvent être débarrassés des logiciels malveillants intégrés et reconstruits avant d'être ouverts par un utilisateur. Cela inclut la suppression des logiciels malveillants intégrés dans une image à l'aide de la stéganographie.
- **Classification Forcepoint.** La Data classification fonctionne avec des suggestions basées sur l'IA pour améliorer la précision du marquage.
- **Advanced Malware Detection and Prevention (AMDP).** Analyse le comportement des fichiers dans une sandbox de logiciels malveillants contrôlée pour identifier le contenu caché et malveillant.

Fonctionnalités et avantages de Forcepoint ONE

| CHAMP D'APPLICATION | CARACTÉRISTIQUES | AVANTAGES |
|---|---|---|
| À l'échelle de la plateforme | Architecture distribuée avec mise à échelle automatique sur AWS avec plus de 300 POP dans le monde. | → Disponibilité de 99,99 %.<br>→ Latence minimale : souvent même plus rapide que l'accès direct aux applications.<br>→ Analyse plus rapide des données au repos : heures par rapport aux jours d'analyse de l'intégralité du client de l'application. |
| | Intégration à n'importe quel IdP compatible SAML. Mode relais SAML ou proxy ACS. IdP intégré en option utilisant Microsoft ADFS. | → Déploiement flexible.<br>→ Protection par déni de service lors de l'utilisation du mode relais SAML. |
| | Agent de synchronisation Active Directory. Synchronise vos utilisateurs et groupes AD actuels avec les utilisateurs et les groupes Forcepoint ONE. | → Tirez parti de votre instance Microsoft AD existante pour intégrer rapidement les utilisateurs et gérer les groupes dans lesquels ils se trouvent. |
| | Intégration SCIM. Synchronise vos utilisateurs et groupes Azure AD actuels avec les utilisateurs et les groupes Forcepoint ONE. | → Tirez parti de votre client Azure AD existant pour intégrer rapidement les utilisateurs et gérer les groupes dans lesquels ils se trouvent. |
| | Contrôle d'accès contextuel. Donne aux utilisateurs un accès à Forcepoint ONE en fonction du groupe d'utilisateurs, du type d'appareil, de l'emplacement ou de l'heure de la journée. Passe en option à l'authentification multifacteur en fonction du « voyage impossible », d'emplacement non autorisé ou d'appareil non identifié. Couche supplémentaire de contrôle d'accès pour les sites Web ou les applications individuelles en fonction du groupe d'utilisateurs, du type d'appareil ou de l'emplacement. | → La détection et le blocage des tentatives d'identification suspicieuses réduisent les risques associés au vol de mot de passe.<br>→ Le contrôle d'accès granulaire permet de segmenter les utilisateurs en fonction du risque et du besoin d'accès. |
| | Support basé sur des agents pour SWG, CASB proxy direct, et ZTNA pour les applications non-Web. | → Déploiement simplifié des agents, y compris le déploiement via des systèmes MDM sélectionnés.<br>→ Faible usage du processeur et de la mémoire.<br>→ Les certificats autogénérés à rotation automatique garantissent la sécurité et réduisent les frais généraux de l'IT. |
| | Un administrateur intégré pour gérer toutes les fonctionnalités du système sur toutes les applications, utilisateurs et appareils. | → La console intégrée réduit la complexité et le temps de rentabilisation tout en augmentant la visibilité et le contrôle. |
| | Insights fournit des tableaux de bord d'analyses sécurité avec des widgets et des visualisations personnalisables montrant l'impact de votre état de sécurité au fil du temps, y compris les évaluations de valeur financière. | → Mesurez le risque et renforcez la posture de sécurité au fil du temps.<br>→ Estimez l'impact financier de votre plateforme de sécurité cloud. |

| CHAMP D'APPLICATION | CARACTÉRISTIQUES | AVANTAGES |
|---|---|---|
| CASB, SWG et ZTNA pour les applications Web | DLP et analyse antimalware pour toutes les données en mouvement. Analyse les pièces jointes téléchargées ou chargées vers n'importe quelle application ou site Web à la recherche de programmes malveillants ou de données sensibles. Enregistre et applique une action de remédiation appropriée comme le blocage (option unique pour SWG), la quarantaine, le chiffrement, l'application du DRM ou l'application du filigranage et du suivi des fichiers. L'intégration simple à Forcepoint Enterprise DLP fournit une sécurité des données en tout lieu : sur terminal, sur le réseau, sur le Web et dans les services cloud. | → Réduit le risque de fuite de données et de propagation de programmes malveillants en transit entre les utilisateurs et toute application ou site Web.<br>→ Facilite l'extension des politiques Enterprise DLP aux canaux SSE. |
| | Logique SASE programmable sur le terrain. Surveille, enregistre et bloque en option toute méthode de requête HTTP/S sur n'importe quelle partie de la méthode de requête. | → Une maîtrise plus fine de l'utilisation des applications.<br>→ Possibilité de bloquer le téléchargement de données sensibles en tant que publication de messages. |
| | Forcepoint ThreatSeeker fournit un réseau de renseignements de sécurité basé dans le cloud qui utilise plusieurs moteurs d'analyse pour fournir une visibilité en temps réel sur les dernières tendances en matière de menaces, y compris sur les programmes malveillants, l'hameçonnage et les ransomwares. | → Fonctionnement 24h/24 et 7j/7, le système automatisé distribue des informations sur les menaces aux solutions Forcepoint dans le monde entier pour protéger les données et les applications des menaces en évolution. |
| CASB et ZTNA pour les applications Web | Proxy inverse sans agent avec AJAX-VM. Le proxy inverse est un logiciel qui s'exécute dans nos POP principaux et en périphérie, tandis que l'AJAX-VM est une couche d'abstraction JavaScript s'exécutant à l'intérieur du navigateur de l'utilisateur final. Les deux fonctionnent ensemble pour s'assurer que Forcepoint ONE peut gérer le trafic entre n'importe quel appareil et n'importe quelle application Web gérée, sans qu'il soit nécessaire de disposer d'un logiciel agent sur l'appareil. | → Fonctionne avec n'importe quelle application Web, y compris les applications longtail et personnalisées que les autres solutions de proxy inverse ne peuvent pas prendre en charge.<br>→ Aucune installation d'agent n'est nécessaire pour le BYOD ou les sous-traitants.<br>→ Fournit un DLP sans agent.<br>→ Fonctionne avec n'importe quel appareil prenant en charge un navigateur moderne |
| SWG | Surveille, enregistre et contrôle l'accès à tout site Web à partir de points de terminaison Windows et Mac d'entreprise situés n'importe où avec l'analyse DLP et les logiciels malveillants à l'aide des moteurs d'analyse en temps réel de Forcepoint ONE. | → Applique une politique d'utilisation acceptable.<br>→ Surveille l'utilisation des systèmes informatiques fantômes.<br>→ Contrôle l'accès jusqu'au niveau de chemin du répertoire URL.<br>→ Bloque le chargement de données sensibles vers n'importe quel site Web. Bloque le téléchargement de programmes malveillants à partir de n'importe quel site Web.<br>→ L'architecture distribuée réduit le trafic passant par le panneau arrière Forcepoint ONE et permet d'atteindre un débit proche de celle de la fibre. |
| CASB | DLP et analyse des programmes malveillants pour les données au repos dans le cloud. Analyse les données structurées et non structurées dans le stockage SaaS et IaaS à la recherche de programmes malveillants ou de données sensibles, et enregistre et met en œuvre une action de protection appropriée comme la quarantaine, le chiffrement ou la suppression du partage public. | → Analyse les données historiques, pas seulement les fichiers ajoutés récemment.<br>→ Applique l'OCR aux fichiers d'image pour détecter les données de texte sensibles. Désactive le partage public des fichiers comportant des données sensibles. Mise en quarantaine des programmes malveillants stockés dans le cloud.<br>→ Une vaste bibliothèque de modèles de données prédéfinis réduit le temps d'installation. |

| CHAMP D'APPLICATION | CARACTÉRISTIQUES | AVANTAGES |
|---|---|---|
| CASB | Chiffrement des données. Chiffre les données sensibles structurées et non structurées dans le SaaS et l'IaaS gérés. | → Garantit que les données sensibles ne sont visibles que par les utilisateurs autorisés. |
| | Détection et contrôle de Shadow IT. | → Utilise les journaux des pare-feu d'entreprise et des serveurs proxy pour détecter l'utilisation de shadow IT.<br>→ Bloque l'utilisation de n'importe quelle application de shadow IT tout en fournissant un message d'information recommandant une alternative validée par l'entreprise. |
| CSPM | Cloud Security Posture Management. Analyse la configuration des paramètres de sécurité pour AWS, GCP et le SaaS d'administration Azure en fonction de diverses lignes de référence sectorielles et régionales, ainsi que de lignes de référence personnalisées. | → Marque le paramètre à risque pour remédiation. Applique une remédiation oneclick ou une remédiation automatisée, le cas échéant. |
| SSPM | SaaS Security Posture Management. Analyse la configuration des paramètres de sécurité pour les clients SaaS populaires en fonction de diverses lignes de référence de l'industrie et de la région, ainsi que de lignes de référence personnalisées. | → Marque le paramètre à risque pour remédiation. Applique une remédiation oneclick ou une remédiation automatisée, le cas échéant. |
| AMDP | Complète SWG pour analyser le comportement des fichiers dans un environnement sandbox afin de détecter et de prévenir les logiciels malveillants. | → Protège les téléchargements de logiciels malveillants et de ransomware. |
| RBI avec CDR | Remote Browser Isolation avec Content Disarm and Reconstruction. Forcepoint ONE Web Security est livré avec un niveau de RBI « essentiel » pour les sites « non catégorisés » et « nouvellement enregistrés », qui peut être étendu avec des licences en options pour RBI afin de couvrir davantage de catégories Web. Fournit une couche d'abstraction en exécutant un navigateur dans une machine virtuelle hébergée dans le cloud, séparant l'appareil de l'utilisateur final du risque de logiciels malveillants Web. Lorsque l'utilisateur télécharge un document ou un fichier image, CDR est appliqué qui extrait les informations commerciales valides du fichier, vérifie que les informations extraites sont bien structurées, puis crée un tout nouveau fichier pour transporter les informations à sa destination. | → L'expérience de navigation sur le Web est identique<br>→ Capacité de prise en charge d'un large éventail de destinations web : applications cloud modernes comme Google Workspace ou sites construits selon des protocoles plus anciens.<br>→ Maintient les données sensibles des applications Web hors des caches des navigateurs des appareils personnels, limite les fonctions de partage des données des sites Web et intégre le DLP leader du marché.<br>→ Les fichiers traités par CDR sont exempts de programmes malveillants. Cela inclut la suppression des programmes malveillants intégrés à une image utilisant la stéganographie. |