Data Sheet

Plateforme Censornet pour MSP

Liberté. Visibilité. Protection. Le service de sécurité unifiée de Censornet est conçu pour les MSP. Il permet aux partenaires de sécuriser de manière efficace et rentable la surface d'attaque de leurs clients en intégrant la sécurité du courrier électronique, du Web et des applications Cloud (CASB), de l'identité (IDaaS), du MFA et des formations à la sensibilisation à la sécurité.

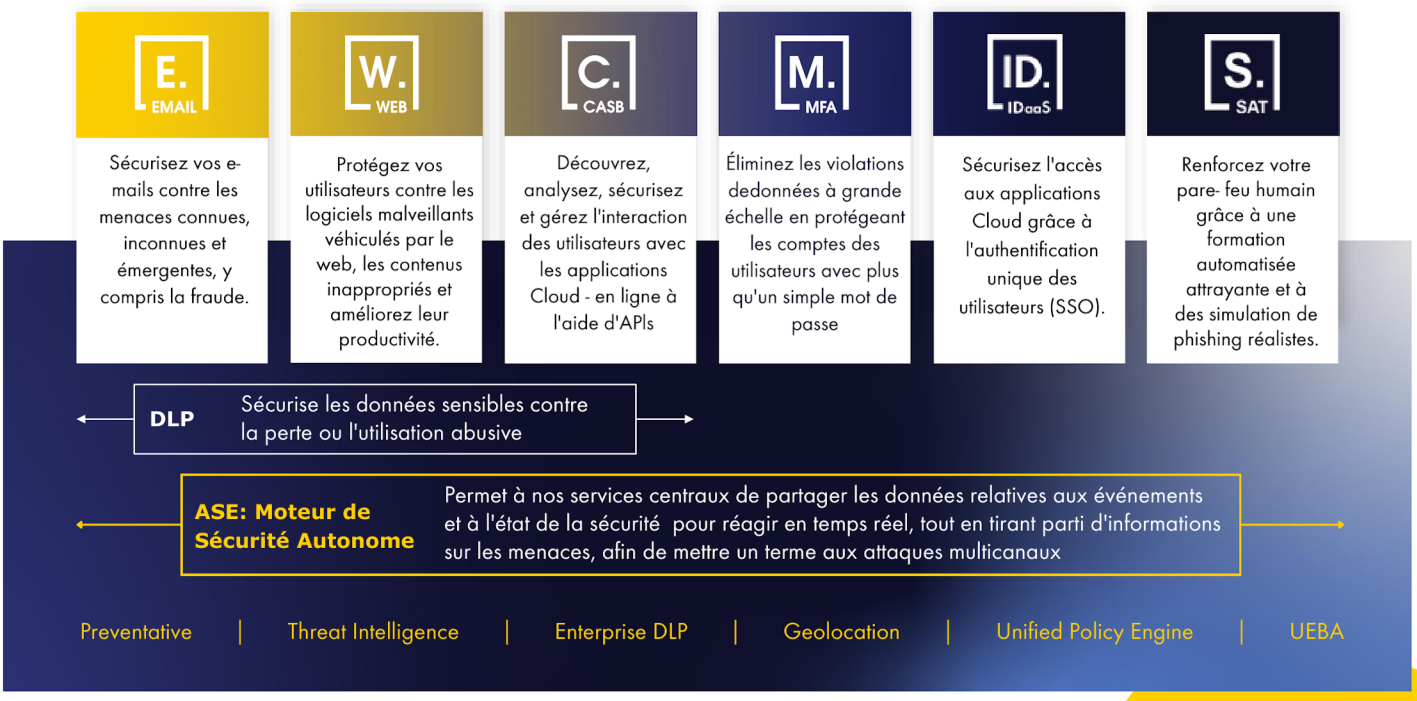
La plateforme Censornet fournit de multiples capacités de sécurité, simplifiant la sécurité, son architecture spécifique permet aux MSP de gérer leurs clients de manière simple et rentable.

En utilisant la plateforme Censornet, les MSP s'éloignent de l'approche plus coûteuse consistant à gérer des solutions cybernétiques différentes. Les MSP sont en mesure de déployer et de gérer efficacement les leviers de sécurité de base pour plusieurs clients.

Avec la plateforme Censornet, les utilisateurs ont la liberté d'accéder aux applications et aux données dont ils ont besoin, quel que soit l'appareil ou l'endroit, tout en assurant la visibilité et la protection de tous.

CENSORNET POUR LES CLIENTS

- Gestion de plusieurs modules de sécurité au sein d'une plateforme unique.
- Les modules intégrés partagent des informations sur les menaces pour stopper les attaques transcanal.
- Rapports complets et automatisés pour tous les modules.
- Déploiement simple et rapide.
- Simplicité et efficacité de la mise en œuvre des politiques de sécurité.
- Réduction des coûts de gestion et de licence.
- Fonctionnalités d'identification à travers le web et les CASB incluses.
- Support de classe mondiale.
- Gestion de plusieurs modules de sécurité au sein d'une plateforme unique.
- Réduction des coûts de déploiement et de gestion.
- Gestion simplifiée des utilisateurs grâce à un modèle de tarification MSP par paliers.
- Architecture multi-niveaux et multi-tenant.
- Marque blanche et co-branding.
- Modèles de politiques et architecture optimisés pour un déploiement rapide.
- intégration marketplace via l'APIs REST.
- Support de classe mondiale.

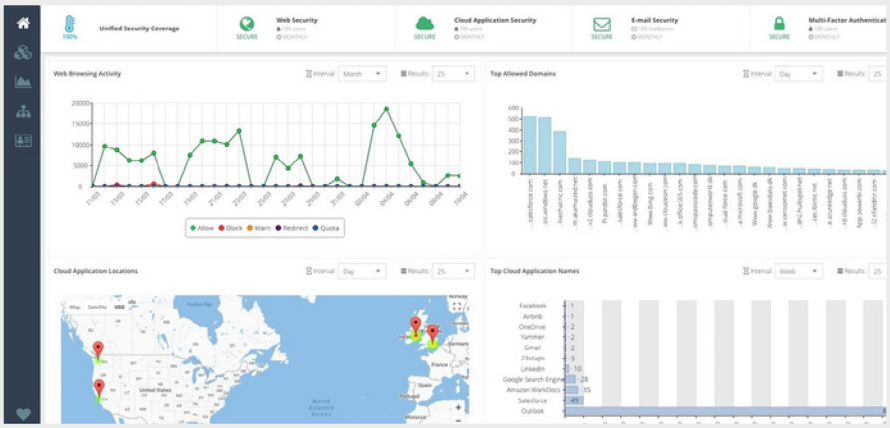


DASHBOARDS & REPORTING

La plateforme Censornet offre une visualisation des données et des rapports riches pour tous les services Censornet sur un ensemble étendu de critères.

Chaque administrateur dispose de son propre tableau de bord avec des graphiques et des widgets spécifiques aux services sous licence. De nombreux rapports standard sont incluspour chaque service dans la section "Analytics" du portail.

Des analyses et des rapports détaillés sont disponibles par nom, utilisateur, appareil (nom d'hôte et adresse MAC), catégorie d'URL, catégorie web, classe d'application Cloud, nom d'application Cloud, action d'application Cloud, mot-clé (par exemple, nom de fichier, commentaire, détails de connexion), nom de la politique,niveau de risque, direction du courrier électronique, état de livraison (livré, spam, virus), résultat (bloquerou autoriser).



Pour optimiser le stockage et la vitesse des rapports, les journaux sont archivés en fonction des périodes de rétention des services individuels. Les périodes standards sont de 90 jours pour Email et WebSecurity et d'un an pour Cloud App Security (CASB) et MFA. Les archives peuvent être téléchargées à la demande au format CSV.

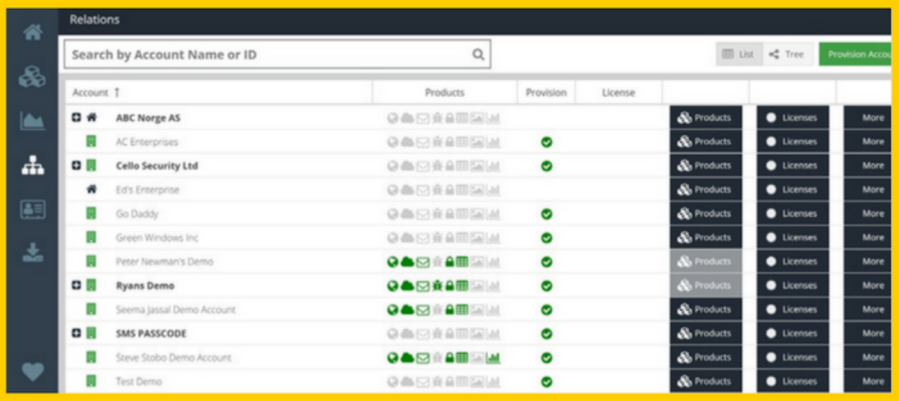
Que les données d'audit soient nécessaires uniquement pour la visibilité ou pour une attestation plus formelle de la conformité; avec les politiques internes ou les normes, réglementations et législations externes,la plateforme Censornet fournira les rapports nécessaires.

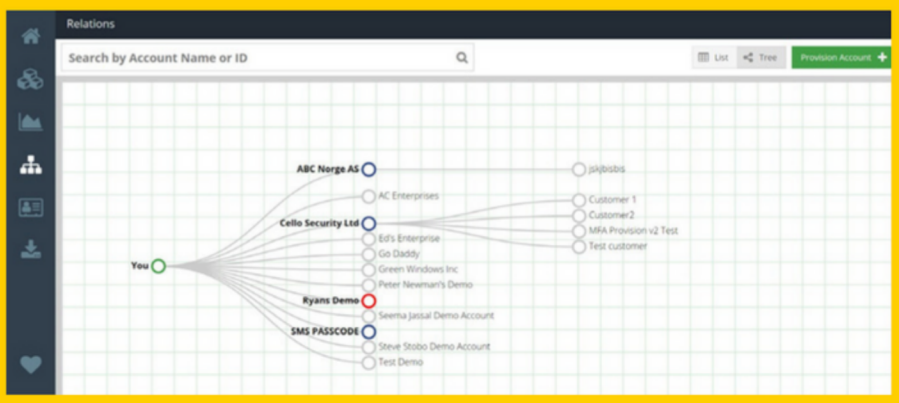
OUTILS POUR LES PARTENAIRES

De puissants outils de la plateforme Censornet fournissent aux MSP des ressources en libre-service pour gérer les comptes.

Les fonctionnalités comprennent le provisionnementde nouveaux comptes, des politiques modélisées, lagestion des licences, ainsi que des rapports sur l'utilisation des services et l'étatdes licences.

Lorsqu'il y a plusieurs niveaux dans la hiérarchie du compte,il est également possible de choisir si les outils partenaires sont visibles dans le compte.

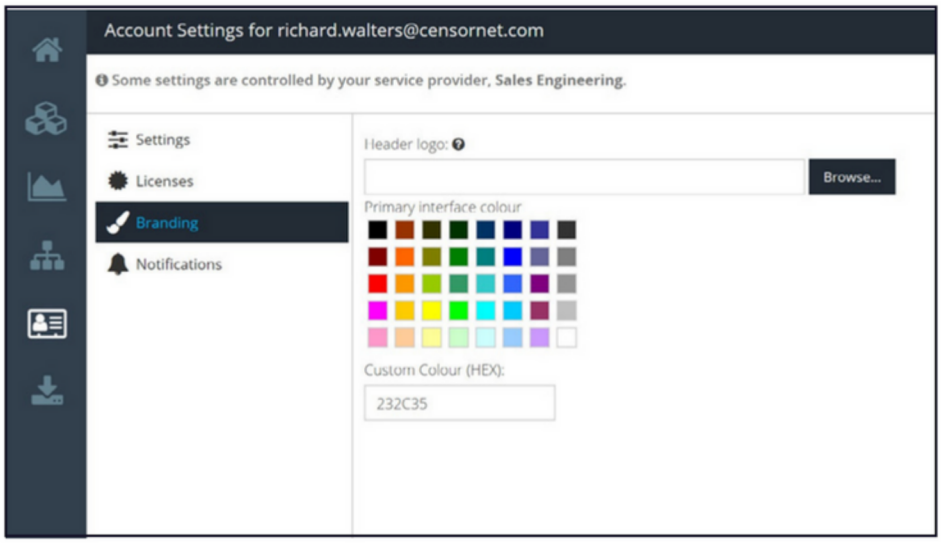




MULTI-TENANTET MULTI-NIVEAUX

La plateforme Censornet est basée à 100% sur le Cloud et en multi-tenant, fournie par des centres de données situés aux États-Unis, au Royaume-Uni, aux Émirats arabes unis et en Europe continentale. Pour répondre aux problèmes de résidence des données, la région est sélectionnée au moment de l'ouverture du compte. Les données des clients sont isolées à l'aide de schémas de base de données distincts et de plusieurs niveaux de cryptage - chaque locataire dispose d'une clé unique garantissant l'isolement de ses données et l'accès à la plateforme Censornet se fait par HTTPS.

Censornet permet aux MSP de mettre facilement la plateforme en marque blanche et, à l'aide d'une API d'intégrer tout élément disponible sur le portail dans leurs propres applications.



La possibilité de créer des "child account" au sein du portail est une fonctionnalité qui rend la plateforme Censornet idéale pour les multinationales, les organisations multi-marques, ou les MSP. La marque, qui comprend le logo et la couleur de l'interface, peut être appliquée à chaque compte pour les différentes unités commerciales, les partenaires ou les clients. Chaque compte dispose d'un ensemble de règles distinctes pour répondre avec souplesse aux exigences locales en matière de conformité législative et réglementaire, en tenant compte des différences dans les lois sur la protection des données et de la vie privée.

IDENTITEINTEGREE

Il existe un magasin d'identité unique au sein de la plateforme qui est partagé entre la sécurité des emails, la sécurité web, la sécurité des applications cloud (CASB), l'identité en tant que service (IDaaS) et l'authentification multifactorielle (MFA).

Pour les organisations disposant de Microsoft® Active Directory (AD), il existe des options pour Local Sync ou Cloud Sync. La synchronisation locale utilise un service de connexion AD installé localement (agent) qui pousse les éléments vers le Cloud Censornet.

La synchronisation dans le Cloud utilise une connexion LDAP ou LDAPS pour extraire les éléments. La synchronisation locale présente l'avantage de ne pas nécessiter de modification des règles du pare-feu. Les deux méthodes nécessitent un compte de service en lecture seule dans l'AD.

Pour les organisations qui ne disposent pas d'AD, les noms d'utilisateur locaux seront toujours enregistrés dans la mesure dupossible.

ADMINISTRATION FACILITEE

La plateforme Censornet offre la flexibilité de créer un nombre illimité de rôles administrateur basés sur plus de 100 contrôles d'accès, avec la possibilité de protéger les comptes d'administrateur par un e authentification à deux facteurs. La fonction d'administration peut être divisée pour répondre aux exigences organisationnelles, en séparant provisionnement des comptes et des agents, l'affichage des rapports d'utilisation du web, la maintenance des catégories d'URL ou la gestion du catalogue d'applications Cloud.

Les entreprises peuvent déléguer les activités d'administration à des équipes locales, tandis que les MSP peuvent définir les responsabilités en fonction des SLA contractés, ou utiliser un contrôle d'accès basé sur les rôles pour mettre en place des services à valeur ajoutée.

Différentes adresses électroniques peuvent être saisies pour recevoir les notifications relatives au système, à la maintenance, au déblocage et à l'archivage des rapports.

Les comptes parents peuvent assumer le rôle d'administrateur pour un compte enfant afin de gérer les paramètres, les politiques et les règles de tous les services, ou de résoudre les problèmes, au nomdes unités commerciales ou des clients.

SECURISATION DE MICROSOFT 365

Les configurations prêtes à l'emploi de M365 ne sont pas conçues pour répondre aux besoins spécifiques de vos clients ou pour les protéger contre toutes les menaces. De plus les produits Microsoft sont complexes et coûteux à gérer pour les MSP.

Pour les organisations qui souaitent une protetion complète, une disponibilité permanente et une expérience utilisateur supérieure, notre plateforme cloud intégrée combine la sécurité de la messagerie, la sécurité web, le CASB et le MFA pour protéger votre environnement M365.

censornet

E. EMAIL

Sécurisez l'ensemble de votre organisation contre les menaces connues, inconnues et émergentes visant la sécurité des e-mails, y compris la fraude.

S. SAT

Défendez votre organisation contre les cybercriminels grâce à une formation en ligne engageante et stimulante.

W. WEB

Protègez les utilisateurs contre les logiciels malveillants, les contenus inappropriés et améliore la productivité.

C. CASB

Découvrez, analysez, sécurisez et gérez l'interaction des utilisateurs avec les applications Cloud - en ligne à l'aide d'APIs.

M. MFA

Réduit l'impact des violations de données à grande échelle en protégeant les comptes des utilisateurs avec plus qu'un simple mot de passe.

ID. IDaaS

Accès sécurisé aux applications Cloud grâce à l'authentification unique des utilisateurs (SSO).

Notre plateforme

Notre plateforme Cloud intègre la sécurité du courrier électronique, du web et des applications Cloud, ainsi que la gestion des identités et la prévention avancée de la perte de données via le moteur de Sécurité Autonome (ASE).

DLP avancé

Empêchez que des données sensibles ne tombent entre de mauvaises mains.

Le DLP s'applique à la messagerie électronique, au web et aux applications Cloud pour une protection optimale en temps réel.

Moteur de sécurité autonome

Prévient les attaques avant qu'elles n'entrent dans la chaîne d'exécution.

Permet à des produits traditionnellement cloisonnés de partager les informations et de réagir aux événements de sécurité et aux données tout en renseignant sur les menaces de classe mondiale.

CENSORNET LTD

Matrix House, Basing View,
Basingstoke, RG21 4FF, UK

Téléphone: +44 (0) 845 230 9590

CONNECT DATA – SINTEL

Rte de Gisy, Parc Burospace Bat 21,
91570 BIEVRES, FR

Téléphone: 01 30 85 44 44

censornet.com

censornet.