OLFEO, LEADER FRANÇAIS DE LA SÉCURITÉ WEB

FICHE PRODUITS

Olfeo
La sécurité positive

LA PASSERELLE DE SÉCURITÉ WEB DISRUPTIVE, BASÉE SUR UNE VISION À 360°

Nous accompagnons depuis plus de 16 ans les entreprises exigeantes dans la sécurisation, l'analyse et l'optimisation de leur flux web. Grâce à notre connaissance extrêmement fine des besoins des organisations françaises, nous avons développé une passerelle de sécurité web disruptive, basée sur une vision globale, et pas uniquement technologique.

Nos solutions allient :

- La **sécurisation** intégrale de vos accès web grâce à des solutions technologiques de haut niveau et à une base de données d'une qualité inégalée ;
- La **responsabilisation** et **la formation** de vos collaborateurs en les rendant acteurs de votre politique de sécurité ;
- La **protection juridique** totale grâce à l'intégration des lois françaises & européennes (droit pénal, droit social, RGPD, etc.) ;
- La **confiance d'un éditeur français** pour assurer la proximité et la souveraineté de vos données.

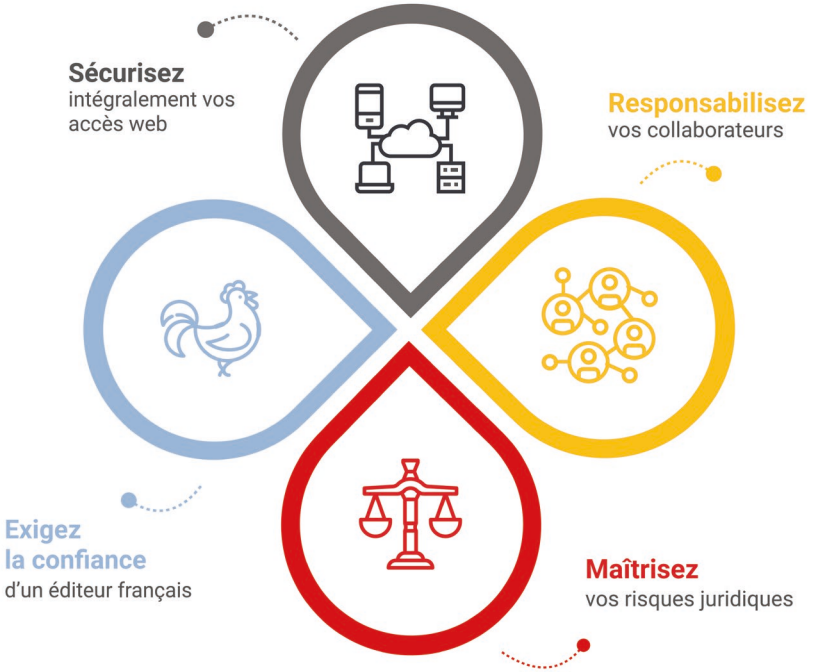
C'est ce que l'on appelle la **sécurité positive**.

Notre solution a aujourd'hui été adoptée par 1000 clients et a obtenu de nombreux labels, notamment :

« Utilisé par les armées françaises » ou « France Cybersecurity ».

Notre passerelle de sécurité web, basée sur une infrastructure proxy inclut les produits suivants :

Filtrage web P.3
Proxy avancé P.5
Antivirus web P.7
Campus P.9
Filtrage DNS P.11
Nomadisme P.13
Portail public P.15
Filtrage protocolaire P.17



Olfeo, la proximité et le service

Toutes les équipes Olfeo sont basées à Paris; elles répondent en français à toutes vos sollicitations.

Olfeo, des coûts maîtrisés

Olfeo indexe ses prix uniquement sur le nombre d'utilisateurs. Pas de risques de débordements liés à l'augmentation de la bande passante ou à la nécessité d'acquérir de nouveaux serveurs.

FILTRAGE WEB : MAÎTRISEZ ET SÉCURISEZ VOS ACCÈS WEB

VOTRE ENJEU

Les risques liés à l'usage du web sont multiples :

- risques de sécurité ;
- risques légaux ;
- risques d'abus de surf personnel, etc.

90 % des entreprises de plus de 250 employés ont naturellement mis en place des solutions de filtrage web.

Comment supprimer les risques liés au web tout en associant les employés et en faire des maillons forts de votre politique de sécurité ?

NOTRE REPONSE

Filtrage web

En 16 ans d'expérience, le produit Filtrage web d'Olfeo est le plus utilisé en France car il sait répondre à ce double besoin. Cela a été rendu possible car Olfeo exerce un double métier :

- celui d'éditeur de logiciels ;
- et aussi celui **d'analyste de contenus** qui lui a permis de construire des bases de données par pays d'une qualité inégalée.

La parfaite connaissance des habitudes de surf en Europe nous a permis de construire une offre parfaitement adaptée pour combattre les risques :

- De **sécurité** grâce à une base de réputation particulièrement efficace pour les attaques européennes ;
- **Légaux** par la construction d'une base de données intégrant le périmètre illicite du pays en reprenant les textes de lois applicables ;
- **Sociaux** en s'intégrant dans le contexte précis du droit du travail : diffusion de la charte internet, droits d'administration très fins,… ;
- D'**abus** de surf personnel grâce à une base de données de grande qualité répartie en plus de **100 catégories** et à des politiques de filtrage ultra granulaire : plages horaires, quotas de temps et de volume, capacité d'outrepassement avec ou sans mot de passe.

L'adoption par les collaborateurs et leur engagement est immédiat :

- **Absence de faux positifs** donc pas de blocages intempestifs grâce à une classification manuelle des contenus ;
- Des **pages de sensibilisation** précises et contextuelles en cas de blocage pouvant intégrer des images, des vidéos, un rappel de la charte, etc. ;
- La possibilité de recevoir des mails leur présentant leur usage dans un objectif **d'autorégulation.**

L'exhaustivité de notre base de données (plus de 98 % de taux de reconnaissance) est telle qu'Olfeo est le seul produit pouvant être utilisé sereinement en **liste blanche**. C'est le plus haut niveau de sécurité possible : les accès à des contenus n'ayant pas fait l'objet d'une analyse préalable par Olfeo sont bloqués (**recommandation de l'ANSSI**).

FILTRAGE WEB : MAÎTRISEZ ET SÉCURISEZ VOS ACCÈS WEB

LES BÉNÉFICES CLIENTS

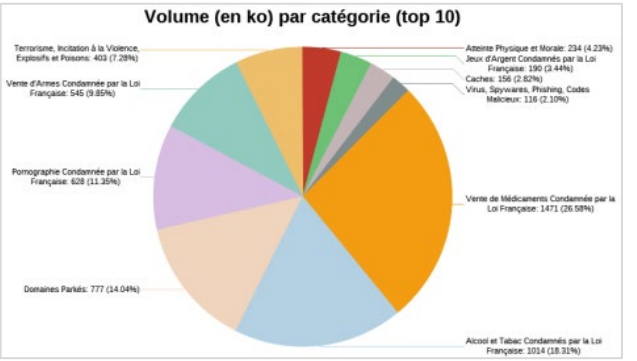
- Maîtriser et sécuriser intégralement vos accès web avec la solution leader du marché
- Vous protéger des risques juridiques : civil, pénal, droit du travail, RGPD, etc.
- Associer et responsabiliser vos collaborateurs à votre politique de sécurité par la meilleure expérience utilisateur et des fonctions avancées qui leur sont dédiées

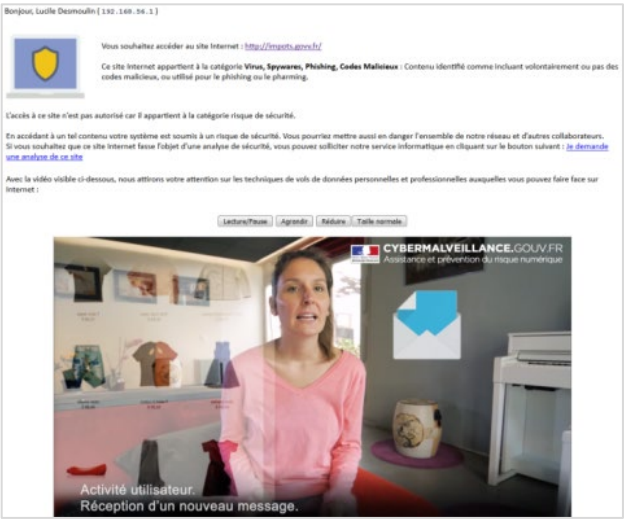
LES FONCTIONNALITÉS CLÉS

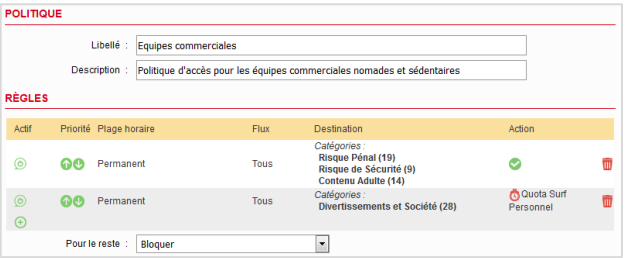
- Plus de 100 catégories d'URL reprenant les lois du pays ainsi que les centres d'intérêts locaux;
- Construction de politique de filtrage ultra granulaire : plages horaires, quotas de temps et de volume, capacité d'outre passement avec ou sans mot de passe…
- Authentifications multiples : transparente, portail captif,… avec reprise des données des annuaires
- Respect du code du travail via la diffusion individuelle de la charte informatique
- Paramétrage très fin des pages de blocage contextuelles grâce à notre studio de personnalisation qui permet d'intégrer des images, des vidéos pédagogiques, etc.
- Puissants outils d'analyse et de reporting pour mesurer et comprendre les usages web, identifier les postes à risque, détecter des attaques,…

LES PLUS OLFEO

- Un taux de reconnaissance de 98 % permettant une utilisation en liste blanche
- Des catégories de blocage des contenus illicites co-construites avec des cabinets d'avocats européens
- Une classification manuelle des contenus pour une qualité inégalée et un accès direct aux équipes de classification







PROXY AVANCÉ & DÉCHIFFREMENT HTTPS : REPRENEZ LA MAIN SUR VOS FLUX

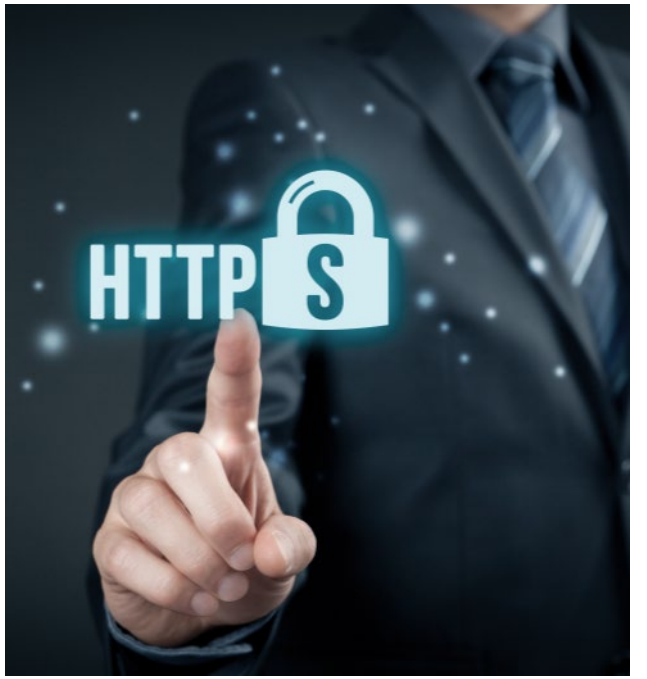
VOTRE ENJEU

L'ANSSI recommande l'utilisation d'un proxy dédié pour centraliser en un seul point tous les flux Internet. Cette concentration permet :

- De bloquer les contenus indésirables ;
- D'appliquer des analyses antivirales ;
- D'offrir des fonctions d'optimisation : cache, QoS ;
- De fournir de l'analyse de trafic et des logs nominatifs …

Comment remplir efficacement toutes ces fonctions en allégeant vos firewalls déjà fortement sollicités ?

90% des flux web sont chiffrés (HTTPS), il est donc devenu indispensable de les analyser. **Comment les déchiffrer tout en respectant les contraintes techniques et légales ?**



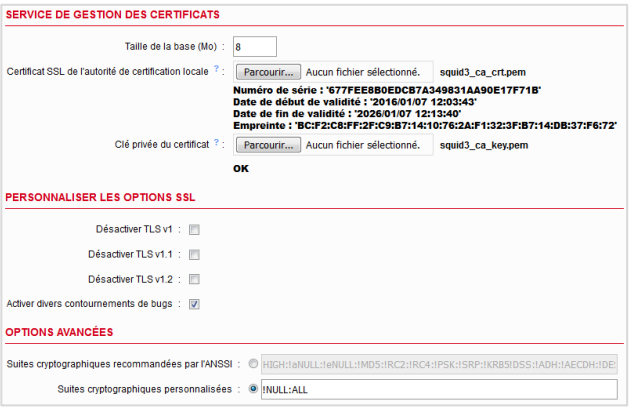
NOTRE REPONSE

Proxy avancé

Le produit Proxy avancé Olfeo regroupe un ensemble de proxies complémentaires permettant de contrôler précisément les accès, les connexions et les contenus des flux **HTTP, HTTPS, FTP, RTSP, TCP et SOCKS.** Utilisé de façon totalement dédiée, il permet d'alléger les firewalls et apporte des fonctions bien plus avancées.
De puissants moteurs de règles offrent une gestion simplifiée des **contrôles de contenus** fichiers... Des méthodes d'authentifications multiples permettent de garantir l'identification précise des utilisateurs. Les fonctionnalités de **cache** permettent d'améliorer l'expérience utilisateur et d'économiser de la bande passante.

Les fonctions de **QoS**, fortement granulaires, assurent l'optimisation et l'accélération des flux web professionnels en fonction des groupes d'utilisateurs.

L'option **déchiffrement SSL** offre une riche capacité de paramétrage et d'optimisation pour une performance et une sécurité maximum : traitement des erreurs de certificats,….
Des fonctionnalités avancées permettent d'effectuer cette désencapsulation dans le parfait **respect de la législation** : exclusion des catégories sensibles, présentation d'une charte SSL dédiée,…



PROXY AVANCÉ & DÉCHIFFREMENT HTTPS : REPRENEZ LA MAIN SUR VOS FLUX

LES BÉNÉFICES CLIENTS

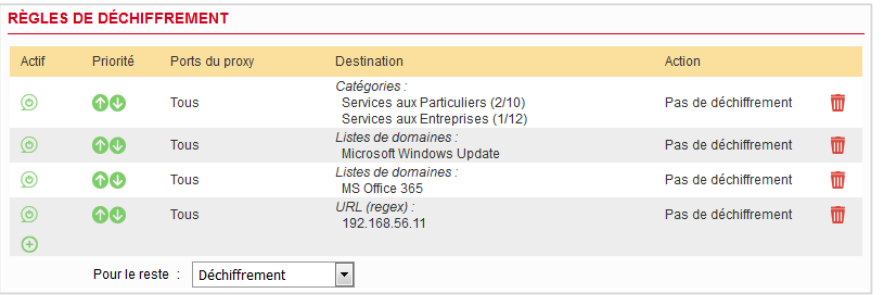
- Disposer d'un proxy dédié performant et libérer vos firewalls de cette charge
- Maîtriser les flux HTTPS en les déchiffrant de manière transparente
- Accélérer l'accès à Internet de vos collaborateurs

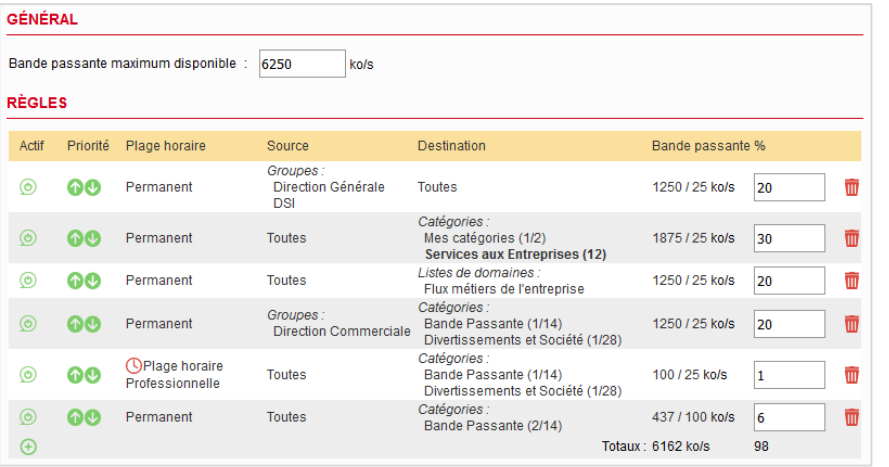
LES FONCTIONNALITÉS CLÉS

- Contrôle de nombreux types de flux HTTP, HTTPS, FTP, RTSP, TCP et SOCKS
- Authentification transparente sur les différents annuaires du marché
- Contrôle avancé des règles de proxy grâce à l'enchaînement des règles : connexion, accès, aperçu, contenu
- Gestion fine du cache et des règles de QoS
- Multiples outils de supervision, d'analyse et de conservation des logs

LES PLUS OLFEO

- Le déchiffrement du SSL dans le strict cadre juridique
- Le blocage des flux HTTPS en fonction des types d'erreurs de certificat
- L'interface statistique dédiée ultra performante grâce à sa base Elasticsearch





ANTIVIRUS WEB : DÉTECTEZ LES ATTAQUES QUI PROVIENNENT DU WEB AVEC UN PRODUIT DÉDIÉ

VOTRE ENJEU

Malgré l'empilement des solutions de sécurité et notamment des antivirus, l'actualité nous montre quotidiennement que les codes malveillants pénètrent les entreprises : ransomwares, vandalisme,… Les documents infectés proviennent soit :

1. des mails,
2. des installations directes sur les postes clients (clé USB,…)
3. des fichiers téléchargés sur Internet notamment après des campagnes de phishing.

100 % des entreprises sérieuses disposent d'antivirus de mails et de postes capables de détecter les deux premiers cas. Seules les entreprises exigeantes (60 %) sont équipées d'antivirus web, seuls outils capables de bloquer les attaques provenant du cas 3. Les hackers l'ont bien compris, ce point de vulnérabilité aiguise leur appétit. Mieux vaut traiter la menace avant qu'elle ne s'installe sur le poste de l'utilisateur, plutôt que chercher à l'éradiquer une fois installée.

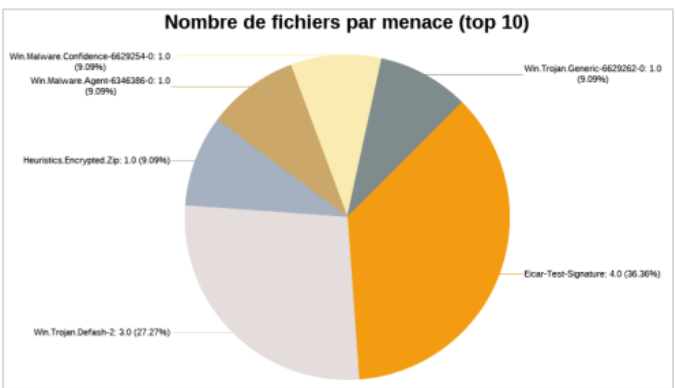
Comment protéger efficacement votre entreprise des malwares qui proviennent directement d'Internet ?

NOTRE REPONSE

Antivirus web

Le produit Antivirus web permet de bloquer ces malwares grâce à une analyse du flux web en **temps réel**. Tous les fichiers sont analysés lorsqu'ils passent par le proxy et automatiquement bloqués s'ils présentent une menace.

L'Antivirus web Olfeo offre la possibilité de contrôler finement les fichiers à analyser : origine (catégorie), type MIME, taille,… il est ainsi possible de ne pas appliquer l'analyse antivirale sur les mises à jour de logiciels connus dans un souci d'**optimisation**.



L'antivirus de flux Olfeo détecte ainsi **tous les types de menaces** : ransomware, cryptolocker, virus, vers, spyware, phishing, rootkits, keyloggers… sur **tous types de fichiers.**

Plusieurs méthodes complémentaires de détection sont utilisées : signature, analyse heuristique, scan des macros, …. L'Antivirus web est un complément indispensable à **la base de réputation** présente dans notre produit Filtrage web.

ANTIVIRUS WEB : DÉTECTEZ LES ATTAQUES QUI PROVIENNENT DU WEB AVEC UN PRODUIT DÉDIÉ

LES BÉNÉFICES CLIENTS

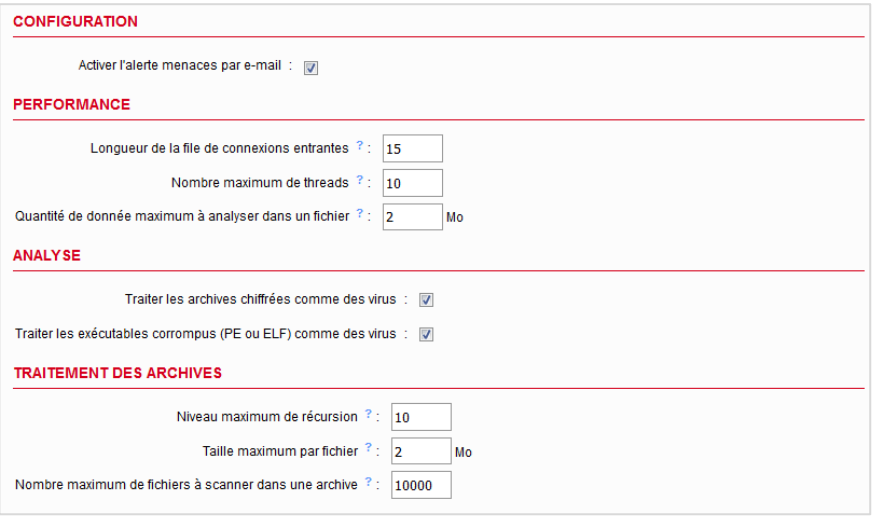
- Éradiquer les menaces qui proviennent du web avant qu'elles n'atteignent le poste utilisateur
- S'appuyer sur un expert reconnu de ces menaces particulières
- Centraliser au niveau du proxy toutes les fonctions de détection des menaces provenant du web : antivirus, filtrage d'URL, contrôle de contenus,…

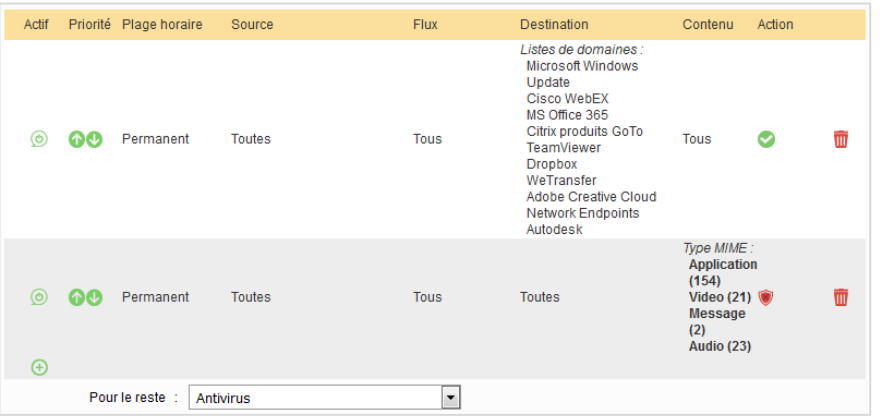
LES FONCTIONNALITÉS CLÉS

- Utilisation des méthodes de détection et des bases de signatures dédiées au web et complémentaires à celles de vos antivirus de poste
- Application de scans heuristiques afin de détecter des malwares encore inconnus des bases antivirales
- Analyse en profondeur des macros et des documents Office
- Paramétrage fin des fichiers à analyser : origine, type MIME, taille,…
- Prise en charge du maintien de la session entre le serveur et le navigateur grâce au data-trickling et aux pages de patience
- Accès à un tableau de bord des menaces détectées : nom des virus, postes infectés,…

LES PLUS OLFEO

- Le complément indispensable de la base de réputation du filtrage web Olfeo
- La présentation à l'utilisateur de pages de sensibilisation explicatives incluant des vidéos pédagogiques en cas de détection de codes malveillants





CAMPUS : FORMEZ VOS UTILISATEURS À LA SÉCURITÉ WEB

VOTRE ENJEU

Pour atteindre votre système d'information, les hackers n'hésitent pas à utiliser les failles humaines en ciblant vos collaborateurs : phishing, obtention d'informations confidentielles par réseaux sociaux ou téléphones, arnaque au président … 80 % des cyberattaques réussies utilisent l'ingénierie sociale.

Les nouveaux usages de vos collaborateurs (mobilité, wifi, applications Saas, réseaux sociaux, etc.) rendent les attaques plus difficiles à contrer car elles peuvent avoir lieu aussi en dehors de l'entreprise et sur des équipements que vous ne maîtrisez plus.
L'accumulation d'équipements de sécurité dans vos datacenters ne suffit donc plus, l'approche technique doit être complétée par une formation humaine. C'est aussi une forte préconisation du RGPD et de l'ANSSI.

Comment faire monter en compétences vos collaborateurs pour qu'ils déjouent les pièges ?

NOTRE REPONSE

Campus

Le produit CAMPUS s'inscrit parfaitement dans la démarche qu'Olfeo a engagée depuis plusieurs années sur la responsabilisation des collaborateurs. Ce nouveau produit permet **de lancer des campagnes** de formation via des parcours pédagogiques envoyés par e-mail à vos collaborateurs.

Pour obtenir l'adhésion des équipes, notre solution offre des contenus ludiques de vidéos et de saynètes ainsi que des quizz d'évaluation des connaissances. Les parcours sont courts, évolutifs et pratiques avec un passage de certification.
L'outil de reporting des campagnes de formation permet aux administrateurs de suivre l'avancement et le **taux de réussite** des participants.

Grâce à Campus vous protégez mieux votre entreprise tout en **valorisant** vos collaborateurs en développant leurs compétences sécurité.

CAMPUS : FORMEZ VOS UTILISATEURS À LA SÉCURITÉ WEB

LES BÉNÉFICES CLIENTS

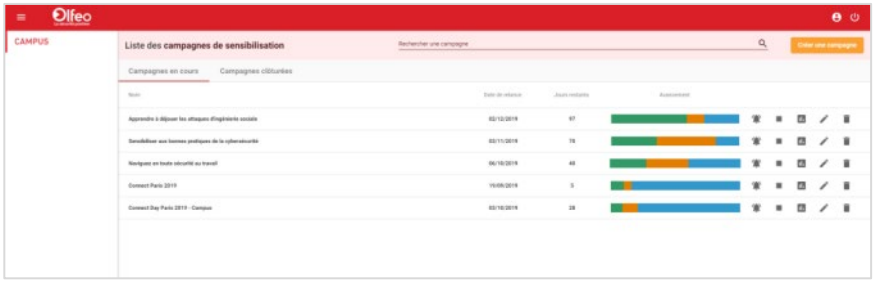
- Faire de tous vos collaborateurs des acteurs de votre politique de sécurité
- Déjouer les attaques utilisant l'ingénierie sociale insuffisamment détectées par les seuls équipements techniques
- Gagner du temps en utilisant directement les contenus pédagogiques adaptés et évolutifs mis à votre disposition dans la plateforme

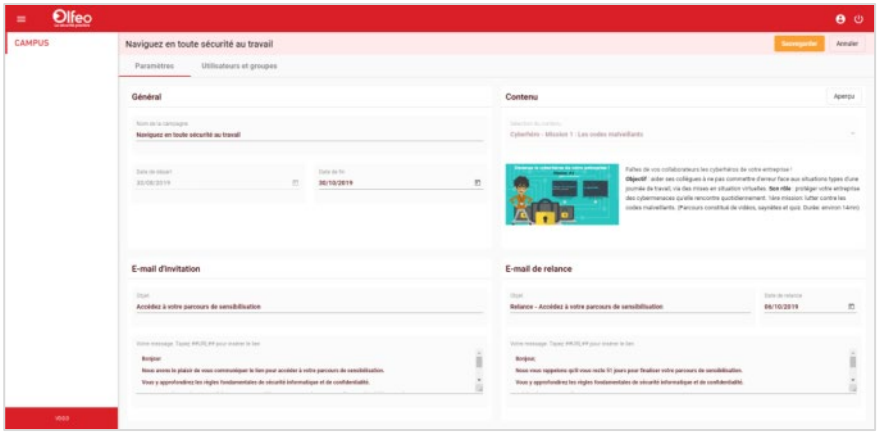
LES FONCTIONNALITÉS CLÉS

- Reporting détaillé des campagnes de formation lancées et du taux de succès
- Catalogue de formations riche et évolutif
- Quizz pour tester et valider la maîtrise de vos collaborateurs des concepts introduits
- Délivrance de diplômes individuels

LES PLUS OLFEO

- Un produit éligible au budget formation
- Une intégration complète à la passerelle de sécurité web : suivi des utilisateurs, intégration de contenus dans les pages de sensibilisation, …
- Un module de formation spécial RGPD pour assurer votre conformité





FILTRAGE DNS : BÉNÉFICIEZ DU FILTRAGE OLFEO SUR LES POSTES NON MAÎTRISÉS

VOTRE ENJEU

Dans un parc informatique, une DSI peut disposer de postes pas ou peu maîtrisés :

- sites distants sans équipes locales dédiées (exemple : établissements scolaires, médiathèques,…) ;
- accès wifi auxquels se connectent des personnes externes (BYOD) ;
- objets connectés à internet (IOT) : imprimantes, caméras de télésurveillance, machines/capteurs industriels…

Cette partie du SI devient immédiatement un point de vulnérabilité et donc une cible appétissante pour les hackers. Cette situation peut s'avérer encore plus dangereuse quand les équipements se connectent eux-mêmes régulièrement au SI, ils ne doivent donc pas devenir des sources de contamination.

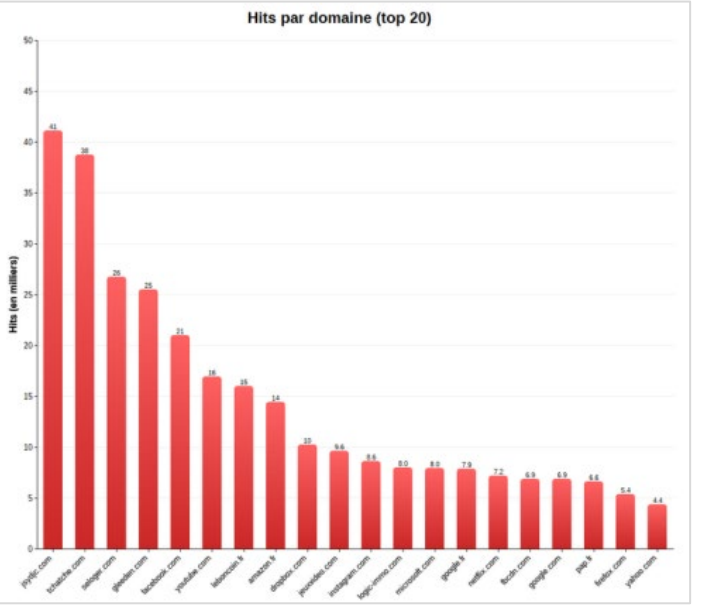
Comment offrir un niveau de sécurité élevé à ces équipements alors que le déploiement d'un proxy est impossible pour des raisons techniques ou d'absence de compétences locales ?

NOTRE RÉPONSE

Filtrage DNS

Le produit Filtrage DNS répond parfaitement à ce besoin :

- Il offre la fonction de filtrage en bénéficiant de l'exceptionnelle qualité de la **base Olfeo**. Il permet ainsi de combattre efficacement les risques de sécurité, juridique… ;
- il se met en œuvre très simplement sans aucune action sur les équipements en se plaçant soit directement en tant que serveur DNS soit en **DNS parent**. Son déploiement rapide uniquement sur la partie serveur est un véritable atout ;



Il nécessite une très faible bande passante entre le serveur et les matériels à protéger.
Il est pleinement compatible avec notre produit Portail public pour assurer la sécurité de vos accès internet avec des équipements **BYOD**.

FILTRAGE DNS : BÉNÉFICIEZ DU FILTRAGE OLFEO SUR LES POSTES NON MAÎTRISÉS

LES BÉNÉFICES CLIENTS

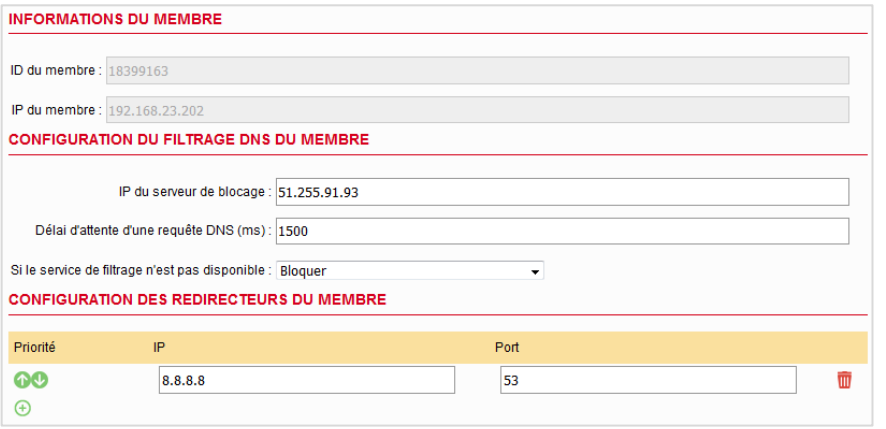
- Protégez tous les équipements que vous ne pouvez pas facilement proxifier : sites distants, IOT, BYOD…
- Limiter la bande passante nécessaire entre l'équipement et le serveur Olfeo
- Déployer simplement la solution

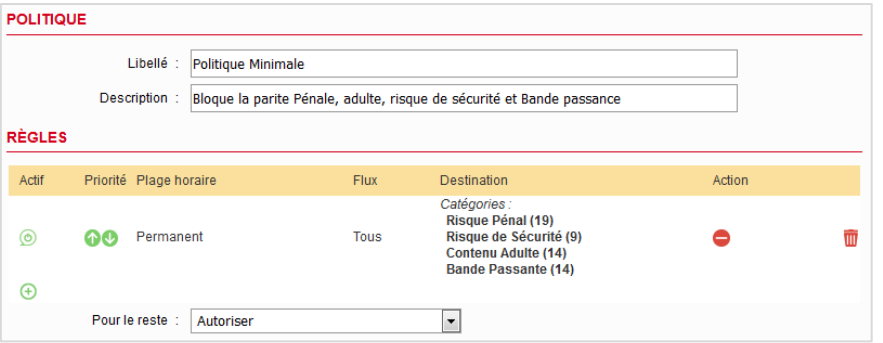
LES FONCTIONNALITÉS CLÉS

- Bloquer les accès aux contenus à risque : sécurité, légale, contenu adulte pour les mineurs…
- Retrouver l'activé Internet de vos équipements dans les outils d'analyse Olfeo
- Olfeo peut se positionner directement en serveur DNS ou en DNS parent

LES PLUS OLFEO

- Le bénéfice du filtrage par l'exceptionnelle base Olfeo : plus de 100 catégories, qualité de filtrage,…
- Une compatibilité complète avec le produit Portail public
- Évaluation des règles et politiques de filtrage suite à la réception de la requête



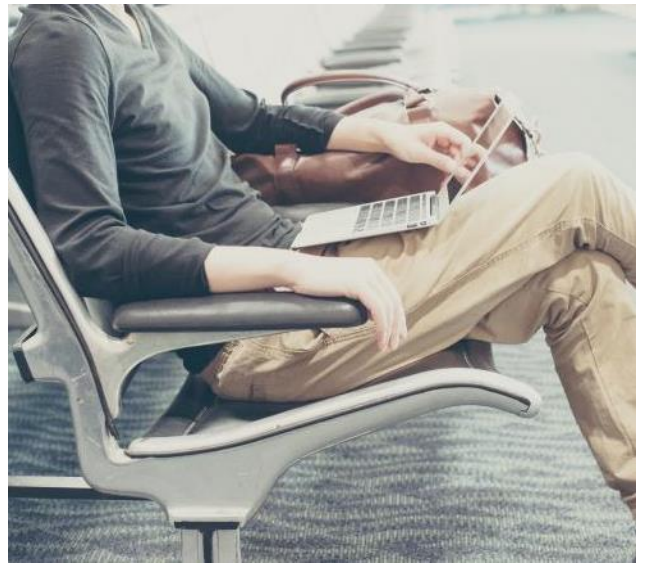


NOMADISME : OFFREZ LE MÊME NIVEAU DE PROTECTION À VOS COLLABORATEURS NOMADES

VOTRE ENJEU

Selon l'observatoire de la qualité de vie au bureau, Actineo, plus de 50% des employés ont l'occasion de travailler hors du bureau régulièrement et 30 % au moins une fois par semaine. Cette population croît chaque année : commerciaux, équipes SAV, etc …
Ces personnes en situation de mobilité sont très souvent dotées d'équipements informatiques nomades pour accéder au SI de l'entreprise et accéder à internet.
La sécurisation de cette flotte ainsi que les risques liés à l'accès au SI de l'extérieur constituent un défi pour la DSI.

Comment protéger ces équipements qui ont un double usage professionnel et personnel ? Comment s'assurer que des malwares collectés lors de la navigation internet ne contaminent pas le SI une fois l'équipement revenu au bureau ? Comment déployer une solution simple et transparente pour l'utilisateur ?



NOTRE RÉPONSE

Nomadisme

Le produit Nomadisme permet de maîtriser l'accès internet des équipements nomades en appliquant les mêmes politiques de sécurité à l'extérieur du bureau. Les utilisateurs retrouveront l'intégralité des fonctions Olfeo : qualité du filtrage, pages de sensibilisation,…

Le produit nomadisme se compose d'un **agent déployable** sur les postes clients. Il évite le déploiement d'un VPN plus lourd et plus contraignant. Le déploiement rapide et facile de cet agent est un véritable atout. Il détecte les scénarios de mobilité rencontrés et s'adapte automatiquement dans le cas des portails captifs en **wifi public.**

Il vous permet de retrouver toute l'activité de l'utilisateur y compris à l'extérieur dans les **outils d'analyse**.

NOMADISME : OFFREZ LE MÊME NIVEAU DE PROTECTION À VOS COLLABORATEURS NOMADES

LES BÉNÉFICES CLIENTS

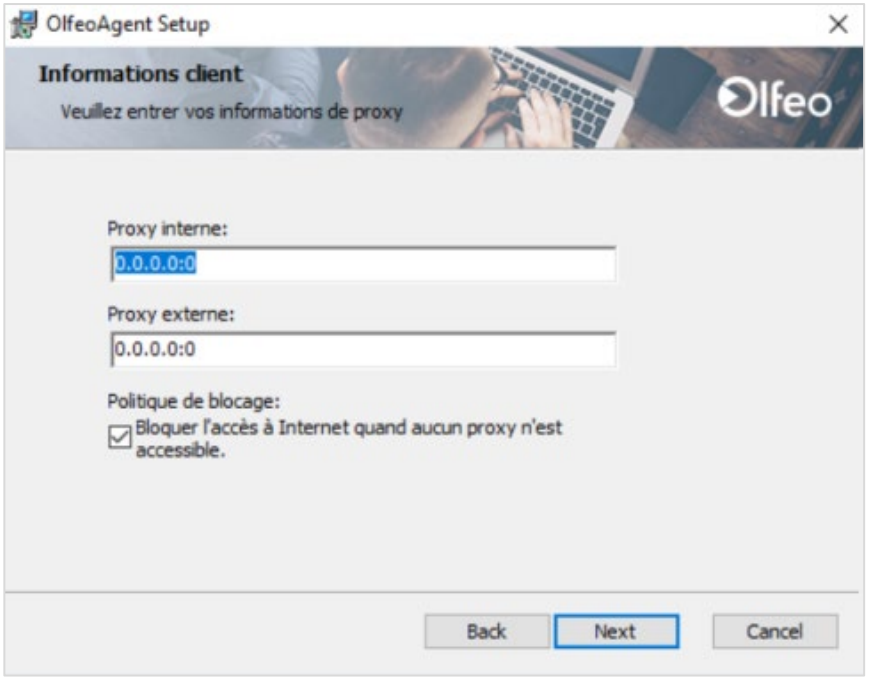
- Sécuriser les flux web pour tous les équipements de mobilité mis à disposition : malware, risques juridiques…
- Bénéficier de la même politique de sécurité en interne et en externe
- Déployer simplement et efficacement le produit pour une mise en œuvre immédiate

LES FONCTIONNALITÉS CLÉS

- Un agent Olfeo intelligent intégré au système d'exploitation et transparent pour l'utilisateur
- Une authentification des utilisateurs transparente et sécurisée
- Une interface de gestion des utilisateurs nomades intégrée avec statistiques
- La conservation des logs sur une durée personnalisable

LES PLUS OLFEO

- Le bénéfice des fonctions exclusives des autres produits Olfeo même en situation de mobilité : qualité de la base, pages de sensibilisation, protection juridique optimale, formation…
- La détection des portails captifs pour un usage serein en cas d'utilisation d'un wifi public



LE PORTAIL PUBLIC : MAÎTRISEZ ET SÉCURISEZ VOS ACCÈS PUBLICS

VOTRE ENJEU

Fournir un accès Internet Wi-Fi ou filaire à des visiteurs, des prestataires, des étudiants, des patients et plus généralement à toute personne extérieure est un usage de plus en plus répandu.

L'ouverture d'une partie de votre SI à ces populations externes peut présenter des risques. Risques de sécurité bien sûr, mais aussi légaux car la règlementation impose d'authentifier, de logger et de filtrer les accès internet de ces utilisateurs occasionnels sous peine de voir votre responsabilité engagée.

Comment ouvrir partiellement votre réseau en toute sécurité et en respectant la législation ?

NOTRE RÉPONSE

Portail public

Le produit Portail public a été conçu pour apporter une solution précise et efficace à ce dilemme.

Il permet de créer des formulaires pour authentifier les utilisateurs, qui peuvent **s'auto-enregistrer** puis logger leurs accès. Les identifiants et mots de passe peuvent être envoyés par mail et par SMS pour sécuriser l'authentification.

Des tickets d'accès peuvent être créés pour des durées paramétrables et avec des politiques d'accès aux contenus Internet que vous déterminez.
Pour responsabiliser l'utilisateur et vous protéger légalement, le Portail public permet de présenter et de faire signer la **charte utilisateur** avant l'accès. Toutes les **connexions sont tracées** et vous les retrouvez dans les outils d'analyse et de reporting.

LE PORTAIL PUBLIC : MAÎTRISEZ ET SÉCURISEZ VOS ACCÈS PUBLICS

LES BÉNÉFICES CLIENTS

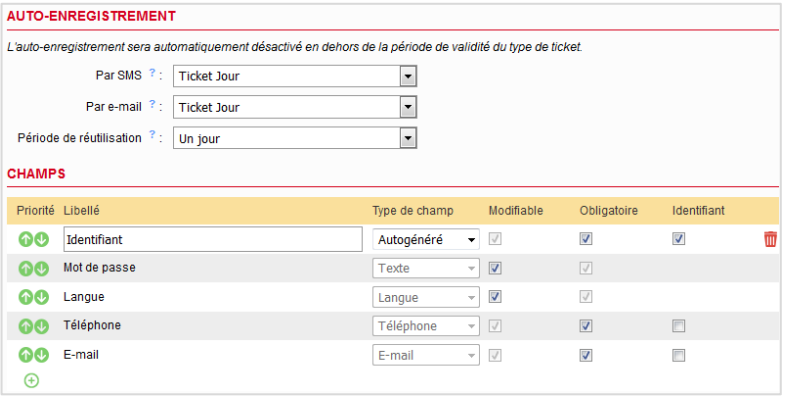
- Offrir un accès internet à des populations externes : visiteurs, consultants, patients, etc. en toute sécurité
- Gagner du temps en permettant l'auto-enregistrement de ces populations
- Respecter les obligations légales : traçabilité, filtrage de contenus

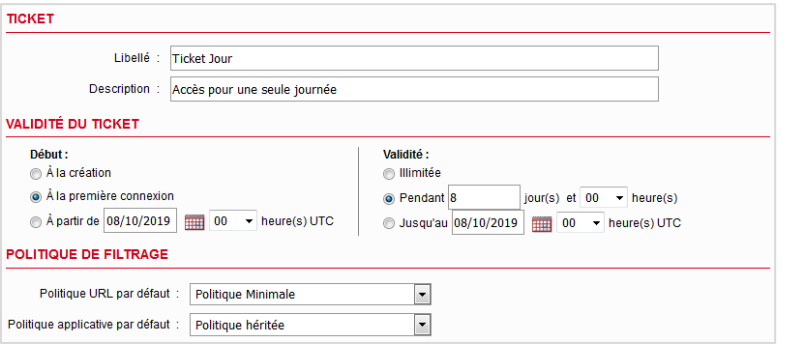
LES FONCTIONNALITÉS CLÉS

- Création illimitée de comptes utilisateurs par un opérateur ou directement par le visiteur (auto-enregistrement)
- Diffusion des identifiants utilisateurs par e-mail, SMS ou impression
- Création illimitée de portails et de tickets permettant de définir la langue, les messages, le formulaire de renseignement, la durée de validité
- Personnalisation de la charte graphique, des textes et de la langue du portail
- Analyse complète des accès effectués par les visiteurs

LES PLUS OLFEO

- La définition des politiques de Filtrage d'URL grâce aux catégories Olfeo
- La diffusion individuelle de la charte d'accès aux visiteurs et archivage de leur confirmation de lecture
- La visualisation en temps réel des comptes actifs, inactifs et expirés
- Un couplage facile avec le produit Filtrage DNS pour répondre aux besoins du BYOD





FILTRAGE PROTOCOLAIRE : CONTRÔLEZ TOUS LES PROTOCOLES PRÉSENTS SUR VOTRE RÉSEAU

VOTRE ENJEU

De nombreux protocoles applicatifs peuvent représenter une menace pour l'organisation. Ces menaces font courir de nombreux risques juridiques, de sécurité ou de fuite d'informations : Peer to Peer, Tor, iTunes, Google Play...

Les firewalls ne sont pas toujours efficaces face à la multiplication du nombre de protocoles, à leur complexité croissante et à leur capacité à muter.

Comment identifier et contrôler tous les protocoles présents sur le réseau ?

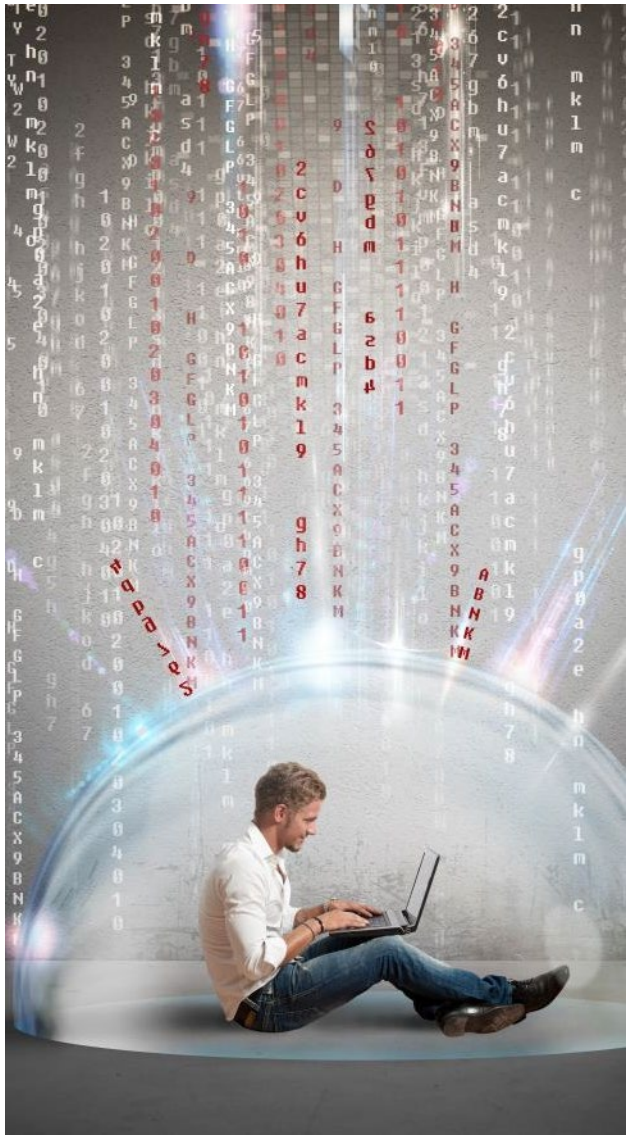
NOTRE RÉPONSE

Filtrage protocolaire

Le produit de Filtrage protocolaire Olfeo permet d'identifier les protocoles grâce à une analyse approfondie des paquets jusqu'à la **couche 7 du modèle OSI** (DPI).

Des centaines de protocoles sont répertoriés dans 28 thèmes. L'excellente connaissance de la structure des données échangées permet d'identifier le **protocole réel** quel que soit le port utilisé.

L'analyse multi-ports détecte les attaques par usurpation de ports. Les politiques de filtrage protocolaire peuvent être associées individuellement aux groupes ou aux utilisateurs dans la même interface graphique que celle du filtrage web afin de disposer d'une **vue globale de vos politiques de filtrage.**



FILTRAGE PROTOCOLAIRE : CONTRÔLEZ TOUS LES PROTOCOLES PRÉSENTS SUR VOTRE RÉSEAU

LES BÉNÉFICES CLIENTS

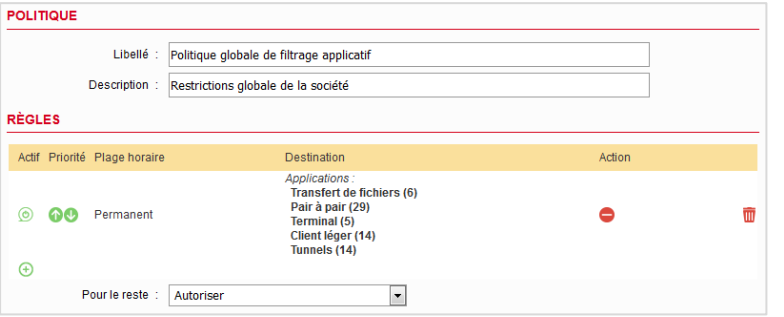
- Maîtriser les protocoles présents sur votre réseau
- Bloquer les protocoles connus pour transporter des informations sensibles, dangereuses ou consommatrices de bande passante : Jeux en ligne, Peer To Peer, Tor
- Disposer de la visibilité et du reporting dans la même interface conviviale que celle des autres contenus : web, fichier, antivirus

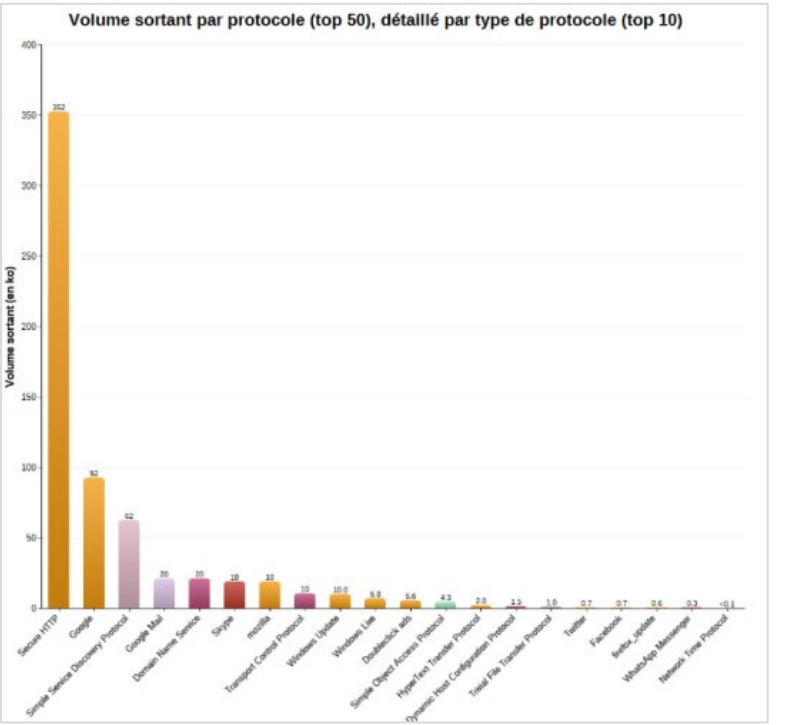
LES FONCTIONNALITÉS CLÉS

- Analyse des signatures applicatives jusqu'à la couche 7 afin d'identifier le protocole réel
- Analyse du type de flux indépendamment des ports utilisés
- Gestion précise des politiques de filtrage protocolaire (plus de 28 thèmes)
- Analyse précise des flux réseaux en temps réel sans impacter les performances du réseau
- Reporting complet sur la consommation de la bande passante par protocole

LES PLUS OLFEO

- La vision globale des politiques de filtrage web et protocolaires à travers une vue RH unifiée
- L'identification de protocoles non IP ou encore de protocoles de communication fréquemment utilisés par les postes zombies tel que IRC, ICQ
- L'optimisation de la bande passante grâce à la détection de protocoles de jeux en ligne, de P2P, de streaming, de téléchargement de fichiers





Olfeo
La sécurité positive

LA PASSERELLE DE SECURITE WEB DISRUPTIVE, BASÉE SUR UNE VISION A 360°

contact@olfeo.com

+33 (0) 969 396 999

www.olfeo.com