Forcepoint

Présentation succincte

Forcepoint ONE Web Security

Arrêtez les pertes de données et les attaques de malware, pas la productivité.

Études de cas

- Offrez aux employés un accès rapide et sûr au Web
- Mettez en place des politiques d'utilisation acceptable
- Bloquez le téléchargement de données sensibles vers des sites web non sanctionnés
- Empêchez les malwares de pénétrer sur les appareils des utilisateurs sans entraver l'expérience de l'utilisateur.
- Détectez et contrôlez la Shadow IT
- Empêchez que les entreprises exposent par accident

La Solution

- Sécurité web rapide avec DLP intégré et protection avancée contre les menaces
- Contrôles Zero Trust granulaires d'accès et de données basés sur le groupe d'utilisateurs, le type d'appareil, l'emplacement de l'utilisateur, la catégorie de site Web, le score de risque du site Web et bien plus
- L'architecture distribuée élimine les points d'étranglement sur la plate-forme à haute disponibilité
- Inclut Remote Browser Isolation (RBI) pour une navigation et des téléchargements sûrs à partir de sites non catégorisés et nouvellement enregistrés

Résultats

- Augmentez la productivité, en permettant à vos utilisateurs de naviguer sur le Web depuis n'importe où, de manière transparente et en toute sécurité
- Réduisez les risques en contrôlant les données sensibles dans le cloud et en stoppant les malwares
- Réduits les coûts en simplifiant les opérations de sécurité

Le Web est à la fois un atout et un fléau. La plupart des gens y puisent des informations pour faire leur travail, mais le web crée aussi des risques d'exfiltration de données, de violation de la politique des RH, de perte de productivité et de propagation de logiciels malveillants. L'IAg n'a fait que relever les enjeux - si elle promet un accroissement massif de la productivité, elle expose également votre organisation à des risques beaucoup plus important. Cependant, avec les mesures de protection appropriées, vous pouvez tirer profit des accroissements de productivité que l'IA peut offrir tout en assurant la sécurité des données sensibles et en garantissant une utilisation acceptable. Si les conséquences d'un manque de sécurité des données et des personnes ne cessent de croître, la sécurisation des interactions Web est une exigence stratégique pour les organisations modernes.

Offrez aux employés un accès rapide et sûr au Web

La plupart des solutions de sécurité Web modernes forcent l'ensemble du trafic Web à faire un détour par un centre de données centralisé - qu'il soit sur site ou dans le cloud - ce qui ajoute un temps de latence susceptible d'interférer de manière significative avec les applications Web modernes. De plus, alors que les architectures cloud sont spécifiquement conçues pour évoluer en fonction de la demande, de nombreux fournisseurs de SWG ne disposent pas d'une telle couverture hautement décentralisée dans le cloud. À l'inverse Forcepoint ONE dispose d'une architecture décentralisée qui non seulement fournit une architecture cloud hautement robuste avec plus de 300 points de présence dans le monde, mais va encore plus loin avec une option alternative pour donner aux clients encore plus de flexibilité - un agent intégré au dispositif qui élimine les points d'étranglement et peut fournir jusqu'à deux fois plus de débit pour les contenus et applications web sensibles aux performances que les passerelles web sécurisées concurrent. Cette option permet de faire appliquer les politiques de sécurité en local sur le dispositif de l'utilisateur, de sorte que le trafic puisse être échangé directement entre l'utilisateur et le site Web.

Mettez en place des politiques d'utilisation acceptable (PUA) pour les sites à risque

Le Web peut être un endroit distrayant qui n'est pas toujours utilisé pour les affaires d'entreprise. Les paramètres de commande de Forcepoint ONE vous permettent de bloquer, d'utiliser une page de confirmation, d'utiliser un quota de temps, de demander une authentification multi facteurs, d'autoriser, ou même d'utiliser RBI pour isoler le trafic. Vous pouvez administrer l'accès en fonction du groupe d'utilisateurs, de la posture du dispositif, de l'emplacement. Ceci peut permettre à une organisation de renforcer facilement les contrôles pour bloquer l'utilisation d'un site IAg par l'informatique fantôme, par exemple, pour générer du code avec une page de blocage pour les diriger vers les ressources approuvées par l'entreprise, et la granularité pour distinguer d'autres sites d'IA, par exemple pour permettre l'accès à des sites d'IA conversationnels ou multimédias tout en renforçant la protection des données qui peuvent être publiées sur ces sites.

Bloquez le téléchargement de données sensibles vers des sites web non sanctionnés

Grâce à notre moteur de sécurité, vous pouvez empêcher l'envoi de données réglementées ou de propriété intellectuelle vers des sites de stockage de fichiers personnels, des médias sociaux, des comptes de messagerie personnels ou des sites IAg. Vous pouvez scanner et bloquer les téléversements de fichiers et les messages textes à la recherche de données sensibles à l'aide de commandes faciles à utiliser. Les clients peuvent également hériter des politiques DLP avancées de Forcepoint ONE Data Security pour renforcer la meilleure solution de sécurité des données de l'industrie.

Empêchez les malwares de pénétrer sur les appareils des utilisateurs sans entraver l'expérience de l'utilisateur.

Le service Forcepoint ONE Web Security offre de multiples formes de protection contre les logiciels malveillants véhiculés par le Web, y compris le blocage de certaines catégories de sites Web, l'analyse en ligne des fichiers téléchargés, et une protection avancée contre les menaces basée sur Zero Trust, telle que Remote Browser Isolation (Isolation du navigateur à distance). Avec Forcepoint RBI, même les sites ou les fichiers téléchargés qui sont contaminés peuvent être utilisés en toute sécurité et efficacement.

Détectez et contrôlez la Shadow IT

Le service de sécurité Web identifie les sites Web qui sont utilisés à la place des applications traditionnelles de l'entreprise. Ces sites « informatiques fantômes » sont recueillis automatiquement et affichés dans le tableau de bord des applications cloud.

Empêchez que les entreprises exposent par accident les données privées de leurs clients

Pour protéger la confidentialité des employés, les organisations peuvent empêcher le décryptage et l'inspection du trafic en provenance et à destination de catégories spécifiques de sites Web qui sont généralement utilisés avec des informations personnelles identifiables (IPI), comme les données bancaires, de santé et d'assurance.

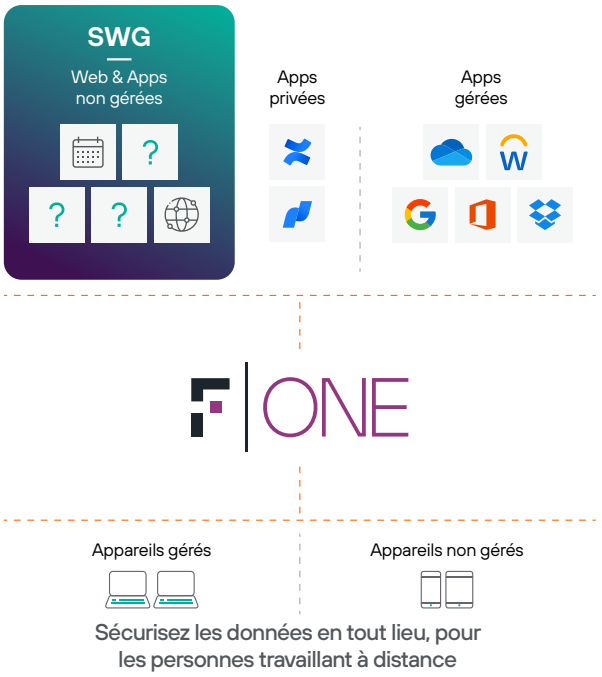
Forcepoint ONE Web Security optimise le temps de disponibilité, de productivité et de performance

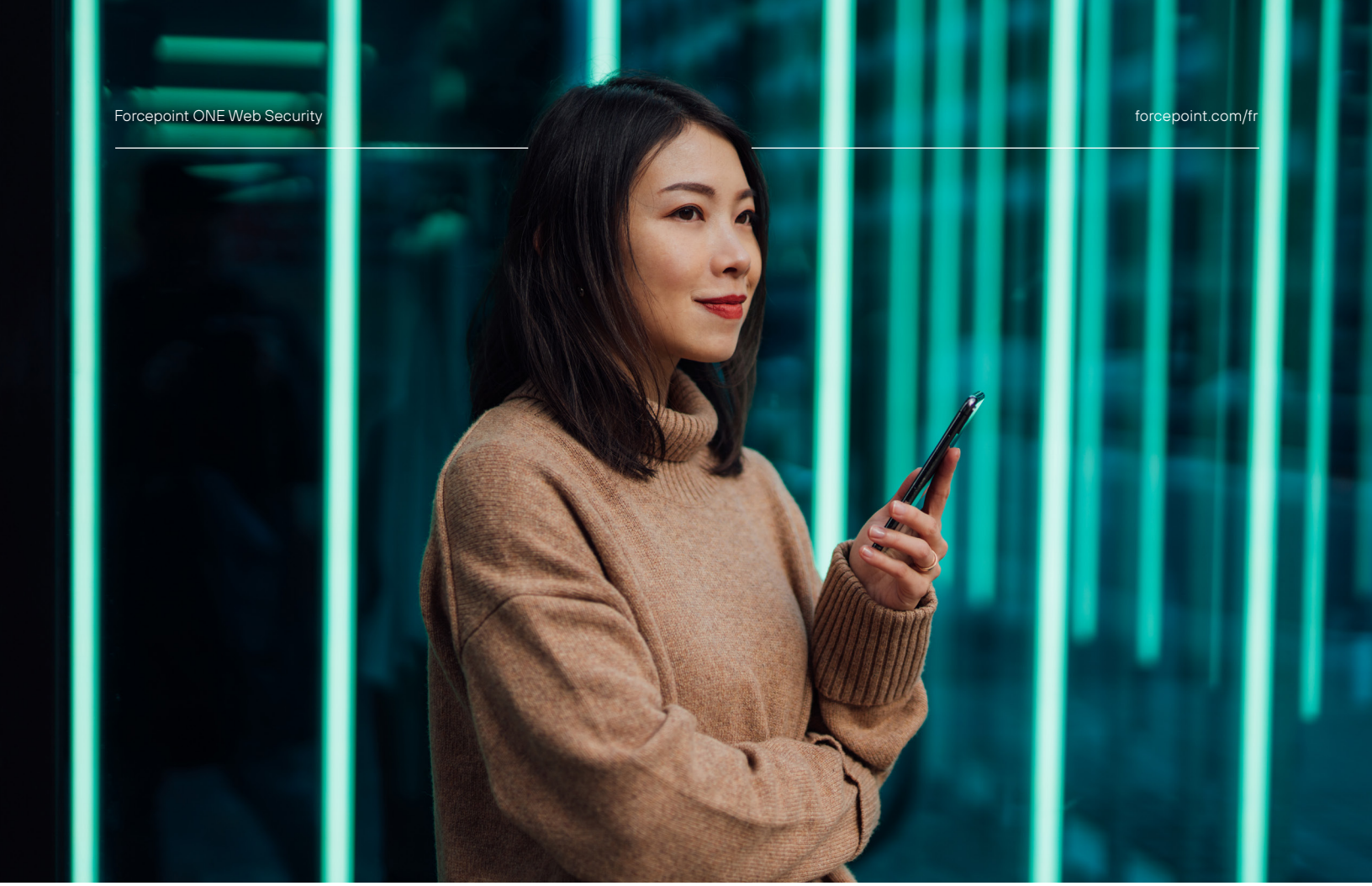
Le service de sécurité Web fait partie de Forcepoint ONE, notre plateforme cloud avancée avec 300 points de présence (PoPs), une accessibilité universelle et temps de disponibilité avéré de 99,999 % pour sécuriser l'accès au Web et préserver la productivité des utilisateurs. Forcepoint ONE inclut CASB, SWG et ZTNA pour sécuriser l'accès aux applications SaaS, Web et privées de l'entreprise, ce qui simplifie la sécurité.

Simplifier la sécurité Web dans le monde réel

La plateforme cloud Forcepoint ONE offre un simple « bouton poussoir » pour mettre en oeuvre la sécurité dans le cloud.

À partir d'une seule console, les administrateurs peuvent gérer l'accès et contrôler les téléchargements et les téléversements de fichiers avec n'importe quel site en temps réel, y compris l'application de Zero Trust Web Access à l'aide de Forcepoint RBI.





Voyons comment le service de sécurité Web facilite les choses lorsque Kris, un analyste commerciale travaillant à domicile, commence sa journée de travail.

Kris se rend sur reddit.com pour des recherches liées à l'entreprise.	Kris se rend sur reddit.com/r/technology pour rechercher des messages récents sur les malwares. Les politiques de contenu SWG autorisent une granularité au niveau du répertoire. Ce subreddit est considéré comme lié au travail, donc Kris peut y accéder.
Dans le subreddit r/technologie, Kris clique accidentellement sur un lien vers une page inappropriée.	L'administrateur Forcepoint ONE de Kris a créé des politiques de contenu SWG qui autorisent l'accès à des répertoires tels que r/technologie, mais bloquent l'accès aux subreddits et aux pages inappropriées. La SWG remarque l'erreur de Kris et bloque la nouvelle page.
Kris commence une feuille de calcul confidentielle sur son ordinateur portable de l'entreprise, qui comprend des IPI de clients, et veut continuer à travailler sur son ordinateur portable personnel. Krys essaie de télécharger le fichier sur son stockage cloud personnel puis de le télécharger sur son ordinateur portable personnel.	Pour empêcher la perte de données commerciales, l'administrateur Forcepoint ONE de l'entreprise a créé une politique de contenu SWG qui bloque le téléchargement des informations personnelles identifiables des clients (PII) sur tout site Web de partage de fichiers personnels. Lorsque Kris tente le téléchargement, il est bloqué et un message s'affiche pour expliquer pourquoi le téléchargement a été bloqué.

Une partie d'une solution de sécurité intégrée pour les applications Web, cloud et privées

En plus de la sécurité Web, la plateforme de sécurité cloud Forcepoint ONE sécurise l'accès aux informations professionnelles sur n'importe quel hébergement SaaS de l'entreprise et sur les applications privées :

- **Cloud (SaaS et IaaS) :** CASB apporte un contrôle d'accès contextuel, une prévention des pertes de données (DLP) et une protection contre les logiciels malveillants à toute application Web publique prenant en charge l'intégration SAML 2 avec des fournisseurs d'identitié tiers (IdP), à partir de n'importe quel navigateur moderne sur n'importe quel dispositif connecté à Internet. Les données au repos dans les IaaS et SaaS les plus répandus peuvent également être scannées à des fins de détection de données sensibles et de logiciels malveillants, puis remédiées. S'intègre à Forcepoint ONE Data Security pour renforcer les politiques DLP avancées sur les canaux SSE.
- **Applications privées :** ZTNA sécurise et simplifie l'accès aux applications privées sans la complication ou le risque associés aux VPN. Comme les autres solutions Forcepoint ONE, ZTNA applique également le contrôle d'accès contextuel, la DLP et la protection contre les malwares à toute application Web privée.
- **Fonctions supplémentaires :** Développez le niveau essentiel de RBI avec CDR pour l'utiliser au-delà des sites inconnus ou nouvellement enregistrés pour la forme ultime de protection contre les menaces en ligne, ou ajoutez la détection et la protection avancées des logiciels malveillants pour une analyse et une mis en bac à sable des logiciels malveillants de niveau professionnel.

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

Prêt à sécuriser les données dans les applications cloud à partir de n'importe quel appareil ?

Commençons par une démonstration.

forcepoint.com/contact

©2024 Forcepoint. Forcepoint et le logo FORCEPOINT sont des marques déposées par Forcepoint. Toutes les autres marques citées dans ce document appartiennent à leurs propriétaires respectifs. [FP ONE Web Security Solution Brief-FR] 03Jul2024