NOTE D'APPLICATION

Solutions Wavelogic Encryption

Sécuriser toutes les données en transit, à chaque instant

La sécurité est devenue une préoccupation du conseil d'entreprise. Un rapport sur les menaces pesant sur les données de Thales en 2020[1] a révélé que 49 % des multinationales, dont faisaient partie les personnes qui ont répondu, ont subi une violation de données à une certaine période de leur histoire. Les secteurs les plus ciblés, comme ceux de la santé, de l'enseignement, de la finance et des administrations, déclarent, quant à eux, un nombre de violations de données bien supérieur à la moyenne.

En plus de mettre en danger les informations liées aux clients, une brèche dans les données a un impact direct sur le bilan comptable d'une organisation. Selon une étude mondiale de Ponemon[2], environ 25 500 dossiers sont exposés lors de chaque brèche dans les données, chiffrant le coût de chaque violation à plusieurs millions, en plus de la perte incommensurable de confiance chez les clients. Cette étude révèle également que le coût total moyen d'une brèche dans les données en 2019 aux États-Unis s'élevait à 8,19 millions de dollars. Ce montant varie à nouveau selon le secteur : le coût par dossier perdu dans celui de la santé étant pratiquement le double de celui des autres.

Cependant, alors même que la menace de piratage grandit, le flux du trafic sur le réseau augmente. Les besoins en bande passante continuent de grimper et réclament un réseau qui puisse s'étendre de manière élégante pour traiter plus de capacité avec moins de complexité opérationnelle. De plus, avec l'augmentation de la sophistication et de la fréquence des brèches dans les données, aucune organisation n'est immunisée contre la menace omniprésente d'attaques malveillantes visant à recueillir des informations confidentielles et privées. Les réseaux de haute capacité actuels demandent bien plus qu'une bande passante de haute capacité : ils ont besoin d'une stratégie de sécurité pour protéger toutes les données critiques, qu'elles soient au repos ou en transit, tandis qu'elles parcourent le monde entier sur des distances métropolitaines, régionales, longue portée et sous-marines.

Conçue pour sécuriser les réseaux de haute capacité actuels, la solution WaveLogic™ Encryption de Ciena active de manière rentable une solution de chiffrement évolutive, indépendante du protocole, à délai de transit ultra-faible sur le système largement déployé, 6500 Packet-Optical Platform. Cette solution s'étend à la gamme Waveserver® de Ciena regroupant des dispositifs de transport modulaires, compacts à haute capacité, ce qui permet de bénéficier d'applications de DCI (Data Center Interconnect) sécurisées et rentables. Ce chiffrement toujours actif allie facilité de fonctionnement et de gestion pour permettre une stratégie de protection des données simple à mettre

1 https://cpl.thalesgroup.com/sites/default/files/2020-04/2020-data-threat-report-global-edition-infographics.pdf
2 Ponemon, Étude IBM : coût d'une donnée piratée en 2020 ; http://ibm.co/2020MkF2020s

Avantages

- Offre une solution de chiffrement conforme FIPS, à hautes performances et délai de transit ultra-faible pour des communications de bout en bout transparentes et hautement sécurisées.
- Peut évoluer avec la technologie cohérente programmable WaveLogic pour un chiffrement flexible et hautes performances de 100G à 400G.
- Dispose d'un chiffrement indépendant du protocole offrant la flexibilité de prendre en charge toute une variété de services.
- Tire parti des fonctions de sécurité améliorée, notamment deux ensembles distincts de clé pour les fonctions d'authentification et de chiffrement des données, avec une rotation rapide des clés de chiffrement de quelques secondes.
- S'intègre de façon transparente aux infrastructures PKI (à clé publique) existant en entreprise grâce à une authentification à certificat X.509.
- Permet une gestion sécurisée de la capacité de type EaaS (chiffrement en tant que service) par l'utilisateur final via un outil de gestion intégré.
- Offre une solution de chiffrement ayant fait ses preuves sur le terrain largement déployée dans le monde sur des réseaux de la finance, de la justice, de la santé, de la distribution électrique, des armées et des gouvernements.

en œuvre, s'appuyant sur la technologie cohérente leader du secteur WaveLogic de Ciena et pour donner un niveau sans précédent de flexibilité et de performances, ainsi que la première solution de chiffrement de 100G à 400G cohérente à hautes performances de l'industrie.

Technologie de chiffrement

Le chiffrement est défini comme le processus transformant les informations en utilisant un algorithme pour les rendre indéchiffrables sauf aux personnes dépositaires d'une connaissance spéciale, appelée clé en cryptographie. Ce processus consiste essentiellement à verrouiller le réseau en encodant ces données, les rendant ainsi totalement inutilisables par un intrus qui les récupère ou par quiconque ne disposant pas de la clé correcte pour déchiffrer le message.

Il existe de nombreuses façons d'encoder les données qui sont définies par différentes normes spécifiant les exigences du chiffrement des clés et des produits associés et établissant un processus de certification des équipements réseau. Il existe plusieurs algorithmes de chiffrement normalisés, notamment la norme AES (Advanced Encryption Standard) disposant de différentes tailles de clé (56, 128 et 256 bits) et publiée par le NIST (National Institute of Standards and Technology). Ces normes sont publiées aux États-Unis sous le nom de Federal Information Processing Standard (FIPS). Par exemple, l'algorithme de chiffrement AES-256 est publié en tant que norme FIPS 197. En plus des publications spécifiques aux algorithmes comme la norme FIPS 197, le NIST publie également des normes regroupant les exigences relatives aux modules d'encodage et incluant à la fois les composants logiciels et matériels dans la norme FIPS 140-2.

Il existe d'autres cadres similaires qui sont utilisés pour certifier les solutions de chiffrement. Une autre norme importante est appelée les Common Criteria (CC) pour l'évaluation de la sécurité des technologies de l'information, qui est une norme internationale (ISO/CEI 15408) en matière de certification de sécurité informatique. La norme Common Criteria fournit un moyen de garantir que le processus de spécification, de mise en œuvre et d'évaluation d'un appareil sur le réseau, comme par exemple un élément de réseau optique, a été mené selon une norme et avec rigueur. En Allemagne, le BSI (office fédéral allemand pour la sécurité en matière de technologies de l'information) délivre des homologations de sécurité qui incluent la certification Common Criteria. Les certificats BSI basés sur les Common Criteria sont souvent utilisés pour l'homologation locale, ce qui permet d'économiser du temps et de l'argent dans le processus de certification. Cet ensemble de normes et processus de certification fournit aux prestataires de services et aux utilisateurs l'assurance que la solution de chiffrement a démontré sa conformité aux critères définis en passant avec succès les tests rigoureux en laboratoire et les examens exigés par les normes.

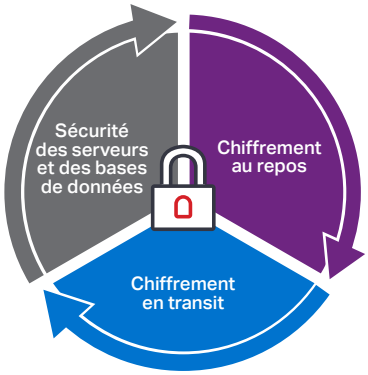

Figure 1. Un chiffrement des données en transit fait partie d'une stratégie de sécurité holistique

Sécuriser les réseaux d'aujourd'hui

Le chiffrement est largement utilisé de nos jours pour sécuriser les données au repos et en transit. Selon un rapport Ponemon relatif aux tendances du chiffrement, seulement 13 % des participants au niveau mondial ne disposaient d'aucune stratégie de chiffrement[3]. Des organisations de toute taille et sur tous les secteurs doivent engager de gros efforts afin de protéger les informations stockées dans leurs data centers contre tout accès non autorisé. L'impact et le coût d'une brèche dans les données ne peuvent pas être ignorés et ont des conséquences de plus en plus sévères sur une organisation, notamment une réputation ternie pour l'entreprise, des poursuites pénales, des amendes coûteuses de régulation et une forte perte de clients.

Une variété de techniques habituellement utilisées existe aujourd'hui pour protéger les données au repos, pour sécuriser les serveurs, les bases de données, les routeurs et les commutateurs en gérant l'accès des utilisateurs et les identifiants de connexion. Toutefois, sur les réseaux à l'échelle du web d'aujourd'hui, de grandes quantités de données critiques sont en transit car des communications à haut débit ont lieu par-delà les murs du data center et empruntent un réseau plus vaste, potentiellement dans le monde entier. Une approche complète de sécurité informatique doit donc englober une solution solide de chiffrement des données en transit dans sa stratégie de sécurité holistique, comme le présente la figure 1. En chiffrant les données qui partent en dehors du cloud privé sécurisé, les opérateurs peuvent assurer leur protection contre toute interception non autorisée au fil de leur parcours sur le réseau, pendant qu'elles traversent différents niveaux de sécurité et atteignent leur destination.

Même si de nombreuses organisations ont ajouté un chiffrement des données en transit à leur stratégie de sécurité, celui-ci se cantonne généralement à chiffrer les données en transit au niveau de la couche 2 ou à une couche supérieure. Si cette approche peut être une bonne option pour certaines applications informatiques à bas débit qui ne sont ni intenses en données, ni sensibles au délai, cela ne s'étend souvent pas à toute l'entreprise et chiffre uniquement les données des applications sur IP. Ce modèle opérationnel pour déployer une solution de chiffrement est plutôt laborieux et coûteux,

3 Ponemon, rapport de recherche e-Security Thales : Étude des tendances du chiffrement mondial 2018 ; avril 2018 ; https://go.ncipher.com/rs/104-QOX-775/images/2018-nCipher-Ponemon-Global-Encryption-Trends-Study-ar.pdf

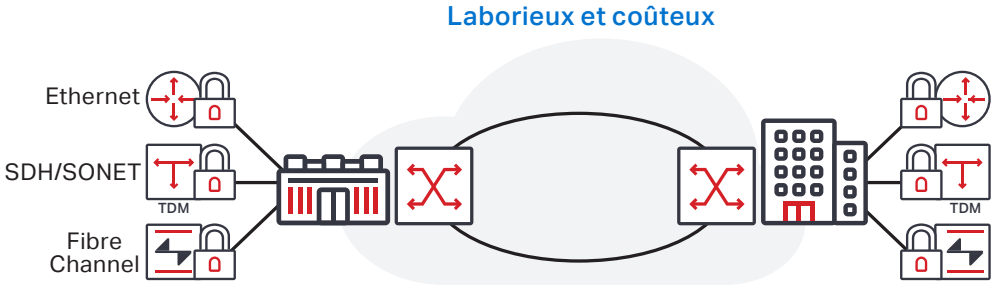

Figure 2. Chiffrement traditionnel, spécifique au protocole déployé dans un réseau multiservice

comme le présente la figure 2, car il requiert habituellement des appareils de chiffrement autonomes et spécifiques au protocole utilisé et peut entraîner un délai de transit conséquent, affectant le rendement de l'application et entraînant une utilisation inefficace de la bande passante. De plus, l'authentification et la gestion des clés de chiffrement sur de multiples appareils indépendants sont des procédures complexes et coûteuses en termes de main-d'œuvre ; le dépannage du réseau de bout en bout étant encore compliqué par la multiplicité des appareils indépendants. Cette approche laisse aussi un vide dans la stratégie de protection des données en transit de l'organisation. Même si, habituellement, le risque d'intrusion sur un câble de fibre optique n'est pas pris en compte dans la stratégie de sécurité d'une organisation, le risque d'une intrusion sur le câble optique pour accéder aux données qu'il transporte est bien réel. Les câbles de fibre optique sont habituellement très accessibles et sans protection. Ainsi, quiconque équipé des outils adéquats peut se brancher sur un câble de fibre optique et recueillir des données sans être détecté pendant des jours, des mois, voire plusieurs années. Déployer une solution de chiffrement au niveau de la couche de transport protège toutes les données en transit, tout le temps et assure ainsi la sécurité de chaque bit.

Data Security with Optical Encryption
Télécharger maintenant l'infographie

Solution WaveLogic Encryption

Partie intégrante de l'approche de la sécurité multicouche de Ciena garantissant la confidentialité, l'intégrité et la disponibilité des données sur le réseau, la solution WaveLogic Encryption associe la technologie de chiffrement éprouvée et déployée sur des plates-formes avec une vaste base installée au niveau mondial et la fiabilité démontrée du système leader du marché, 6500 Packet-Optical Platform, déployé chez plus de 600 opérateurs dans le monde entier. De plus, les capacités WaveLogic Encryption s'étendent aux systèmes d'interconnexion empilables Waveserver et Waveserver Ai de Ciena, permettant jusqu'à 1,2 Tbit de capacité de chiffrement à hautes performances en format 1RU pour des applications DCI simples en baie à empiler.

Simple à déployer

Grâce à WaveLogic Encryption, les opérateurs peuvent bénéficier d'une solution qui simplifie le déploiement du chiffrement en intégrant la fonctionnalité de chiffrement directement dans les éléments au sein du réseau de transport. Une telle approche réduit la complexité du réseau et élimine le besoin de gérer différentes solutions de chiffrement pour différentes applications, comme le présente la figure 3. Cette simplification au niveau opérationnel s'étend aussi à la gestion de la solution de chiffrement, en incluant un outil dédié à l'authentification et à la gestion des clés, et une intégration simple aux infrastructures à clé publique (PKI) de l'entreprise.

La flexibilité de la plate-forme 6500 permet aux clients de sélectionner la taille de baie optimale correspondant le mieux à leurs besoins spécifiques sur site en termes de capacité, d'espace et de puissance pour un transport rentable des services chiffrés. Un autre avantage clé de la solution est qu'elle est totalement indépendante du protocole et prend en charge une large variété de clients flexibles (Ethernet, SDH/SONET, Fibre Channel et OTN, par exemple) pour répondre aux multiples applications parmi les clients soucieux de sécurité.

Se différencier par un chiffrement 24 heures sur 24

Le chiffrement est toujours actif dans les solutions WaveLogic Encryption de Ciena, assurant ainsi le plus haut niveau de sécurité possible, car tout le trafic sur le réseau est toujours chiffré. Même si la possibilité d'activer ou de désactiver le chiffrement paraît donner davantage de souplesse, une simple erreur humaine peut entraîner l'envoi non-chiffré de données

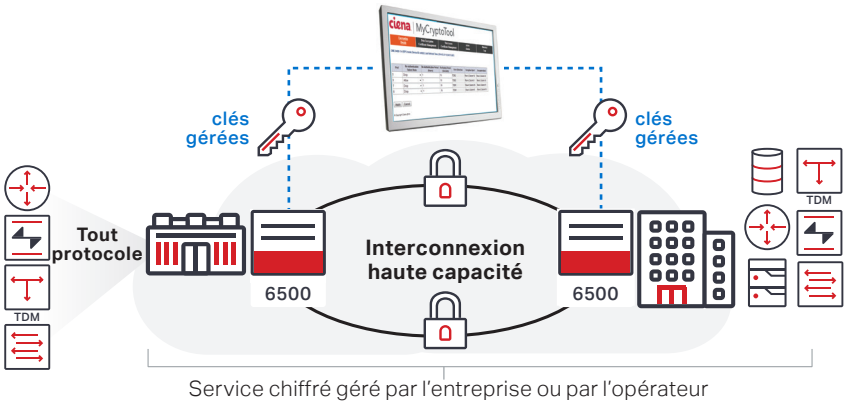

Figure 3. Solution WaveLogic Encryption des 6500 de Ciena

confidentielles sur le réseau. Les opérateurs peuvent tirer parti d'une infrastructure différenciée qui protège toutes les données en transit, à chaque instant, tandis qu'elles parcourent le monde entier sur des distances métropolitaines, régionales, longue portée ou sous-marines. De plus, les opérateurs peuvent augmenter leurs revenus et la fidélité de leurs clients en offrant des SLA (accords de niveau de services) à haut débit différenciés, tirant parti des services chiffrés avec une connectivité à délai de transit ultra-faible et plusieurs options de protection de trajet et d'équipement.

Un chiffrement invulnérable

La solution WaveLogic Encryption de Ciena est validée en externe et certifiée de façon indépendante par un tiers afin d'assurer sa mise en place avec des algorithmes aux normes du secteur et des fonctionnalités de sécurité avancées qui incluent l'homologation Common Criteria et FIPS. Elle offre un moteur de chiffrement AES 256 certifié par le FIPS avec des mécanismes d'authentification normalisés (tels que les certificats X.509), permettant son intégration transparente aux infrastructures PKI de l'entreprise. De plus, les composants matériels et logiciels 6500 des modules cryptographiques sont conformes à la norme FIPS 140-2 et disposent d'une certification BSI complète selon Common Criteria pour l'évaluation de la sécurité des technologies de l'information, garantissant ainsi aux prestataires de services et aux utilisateurs une solution de chiffrement conforme à tous les aspects couverts par cette évaluation exhaustive, notamment au niveau des algorithmes de chiffrement, des mécanismes d'échange des clés et de l'authentification des utilisateurs.

Pour mieux protéger les données, deux ensembles de clés distincts et indépendants sont utilisés pour les fonctions d'authentification et de chiffrement des données avec un intervalle de rotation des clés de chiffrement rapide, de quelques secondes au lieu de plusieurs minutes. Les clés pour la session de chiffrement AES-256 des données font l'objet de négociation et rotation à chaque seconde, de façon autonome et indépendante sur chaque ligne de port, sans impact sur le trafic ou le débit, ni intervention de l'utilisateur. Les opérateurs peuvent déployer la nouvelle génération d'algorithmes de cryptographie à clé publique avec une prise en charge ECC (encodage à courbes elliptiques), qui donne une stratégie plus sûre que les systèmes de cryptographie à clé publique de première génération.

Chiffrement hautes performances programmable de 100G à 400G

Afin de satisfaire les besoins des communications à haute capacité d'aujourd'hui, la solution WaveLogic Encryption de Ciena tire parti de la technologie cohérente WaveLogic, leader du secteur, pour permettre des solutions de chiffrement de hautes capacité, flexibles et personnalisables. Basé sur les capacités de WaveLogic 3, WaveLogic 3 Extreme offre des performances extrêmes pour toutes les applications de réseau cohérent avec des modulations supplémentaires et en réduisant mieux les détériorations, qu'elles soient linéaires ou non. Cette solution à la pointe de la technologie offre une modulation programmable par logiciel pour permettre un chiffrement hautes performances 100G en modulation QPSK, 150G en modulation 8QAM et 200G en modulation 16QAM. WaveLogic Ai s'appuie sur les performances des WaveLogic 3, les meilleures de leur catégorie, et utilise un système avancé, optimisé pour 400G afin d'améliorer considérablement le modèle économique de la transmission : en doublant la capacité par canal, en triplant la distance à capacité équivalente et en quadruplant la densité des services.

Sur le 6500, les opérateurs peuvent intégrer un module de ligne WaveLogic 3 Extreme avec chiffrement à n'importe quelle interface client, afin de déployer de manière flexible une solution sur mesure afin de satisfaire à leurs besoins de trafic spécifiques, qu'il s'agisse de transport de service 10G, 40G ou 100G. À mesure que la demande augmente, avec une offre modulaire à paiement selon croissance, le même module de ligne peut être programmé pour transporter 200G de trafic chiffré simplement en ajoutant une autre carte client. De plus, les opérateurs peuvent déployer des services chiffrés de haute capacité à travers le réseau en tirant parti de la matrice haute capacité hybride paquets/OTN du système 6500 et ainsi optimiser l'efficacité des ressources du réseau.

Sur le Waveserver, des opérateurs tirent parti de 400 Gbit/s au maximum de capacité de ligne à chiffrement AES-256 hautes performances, homologué par le FIPS au format de seulement 1RU et de la flexibilité de prendre en charge un mélange de clients 10GE, 40GE et 100GE sur le même appareil. La modulation programmable permet à Waveserver d'optimiser sa capacité de chiffrement haute performance pour chaque application et en fonction de chaque exigence, donnant ainsi accès à deux longueurs d'onde à 100 Gbit/s, 150 Gbit/s ou 200 Gbit/s. Pour répondre aux applications d'interconnexion sécurisées à ultra-haute capacité, les opérateurs peuvent déployer Waveserver Ai et ainsi assurer jusqu'à 1,2 Tbit/s de capacité chiffrée en format 1RU, avec la possibilité de prendre en charge trois modules de trafic offrant chacun jusqu'à 400 Gbit/s de capacité chiffrée. Waveserver et Waveserver Ai offrent une protection des données en transit hautement sécurisée, à délai de transit ultra-faible sur l'ensemble des distances métropolitaines, régionales et longue portée.

Chiffrement hautes performances 6500 10G

Les opérateurs peuvent fournir de façon rentable des services chiffrés 10G en tirant parti du transpondeur optique 4x10G à module de chiffrement. Ce module à emplacement unique fournit 40G de capacité de services chiffrés hautes performances via quatre ports de ligne 10G distincts chiffrés, indépendants du protocole afin que les clients puissent bénéficier d'une conception de réseau plus simple avec une capacité de chiffrement intégré sur n'importe quelle variante

High-capacity Wire-speed Encryption Modules
Télécharger tout de suite la fiche technique

de châssis 6500. Le module offre une sécurité avancée avec sa conception conforme à la norme FIPS 140-2 de niveau 3, donnant ainsi une protection contre les tentatives d'intrusion physique sur la carte, avec une prise en charge de zéro-isation. Ceci assure que toutes les informations de sécurité critique seront effacées dès détection d'une tentative d'intrusion du module de chiffrement avec une remise à zéro de toutes les données, même quand la carte n'est pas branchée dans la baie.

Une gestion du chiffrement simplifiée

Une solution de sécurité parmi les meilleures de sa catégorie au niveau de la couche de transport ne saurait être complète sans une approche simplifiée et intégrée de la gestion du chiffrement. Séparer la gestion du chiffrement de la gestion du transport accroît la flexibilité d'une infrastructure, qu'elle soit assurée par l'entreprise ou par l'opérateur. Dans les deux cas, il est important que le « propriétaire » des données (l'utilisateur final) conserve un contrôle complet des paramètres de sécurité du chiffrement associés à ses données critiques et puisse créer de nouvelles clés ou certificats selon les exigences de ses politiques de sécurité, tout en restant informé de toute alerte de sécurité et des rapports d'activité de bout en bout.

La solution 6500 WaveLogic Encryption de Ciena comprend MyCryptoTool, une interface dédiée à la gestion du chiffrement conçue pour une gestion distribuée du réseau donnant au responsable de la sécurité, ou à l'utilisateur final, la possibilité de gérer indépendamment les paramètres de sécurité et les alertes sur des réseaux gérés par l'entreprise ou par l'opérateur. MyCryptoTool est une interface facile à utiliser qui se connecte en toute sécurité au module de chiffrement et assure une authentification mutuelle, limitant l'accès au personnel de sécurité autorisé. Dans le cas où le service chiffré est acheté auprès d'un prestataire de services, ce dernier gère les liaisons et leur dimensionnement, l'administration et la surveillance des performances comme dans n'importe quel autre service. Par contre, il n'a pas de contrôle ni de visibilité sur les paramètres de chiffrement. La même approche est valable quand la solution de chiffrement est déployée et gérée par deux groupes distincts au sein d'une même entreprise ou d'une même administration gouvernementale.

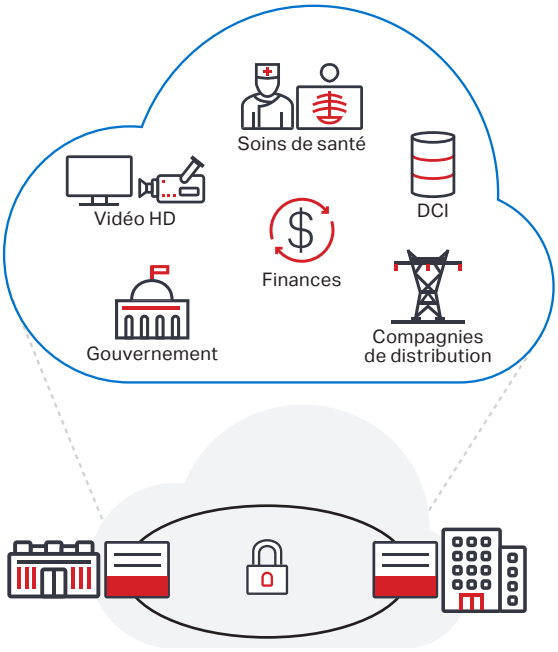

Figure 4. Exemples des applications principales de WaveLogic Encryption

Applications clés

Les solutions WaveLogic Encryption de Ciena sont conçues sur mesure afin de protéger les données critiques en transit dans toutes les applications à haute capacité d'aujourd'hui. Les principales applications qui pourraient bénéficier de ces solutions comprennent :

- Interconnexion de data centers d'entreprise pour le stockage de haute capacité et le transport chiffré des données.
- Administrations et institutions nécessitant des communications à haut débit sécurisées et certifiées entre des sites distincts.
- Applications médicales avec des exigences en matière de haute qualité et de faible délai de transit pour une collaboration sécurisée, efficace et à temps entre les différents acteurs du domaine de la santé.
- Applications de services gérés.
- Applications sensibles au délai de transit, comme la vidéo haute définition ou les transactions financières à haute vitesse, qui ont besoin d'une solution de transport sécurisée à délai de transit ultra-faible.
- Compagnies électriques qui veulent protéger leurs infrastructures de communication critiques.

En résumé

À mesure que de plus en plus d'informations, elles-mêmes de plus en plus sensibles, sont distribuées sur les réseaux à fibre optique, les communications à haute capacité actuelles doivent déployer une approche de sécurité informatique qui englobe non seulement la sécurité du serveur et le chiffrement au repos, mais aussi une solution robuste de chiffrement des données en transit. La solution WaveLogic Encryption de Ciena associe un haut degré de flexibilité et de sécurité à une simplicité de fonctionnement et de gestion, pour donner des solutions de chiffrement rentables, évolutives et hautes performances afin de sécuriser pratiquement toutes les données en transit, qu'elles traversent la rue, la ville, les frontières ou les océans.