

# Proofpoint Web Security

## Principales fonctionnalités

- **Surveillance et visibilité** — Déchiffrement et inspection du trafic SSL ; filtrage par domaine, URL et adresse IP ; filtrage par catégorie de contenu et de menaces ; application par le biais d'une page de blocage personnalisable et de l'isolation du navigateur ; découverte des applications SaaS en ligne (shadow IT) et contrôle des applications
- **Protection contre les menaces avancées** — Protection en ligne contre le téléchargement de fichiers malveillants ; application par le biais d'une page de blocage personnalisable et de l'isolation du navigateur ; détection et prévention basées sur la réputation s'appuyant sur la threat intelligence de Proofpoint ; sandboxing ; protection contre les menaces « zero day »
- **Prévention des fuites de données** — Protection en ligne contre le téléchargement ; application par le biais de l'isolation sélective du navigateur ; plusieurs centaines de détecteurs, de dictionnaires et d'identifiants intelligents prédéfinis ; types de données personnalisables
- **Gestion** — Solution native au cloud ; proxy distribué dans le monde entier ; gestion dans le cloud ; client commun avec Proofpoint ZTNA et Proofpoint CASB ; composant modulaire de la plate-forme Proofpoint Information and Cloud Security ; prise en charge de Windows et macOS ; authentification unique ; allocation de ressources aux utilisateurs grâce à une solution IdP (SCIM, SAML, JIT) ; intégration SIEM

Proofpoint Web Security protège vos utilisateurs contre les menaces avancées lorsqu'ils naviguent sur le Web. Cette solution sécurise l'accès Internet de tous vos collaborateurs, qu'ils se trouvent à l'intérieur ou à l'extérieur de votre périmètre. Elle applique des règles de surveillance et de visibilité, de protection contre les menaces avancées et de prévention des fuites de données (DLP) dans le cadre d'une approche de la sécurité centrée sur les personnes.

## Surveillance et visibilité

La surveillance et la visibilité sont au cœur de l'approche de Proofpoint Web Security. La solution inspecte tout le trafic SSL dès sa mise en service, ce qui permet d'identifier les menaces et tout accès à du contenu non conforme. La solution détecte également les applications SaaS et applique des contrôles afin de les sécuriser. Ces contrôles permettent de bloquer les activités suivantes :

- Vol d'identifiants de connexion
- Affichage de contenu soumis à des restrictions
- Consultation de sites non conformes
- Comportement des botnets et communications de commande et contrôle
- Utilisation d'applications SaaS non approuvées (Shadow IT)

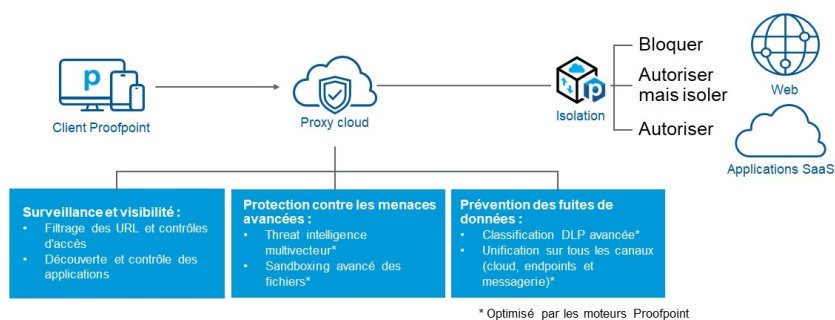


Figure 1. Fonctionnement de Proofpoint Web Security

Proofpoint Web Security identifie les menaces en temps réel. Elle surveille les dangers au niveau des domaines, des URL et des adresses IP, offrant ainsi une couverture complète qui réduit la charge de travail. La solution peut en outre bloquer des sites, de même qu'isoler automatiquement les sessions Web des utilisateurs s'ils accèdent à des URL suspectes. Vous pouvez appliquer ces contrôles à l'ensemble de votre entreprise. Vous pouvez également choisir de les appliquer uniquement à certains groupes d'utilisateurs ou aux utilisateurs à haut risque.

## Protection contre les menaces avancées

La protection contre les menaces avancées de Proofpoint Web Security assure la sécurité de vos endpoints. Elle bloque les menaces connues grâce à la détection basée sur les signatures. Elle inspecte en outre les fichiers « zero day » inconnus en temps réel dans un environnement sandbox hébergé dans le cloud. Proofpoint Web Security fonctionne de manière transparente. La solution n'a pas d'impact notable sur l'expérience de l'utilisateur lorsqu'il télécharge des fichiers malveillants ou consulte des sites suspects. Elle s'appuie sur la threat intelligence de Proofpoint, optimisée par le graphique des menaces Nexus.

## Prévention des fuites de données

Intégrée à Proofpoint Enterprise DLP, la solution Proofpoint Web Security offre des fonctionnalités intégrées de prévention des fuites de données pour toutes les applications Web. Elle assure également la classification des données partagées et propose une console unique pour la gestion des alertes et les investigations. Vous pouvez restreindre les téléchargements et les téléchargements par catégorie, URL ou niveau de risque. Vous pouvez également appliquer un mode en lecture seule lorsque les utilisateurs consultent des sites Web suspects.

Proofpoint Web Security dispose de plus de 240 détecteurs, dictionnaires et identifiants intelligents de classification des données couvrant de nombreux types de données. Elle propose également des définitions de règles de classification simples et unifiées, associées à des modèles intégrés. Comme de nombreuses entreprises ont besoin d'ensembles de données personnalisés, il est également possible d'utiliser une fonctionnalité de mise en correspondance exacte des données. Toutes les règles peuvent être appliquées à l'échelle de l'entreprise, à certains groupes d'utilisateurs ou à des collaborateurs clés uniquement.

## Gestion

Proofpoint Web Security est une solution native au cloud, capable d'évoluer pour répondre à tous vos besoins. Sa distribution dans le monde entier garantit également une faible latence, indépendamment de l'emplacement de vos utilisateurs. Par ailleurs, toutes les opérations de gestion s'effectuent via une console hébergée dans le cloud. Et comme la solution est basée sur une API, elle peut être gérée à distance. Elle s'intègre également parfaitement avec votre système de gestion des événements et des incidents de sécurité (SIEM). Proofpoint Web Security utilise le même client de gestion des endpoints que Proofpoint ZeroTrust Network Access (ZTNA) et Proofpoint Cloud App Security Broker (CASB).

## Plate-forme Proofpoint Information and Cloud Security

Proofpoint Web Security est un composant de la plate-forme Proofpoint Information and Cloud Security. Celle-ci offre une sécurité cohérente à l'échelle de votre entreprise dans le cadre de votre stratégie SSE (Security Service Edge). Elle propose en outre une console unifiée d'administration et de réponse aux incidents.

La plate-forme inclut les produits suivants :

- Proofpoint Cloud App Security Broker (CASB)
- Proofpoint Zero Trust Network Access (ZTNA)
- Proofpoint Web Security et Proofpoint Browser Isolation
- Proofpoint Email Data Loss Prevention (DLP) et Proofpoint Email Encryption
- Proofpoint Insider Threat Management (ITM) et Proofpoint Endpoint Data Loss Prevention

La plate-forme offre également une modélisation intelligente des risques, une détection de pointe des menaces, des contenus et des comportements, ainsi qu'une visibilité et un contrôle complets.

## EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : [proofpoint.com/fr](https://www.proofpoint.com/fr).

### À PROPOS DE PROOFPOINT

Proofpoint, Inc. est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risques des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris plus de la moitié des entreprises de l'index Fortune 1000, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via les emails, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur [www.proofpoint.com/fr](https://www.proofpoint.com/fr).

© Proofpoint, Inc. Proofpoint est une marque commerciale de Proofpoint, Inc. aux États-Unis et dans d'autres pays. Toutes les autres marques citées dans ce document sont la propriété de leurs détenteurs respectifs.