Akamai

GUIDE DESTINÉ AUX ACHETEURS

# Comment sélectionner une passerelle Web sécurisée basée dans le cloud

Protéger le personnel en télétravail et simplifier la sécurité de l'entreprise

# Table des matières



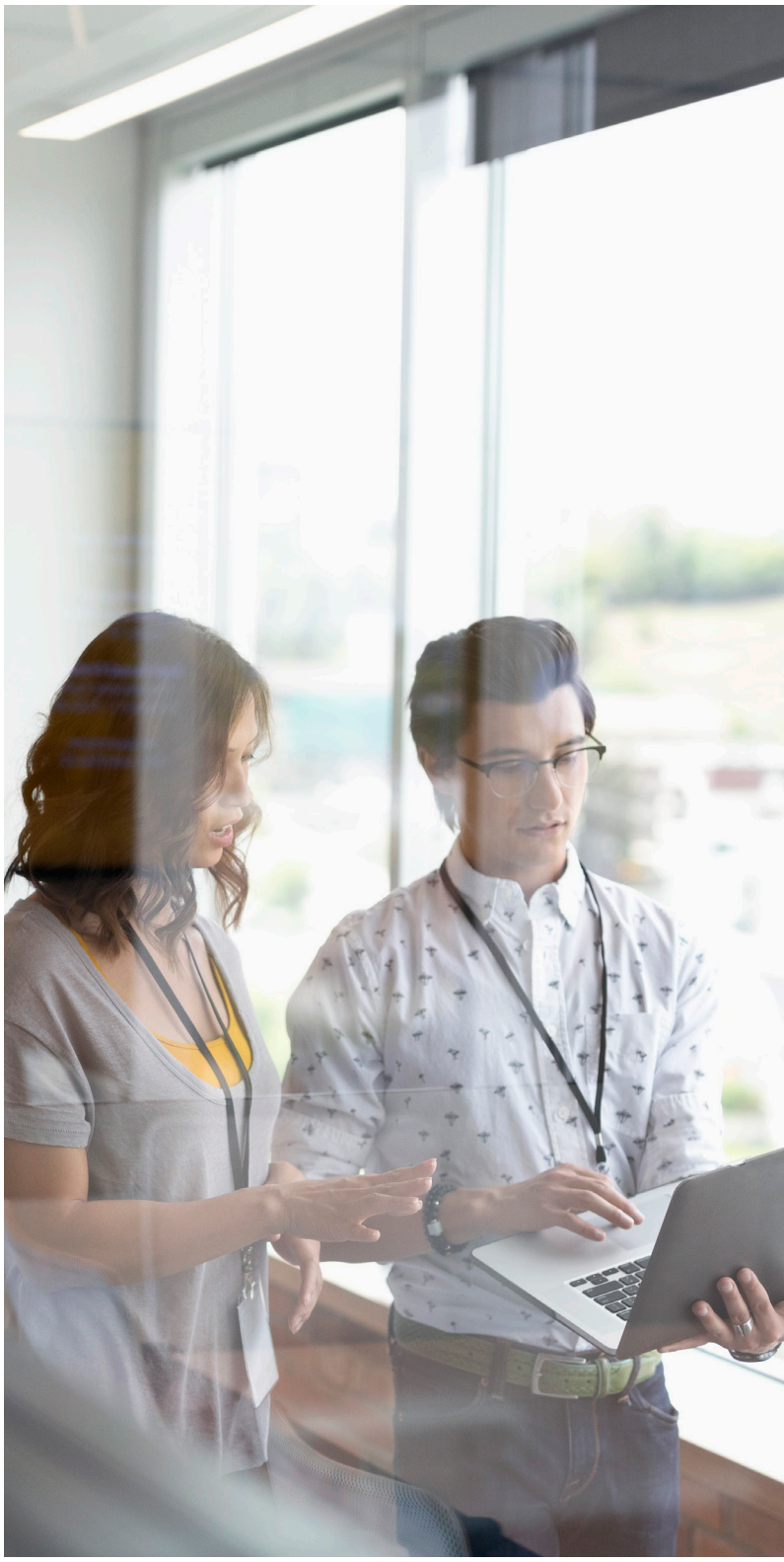
# Sécuriser les entreprises : repenser l'acheminement des centres de données

Le cloud computing, le logiciel en tant que service (SaaS), la mobilité et les architectures réseau mises à jour ont révolutionné les pratiques commerciales. Mais ils ont également provoqué une véritable tempête pour les équipes informatiques qui tentent de sécuriser le personnel sans limiter la valeur de ces nouvelles technologies. Un nouveau défi se pose désormais : quel que soit le niveau d'avancement de leur transformation digitale, beaucoup d'entreprises ont dû rapidement changer de cap pour prendre en charge une augmentation considérable du nombre d'utilisateurs en télétravail en 2020.

Une passerelle Web sécurisée est un composant essentiel de la protection des employés, mais de nombreuses entreprises utilisent encore des équipements physiques déployés dans des centres de données. Ce matériel nécessite une gestion, une maintenance et des mises à niveau continues, et utilise un acheminement de trafic obsolète pour inspecter et contrôler le trafic Web, ce qui finit par réduire les performances.

Les entreprises ont besoin d'une approche nouvelle et rationalisée pour sécuriser cette nouvelle réalité d'un environnement professionnel distribué. La solution : se passer des équipements matériels et déplacer cette fonctionnalité de passerelle Web sécurisée vers le cloud.

Ce guide destiné aux acheteurs décrit les avantages des passerelles Web sécurisées basées dans le cloud et les fonctionnalités à rechercher dans une technologie de passerelle Web actuelle.



# La généralisation du télétravail crée de nouvelles exigences en matière d'informatique et de sécurité

Au cours des dix dernières années, les entreprises ont vu régulièrement augmenter leur main-d'œuvre en télétravail. Cette tendance s'est accélérée en raison de la crise de la COVID-19 et devrait se poursuivre bien au-delà de la pandémie. Gartner a relevé que 74 % des directeurs financiers interrogés passeront au moins 5 % de leur personnel sur site vers des postes en télétravail permanent après la fin de la pandémie.[1]

En parallèle, le nombre d'attaques ciblées sophistiquées telles que l'hameçonnage, les ransomware et les programmes malveillants a grimpé en flèche. Cinquante-trois pour cent des personnes interrogées dans le cadre d'une enquête récente ont déclaré avoir été témoins d'une augmentation de l'activité d'hameçonnage depuis le début de la pandémie de COVID-19.[2] Le département du Trésor des États-Unis a déclaré dans un avis récent que les demandes de paiements de ransomware ont augmenté pendant la pandémie de COVID-19, car les cyberacteurs ciblent les systèmes en ligne utilisés pour assurer la continuité des activités.[3]

Jusqu'ici, les entreprises sécurisaient l'accès Internet à la fois des utilisateurs sur leurs sites principaux et succursales et des travailleurs en télétravail en installant des dispositifs de sécurité dans leurs centres de données, tels que des passerelles Web sécurisées. Elles pouvaient ensuite acheminer tout le trafic Web vers cet emplacement central pour inspection et contrôle.

Les entreprises utilisaient ces passerelles Web sécurisées pour filtrer les programmes malveillants indésirables du trafic Web initié par les utilisateurs, empêcher les utilisateurs d'accéder à des sites Web malveillants, et appliquer les politiques de l'entreprise et réglementaires.

Ces solutions de passerelle ont été initialement conçues et déployées dans des environnements où la plupart des employés utilisaient sur leurs bureaux des terminaux gérés par l'entreprise. Cependant, à mesure de l'augmentation du nombre d'utilisateurs en télétravail et dans des succursales, et du trafic passant par l'Internet public pour accéder aux applications SaaS, les entreprises ont commencé à installer des passerelles Web sécurisées multiples et redondantes dans le centre de données central afin d'assurer des performances satisfaisantes. L'achat et la gestion de ces dispositifs sont devenus de plus en plus complexes, coûteux et chronophages.

> **« Le pourcentage du budget informatique consacré aux centres de données a diminué au cours des dernières années et ne représente aujourd'hui que 17 % du budget total. »**
>
> — Gartner, Données clés 2019 sur l'informatique

Les entreprises ont également ajouté des équipements de passerelle Web sécurisée à leurs succursales tout en assurant l'acheminement du trafic pour tous les utilisateurs en télétravail. Cette redondance a entraîné une prolifération d'équipements et les coûts qui en découlent, ainsi qu'un déploiement et une gestion nécessitant beaucoup de main-d'œuvre.

Il est également devenu de plus en plus difficile d'appliquer des règles de sécurité cohérentes sur un grand nombre de sites. Même lorsque les entreprises ont déployé des équipements virtualisés pour réduire cette multiplication des équipements, elles ont dû déployer et gérer du matériel supplémentaire.

Une troisième approche a été le déploiement hybride : des entreprises ont continué d'utiliser des passerelles Web sécurisées sur site pour les principaux sites, et envoyé le trafic Web des succursales vers une passerelle Web sécurisée basée dans le cloud, tout en acheminant le trafic pour les employés en télétravail. Cette approche a maintenu les investissements matériels déjà existants dans les équipements sur site. Toutefois, elle a rajouté de la complexité, car les entreprises ont géré au bout du compte des systèmes disparates. Non seulement l'équipement additionnel et la gestion supplémentaire étaient beaucoup plus coûteux qu'une approche entièrement dans le cloud, mais il était également difficile d'assurer des politiques cohérentes sur les systèmes locaux et ceux basés dans le cloud.

> **Selon Gartner, d'ici 2025, 80 % des entreprises fermeront leurs centres de données traditionnels.[4]**

Pire encore, alors même que les entreprises adoptaient ces solutions de plus en plus complexes, elles ont commencé à faire face à une pénurie de ressources en cybersécurité. Selon une étude de (ISC)[2], il faudrait augmenter de 62 % le nombre de personnes travaillant dans la sécurité aux États-Unis pour combler la pénurie actuelle.[5]

# Pourquoi opter pour une passerelle Web sécurisée basée dans le cloud ?

Les entreprises ont besoin d'adopter une approche moderne de la sécurité Web, qui s'associe à la stratégie d'entreprise de migration dans le cloud, en adoptant et en permettant le télétravail. Une passerelle Web sécurisée basée dans le cloud offre aux entreprises un haut niveau de sécurité et réduit la complexité en connectant directement à Internet, éliminant ainsi le besoin de plusieurs équipements et acheminements.

Avec une passerelle Web sécurisée basée dans le cloud, les entreprises bénéficient des avantages suivants :

**Moins de complexité liée à la sécurité :** en tant que service dans le cloud, ces passerelles Web sécurisées éliminent le besoin de déployer du matériel ou des équipements virtuels, ou de configurer, gérer et remplacer/mettre à niveau du matériel tous les trois ans.

**Moins de goulets d'étranglement des performances :** une passerelle Web sécurisée basée sur Internet élimine le besoin d'ajouter des équipements supplémentaires pour faire face à l'augmentation des charges de trafic Web et à l'augmentation des niveaux de trafic chiffré. Les clients peuvent simplement ajouter des services supplémentaires en fonction de leurs besoins, avec un impact minimal sur les performances.

**Réduction des frais d'acheminement/de hairpinning du trafic :** les passerelles Web sécurisées basées dans le cloud assurent la sécurité du trafic Web sans l'acheminer pour permettre une connexion directe à Internet, réduisant ainsi les coûts de réseau de la commutation multiprotocole par étiquette (MPLS).

**Meilleure efficacité de l'équipe de sécurité :** étant donné que les passerelles Web sécurisées dans le cloud ne nécessitent aucune maintenance continue du matériel ou des logiciels, le personnel réduit en charge de la sécurité a plus de temps pour se concentrer sur d'autres mesures de sécurité proactives.

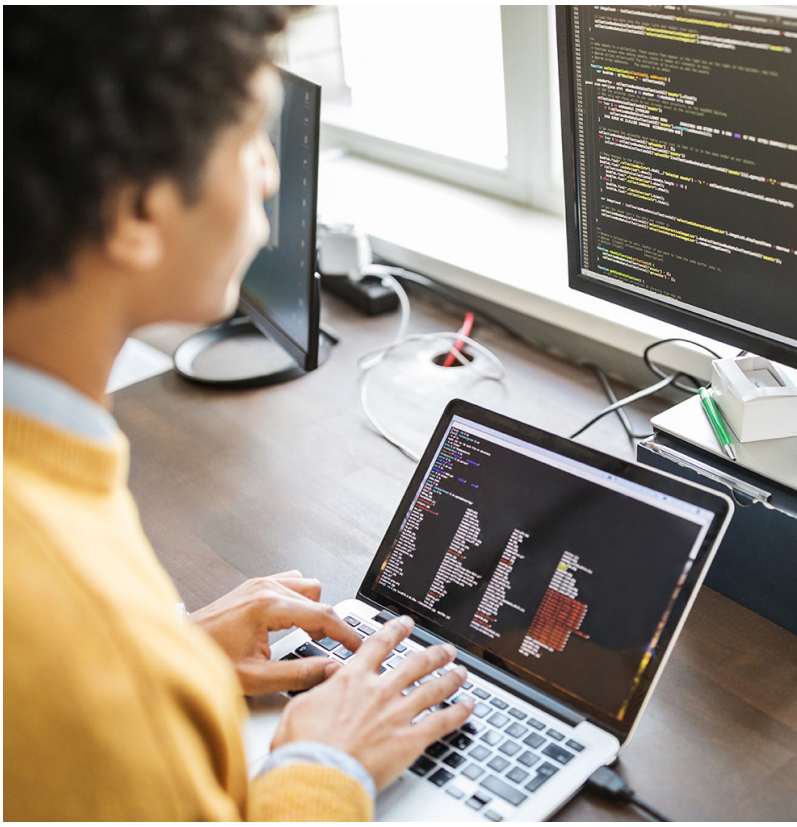
**Stratégies de sécurité cohérentes :** les organisations peuvent utiliser des stratégies gérées de manière centralisée, mais déployées à l'échelle mondiale, pour tous les utilisateurs qui se connectent à partir de n'importe quel terminal. Même si l'entreprise a des stratégies différentes pour différentes régions, elle peut utiliser la même interface utilisateur pour toutes les gérer.

# Principales exigences pour une passerelle Web sécurisée

Lors de la sélection d'une passerelle Web sécurisée basée dans le cloud, il est important de reconnaître que la sécurité est la caractéristique la plus importante. Par exemple, elles comprennent un contrôle de la bande passante, qui a été conçu à une époque où la bande passante était coûteuse. Par exemple, elles disposent du contrôle de la bande passante, qui a été conçu à une époque où la bande passante était coûteuse. Elles empêchent également les employés d'utiliser YouTube ou Facebook pendant les heures de travail. Aujourd'hui, ces fonctionnalités ne sont plus nécessaires, car la bande passante est abondante et le nombre de personnes qui utilisent leurs terminaux mobiles est si élevé que les entreprises n'ont plus besoin d'interdire l'accès à ces services sur ses propres terminaux.

Aujourd'hui, les entreprises ont besoin d'une passerelle Web sécurisée basée dans le cloud spécialement conçue pour gérer les problèmes de sécurité actuels. La solution devrait notamment suivre une stratégie de défense en profondeur qui utilise plusieurs mesures de sécurité pour assurer le plus haut niveau de protection. Une telle approche devrait couvrir tous les aspects de la cybersécurité et fournir des mesures de sécurité redondantes. De cette façon, si une ligne de défense est compromise, des couches supplémentaires de défense sont en place pour empêcher les attaques de se glisser au travers des fissures. Cette approche par couches permet de garantir que les menaces telles que les programmes malveillants, les ransomware et l'hameçonnage sont bloquées de manière anticipée et plus rapidement, et ce avant que le terminal de l'utilisateur ne soit compromis.

Une passerelle Web sécurisée qui déploie une stratégie de défense en profondeur doit proposer les fonctionnalités de sécurité suivantes :



## Évaluation de toutes les requêtes DNS et URL

Une solution de passerelle Web sécurisée basée dans le cloud doit évaluer toutes les requêtes URL et DNS par rapport aux informations sur les menaces en temps réel, et bloquer les requêtes malveillantes dès le début de la chaîne d'attaque. Si la passerelle Web sécurisée peut bloquer les menaces avant qu'une connexion sortante ne soit établie, la ressource Web n'a pas besoin d'ouvrir ou d'inspecter le contenu renvoyé. Cette efficacité évite un processus informatiquement lourd et réduit la quantité de trafic que la passerelle Web sécurisée doit analyser à l'étape de la charge utile. Le résultat ? Amélioration des performances générales de la passerelle Web sécurisée.

Les informations sur les menaces doivent protéger contre les programmes malveillants, les ransomware, l'hameçonnage et l'exfiltration de données DNS à faible débit. Elles doivent également être conçues pour fournir une protection pertinente contre les menaces actuelles, avec un faible taux de faux positifs.

## Techniques multiples d'analyse de la charge utile

Étant donné que toutes les menaces sont différentes et qu'aucune technique ou approche de détection unique ne peut faire face à tous les types de programmes malveillants, la solution de passerelle Web sécurisée doit comprendre plusieurs moteurs d'analyse de programmes malveillants. Ces moteurs doivent analyser les charges utiles HTTP et HTTPS en ligne ou hors ligne à l'aide de nombreuses techniques d'identification, y compris la détection des signatures, la détection des menaces sans signature, l'apprentissage automatique et des bacs à sable. Cette analyse offre une protection « zero day » complète contre les fichiers potentiellement malveillants, tels que les exécutables et les documents.

## Détection d'hameçonnage « zero day »

Les employés en télétravail restent confrontés à des attaques d'hameçonnage en hausse depuis l'épidémie de COVID-19. Les acteurs malveillants lancent ces attaques par e-mail, sur les réseaux sociaux et les applications de messagerie instantanée, ainsi que par le biais de canaux de partage de fichiers et de collaboration en ligne, pour dérober les informations d'identification de l'entreprise leur permettant d'accéder à son réseau. À partir de là, les attaquants peuvent parcourir le réseau pour rechercher et exfiltrer des données et de la propriété intellectuelle, ou promulguer des campagnes de ransomware.

Pour identifier et bloquer l'accès à une page d'hameçonnage, la plupart des fournisseurs de solutions de sécurité procèdent comme suit :

1. **Ils observent le trafic inhabituel sur un domaine**
2. **Ils analysent ce domaine**
3. **Ils déterminent s'il s'agit d'un domaine d'hameçonnage**
4. **Ils l'ajoutent à la liste des domaines bloqués**
5. **Ils transmettent la mise à jour de la liste aux clients**

Ce processus peut prendre des heures. Et pire encore, les cybercriminels d'aujourd'hui utilisent des kits d'hameçonnage pour créer et lancer facilement des attaques de courte durée, rendant la détection encore plus difficile. Lorsque l'URL ou le domaine d'hameçonnage est découvert, l'attaque est terminée. En effet, plus l'attaque d'hameçonnage est sophistiquée et ciblée, plus sa durée est courte.

Bien que ces campagnes puissent se terminer rapidement, un moteur de détection d'hameçonnage « zero day » avancé peut tout de même les identifier et les bloquer. Les éléments récurrents de ces attaques basées sur un kit sont visibles dans le code des pages d'hameçonnage. Avec ces informations, il est possible d'identifier les « empreintes digitales » de ces pages qui permettent une identification précise.

Une solution de passerelle Web sécurisée doit inclure un moteur de détection d'hameçonnage « zero day » pouvant analyser les pages Web demandées et les comparer aux « empreintes digitales » des pages d'hameçonnages précédemment observées.

## Inspection du trafic chiffré

Internet est un canal intrinsèquement non sécurisé pour le transfert de données. Il est donc devenu désormais monnaie courante de chiffrer le trafic Web pour empêcher les attaquants d'espionner des conversations, de frauder ou de manipuler le trafic. Le protocole TLS (Transport Layer Security) est la norme de chiffrement de fait pour la navigation Web sécurisée. TLS crée un tunnel sécurisé entre deux points de terminaison, comme un navigateur client et un serveur Web.

> **Le pourcentage de trafic Web chiffré sur Internet a augmenté régulièrement, passant d'environ 50 % en 2014 à entre 80 et 90 % aujourd'hui. La plupart (96 %) des 100 sites les plus populaires au monde utilisent HTTPS par défaut.**
>
> — Rapport de transparence Google, 2020

Mais le trafic HTTPS n'est pas toujours inoffensif. Les attaquants et les développeurs de programmes malveillants utilisent également le chiffrement pour masquer leurs activités, empêcher les utilisateurs d'accéder à des fichiers (par ransomware) et sécuriser les communications réseau malveillantes. Une étude récente a révélé que près d'un quart des programmes malveillants qui ont établi une connexion Internet utilisaient TLS pour communiquer.[6]

Pour inspecter et contrôler de manière proactive le trafic Web HTTPS, il est nécessaire de regarder à l'intérieur du tunnel sécurisé et d'examiner le trafic chiffré, à l'aide d'un serveur proxy (intermédiaire de confiance). Le serveur proxy doit déchiffrer le trafic HTTPS en texte brut, l'analyser, chiffrer à nouveau le trafic, puis créer une autre connexion sécurisée à l'aide d'une technique dite « machine-in-the-middle » (MITM). La technique MITM inspecte les URL demandées afin de déterminer si elles sont sûres ou malveillantes, fournir une visibilité sur le trafic chiffré TLS et protéger l'entreprise contre les menaces tout en préservant la confidentialité et l'intégrité du trafic vers les sites Web d'origine.

Les inspections MITM nécessitent une capacité de traitement considérable. La navigation Web peut donc ralentir en raison de la latence. La passerelle Web sécurisée doit offrir des services qui améliorent les performances des applications. Elle doit inclure un réseau mondial de serveurs et de logiciels intelligents situés à proximité des utilisateurs et des centres de données dans le monde entier pour mettre en place des optimisations Web qui améliorent les performances et la disponibilité des applications.

En outre, la technique MITM vérifie que le fournisseur de la passerelle Web sécurisée dans le cloud gère une liste centralisée des domaines et URL défectueux à contourner. De plus, la passerelle Web sécurisée dans le cloud doit être en mesure de contourner l'inspection MITM pour des types spécifiques de contenu Web sensible, comme les services financiers et les soins de santé.

## Prévention intégrée des pertes de données

Il est essentiel d'empêcher de manière proactive la perte de données personnelles identifiables et d'autres données commerciales confidentielles, compte tenu des risques de perte financière ou d'atteinte à la réputation. La passerelle Web sécurisée dans le cloud doit comprendre une prévention des pertes de données intégrée, facile à configurer et rapide à déployer. Des dictionnaires fréquemment mis à jour doivent couvrir les réglementations de protection et de confidentialité des données telles que PII, PCI, DSS et HIPAA, et les entreprises doivent pouvoir facilement créer des dictionnaires personnalisés.

## Identification et gestion du Shadow IT

Les utilisateurs peuvent télécharger, installer et utiliser sur des terminaux gérés des centaines de milliers d'applications à leur disposition, sans que l'équipe en charge de la sécurité de l'entreprise ne soit au courant. Mais l'utilisation d'applications non approuvées peut considérablement étendre la surface d'attaque de l'entreprise et augmenter son profil de risque.

> **L'entreprise moyenne utilise plus de 1 295 applications et services cloud. Plus de 95 % de ces derniers ne sont pas gérés, sans droit d'administration informatique.**
>
> — Cybersecurity Insiders,
> Rapport sur la sécurité dans le cloud, 2019

Une passerelle Web sécurisée dans le cloud doit être capable d'identifier les applications utilisées, de détecter le nombre d'utilisateurs ayant installé des applications spécifiques et de mettre en évidence les applications susceptibles de présenter un risque de sécurité potentiellement grave. Après cette identification, la solution doit être en mesure de bloquer l'ensemble des applications ou certaines de leurs opérations spécifiques (par exemple, autoriser les chargements, mais pas les téléchargements).

## Protection pour tous les terminaux où qu'ils se trouvent

Les modes de travail sont devenus de plus en plus souples au cours des dix dernères années. Les utilisateurs peuvent désormais travailler où qu'ils se trouvent et sur n'importe quel terminal. Conséquemment à l'augmentation du télétravail pendant la pandémie, 59 % des outils utilisés par les employés sont désormais des mobiles, en supplément ou en remplacement des PC et des ordinateurs portables. Ce changement devrait se poursuivre même après la reprise du travail au bureau.[7]

Le passage aux terminaux mobiles et l'utilisation accrue des réseaux Wi-Fi peuvent créer une faille dans la sécurité des entreprises. Les entreprises doivent pouvoir appliquer un niveau de sécurité uniforme et universel, sans compromettre les performances des terminaux.

Une passerelle Web sécurisée dans le cloud doit identifier, bloquer et atténuer de manière proactive les menaces ciblées telles que les programmes malveillants, les ransomware, l'hameçonnage, l'exfiltration de données DNS et les attaques « zero day » sur tous les terminaux (iOS, Android OS, Chrome OS), et sur tous les réseaux que l'utilisateur rejoint. La solution de passerelle doit fournir des contrôles omniprésents et une gestion rationalisée, à l'échelle mondiale, tout en assurant des performances optimales pour les terminaux.

## Accès sécurisé à toutes les applications de l'entreprise

Une passerelle Web sécurisée dans le cloud protège les utilisateurs et les terminaux contre les programmes malveillants lorsqu'ils accèdent à l'Internet public. Mais cela ne représente qu'une pièce du casse-tête de la sécurité pour une entreprise.

Pour créer une approche globale de la sécurité pour l'ensemble de l'entreprise, les organisations doivent également protéger des acteurs malveillants les applications gérées par l'entreprise et lui appartenant, qu'elles se trouvent dans le centre de données de l'entreprise ou dans un environnement

**Les attaques d'hameçonnage contre les entreprises sont de plus en plus fréquentes**

**Attaques observées, de mars à octobre 2020**

**64 %**

**D'AUGMENTATION DES ATTAQUES CONTRE**

**LES ENTREPRISES**

**17 %**

**D'AUGMENTATION DES ATTAQUES CONTRE**

**LES CLIENTS**

Source : Passerelle Web sécurisée Akamai Enterprise Threat Protector

IaaS. Les outils de sécurité réseau traditionnels protègent le périmètre du réseau, mais en cas d'intrusion (par exemple, à travers le vol d'informations d'identification utilisateur ou l'instalation de programmes malveillants sur un terminal utilisateur), les attaquants peuvent se déplacer librement à l'intérieur du réseau.

Les entreprises ont besoin d'une passerelle Web sécurisée dans le cloud qui offre également une technologie Zero Trust Network Access (ZTNA) pour protéger les applications d'entreprise. Le ZTNA est un composant essentiel de l'adoption d'une sécurité Zero Trust, qui n'accorde accès qu'à certaines applications spécifiques aux utilisateurs (et non à des réseaux ou segments entiers), selon leur identité. La solution protège l'identité des utilisateurs grâce à l'intégration à la gestion des identités et des accès, à l'authentification multifactorielle et aux technologies d'authentification unique. En utilisant un outil ZTNA, les entreprises se libèrent des complications liées à la gestion sécurisée des terminaux, à la maintenance d'un réseau étendu et complexe ou à la connectivité à un réseau privé virtuel. Une fois correctement authentifiés, les utilisateurs n'ont accès qu'aux applications et aux données dont ils ont besoin, ce qui

réduit à zéro la surface d'attaque des applications et minimise le risque de mouvement latéral. Lorsque les entreprises évaluent une passerelle Web sécurisée dans le cloud, elles doivent prendre en compte les fonctionnalités du service ZTNA du fournisseur. Le service peut-il fournir un accès aux applications Web actuelles, ainsi qu'aux applications héritées non Web ? Le service peut-il s'intégrer au service du fournisseur d'identités existant de l'entreprise ? Prend-il en charge l'authentification multifactorielle ?

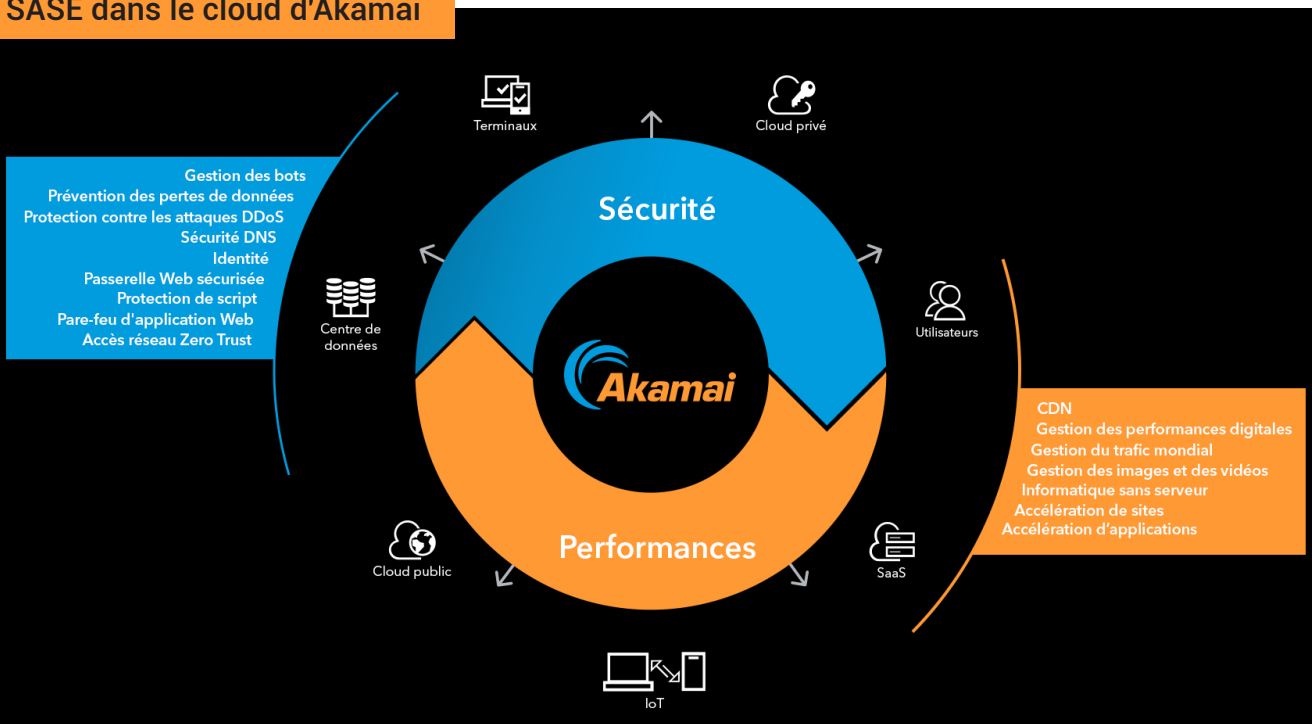
La passerelle Web sécurisée doit s'intégrer au service ZTNA et fonctionner de pair avec ce dernier, de façon à ce que si un terminal est compromis, il ne puisse pas accéder aux applications de l'entreprise. Les journaux d'une passerelle Web sécurisée peuvent s'élargir à d'autres signaux de menace pour fournir une image plus précise de la situation de sécurité d'un terminal. Par exemple, si le terminal fait appel à des serveurs de contrôle et de commande, la solution doit utiliser cela comme un signal pour limiter l'accès aux applications jusqu'à ce que le terminal soit réparé.

En ajoutant une passerelle Web sécurisée et des fonctionnalités ZTNA, les entreprises se tournent vers l'adoption d'une structure Secure Access Service Edge (SASE). SASE déplace la base de la sécurité des entreprises à distance des centres de données et équipements matériels inadaptés aux environnements professionnels et commerciaux hautement distribués d'aujourd'hui. SASE propose à la place des architectures traditionnelles un accès reposant sur des règles en fonction de l'identité de l'utilisateur et/ou du terminal. SASE fournit également une large gamme de contrôles de sécurité supplémentaires, y compris le Web Application Firewall (WAF), la sécurité des API, la gestion des bots et la protection contre le déni de service distribué pour les applications Web.

> **ZTNA améliore la flexibilité, l'agilité et l'évolutivité de l'accès aux applications, permettant ainsi aux entreprises du digital de se développer sans exposer directement les applications internes sur Internet, ce qui contribue à réduire le risque d'attaque.**
>
> — Gartner, Market Guide for Zero Trust Network Access, Steve Riley, Neil MacDonald, Lawrence Orans, 8 juin 2020

En outre, les contrôles de sécurité sont fournis sur la plateforme SASE, à un point de réseau Internet de l'utilisateur, afin de fournir un accès à faible latence aux utilisateurs, aux terminaux et aux services cloud, où qu'ils se trouvent.

## SASE dans le cloud d'Akamai



## Performances optimales

Bien que la sécurité soit primordiale, il ne faut pas qu'elle compromette l'expérience utilisateur en réduisant les performances. En plus de fournir une approche de défense en profondeur pour la sécurité, une passerelle Web sécurisée basée dans le cloud doit fournir les services ci-dessus sans introduire de latence.

Pour éviter toute latence, la passerelle Web sécurisée dans le cloud doit être déployée à l'échelle mondiale avec des points de présence à proximité de tous les endroits où se connectent les utilisateurs. Après tout, remplacer un type d'acheminement par un autre n'a pas beaucoup de sens.

La plateforme cloud doit également évoluer rapidement pour éviter d'affecter l'expérience utilisateur, même durant les pics de trafic. Cette capacité est particulièrement importante lorsqu'il s'agit d'inspecter le trafic HTTPS, qui augmente de façon exponentielle et qui, en fin de compte, représente près de 100 % de tout le trafic Web. Il est essentiel d'inspecter le trafic chiffré avec un impact minimal sur les utilisateurs finaux, car la grande majorité des programmes malveillants sont désormais envoyés via HTTPS. La plateforme doit également fournir une disponibilité de 100 % garantie par un accord de niveau de service (SLA).

> **Plus de la moitié des 81 % des entreprises ayant migré vers le cloud utilisent aujourd'hui Office 365.[8]**

**Intégration à Office 365 :** il est particulièrement important de garantir un niveau élevé de sécurité et de performances pour Microsoft Office 365, car il s'agit d'une suite essentielle à la productivité de nombreuses entreprises. Lors du déploiement d'une passerelle Web sécurisée dans le cloud, Office 365, comme de nombreuses autres applications SaaS courantes, ne fonctionne pas correctement lorsque les utilisateurs accèdent à ses applications via un proxy de transfert, qui effectue l'inspection TLS MITM.

Pour éviter de réduire les performances d'Office 365, il est essentiel que la passerelle Web

sécurisée dans le cloud soit fournie via une plateforme Edge mondiale qui puisse :

- Utiliser l'adresse IP source de la demande pour diriger celle-ci vers le centre de données Microsoft Office 365 le plus proche géographiquement, plutôt que vers des solutions DNS acheminées qui orienteraient la demande vers le centre de données le plus proche du résolveur DNS de l'entreprise. Par exemple, un utilisateur qui accède à Office 365 depuis Singapour et serait routé vers un serveur Office 365 à New York vivrait une très mauvaise expérience utilisateur.
- S'assurer que les emplacements des serveurs de passerelle Web sécurisée sont situés à proximité des centres de données Microsoft Office 365 et que, dans l'idéal, ces serveurs et centres de données sont interconnectés.
- Fournir un paramètre d'optimisation du trafic Office 365 en un clic qui utilise une liste de domaines Office 365 et d'adresses IP publiée et mise à jour par Microsoft. Les demandes adressées à ces domaines doivent être envoyées directement aux serveurs Office 365 conformément aux recommandations de Microsoft, ce qui permet de gagner du temps et d'économiser des efforts en éliminant le besoin de mettre à jour manuellement les pare-feu et autres produits de sécurité lorsque Microsoft ajoute de nouveaux domaines ou adresses IP.

## Déplacer la sécurité vers la bordure de l'Internet

Avec le développement rapide du télétravail, les télétravailleurs sont plus exposés à des cyberattaques de plus en plus fréquentes et sévères. Les meilleures solutions de passerelle Web sécurisée basée dans le cloud auront pour but exclusif de répondre à ces exigences de sécurité actuelles en proposant une fonctionnalité de défense en profondeur éprouvée. Elles permettront également de mettre en place des modèles de sécurité d'entreprise récents tels que Zero Trust et SASE en sécurisant l'accès à Internet pour tous les utilisateurs, où qu'ils se trouvent.

Une passerelle Web sécurisée complète dans le cloud doit évaluer toutes les demandes DNS et URL, fournir plusieurs techniques d'analyse de la charge utile, gérer l'hameçonnage « zero day », inspecter le trafic chiffré, intégrer la prévention des pertes de données, identifier et gérer le Shadow IT, et fournir une protection pour tous les terminaux où qu'ils se trouvent, tout en offrant un haut niveau de performance et en s'intégrant aux technologies de sécurité des applications d'entreprise. Avec une telle solution, les entreprises peuvent simplifier la sécurité, éliminer les coûts de l'acheminement du trafic, améliorer l'efficacité de l'équipe en charge de la sécurité et appliquer des stratégies de sécurité cohérentes.

## Découvrez plus en détail Secure Internet Access, la passerelle Web sécurisée dans le cloud d'Akamai et essayez-la gratuitement sur akamai.com.


1. https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2
2. https://www.helpnetsecurity.com/2020/09/02/phishing-attacks-pandemic/
3. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf
4. https://blogs.gartner.com/david_cappuccio/2018/07/26/the-data-center-is-dead/
5. https://www.brinknews.com/a-global-shortage-of-cybersecurity-professionals-leaves-businesses-at-risk/
6. https://news.sophos.com/en-us/2020/02/18/nearly-a-quarter-of-malware-now-communicates-using-tls/
7. https://www.mobolize.com/2020/10/29/mobolize-announces-technology-partnership-with-akamai-to-enable-security-on-mobile-devices/
8. https://blog.goptg.com/microsoft-office-365-statistics#:~:text=According%20to%20Bitglass%2C%20usage%20of,the%20shift%20to%20cloud%20services