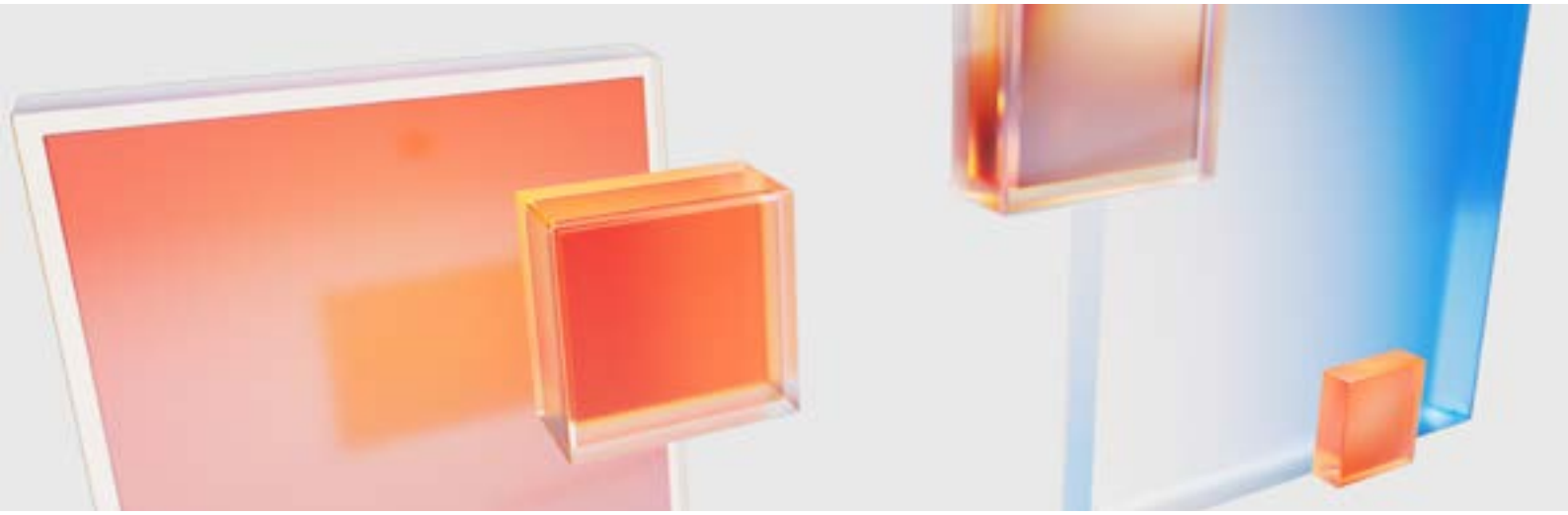
SONICWALL



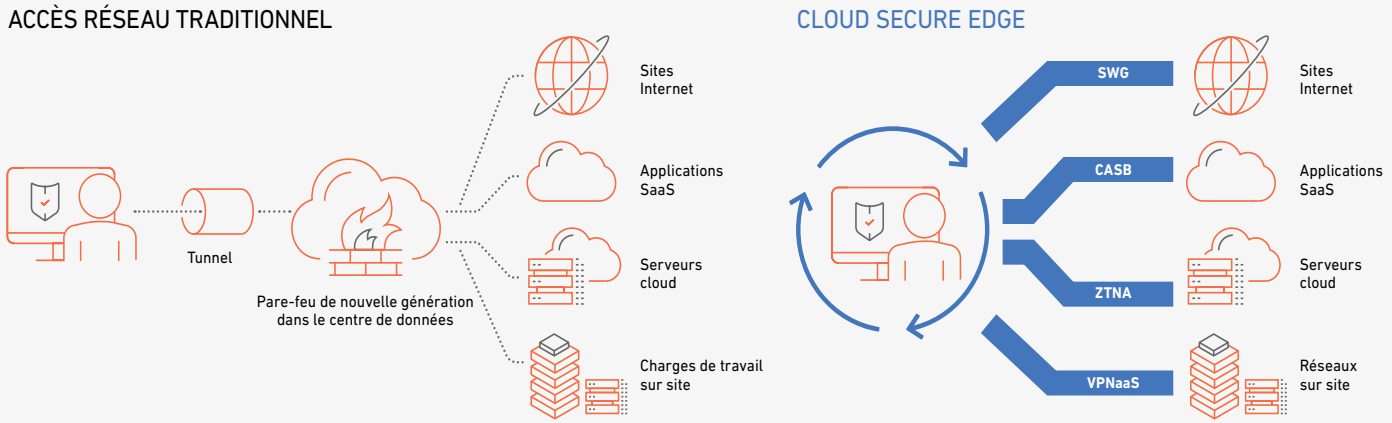
Améliorer la sécurité et les résultats de l'entreprise

Le défi

Alors que les entreprises transfèrent de plus en plus leurs applications, leurs ressources et leurs données vers des environnements cloud, le périmètre de sécurité traditionnel devient obsolète. Le passage au télétravail et l'essor de l'informatique distribuée et du cloud computing ont créé une nouvelle surface d'attaque qu'il est difficile de protéger avec les solutions traditionnelles de sécurité du périmètre. Les environnements cloud et les fournisseurs de solutions SaaS (Software-as-a-Service) s'appuient tous sur des méthodes d'authentification et d'autorisation différentes, ce qui compromet la sécurité et la convivialité. Pour relever ce défi, une nouvelle approche de la sécurité et de l'accès est nécessaire, et cette approche est le SSE (Security Services Edge) moderne.

La plateforme Cloud Secure Edge Security étend notre exceptionnelle solution ZTNA (Zero Trust Network Access) en fournissant un SSE (Security Services Edge) centré sur le terminal qui sécurise l'accès aux applications et aux ressources depuis n'importe où, tout en autonomisant le personnel moderne.

Dans ce livre blanc, nous allons détailler notre approche moderne du SSE, notamment son architecture, ses avantages et la façon dont il peut aider les entreprises à améliorer leur stratégie de sécurité face à l'évolution rapide du paysage des menaces. À la fin de ce livre blanc, vous aurez une vision claire de la manière dont le SSE centré sur le terminal de Cloud Secure Edge Security aide les entreprises à se protéger contre les cybermenaces modernes.



WHITE PAPER

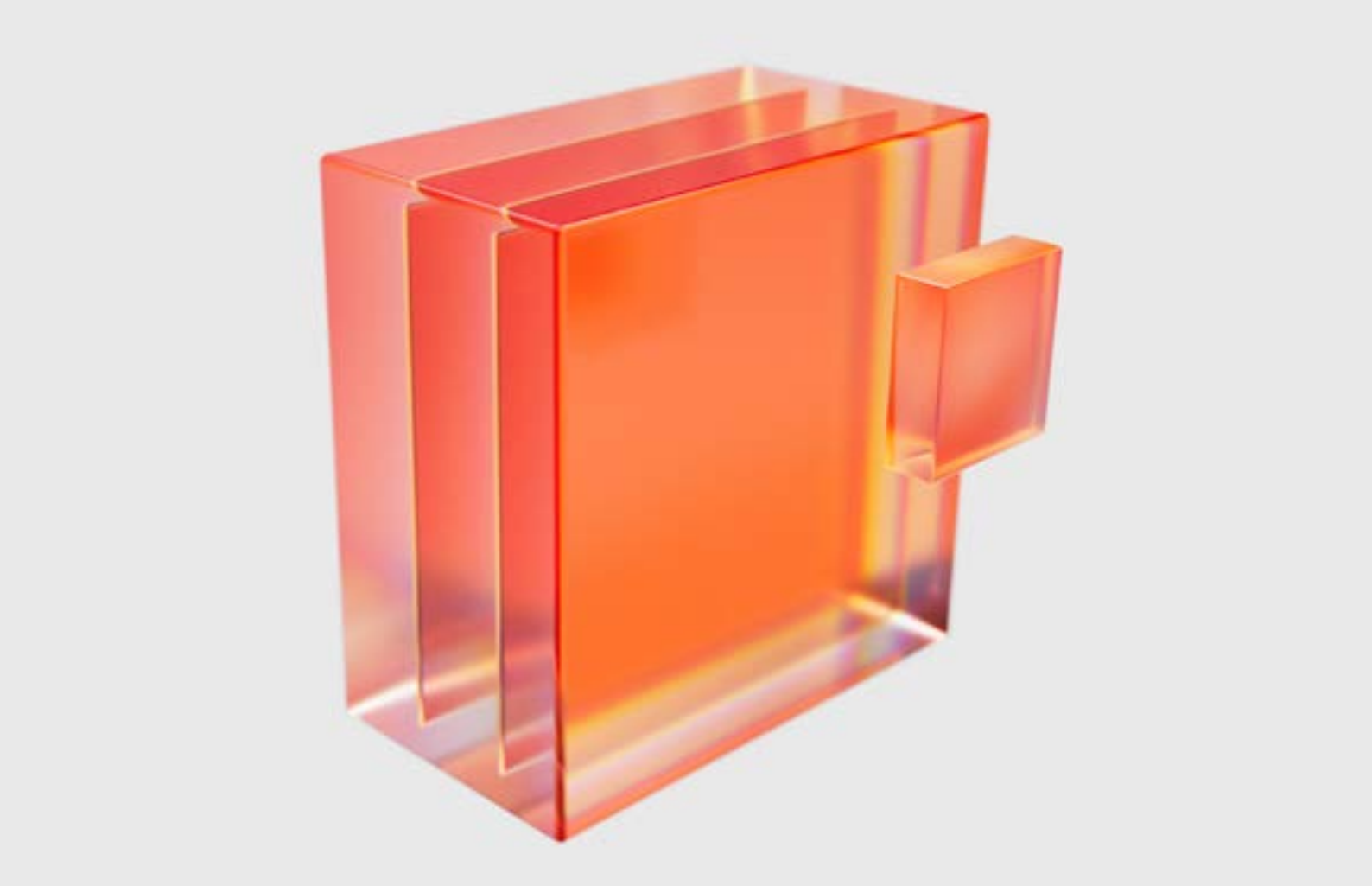
Contexte

Les entreprises ont adopté des approches traditionnelles pour sécuriser le périmètre de leur réseau. Elles ont également fait confiance aux fournisseurs de SaaS pour assurer un minimum de sécurité. Cela a eu pour conséquence de compromettre la sécurité et de rendre l'expérience utilisateur insatisfaisante.

Bien qu'il existe d'autres fournisseurs sur le marché qui promettent de résoudre ces problèmes, ceux-ci s'appuient généralement sur des produits qui reconditionnent des technologies « old school », comme des pare-feux et des proxies de périphérie qui ont été virtualisés, placés dans le cloud et vendus comme un nouveau service. Non seulement cette approche n'est pas évolutive, mais elle se fonde également sur l'assemblage de tunnels, ce qui se traduit par des performances médiocres et une latence accrue. En outre, cette approche exige que les données confidentielles de l'entreprise soient déchiffrées, inspectées, puis rechiffrées par le fournisseur avant d'être envoyées à leur destination finale. En plus de prendre du temps, ce qui nuit une nouvelle fois aux performances, cette opération a d'énormes répercussions sur la confidentialité et la souveraineté des données.

Les utilisateurs finaux et l'entreprise ne sont pas mieux lotis avec cette approche. Pour bénéficier d'une connectivité et d'une sécurité de base, ils doivent penser à se connecter avec l'agent approprié pour chaque ressource. Du point de vue de la sécurité, cette complexité incite souvent les utilisateurs finaux à contourner l'agent fourni, mettant ainsi l'entreprise en danger.

Fort heureusement, Cloud Secure Edge Security est un partenaire de confiance qui comprend combien il est difficile de vivre avec des produits hérités, et qui s'enorgueillit de ne pas avoir les lacunes techniques des approches médiocres du SSE.



L'approche de Cloud Secure Edge

La solution moderne de Cloud Secure Edge a été élaborée en pensant à la facilité de déploiement et d'utilisation. Intégralement développée sur la base de méthodes et de technologies modernes, et non à partir d'un ancien code virtualisé pour être exécuté dans le cloud, elle offre des performances exceptionnelles.

Notre approche centrée sur l'appareil est aussi largement supérieure aux anciens modèles concurrents. Les appareils modernes ont la puissance de traitement nécessaire pour activer des fonctionnalités locales qui améliorent l'expérience de l'utilisateur final, minimisent la nécessité d'envoyer le trafic pour inspection et permettent véritablement de sécuriser le personnel nomade.

Les avantages d'une approche centrée sur le terminal

- **Contrôles granulaires :** la sécurité centrée sur le terminal permet un contrôle granulaire sur les paramètres et les règles de sécurité pour chaque utilisateur, terminal et ressource, garantissant ainsi leur protection contre les menaces potentielles.
- **Visibilité accrue :** l'appareil, source de trafic et d'interactions avec les ressources, est le meilleur moyen de connaître leur destination et leur comportement une fois qu'ils ont accédé aux ressources.
- **Conformité améliorée :** la sécurité centrée sur le terminal aide les entreprises à répondre aux exigences réglementaires et de conformité en veillant à ce que les terminaux soient configurés conformément aux normes et bonnes pratiques du secteur, tout en appliquant des stratégies d'utilisation acceptables.
- **Protection contre les menaces avancées :** la sécurité centrée sur le terminal permet de se protéger contre les menaces évoluées, comme les attaques zero-day et les menaces persistantes avancées, en offrant des fonctionnalités de sécurité renforcées et une surveillance continue, et en bloquant les tentatives de trafic sortant, même lorsque les utilisateurs cliquent sur des liens sur lesquels ils ne devraient pas cliquer.
- **Expérience utilisateur optimisée :** les approches centrées sur le terminal améliorent l'expérience utilisateur en fournissant un accès sécurisé aux ressources de l'entreprise partout et depuis n'importe quel appareil, avec un minimum d'interaction avec le client ou l'agent. L'accès pratique et la sécurité permanente sont assurés même lorsque l'utilisateur n'est pas connecté à l'agent.
- **Économique :** la sécurité centrée sur le terminal est plus rentable que les approches de sécurité centrées sur le réseau traditionnelles, car elle limite le recours à des appliances de sécurité coûteuses, réduit les frais de trafic des fournisseurs de services cloud (CSP) et améliore la stratégie de sécurité globale.

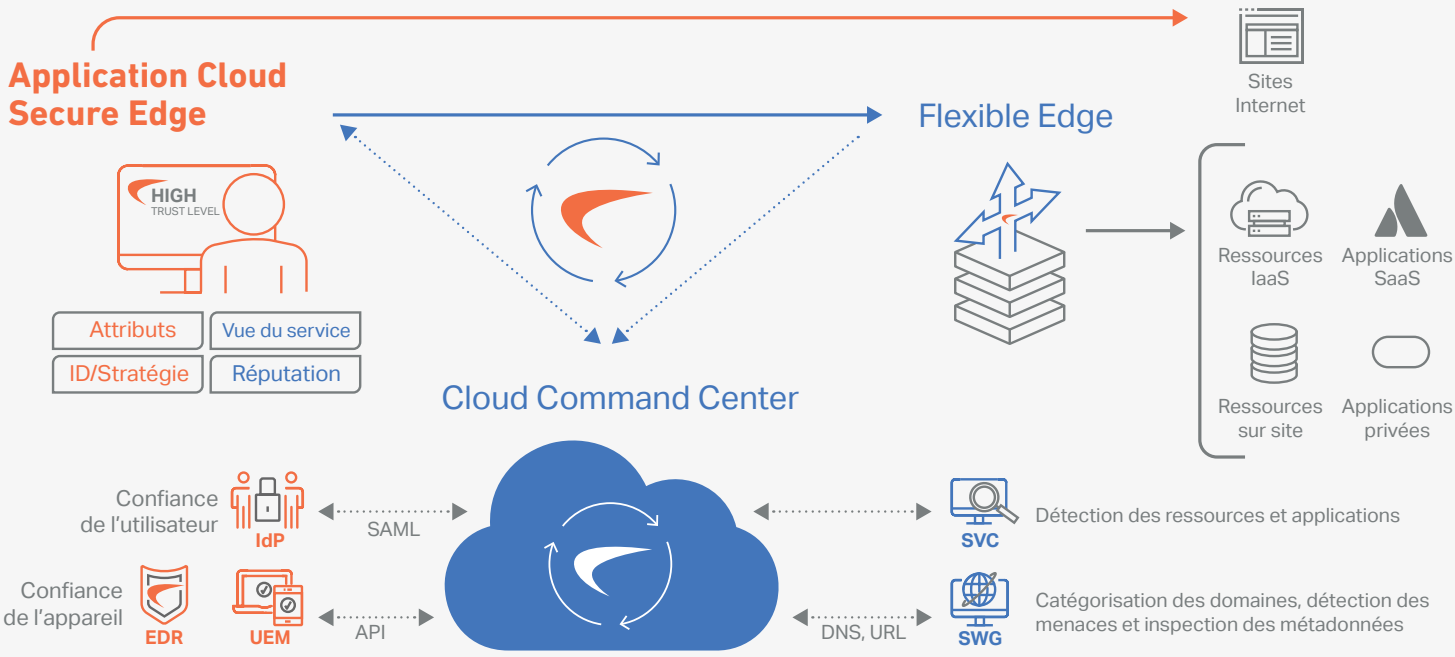
L'approche de Cloud Secure Edge, qui n'exige pas que le trafic soit acheminé vers notre cloud pour être inspecté, se traduit par une disponibilité et une stabilité accrues. De nombreux clients se sont adressés à nous après avoir supporté des pannes non planifiées entraînant des pertes de revenus, une augmentation des recours au support technique et le mécontentement des cadres et des employés.

La plateforme Cloud Secure Edge Security

La plateforme Cloud Secure Edge Security connecte en toute sécurité les utilisateurs aux applications, aux ressources et à l'infrastructure tout en les protégeant contre les menaces Internet. Les risques et la sécurité sont continuellement évalués et appliqués en temps réel dans les environnements hybrides, multicloud et SaaS.

Fonctionnalités de la solution Cloud Secure Edge :

- ZTNA (Zero Trust Network Access) : accès aux applications et à l'infrastructure. Un accès simple de moindres privilèges aux applications et aux services sur une infrastructure hybride et multicloud, tirant parti de vos investissements existants en outils d'identité et de sécurité d'entreprise.
- VPNaaS (Virtual Private Network as a Service) : accès au réseau. Un accès aux réseaux moderne, performant et basé sur les tunnels, incorporant des contrôles Zero Trust accrus, comme l'autorisation continue et la confiance de l'appareil.
- Courtier en sécurité d'accès au cloud (CASB) : sécurité de l'accès aux applications SaaS. Une sécurité multicouche pour une gestion facile des contrôles sur qui, utilisant quels appareils spécifiques, peut accéder à vos applications SaaS.



Principaux composants de la plateforme Cloud Secure Edge :

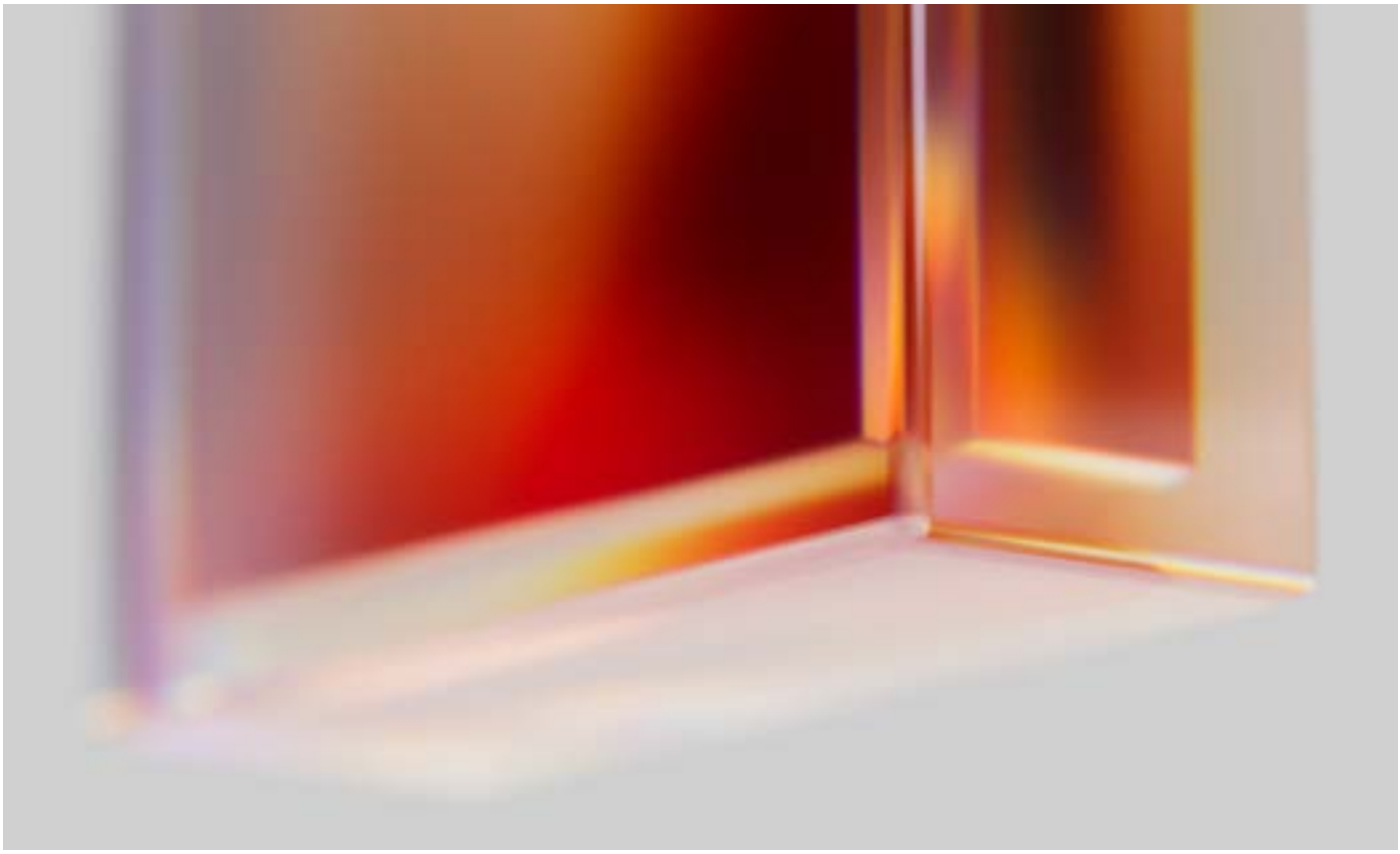
- Passerelle Web sécurisée (SWG) : protection contre les menaces Internet. Protège les utilisateurs contre le phishing, les sites Web malveillants et les ransomwares. Les entreprises peuvent également bloquer des catégories spécifiques de sites Web, comme les jeux d'argent et la pornographie.
- Cloud Command Center : le tableau de bord centralisé et le moteur de règles offrent un accès de moindres privilèges aux applications et ressources sensibles de l'entreprise.
- Application Cloud Secure Edge : algorithmes de calcul des mesures de risque en temps réel, continuellement mis à jour pour quantifier et noter le contexte et le comportement de l'utilisateur/appareil.
- Flexible Edge : un proxy d'accès multicloud basé sur l'identité qui dissimule en toute sécurité les applications et serveurs cloud des attaques malveillantes ou d'une exposition involontaire, et qui permet également de faire respecter en temps réel l'accessibilité en cas d'infraction à la règle.
- Flux de menaces : ensemble d'informations directes et tierces servant à étudier les flux de trafic et les sites Web existants et à prendre des décisions en temps réel sur les menaces et les risques.
- Intégrations : des méthodes standard comme les API, SAML et OIDC sont utilisées pour faciliter le déploiement, la gestion et la sécurisation de notre solution de bout en bout. Ces intégrations partagent également les renseignements, tirant parti des investissements existants dans le réseau et la sécurité.

Principaux avantages

La plateforme Cloud Secure Edge Security offre des avantages significatifs à la fois pour la sécurité de l'organisation et pour l'expérience utilisateur.

Fonctionnalités de Cloud Secure Edge	Avantage pour le client
Plateforme d'administration et application utilisateur uniques	**Une approche unifiée pour l'accès et la sécurité** Méthode unique d'authentification et d'autorisation Création des règles centralisée, où que se trouve l'utilisateur final ou la ressource Application unique assurant l'accès et la sécurité Visibilité de tous les utilisateurs, appareils et ressources
Déploiement d'un modèle de confiance distribué dans n'importe quel environnement d'entreprise	**Renforcement de la sécurité des ressources internes essentielles** Invisibilité des applications pour les appareils non fiables Accès restreint des utilisateurs au réseau Contrôles unifiés pour les communications HTTP, SSH, RDP et interservices
Trafic Internet sécurisé	**Respect de la conformité et réduction des menaces Internet** Application de stratégies d'utilisation acceptables Blocage automatique des malwares et des tentatives de phishing Accès granulaire aux URL sans blocage de sites entiers
Tunnels de service	**Accès par tunnel sans accès complet au réseau** Solution unique avec connectivité par proxy et tunnel Fourniture de tunnels chiffrés permettant de doubler le chiffrement du trafic ou d'ajouter un chiffrement aux anciennes applications non sécurisées Split-tunneling basé sur le domaine permettant d'établir rapidement une liste blanche/noire du trafic
Utilisation d'un cadre de confiance basé sur le score pour l'autorisation continue	**Gestion des contrôles en fonction du contexte et du comportement de l'utilisateur** Accès direct et rapide aux applications pour les utilisateurs Création rapide de règles à l'aide de modèles prédéfinis Intégration des signaux provenant des outils UEBA et EDR
Architecture conçue pour les environnements hybrides et multicloud	**Simplification des opérations du réseau** Utilisation des fonctionnalités d'automatisation et natives CSP Segmentation de l'application sans segmentation complexe du réseau Connecteurs conteneurisés portables pouvant être déployés n'importe où

Fonctionnalités de Cloud Secure Edge	Avantage pour le client
Possibilité pour les clients de rester propriétaires de leur plan de données	**Maintien de la sécurité et de la conformité dans les clouds hybrides** Cohérence des règles entre les environnements IaaS, SaaS et sur site Protection des clés et droits d'administration
Authentification avancée et reconnaissance de l'appareil pour les applications SaaS et existantes	**Cohérence de l'ensemble des ressources** Activation de l'authentification avancée des applications SaaS Possibilité d'authentification unique et de reconnaissance de l'appareil pour les applications existantes sans modification du code Visibilité sur la façon dont les utilisateurs accèdent aux applications cloud Application de restrictions sur l'adresse IP source pour les applications SaaS
Utilisation de protocoles de sécurité standard : TLS mutuel, SAML et OpenID Connect	**Accélération de l'adoption à l'échelle de l'entreprise** Prévention de l'enfermement propriétaire Évolutivité pour Kubernetes et les microservices
Détection et publication de serveurs et de services	**Possibilité de voir l'inconnu et de réagir rapidement** Détection de serveurs, services et applications sur site, dans le cloud et SaaS Détection des ressources Shadow IT déployées et utilisées au sein de l'entreprise Publication (ou blocage) rapide de ces ressources de manière granulaire basée sur le workflow



SONICWALL

En quoi Cloud Secure Edge se différencie

Partout dans le monde, des entreprises de toutes tailles et de tous secteurs font confiance à la plateforme Cloud Secure Edge Security pour ces différences précieuses uniques :

Approche centrée sur le terminal

- La simplicité du réseau et les performances supérieures sont obtenues en limitant les goulets d'étranglement traditionnels, en éliminant les sauts inutiles et en évitant les concentrateurs.
- La puissance de calcul des appareils modernes permet de mettre en place un routage fondé sur le risque. Les décisions prises à la source du trafic réduisent la consommation de bande passante, envoyant le trafic directement à la destination. Il n'est pas nécessaire de tout envoyer dans un cloud tiers en amont des appareils.
- L'intégration intelligence de l'application sur l'appareil, plutôt que dans le cloud, permet de préserver la confidentialité. La portabilité d'une plateforme complète signifie également la souveraineté totale des données.

Sécurité avancée

- L'autorisation continue fondée sur des règles de contrôle d'accès granulaire basé sur la confiance (TBAC) permet d'établir la confiance de l'appareil en temps réel.
- Seul Cloud Secure Edge Security offre un accès Zero Trust qui s'étend aux environnements hybrides, multicloud et SaaS.
- Une sécurité permanente contre les menaces et les malwares qui ne nécessite pas de se connecter à un agent.
- Double chiffrement des protocoles de transport sécurisés comme HTTPS et SSL.
- Authentification multifacteur basée sur l'utilisateur et l'appareil.
- Renforcement des connecteurs périphériques qui autorisent uniquement l'ouverture d'une session sortante.
- Sessions basées sur un certificat client X.509 éphémère dans le handshake TLS.
- Catégorisation de domaine en temps réel pour le DNS et le filtrage de contenu.
- Validation de l'adresse IP source pour l'accès aux applications SaaS.

« Le surcroît de sécurité dont nous bénéficions avec Cloud Secure Edge est considérable. En comparaison avec notre VPN, c'est le jour et la nuit. »

— JONATHAN JAFFE
LEMONADE CISO

Architecture flexible

- Flexible Edge, l'architecture en maillage de Cloud Secure Edge étend les contrôles de sécurité aux ressources distribuées, couvrant tous les environnements et protocoles. L'approche cloud native exploite l'Internet public sans nécessiter de tunnels réseau ou de cloud MitM, ce qui permet d'obtenir une solution hautement performante et évolutive qui ne met pas en péril la confidentialité ou la souveraineté des données. Seul Cloud Secure Edge prend en charge de manière flexible le cloud IaaS (Global Edge) tout en offrant aux entreprises la possibilité d'héberger elles-mêmes leur périphérie (Private Edge).

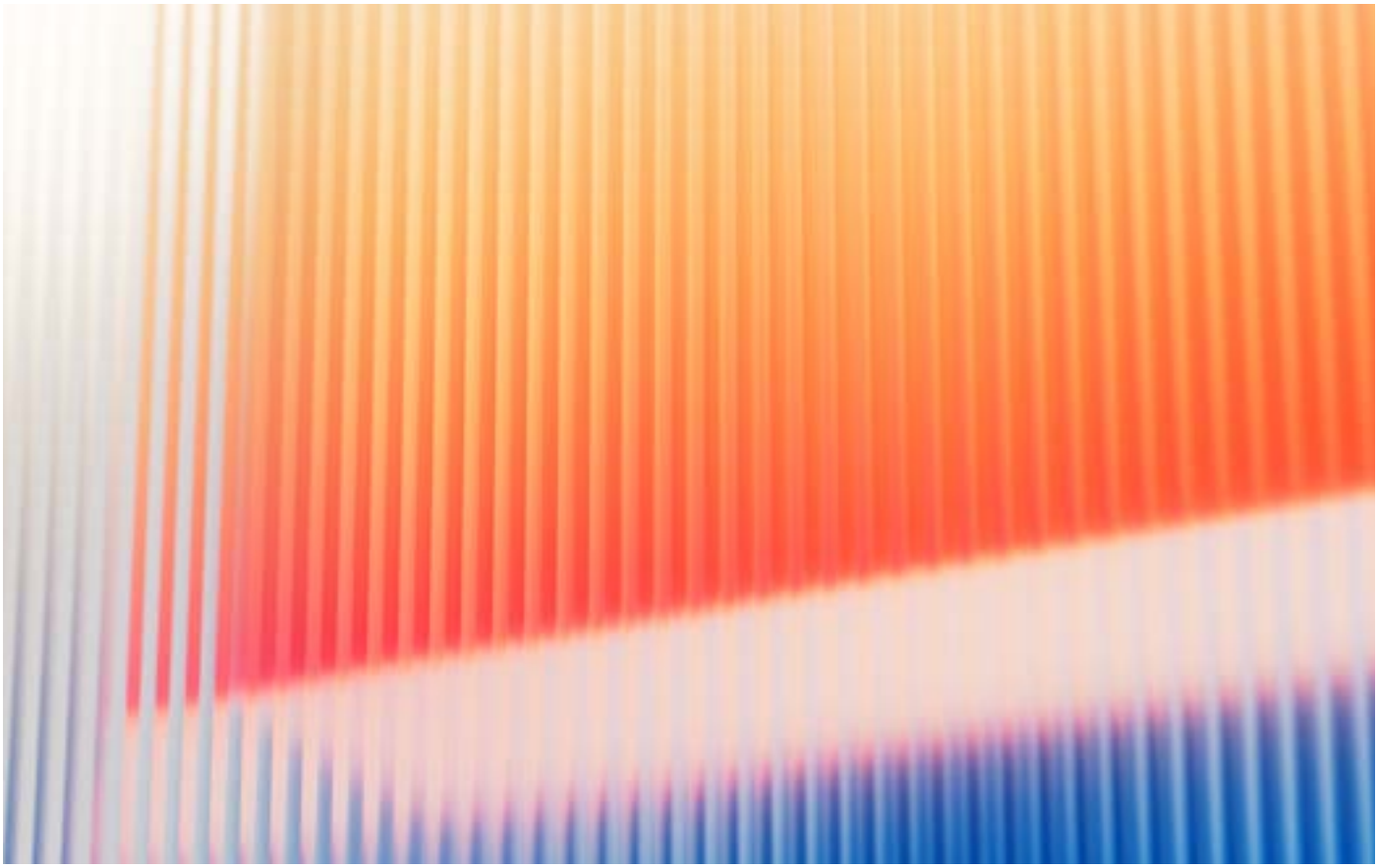
Facilité de déploiement et d'utilisation

- Déploiement en 15 minutes maximum
- Accès en un clic à l'infrastructure et aux applications. Cloud Secure Edge s'intègre aux environnements IaaS et PaaS des clients, fournissant un accès en un clic aux applications et aux ressources, notamment les serveurs SSH/RDP, VNC, Kubernetes et les bases de données. Même les applications SaaS sont protégées. L'accès de moindres privilèges permet un accès différencié pour les ETP et les tiers, facile à déployer, administrer et auditer.
- Le tunnel de service facilite la transition des anciens VPN vers le Zero Trust. Il offre un accès haute performance aux réseaux par le biais de tunnels et repose sur une base WireGuard moderne avec une autorisation continue et une confiance de l'appareil améliorées.
- Accès en un clic rapide, facile, sécurisé et sans mot de passe aux sites Web hébergés, à l'infrastructure IaaS et aux applications SaaS. Même les centres de données complexes et les environnements IaaS sont un jeu d'enfant.
- Service Catalog simplifie l'accès aux environnements Windows, Linux et Kubernetes, y compris les outils de développement comme GitLab, Jira et Jupyter.
- Les fonctions automatisées de détection et de publication permettent aux administrateurs d'inventorier et de mettre rapidement à la disposition des utilisateurs des applications éphémères et des ressources IaaS.
- Le niveau de confiance visible par l'utilisateur permet de remédier soi-même aux problèmes liés à la stratégie de l'appareil.
- Prise en charge du déploiement sans client.
- Prise en charge de Terraform pour le déploiement automatisé de stratégies de sécurité Zero Trust. C'est ce que l'on appelle le « zero trust as code ».

Conclusion

Cloud Secure Edge Security a créé une plateforme fournissant des fonctionnalités SSE (Security Services Edge) modernes, conçues dès le départ pour le cloud. Notre plateforme offre d'exceptionnelles solutions VPNaaS, ZTNA, CASB et SWG, sans sacrifier la satisfaction des utilisateurs et des administrateurs ni compromettre la sécurité. Notre approche centrée sur le terminal est plébiscitée par les clients pour sa simplicité et ses performances supérieures.

La plateforme Cloud Secure Edge Security est la seule à fournir aux équipes tous les outils nécessaires pour sécuriser l'accès aux applications et aux ressources depuis n'importe où, tout en autonomisant votre personnel moderne, aujourd'hui et demain.



À propos de SonicWall

Forte de plus de 30 années d'expertise, SonicWall est une entreprise pionnière dans le domaine de la cybersécurité qui porte une attention constante à ses partenaires. De par sa capacité à créer, faire évoluer et gérer en temps réel la sécurité dans le cloud ainsi que dans les environnements hybrides et traditionnels, SonicWall est en mesure de fournir rapidement et économiquement des solutions de sécurité sur mesure à toute entreprise dans le monde entier. En s'appuyant sur les données de son propre centre de recherche sur les menaces, SonicWall offre une protection sans faille contre les cyberattaques les plus évasives et fournit des renseignements exploitables sur les menaces à ses partenaires, à ses clients et à la communauté de la cybersécurité.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Consultez notre site Internet pour de plus amples informations.
www.sonicwall.com