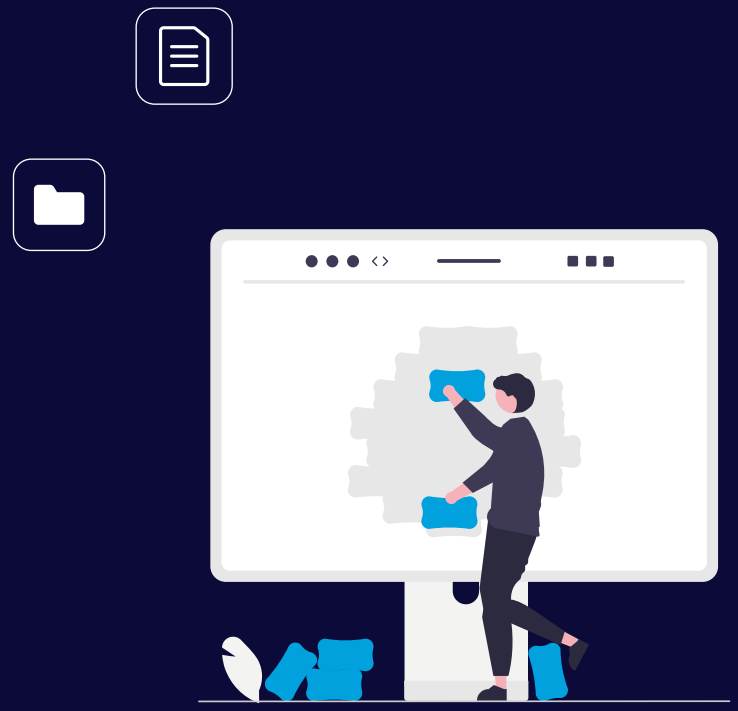
LIVRE BLANC OLFEO SSE

Le Security Service Edge Olfeo

La cybersécurité à l'ère du cloud

Chap 1

La cybersécurité à l'ère du cloud



01

Les cybermenaces, un paysage en évolution constante

Dans le contexte d'informatisation et de digitalisation massif du monde professionnel ces dernières années, le paysage des cybermenaces a considérablement évolué pour englober de nouvelles dimensions.

Aux « traditionnelles » cyberattaques dont les modalités ont considérablement évolué, s'ajoutent aujourd'hui des enjeux liés :

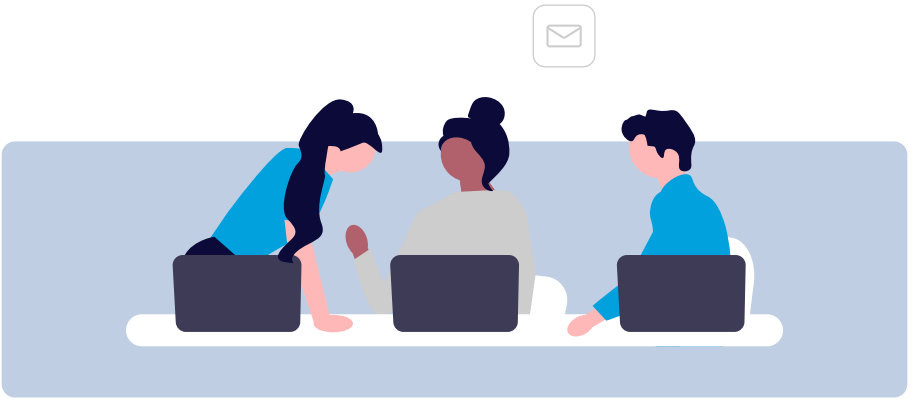
- **À la fuite de données (intentionnelles ou non) dévastatrices pour une organisation**
- **Au mésusage de ressources informatiques sur internet (applications SaaS) exposant l'organisation aux risques de sécurité des données (RGPD, collecte de données à l'insu lors d'un usage supposé anodin d'IA génératives).**

  Plus largement à l'accès sécurisé à ces applications cloud.

Certes, les cyberattaques ne sont pas une nouveauté dans le monde numérique.

Cependant, ce qui est vraiment alarmant aujourd'hui, c'est le **volume croissant de ces attaques ainsi que l'augmentation notable de leur taux de succès.** Selon le rapport de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), les cyber incidents ont augmenté de 400 % entre 2019 et 2023.

Autrefois limitées à des incidents sporadiques visant principalement des grands groupes ou des personnes en particulier, ces attaques se sont maintenant propagées à une échelle sans précédent, touchant tous les secteurs et industries, quel que soit leur taille.



02

Plusieurs facteurs contribuent à l'expansion des attaques

Le volume des cyberattaques s'explique par cinq facteurs principaux :

1 Une simplicité et une facilité de mise en œuvre inédite

Il est devenu beaucoup plus simple de lancer une attaque. Les cybercriminels disposent de nombreux outils automatisés qui réduisent considérablement le temps et les compétences nécessaires pour orchestrer une attaque efficace. Par exemple, les kits de phishing sont facilement disponibles sur le dark web pour moins de 50 euros. D'un autre côté, l'automatisation et la simplification des outils permettent de scanner très rapidement «tout internet» pour trouver et exploiter des vulnérabilités. Quand une vulnérabilité (ou CVE) est relevée, dans les heures et jours qui suivent, des outils automatisés vont scanner l'espace IPv4 pour identifier les équipements qui ne sont pas à jour et qui peuvent être exploités pour des cyberattaques.

2 Un accès aux ressources devenu trivial

L'accès aux ressources nécessaires pour mener des attaques est devenu extrêmement facile. Les outils, les serveurs, les domaines et les adresses IP sont largement disponibles sur le marché noir, souvent à des coûts dérisoires. En France, il a été constaté que de nombreux serveurs utilisés pour des attaques DDoS proviennent de machines compromises hébergées sur le territoire national.

Les outils pour les cyberattaques sont commercialisés par les groupes de pirates et donnent lieu à un vrai business sur le dark web, allant de l'outil mal conçu mais qui permet des attaques basiques efficaces contre des organisations dont la maturité de défense est basse, jusqu'au Ransomware-as-a-Service permettant de «louer» des outils très avancés à des organisations criminelles, comme Lockbit, qui est le rançongiciel le plus utilisé dans les incidents signalés à l'ANSSI en 2022. Pour rappel, LockBit propose un service de Ransomware « as-a-service », c'est-à-dire qu'il met des moyens techniques à disposition d'affiliés qui vont ensuite attaquer diverses cibles, LockBit récupérant 20 % du montant des rançons comme paiement.

3 L'omniprésence d'internet dans tous les contextes professionnels

Dans le monde professionnel moderne, internet, le web et le digital sont devenus des piliers incontournables, restructurant la manière dont les entreprises opèrent et interagissent. L'omniprésence de ces technologies est manifeste dans presque tous les secteurs, que ce soit par la communication instantanée via les emails, la collaboration à distance facilitée par des outils tels que Slack ou Microsoft Teams, ou encore la gestion des données avec des plateformes de cloud computing comme AWS ou encore Google Cloud.

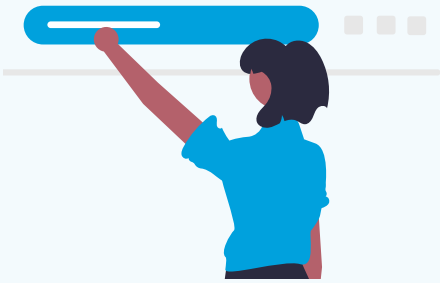
Les professionnels sont de plus en plus dépendants de ces technologies pour assurer la continuité de leurs activités, stimuler l'innovation et maintenir une compétitivité accrue sur le marché globalisé. Cela dit, avec cette dépendance croissante aux technologies numériques, **le monde professionnel doit également affronter des défis inédits, notamment en matière de sécurité.** Le passage massif vers le digital a élargi la surface d'attaque, exposant les organisations à un éventail toujours plus complexe de cybermenaces. Les attaques ciblant les vulnérabilités du protocole HTTP(S), bien que sécurisées, ne sont pas inexistantes, et nécessitent une vigilance constante des professionnels de la cybersécurité pour garantir l'intégrité des données échangées. Le défi réside donc dans la capacité à tirer parti des opportunités offertes par l'omniprésence du web tout en minimisant les risques liés à la cybersécurité, garantissant ainsi un environnement professionnel à la fois productif et sécurisé. Une des composantes majeures de ce défi est d'être capable de détecter et filtrer les contenus légitimes des nombreux contenus malicieux qui sont créés désormais avec une rapidité effroyable.

4 Les domaines internet : au cœur de toutes les cyberattaques

Les domaines et les adresses IP jouent un rôle crucial dans la mise en œuvre des cyberattaques. Les cybercriminels utilisent souvent des domaines malicieux et éphémères, avec des adresses IP détournées pour dissimuler leur véritable identité et localiser les attaques.L'ampleur des enregistrements de domaines malveillants est écrasante et omniprésente. Bien que le nombre précis de rapports d'abus ne soit pas public en raison de la nature décentralisée du système et des problèmes de confidentialité, il est évident que la cybercriminalité s'intensifie. Par exemple, les recherches d'Akamai ont permis d'identifier près de 79 millions de domaines malveillants au cours du seul premier semestre 2022. Ce chiffre représente un pourcentage alarmant de 20 % de tous les domaines nouvellement observés qui ont été résolus avec succès au cours de cette période et représente plus de 13 millions de nouveaux enregistrements de noms de domaine malveillants par mois. Les acteurs malveillants enregistrent souvent des noms de domaine en masse afin d'assurer leur résilience. Lorsqu'un domaine est signalé, ils passent rapidement à un autre de leur stock, ce qui perturbe le moins possible leurs opérations. Le déploiement d'algorithmes de génération de domaines (DGA) est au cœur de cette stratégie, car ces programmes peuvent produire des noms de domaine uniques à grande échelle, en intégrant des chiffres aléatoires pour éviter les doublons. La variété des menaces exploitées par ces tactiques est vaste, y compris le typosquattage pour le phishing, la distribution de logiciels malveillants, les ransomwares, le cryptomining, les serveurs Commande et Contrôle, les opérations de botnet et les menaces persistantes avancées (APT) qui pénètrent furtivement dans les réseaux.

5 Le défi des compétences et de la formation

Le manque de formation en cybersécurité, tant chez les professionnels de l'IT que chez les collaborateurs, contribue également à la vulnérabilité accrue des systèmes. Une enquête réalisée en 2022 a révélé que 60 % des employés français n'avaient pas reçu de sensibilisation aux enjeux de la cybersécurité au cours des deux dernières années, y compris au sein des professionnels de l'informatique (chefs de projets, développeurs, etc.) que des administrateurs système ! De même, on considère qu'il manque plus de 15.000 profils qualifiés en cybersécurité.



Les limites des solutions de sécurité actuelles

Devant ce grand volume et cette sophistication des attaques, aucune solution n'offre de protection réellement efficace. Les solutions traditionnelles de sécurité, ne mettant en jeu que des pare-feux, des antivirus de poste et VPN pour les collaborateurs en déplacement avaient de la valeur dans des contextes de réseaux d'entreprises centralisés (modèle «château fort») et surtout dans un contexte où le modus operandi des attaques ne reposait pas autant sur le trafic HTTP. S'ils conservent néanmoins de la valeur, ces cadres de pensée ne sont plus adaptés aux tendances de fond de mutation des architectures contemporaines de plus en plus déportées et décentralisées et liées aux évolutions du monde du travail.

En tout état de cause, ces modèles ne peuvent plus contrer les menaces émergentes aussi bien qu'il y a quelques années.

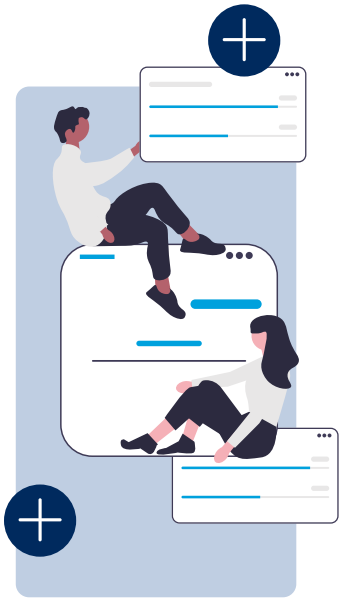
La majorité des solutions maintiennent des listes de blocage qui indexent les URLs connues pour être malicieuses… dont la durée de vie est si éphémère qu'à peine identifiées, elles n'ont déjà presque plus d'intérêt. De même, de nombreux domaines utilisés dans des attaques (comme des serveurs type «Command and Control» ou C2) peuvent être crées quelques minutes avant une attaque, ne pouvant donc figurer dans aucune base de menaces.

Or il semble évident que devant l'augmentation exponentielle des domaines malicieux et leur aspect éphémère, les solutions à base de blocklists sont vouées à l'échec.

La nécessité d'espaces de navigation sécurisés

Face à ces défis croissants, il est crucial d'installer des espaces de navigation sécurisés où les collaborateurs peuvent naviguer en toute confiance. Ces espaces de navigations s'entendent donc aussi bien au sens « physique » : Comment faire pour que mon collaborateur en télétravail ou en déplacement reste protégé, comme « virtuel » ? Comment faire pour limiter efficacement l'accès (volontaire ou non) à des ressources potentiellement dangereuses ?

Par ailleurs, face à une pénurie de ressources compétentes pour mettre en place et maintenir des systèmes toujours plus complexes, mettre en place de tels espaces peut facilement relever de la gageure. Pourtant, ces environnements contrôlés permettraient de se protéger contre le risque d'infection par des logiciels malveillants et d'autres types d'attaques, offrant ainsi une couche supplémentaire de protection indispensable dans le paysage numérique actuel.



03

Le SSE ou Security Service Edge : la première ligne de défense contre les cyberattaques

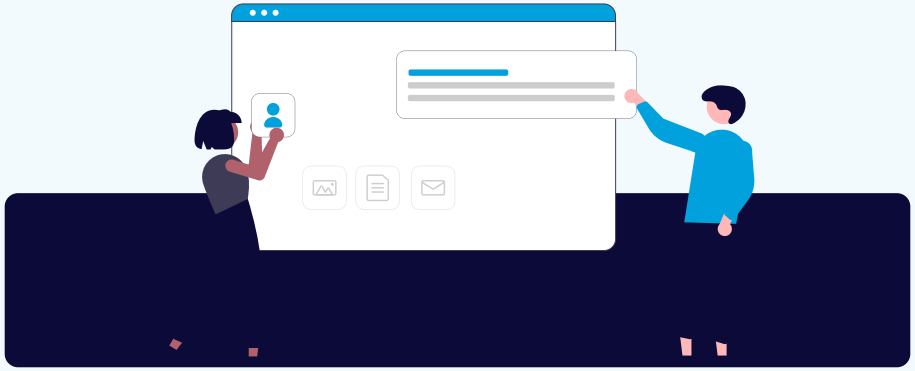
Pour répondre à ces enjeux, l'industrie a apporté au cours des années passées diverses réponses : les pare-feux et les antivirus de poste bien sûr, puis le proxy, puis le VPN pour la gestion des déplacements… À chaque « brique » supplémentaire, un niveau de complexité supplémentaire.

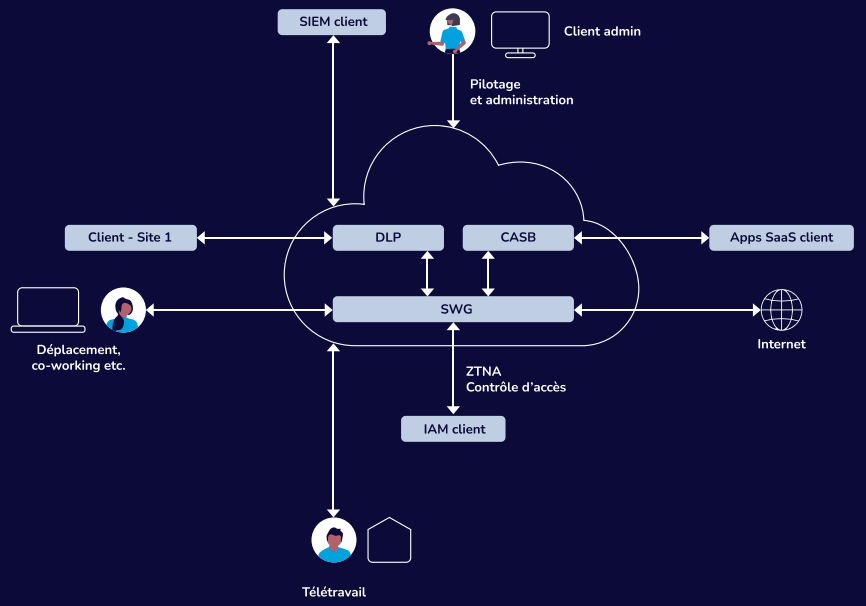
De plus, les solutions de sécurité traditionnelles, souvent basées sur des appliances matérielles sur site protégeant des réseaux d'entreprise internes, ne peuvent plus suivre le rythme des évolutions rapides des menaces et des environnements de travail.

Elles manquent par essence de scalabilité et d'agilité, ce qui les rend limitées pour les architectures modernes qui s'appuient de plus en plus sur le cloud et la mobilité des utilisateurs. Ce sont aussi des compétences souvent pointues à acquérir, conserver et maintenir. Et on a vu que disposer de telles compétences peut parfois être un défi très complexe à relever !

Le Security Service Edge (SSE) répond à ces problématiques avec une approche de sécurité réseau qui combine plusieurs services de sécurité dans une architecture unifiée, basée sur le cloud. **Il offre une protection avancée des données et des réseaux** en intégrant des fonctions telles que le Secure Web Gateway (SWG), le Cloud Access Security Broker (CASB), la DLP (Data Loss Prevention) et le Zero Trust Network Access (ZTNA).

Cette architecture permet une sécurité cohérente et flexible pour les utilisateurs, qu'ils soient au bureau, à domicile ou en déplacement.





Le Secure Web Gateway (SWG)

ou Passerelle de Sécurité Web, protège les utilisateurs contre les menaces basées sur le web et applique les politiques d'accès à Internet de l'organisation.

Les SWG filtrent le trafic web pour protéger contre les malwares, les intrusions et autres menaces en ligne, en garantissant en parallèle la conformité aux politiques de sécurité de l'entreprise.

Un SWG est articulé autour des fonctionnalités suivantes :

- **Le filtrage d'URL pour bloquer l'accès à des sites web dangereux, avec du contenu illicite ou inapproprié dans un environnement professionnel, en se basant sur des catégories prédéfinies ou des listes personnalisées.**
- **L'analyse du trafic web en temps réel pour détecter et bloquer les logiciels ou fichiers malveillants avant qu'ils n'atteignent l'utilisateur**
- **Le déchiffrement et l'inspection du trafic chiffré SSL/TLS pour détecter les menaces cachées dans les communications sécurisées HTTPS**
- **La définition et l'application des politiques d'accès web basées sur des critères tels que l'utilisateur, le groupe, l'heure de la journée, etc.**

Les SWG jouent un rôle crucial dans la sécurisation de l'accès à Internet, protégeant les utilisateurs et les données contre les menaces en ligne tout en assurant la conformité aux politiques de sécurité de l'entreprise.

Le Cloud Access Security Broker (CASB)

se situe entre les utilisateurs d'une organisation et les fournisseurs de services cloud pour appliquer les politiques de sécurité de l'entreprise lors de l'accès aux ressources cloud. Le CASB offre une visibilité, un contrôle et une protection complets sur l'utilisation des applications cloud.

Quelques caractéristiques d'un CASB incluent :

- **L'identification et l'indexation des applications cloud utilisées dans l'organisation**
- **Le suivi en temps réel des activités des utilisateurs dans les applications cloud**
- **L'authentification et l'autorisation avec la garantie que seuls les utilisateurs autorisés puissent accéder aux applications cloud**
- **Les contrôles granulaires et l'application de politiques spécifiques en fonction de divers facteurs comme l'utilisateur et l'appareil**
- **La protection contre les menaces avec l'identification des comportements anormaux dans l'utilisation des applications cloud**

Le DPL (ou Data Loss Protection)

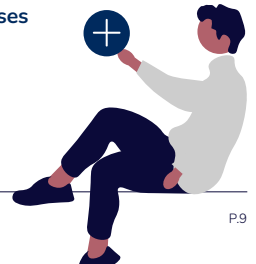
ou protection contre la perte de données est une stratégie visant à détecter et prévenir la perte, le vol ou l'exfiltration de données sensibles.

Cela inclut la surveillance et le contrôle d'accès aux données, ainsi que des mécanismes pour empêcher la transmission non autorisée de ces données à l'extérieur d'un réseau d'entreprises.

Les fonctionnalités clés incluent :

- **La capacité à identifier et classifier les informations sensibles telles que les données personnelles, les informations financières, les secrets commerciaux, etc.**
- **Le contrôle des accès à ces données**
- **La surveillance en temps réel du trafic réseau et de l'activité des utilisateurs pour détecter des comportements anormaux**
- **La mise en place de politiques et de technologies pour bloquer ou alerter sur les tentatives de transfert de données sensibles en dehors de l'entreprise, que ce soit par email, transferts de fichiers, impression, etc.**

Le DLP est essentiel pour prévenir les violations de données coûteuses et protéger la réputation et la viabilité des entreprises.



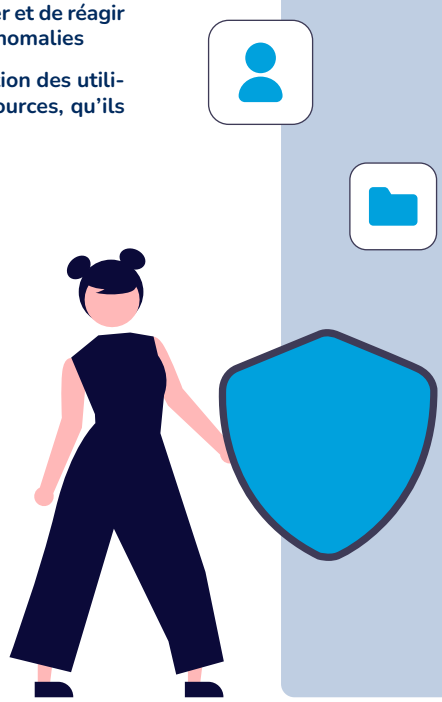
Le Zero Trust Network Access (ZTNA)

est une approche de la sécurité qui offre un accès sécurisé aux ressources d'une organisation en partant du principe que la sécurité ne peut être accordée à aucun utilisateur ou appareil par défaut, que ceux-ci se trouvent à l'intérieur ou à l'extérieur du réseau de l'entreprise.

Ses capacités principales sont :

- **Chaque demande d'accès est évaluée en temps réel, nécessitant une authentification multi-facteur (MFA) et une vérification constante de l'identité**
- **Les décisions d'accès sont basées sur l'identité de l'utilisateur, son rôle, l'appareil utilisé, la localisation et d'autres facteurs contextuels pour garantir que seul le bon utilisateur a accès à la ressource appropriée**
- **Divise le réseau en segments plus petits et gère l'accès à ces segments de manière granulaire, limitant ainsi les mouvements latéraux en cas de compromission**
- **Permet de définir des politiques d'accès spécifiques à l'application, à l'utilisateur, et au contexte.**
  Assurant que les utilisateurs n'accèdent qu'aux ressources nécessaires à leur rôle
- **Fournit une visibilité complète sur les accès et les activités des utilisateurs. Cela permet de détecter et de réagir rapidement aux comportements suspects/anomalies**
- **Fonctionne indépendamment de la localisation des utilisateurs, facilitant l'accès sécurisé aux ressources, qu'ils soient sur site ou à distance**

En ne faisant confiance à aucun utilisateur ou appareil par défaut, le ZTNA minimise ainsi les risques de vulnérabilités exploitées par des cyberattaques.



04

L'importance du SSE dans les stratégies de cybersécurité modernes des entreprises

Le Security Service Edge (SSE) est devenu un élément fondamental de la sécurité des entreprises modernes en raison de plusieurs facteurs déterminants.

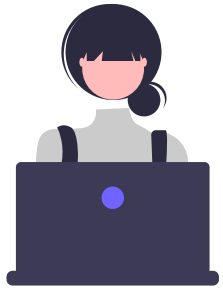
Tout d'abord, avec la généralisation du travail à distance, les entreprises font face à de nouveaux défis. Les VPN traditionnels peinent à répondre aux exigences de performance et d'échelle nécessaires pour supporter des collaborateurs distribués. **Le SSE, en revanche, permet un accès sécurisé depuis n'importe quel endroit, ce qui améliore considérablement la productivité et l'expérience utilisateur.**

En outre, l'adoption rapide de solutions SaaS par les entreprises met en lumière les limitations des modèles de sécurité traditionnels, qui ne sont pas conçus pour protéger efficacement les ressources basées sur le cloud. Le SSE offre une sécurité native dans le cloud et qui s'adapte à l'évolution des environnements distribués, garantissant ainsi une protection continue.

La gestion de la sécurité est un autre domaine où le SSE apporte des avantages significatifs. De nombreuses organisations se débattent avec la complexité de la gestion de multiples solutions de sécurité ponctuelles, ce qui conduit souvent à des lacunes en matière de sécurité et à un risque accru.
Le SSE simplifie cette gestion en consolidant les fonctions de sécurité, ce qui réduit la complexité et améliore la posture de sécurité globale.

De plus, le SSE **facilite la transformation numérique** en soutenant l'adoption sécurisée de nouvelles technologies et de nouveaux modèles de travail, notamment l'usage des applications SaaS. Cela permet aux organisations d'innover et de se développer sans compromettre leur sécurité, offrant ainsi une flexibilité accrue pour répondre aux besoins changeants du marché. En répondant à ces besoins essentiels, le SSE est en train de s'imposer comme un composant indispensable des stratégies de sécurité des organisations. Il permet aux organisations de protéger efficacement leurs actifs, leurs utilisateurs et leurs données dans un environnement numérique de plus en plus mobile, complexe et distribué.

Les fonctionnalités clés et les bénéfices d'une stratégie de sécurité à base de SSE



Le Security Service Edge (SSE) présente de multiples fonctionnalités et avantages.
Faisant de lui une solution attrayante pour toutes les entreprises :

1 Une plateforme de sécurité unifiée

Le SSE intègre plusieurs fonctions de sécurité en une seule plateforme, simplifiant ainsi la gestion et la configuration.
Cela permet une application cohérente des politiques de sécurité, réduit la complexité et améliore l'efficacité de la sécurité grâce au renseignement sur les menaces intégrées.

2 Une visibilité et un contrôle améliorés

Le SSE fournit une visibilité complète sur les utilisateurs, les appareils et les applications, permettant une meilleure détection et réponse aux menaces, une compréhension approfondie de l'utilisation des applications et des flux de données, et pour finir une surveillance de la conformité améliorée.

3 Une protection avancée contre les menaces

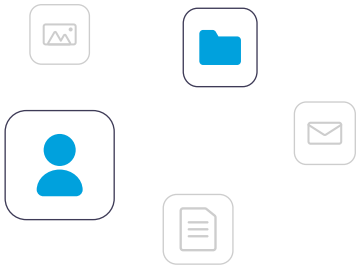
Avec des capacités avancées de détection et de prévention des menaces, le SSE protège contre les cyberattaques sophistiquées, offre des mises à jour rapides des renseignements sur les menaces et réduit le temps de détection et de réponse aux menaces.

4 Une rentabilité et scalabilité

En fournissant des services de sécurité via le cloud, le SSE réduit les coûts matériels et de maintenance. Permettant une évolutivité facile pour s'adapter à la croissance, offre des mises à jour automatiques et de nouveaux déploiements de fonctionnalités, et propose des modèles de tarification flexibles.

5 Une amélioration de l'expérience utilisateur

Grâce à une architecture directe vers le cloud, le SSE réduit la latence pour l'accès aux applications cloud, garantit une sécrité cohérente quel que soit l'emplacement de l'utilisateur, simplifie l'accès aux ressources sans VPN tout en améliorant la productivité des travailleurs à distance et mobiles.



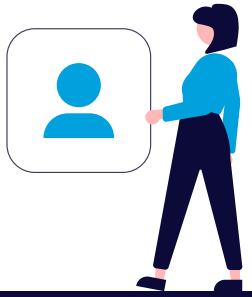
6 Une gestion centralisée des politiques IT

Le SSE permet de créer et d'appliquer des politiques de sécurité cohérentes via une console unique, réduit les risques de conflits ou de lacunes dans les politiques, et accélère la mise en œuvre des changements de politique. Particulièrement adapté pour un usage multi-site, voir multi-pays, le SSE permet d'appliquer des politiques différentes et variées en fonction des sites ou groupes, tout en les pilotant de la console centrale.

7 Une protection des données

Le SSE intègre la prévention de la perte de données et le chiffrement, renforçant ainsi la protection des données sensibles sur tous les canaux, réduisant les risques de violations de données et d'accès non autorisés, et améliorant la capacité à respecter les réglementations sur la protection des données comme le RGPD.

En offrant ces fonctionnalités et avantages, le SSE permet aux entreprises d'améliorer considérablement leur posture de sécurité tout en simplifiant la gestion et en réduisant les coûts. Cette approche globale de la sécurité est particulièrement précieuse dans les environnements commerciaux complexes et centrés sur le cloud d'aujourd'hui.



Déployer un SSE : architecture, meilleures pratiques et considérations

Le Security Service Edge utilise une architecture native du cloud qui permet des options de déploiement flexibles adaptées à divers besoins des entreprises.

Un SSE est par définition basé sur un modèle cloud et une conception basée sur des microservices pour l'évolutivité et la résilience, avec des points de présence (PoPs) distribués pour une couverture multi-site ou multi-pays, complétées par une architecture pilotée par API pour une intégration et une automatisation faciles, et fonctions de sécurité pour des mises à jour rapides et une montée en charge.

Modèles de déploiement :

Déploiement 100 % Cloud

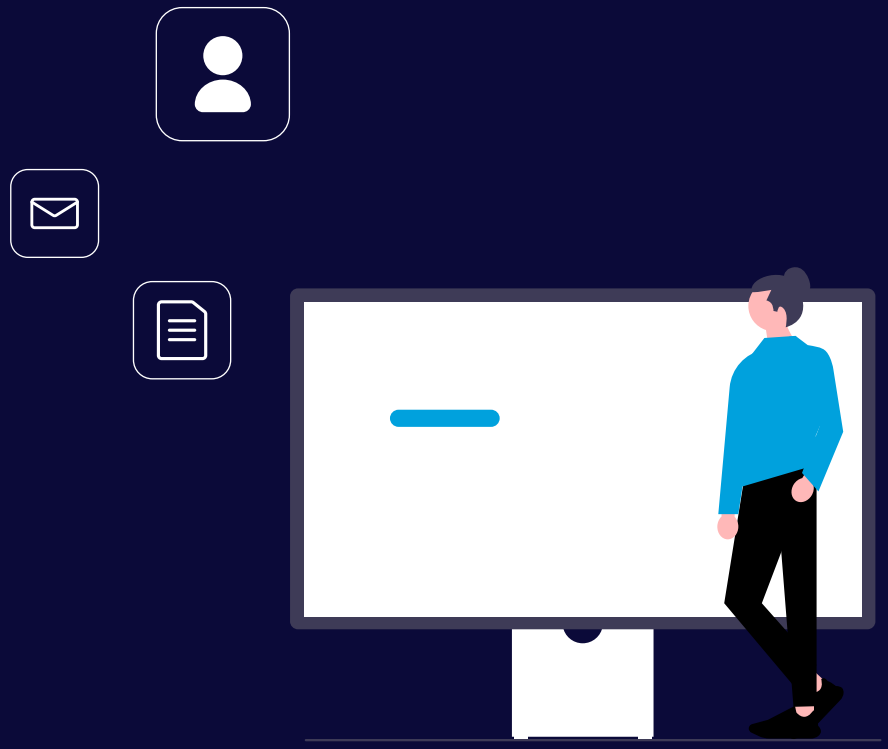
Toutes les fonctions de sécurité sont fournies depuis le cloud, idéal pour les organisations priorisant le cloud, avec une infrastructure sur site minimale requise. Ce déploiement est particulièrement adapté à des organisations multi-site, avec des collaborateurs en déplacement ou bien en télétravail régulier.

Déploiement On-Premise

Bien que particulièrement adapté à un contexte de mobilité et donc de cloud, un SSE peut tout à fait se déployer dans le SI des entreprises, si le cas d'usage ou le contexte de l'entreprise l'impose, notamment en ce qui concerne la confidentialité des données

Chap 2

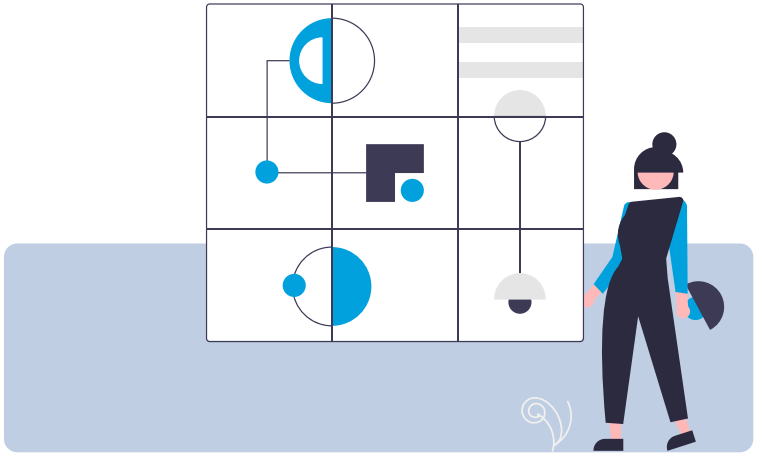
Olfeo : Le seul SSE Européen



Olfeo, reconnu depuis longtemps pour son expertise en filtrage web, a commencé son parcours en offrant des solutions robustes pour sécuriser l'accès à Internet au sein des entreprises françaises. Dès ses débuts, Olfeo s'est distingué par sa capacité à fournir des bases de données d'URLs et d'applications SaaS de très haut niveau, offrant ainsi une protection efficace contre les menaces web.

Cette expertise a permis à Olfeo de gagner la confiance de nombreuses organisations, notamment dans les secteurs des collectivités locales, de la santé et des services essentiels.

Avec l'évolution rapide des besoins en matière de cybersécurité et l'augmentation des menaces sophistiquées, Olfeo a rapidement compris la nécessité d'élargir son offre pour répondre aux exigences d'une protection plus globale et intégrée. **La transition vers une architecture de Security Service Edge (SSE) s'est imposée comme une stratégie naturelle** pour capitaliser sur son expertise existante. Le marché de la sécurité informatique évoluant vers des solutions plus holistiques, Olfeo a commencé à intégrer des fonctionnalités supplémentaires telles que **la détection duShadow IT et le CASB ainsi que d'autres fonctionnalités pour détecter les fuites de données tout en développant des connecteurs vers des IAM Zero Trust tel que Wallix**, permettant de fournir des solutions de sécurité basées sur le principe de la confiance zéro, renforçant ainsi l'accès sécurisé aux ressources critiques des entreprises.



01

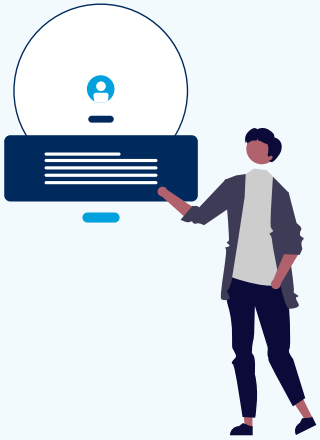
De filtrage web à une suite complète de fonctionnalités SSE

Olfeo, connu depuis longtemps comme un acteur majeur dans le domaine du filtrage web, a entrepris une transformation stratégique mais néanmoins naturelle pour devenir un fournisseur de solutions de Security Service Edge (SSE).

Cette transition s'inscrit dans une volonté de répondre aux évolutions rapides du paysage technologique et des menaces cyber, tout en capitalisant sur son expertise en matière de sécurité web. Historiquement, Olfeo a bâti sa réputation sur la capacité à fournir des solutions de filtrage web adaptées aux besoins spécifiques des entreprises, en tenant compte des réglementations locales et des particularités culturelles. **En passant au SSE, Olfeo élargit considérablement sa proposition de valeur pour répondre aux enjeux contemporains de la menace cyber** avec l'intégration de fonctions avancées de sécurité cloud-native complémentaires de la SWG, telles qu'une protection avancée contre les menaces plus étendue qu'un simple antivirus, la prévention des pertes de données (DLP) et la connexion avec des fournisseurs de gestion des identités et des accès (IAM).

En effet, la montée en puissance du travail à distance et de l'adoption des services cloud a mis en lumière les limites des solutions de sécurité traditionnelles basées sur le périmètre. **Les entreprises nécessitent désormais une protection qui suit les utilisateurs et les données, où qu'ils se trouvent. Olfeo, en intégrant des fonctionnalités SSE, est désormais en mesure de fournir une sécurité homogène, continue et renforcée, adaptée aux environnements de travail hybrides** (applications métier on-prem et cloud, utilisateurs dans le WAN ou en déplacement).

En outre, **le SSE d'Olfeo propose une gestion unifiée des politiques de sécurité via une interface d'administration centrale reconnue comme aisée à comprendre, à utiliser.** Les années d'expérience acquises dans le domaine des passerelles de sécurité web nous ont permis de capitaliser sur les points présentant le plus de valeur pour nos clients et d'éliminer le « bruit » de fonctions ou de paramètres inutiles ou à faible valeur ajoutée pour proposer une expérience utilisateur de référence.



Cette approche nous a permis de réduire considérablement la courbe d'apprentissage et de simplifier la gestion pour les administrateurs, tout en réduisant les risques de conflits ou de lacunes dans les politiques. Cela permet alors une mise en œuvre (très) rapide de la solution lors de l'installation et ensuite un gain de temps non négligeable lorsque des modifications sont nécessaires pour s'adapter à de nouvelles menaces ou des exigences réglementaires.

Le passage au SSE offre également aux administrateurs de nos clients une meilleure visibilité, un contrôle sur l'utilisation des applications et des données et une intégration fluide et simple avec les systèmes de surveillance existants tels que les SIEM/XDR ou avec les fournisseurs d'identité installés.

Enfin, Olfeo s'engage à continuer d'innover et de répondre aux besoins de ses clients avec des solutions à la pointe de la technologie. En évoluant vers un modèle SSE, Olfeo met à profit ses années d'expérience en sécurité web tout en adoptant une approche plus complète et moderne de la sécurité des informations. **Cette transition marque ainsi une étape cruciale dans l'évolution de l'entreprise, nous permettant d'adapter au mieux notre solution aux nouveaux enjeux de sécurité.**

02

Le Trust-Centric, un différentiateur innovant au service d'une sécurité forte

L'internet a été conçu comme un espace de grande liberté. Il s'est transformé en un monde moins utopique où les utilisateurs, même chevronnés, sont dorénavant sur le qui-vive.

L'explosion du nombre de faux sites et des malwares rend complètement illusoire la capacité à contrer les cyberattaques par une approche threat-centric basée sur la reconnaissance exhaustive de ces menaces, telle que la plupart des acteurs utilisent leur solution.

Pour aider à contrer la menace que représente le phishing et les serveurs de contrôle de ransomwares, Olfeo apporte une réponse originale mais très efficace grâce à son approche Trust-Centric. En effet, elle permet de limiter le trafic HTTP vers Internet aux seuls domaines, IP et URLs de confiance vérifiés par Olfeo. **Elle offre ainsi le plus haut niveau de sécurité possible, notamment contre les menaces posées par les domaines éphémères ou créés lors d'une phase d'attaque ou contre le typosquatting à l'origine d'attaques de phishing ou de spearphishing.** Avec ce nouveau paradigme de la sécurité, les attaques par ransomwares, qui utilisent des sites éphémères, sont naturellement repoussées car ils ne figurent pas dans la base d'URLs de confiance et les domaines connus pour poser des risques de sécurité le sont également.

Trier le vrai du faux ?

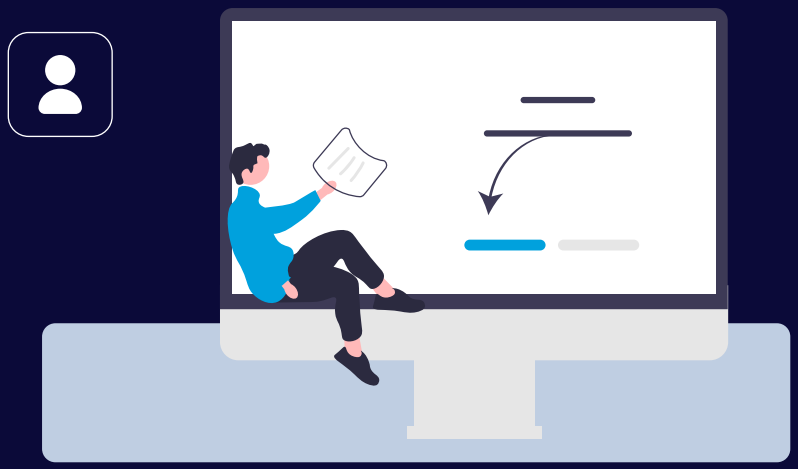
Depuis 20 ans, Olfeo a développé une expertise reconnue d'analyse des contenus web et une base de données de domaines et d'URL de classe mondiale au cœur de nos produits de sécurité. Son savoir-faire unique, allie des méthodes de classification éprouvées par sa très longue expérience.

Cette base de domaines, d'IP et d'URL est alimentée en permanence grâce à de multiples sources. La première d'entre elles est la communauté des clients Olfeo. Par son utilisation quotidienne chez nos clients (et avec leur accord), chaque produit de sécurité d'Olfeo installé chez nos clients contribue activement à son amélioration en remontant très régulièrement à Olfeo les domaines inconnus.

Le partage de l'information et le retour d'expérience permettent de rendre la base toujours plus exhaustive et plus fiable. Cette base est également nourrie jour après jour par les recherches de l'équipe CTI Olfeo.

La classification des contenus se fait ensuite grâce à des technologies à base d'IA mais aussi avec un contrôle humain systématique, assuré par une équipe dédiée, pour éviter tout risque de faux positifs. L'enrichissement continu de la base de domaines, d'IPs et d'URLs de confiance est le facteur-clé de succès de l'approche Trust-Centric. Olfeo reconnaît actuellement plus de 99,5 % des URLs demandées par les entreprises européennes. L'exceptionnelle qualité de cette base de domaines, d'IP et d'URLs de confiance d'Olfeo lui permet d'être la seule solution de sécurité Trust-Centric au monde.

Preuve de sa qualité, cette base est utilisée par de nombreux éditeurs en marque blanche (OEM) pour des cas d'usages connexes à la sécurité informatique , tel que le routage réseau, l'analyse de trafic etc.



03

La confidentialité des données : conformité juridique et technologique

La confidentialité des données personnelles est un enjeu crucial pour les fournisseurs de solutions de proxy web et de Security Service Edge (SSE) pour plusieurs raisons essentielles.

1 Conformité réglementaire

Les entreprises sont tenues de se conformer à diverses lois et réglementations concernant la protection des données personnelles, telles que le Règlement Général sur la Protection des Données (RGPD) en Europe, le California Consumer Privacy Act (CCPA) aux États-Unis, et d'autres réglementations locales. Le non-respect de ces régulations peut entraîner des amendes sévères et des sanctions légales.

2 Confiance des clients

La confiance des clients est un atout inestimable pour tout fournisseur de services.
Les entreprises doivent être assurées que leurs données personnelles et celles de leurs utilisateurs sont traitées avec le plus grand soin. Une fuite ou une mauvaise gestion des données personnelles peut gravement endommager la réputation d'un fournisseur et entraîner la perte de clients.

3 Sécurité des données

La confidentialité des données personnelles est intrinsèquement liée à la sécurité globale des données. Les informations personnelles sensibles, telles que les identifiants, les adresses IP, les historiques de navigation et autres métadonnées, doivent être protégées contre les accès non autorisés et les cyberattaques. Une bonne gestion de la confidentialité contribue à renforcer la sécurité des systèmes ainsi que des réseaux.

4 Risques de violations de données

Les violations de données peuvent avoir des conséquences dévastatrices, tant pour les individus que pour les entreprises. Les informations personnelles volées peuvent être utilisées pour des activités malveillantes telles que le vol d'identité, les fraudes financières et les attaques ciblées. Les fournisseurs de proxy web et de SSE doivent mettre en place des mesures robustes pour prévenir ces incidents.

La confidentialité et la protection des données font partie des valeurs ajoutées de la solution Olfeo. Contrairement à ses concurrents américains, les données personnelles transitant pour le cloud Olfeo ne sont pas soumises aux lois d'extraterritorialité et sont nativement conformes avec le RGPD. Olfeo travaille avec des fournisseurs de cloud souverains, français et avec des data servers localisés en France.

04

Sécurité, simplicité et accessibilité : les solutions Olfeo à destination de toutes les entreprises

Les solutions d'Olfeo se veulent simples, accessibles et faciles à déployer, tout en assurant en même temps un niveau de sécurité irréprochable.

Olfeo comprend que le déploiement d'une solution SSE peut présenter des difficultés, notamment pour des structures de taille intermédiaire. Nous avons donc tout fait pour rendre la solution modulaire, flexible et avec la possibilité de déployer les fonctionnalités de manière progressive, en fonction des besoins et de la maturité des structures.

Les bénéfices de la solution Olfeo s'articulent autour de 3 axes :

1 Une sécurité irréprochable

Les fonctionnalités de protection du trafic web et de gestion des accès aux données permettent de sécuriser les accès web des collaborateurs et de les protéger contre les contenus dangereux, illicites ou encore non-appropriés, comme par exemple les malwares.

2 Une limitation du risque juridique et de conformité

Se déployant dans le respect du droit du travail, la solution Olfeo permet de se protéger du risque juridique civil et pénal en bloquant l'accès à des contenus présentant un risque légal. Elle contribue également à assurer la conformité avec des directives relatives à la cybersécurité telles que NIS2 ou DORA pour le secteur financier par exemple.

3 La protection des données de l'organisation

Les données sont l'or noir des organisations. Avec les fonctionnalisés CASB et DLP, l'exposition des données sensibles des organisations sont surveillés, contrôlés par des politiques groupes et protégés contre la porte ou le vol.

Chap 3

Témoignage du CHU Poitiers :

Pierre Taveau, le RSSI du CHU de Poitiers, est revenu sur l'importance cruciale de la sécurité des établissements de santé, mettant en avant les défis actuels rencontrés dans ce secteur.

Premièrement, la digitalisation croissante du parcours de santé accroît la surface d'attaque, avec une multitude de logiciels et d'applications métier suivant le parcours de soins du patient.

De plus, l'exposition des équipements médicaux sur Internet, notamment dans le domaine de l'IoT, présente un point de vulnérabilité.

Il souligne trois enjeux majeurs :

- **La dette technique accumulée au fur et à mesure des années**
- **Le besoin crucial de formation et de sensibilisation du personnel de santé face aux risques cyber**
- **Le manque de ressources techniques dans ce domaine.**

Renforcer la Sécurité des Services de Santé : Les Solutions Cruciales d'Olfeo

L'année 2023 a été marquée par une **intensification des défis pour les services de santé, tant publics que privés**. Des institutions telles que le Centre Hospitalier de la Réunion ont été touchées, rappelant l'ampleur de ces défis dans le secteur de la santé. Parmi les solutions cruciales, Olfeo et sa passerelle de sécurité Web jouent un rôle central.

Le défi du proxy

Le véritable défi d'un proxy Web aujourd'hui est de **contrôler efficacement l'utilisation d'Internet par les utilisateurs.**

Cela implique non seulement de surveiller les activités des utilisateurs, mais aussi de gérer les dispositifs IoT et autres objets connectés présents sur les différents sites du CHU. Olfeo, avec son moteur de sécurité avancé, offre une protection essentielle grâce au déploiement de politiques de filtrage claires et en mettant en place des mécanismes de déchiffrement de données essentiels pour respecter les réglementations telles que le RGPD.

Les enjeux de sécurité vont au-delà des simples anti-malwares. Olfeo propose une approche globale qui inclut la sécurité DNS, des logs détaillés, une meilleure visibilité des activités en ligne et des pages de sensibilisation pour les utilisateurs. La mise en place d'une politique de filtrage efficace est essentielle pour contrôler l'accès à Internet, prévenir les menaces telles que les malwares, le phishing et les sites illicites, tout en garantissant le respect des chartes informatiques. Une innovation notable introduite par Olfeo est **le concept de Trust-Centric, qui repose sur une base de contenu d'URL solide développée au cours des 20 dernières années.** Cette approche permet de bloquer automatiquement tout contenu non vérifié et non validé par Olfeo, réduisant ainsi les risques liés à la navigation sur Internet.

Concrètement, qu'apporte Olfeo au sein d'un établissement de santé :

Pour revenir au cas concret du Centre Hospitalier Universitaire (CHU) de Poitiers, la démarche adoptée pour assurer la sécurité de quelque 10 000 utilisateurs a été **la simplification des politiques de filtrage en se concentrant sur des accès Internet basés sur des catégories prédéfinies, validées par l'ensemble des instances.** Dans ce contexte, l'établissement de santé est passé d'une solution basée sur une solution américaine, qui devenait de plus en plus compliquée à gérer en interne parce qu'il y avait des dizaines d'exceptions. Le passage à la solution Olfeo fut dans un premier temps compliqué, en raison des différentes exceptions. Cependant, avec l'accompagnement d'Olfeo, l'architecture complète de la solution en interne a pu être revue et adaptée à l'ensemble des établissements du CHU.

Il y a donc un proxy qui sert à faire du load balancing, un maître et quatre esclaves pour gérer les 10 000 utilisateurs, ce qui représente à peu près 7 000 postes sur l'ensemble des sites (5 sites pour le département).

Définition et mise en place du filtrage

La définition des politiques de sécurité de filtrage a été opérée en plusieurs étapes, c'est-à-dire qu'il y a eu **une première validation par les hautes instances du CHU, suivie par une validation par l'ensemble des instances.** Cette démarche a permis d'informer l'ensemble des utilisateurs afin de déterminer une politique simple par niveau de hiérarchie des postes.

Le premier niveau de politique est de supprimer totalement l'accès à Internet. Ce qui est tout à fait envisageable pour certains des équipements biomédicaux par exemple.

Un deuxième niveau est un accès limité avec une liste blanche permettant un accès très restreint à Internet correspondant à l'utilisation des appareils de bloc opératoire, console packs et autres équipements de ce type.

Un troisième niveau correspond à la majorité du CHU qui a un accès qu'on appelle "professionnel" sur lequel les différentes instances ont privilégié un accès lié au métier.

Un autre niveau mis en place est une catégorie qu'on peut qualifier de VIP. Cette catégorie répond à différents cas d'usages précis et très contrôlés. Elle permet un accès complet aux sites de commerce pour des acheteurs, par exemple. Cette catégorie peut permettre des accès spécifiques pour les psychologues qui sont confrontés à devoir faire des recherches sur des sites sensibles. Ceci s'applique également aux différentes exceptions liées aux métiers spécifiques que l'on peut retrouver dans un établissement de santé.

La dernière catégorie d'utilisateurs en place est très limitée, elle s'applique aux développeurs qui ont des besoins d'accès plus spécifiques, en particulier pour les besoins de recherche et développement que l'on peut retrouver dans un établissement comme le CHU de Poitiers.

Les politiques de filtrage

Encore une fois, l'ensemble des instances ont privilégié quelque chose de simple. De plus, **cette politique est connue et validée par tous les membres de l'établissement puisqu'elle est inscrite au règlement intérieur et validée par la charte informatique.**

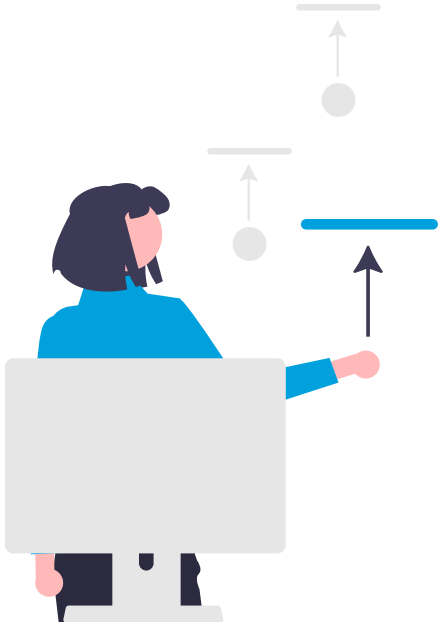
Au sujet de la charte informatique, nous avons souhaité mettre en place des logs individuels pour chaque utilisateur et Olfeo a particulièrement contribué à mettre cette solution en place. Car un certain nombre de connexions dans nos établissements sont génériques sur des postes partagés. Nous avons donc créé, avec l'aide d'Olfeo, **un portail de connexion interne qui oblige chaque utilisateur qui souhaite accéder à Internet à se connecter avec son identifiant/mot de passe individuel.**

Ceci permet, dans un premier temps, de respecter l'ensemble des réglementations et, par ailleurs, cela nous permet d'assurer un suivi et une traçabilité de l'ensemble des accès.

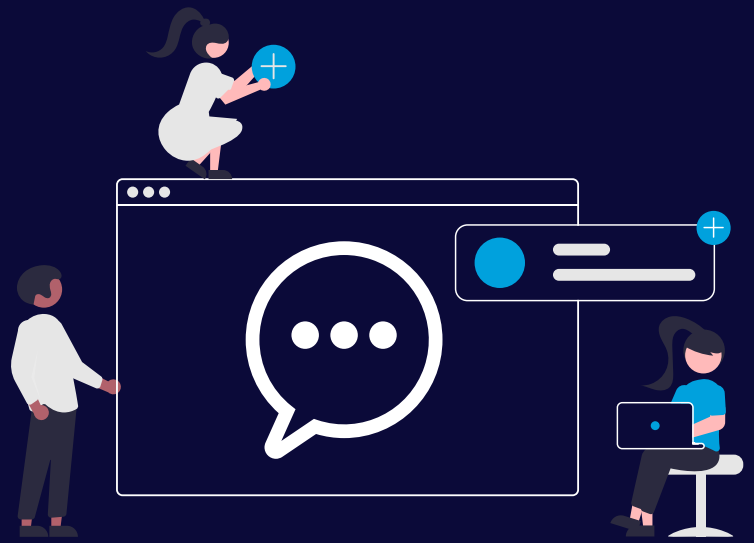
En fonction des politiques, nous pouvons retrouver via Elasticsearch différentes alertes sur nos dashboards et tableaux de bord, en particulier lorsqu'une personne tente d'accéder à des catégories interdites.

En conclusion

Olfeo a permis, non seulement de simplifier la gestion des accès Internet du CHU de Poitiers, mais aussi de renforcer notre conformité aux réglementations et de nous aider à améliorer la traçabilité des activités en ligne.



Contactez nous



contact@olfeo.com www.olfeo.com

retrouvez-nous sur nos réseaux