Zero Trust Network Access

Simplifier la sécurisation des applications privées sans VPN

Études de cas

- Remplacez les VPN pour accéder aux applications privées dans les centres de données et les clouds privés.
- Fournissez un accès sécurisé et sans agent à des applications Web privées à partir d'appareils PAP et non gérés.
- Contrôlez l'envoi et la réception de données sensibles dans n'importe quelle application Web privée.
- Stoppez les malwares cachés dans les fichiers de données d'entreprise des applications Web privées
- Protégez l'accès aux serveurs privés non-Web à partir d'appareils Windows et macOS gérés.

La Solution

- Une sécurité intégrée dans les applications privées incluant une protection contre les menaces avancées et un DLP.
- Contrôles d'accès Zero Trust sans agent pour les applications Web privées à partir d'appareils PAP et gérés.
- Accès à distance aux applications privées non-Web à partir d'appareils Windows et macOS gérés.
- Élément d'un service tout-en-un exécuté dans le cloud incluant SWG, CASB, et d'autres techniques de sécurité modernes.

Résultat

- Augmentez la productivité, en permettant aux salariés d'accéder à des applications privées de manière transparente et sûre, où qu'ils soient.
- Réduisez les coûts en simplifiant les activités de sécurisation en configurant toutes les politiques depuis un seul endroit.
- Réduisez les risques en contrôlant les données sensibles et les malwares transitant vers, et depuis, les applications Web privées.
- Rationalisez la conformité avec des processus démontrables pour contrôler l'information.

Le travail à distance a mis en évidence les limites, les coûts et les risques des réseaux privés virtuels (VPN). Une fois connectés, les VPN accordent une confiance implicite bien trop excessive, permettant aux utilisateurs d'analyser et de sonder d'autres adresses IP dans ce centre de données privé ou ce cloud privé virtuel, ce qui laisse le champ libre à des failles de sécurité. Toutefois, les entreprises qui souhaitent migrer des VPN vers des solutions d'accès réseau à confiance zéro (Zero Trust Network Access ou ZTNA) ne devraient pas rencontrer de complications ni utiliser des produits à fonction unique. Adopter ZTNA devrait être simple et sans heurts.

Le ZTNA de Forcepoint contrôle l'accès aux applications privées Web et non-Web que chaque employé, entrepreneur et partenaire a la permission explicite d'utiliser. Forcepoint ZTNA vous donne un contrôle infiniment plus grand avec la confiance nécessaire pour autoriser les gens à utiliser les appareils qui leur conviennent le mieux, même les appareils non gérés et le PAP.

Contrairement à d'autres solutions, Forcepoint ZTNA offre également des contrôles continus à fine granularité, les meilleures performances du secteur et une solution intégrée contre les malwares et la protection des données, afin d'offrir une excellente expérience utilisateur malgré les complexités des réseaux modernes. Vous pouvez également ajouter facilement d'autres solutions de sécurité comme Cloud Access Security Broker (CASB) et Secure Web Gateway (SWG) selon vos besoins, qui seront entièrement intégrées dans la plateforme cloud Forcepoint ONE.

Remplacez les VPN pour accéder aux applications privées dans les centres de données et les clouds privés.
Pour sécuriser l'accès aux applications privées, il faut un contrôle rapide et précis. Vous pouvez limiter l'accès aux applications privées comme les serveurs ERP ou de chaîne d'approvisionnement en fonction de l'identité, de l'appartenance à un groupe, du type d'appareil et de la localisation. Pour les applications non Web, vous pouvez appliquer des contrôles par port et protéger l'accès à partir de lieux ou d'appareils inconnus. Si la tentative de connexion semble suspecte, les utilisateurs doivent prouver leur identité au moyen d'une authentification multifactorielle (MFA). Tout cela se passe en quelques millisecondes grâce à la plateforme hyperscale de Forcepoint.

Fournir un accès sécurisé et sans agent aux applications Web privées avec PAP
Les utilisateurs peuvent se connecter en toute sécurité et de manière pratique par Internet à des applications Web hébergées derrière un firewall, même à partir d'appareils PAP et non gérés, sans avoir besoin d'agents.

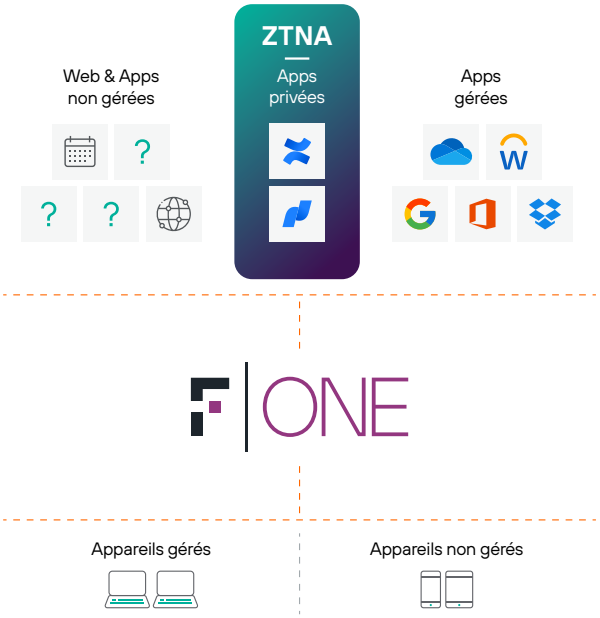
Contrôlez l'envoi et la réception de données sensibles dans n'importe quelle application Web privée.
Gérez un ensemble de politiques de sécurité pour contrôler les données sensibles, avec un accès à l'analyse des malwares et à la DLP intégrée pour stopper les pirates et les violations de données. En combinant la sécurité des données avec des politiques relatives à la position et à la localisation des appareils, il est plus facile de contrôler la façon dont les gens font transiter les données depuis et vers des applications Web privées sur n'importe quel appareil.

Stoppez les malwares cachés dans les fichiers de données d'entreprise ou dans les applications Web privées
Forcepoint freine les ransomwares. Détectez et bloquez les malwares dans les données circulant entre les utilisateurs et toute application Web privée en utilisant les moteurs d'analyse de Bitdefender et CrowdStrike.

Protégez l'accès aux serveurs privés non Web à partir d'appareils gérés.
Notre ZTNA est conçu pour permettre l'accès à des applications privées non Web comme Secure Shell (SSH) et le bureau à distance depuis des PC ou des Mac gérés avec l'agent unifié Forcepoint ONE.

ZTNA dans Forcepoint ONE maximise le temps de fonctionnement, la disponibilité et la productivité
ZTNA 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 % pour sécuriser les applications cloud sans entrave et préserver la productivité des utilisateurs. D'autres solutions détournent le trafic réseau vers des centres de données privés au lieu de sites proches des utilisateurs, ce qui peut générer des performances médiocres. Forcepoint ONE unifie CASB, SWG et ZTNA pour sécuriser l'accès aux applications SaaS, Web et privées de l'entreprise, ce qui simplifie la sécurité.

Faciliter la sécurité des applications privées pour une utilisation réaliste
La plateforme cloud Forcepoint ONE offre un « bouton facile » pour mettre en œuvre la sécurité des applications privées. 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).



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

Regardez comment la capacité ZTNA simplifie la sécurité dans le cloud lors du démarrage de la journée de travail de Kris, un analyste travaillant à domicile.

Kris se connecte à son compte Forcepoint ONE à partir de son ordinateur portable fourni par l'entreprise.	Puisque Kris essaie de se connecter à partir d'un appareil géré, et depuis un endroit autorisé, l'accès lui est accordé. Une tentative de connexion à partir d'un lieu inconnu nécessite une réponse positive via les applications MFA.
Kris bénéficie d'un accès en un clic à l'application de chaîne d'approvisionnement propriétaire de l'entreprise à partir du portail utilisateur Forcepoint ONE.	Le navigateur de Kris affiche le portail Forcepoint ONE, avec des onglets pour chaque application Web à laquelle Kris et ses partenaires de la chaîne d'approvisionnement peuvent accéder (si l'entreprise de Kris utilise Forcepoint ONE CASB, les applications SaaS gérées de Kris sont accessibles depuis le même portail utilisateur pour une expérience cohérente).
Kris se voit accorder l'accès aux applications gérées.	Le trafic entre l'ordinateur portable de Kris et l'application de la chaîne d'approvisionnement passe automatiquement par le proxy inversé de Forcepoint ONE. Forcepoint analyse les envois et téléchargements de fichiers à la recherche de malware et de données sensibles.
Kris envoie un contrat de prestataire en pièce jointe.	Étant donné que la politique de connexion de Kris prévoit l'analyse des fichiers, le téléchargement est autorisé si le fichier est exempt de malware. S'il est infecté, la passerelle ZTNA bloque le téléchargement, alerte Kris et génère un journal et un rapport sur l'événement de blocage.
Kris envoie un contrat de prestataire en pièce jointe.	Étant donné que la politique de connexion de Kris prévoit l'analyse des fichiers, le téléchargement est autorisé si le fichier est exempt de malware. S'il est infecté, la passerelle ZTNA bloque le téléchargement, alerte Kris et génère un journal et un rapport sur l'événement de blocage.

Élément d'une solution de sécurité unifiée pour le Web, le cloud et les applications privées.

Outre ZTNA, 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.
- → **Cloud :** CASB sécurise et simplifie l'accès aux locataires SaaS et IaaS de l'entreprise tout en contrôlant la transmission des données sensibles et des malwares, sans avoir besoin d'un agent sur l'appareil.
- → **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.

forcepoint.com/contact