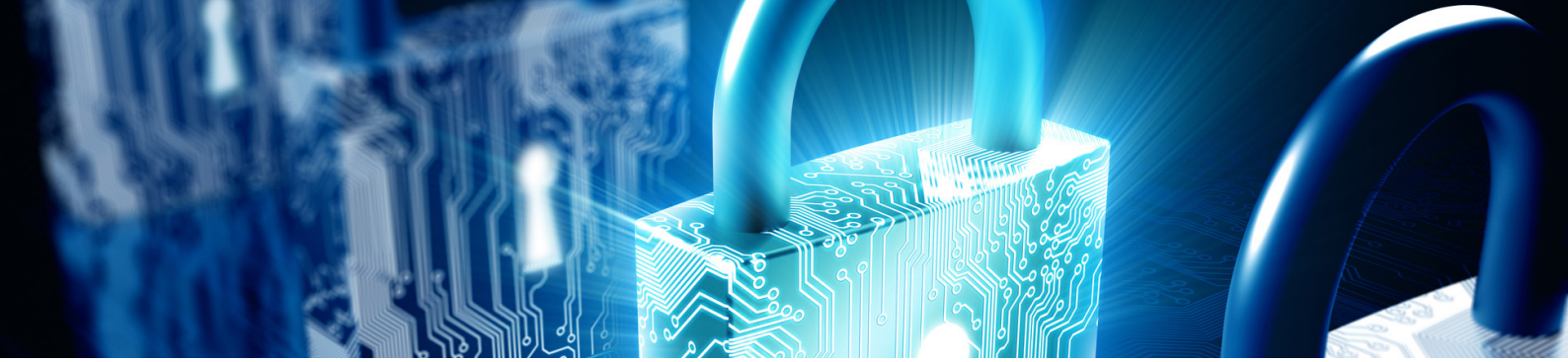
colt

Relever le défi de la sécurité sur les liaisons Ethernet

www.colt.net/fr

ADVA™



Selon les prévisions actuelles, le trafic IP mondial va tripler au cours des cinq prochaines années, avec pour conséquence une augmentation inexorable du volume d'informations confidentielles et sensibles qui seront stockées et échangées. La virtualisation des data centres a créé un environnement où le propriétaire des données ne contrôle plus les paramètres de protection : les opérateurs longue distance (interexchange carriers), les solutions d'hébergement multiclouds et les algorithmes de routage à moindre coût viennent s'ajouter aux points de contact qui ponctuent le transport des données et où les risques de sécurité sont potentiellement accrus. Ces nouveaux risques sont à l'origine de l'augmentation de la fréquence, de la gravité et de l'impact des failles de données.

En mai 2018, l'Union européenne a mis en œuvre le règlement général sur la protection des données **(RGPD)**, une mesure qui s'applique à toute entreprise proposant des biens ou des services au sein de l'UE. En fait, le RGPD concerne toute entité qui reçoit des données dans le cadre normal de ses activités (fournisseurs de services en cloud et data centres), que l'entreprise ou les données se trouvent ou non dans l'UE. La quasi-totalité des data centres ou entreprises qui traitent des données, ou qui sont présents sur le Web, peuvent être tenus responsables d'une violation des informations personnelles des citoyens européens. Les pénalités sont particulièrement dissuasives : 2 à 4 % du CA annuel mondial ou 20 millions d'euros, le montant retenu étant le plus élevé.

Tandis que les régulateurs du monde entier mettent tout en œuvre pour répondre aux enjeux pressants de sécurité de l'information, les entreprises doivent adopter une stratégie cohérente et holistique d'un bout à l'autre de leur infrastructure technologique, faisant du réseau un élément clé que toute entreprise doit sécuriser.

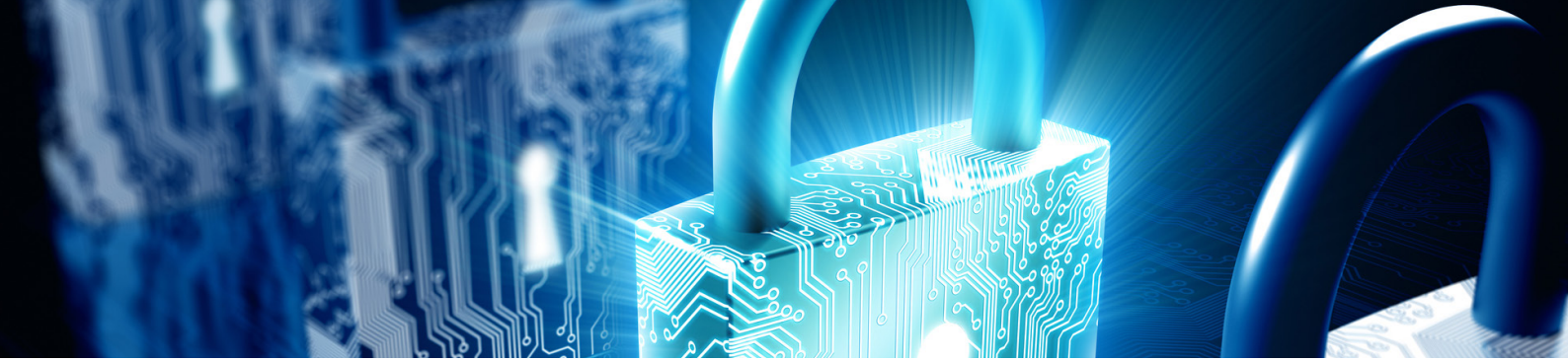
« En avril 2018, opérateur longue distance basé à Chicago a été victime de pirates informatiques qui ont détourné le trafic d'un service en cloud vers un site russe, notamment en cassant le système de chiffrement d'une société de cryptomonnaie. Les pirates avaient alors récupéré des millions de livres sterling dans leur portefeuille électronique. Cet incident souligne les problèmes que rencontre le transport des données sur le réseau, un serveur tierce partie de l'opérateur dont la sécurité était insuffisante ayant été utilisé pour l'attaque. Un haut niveau de sécurité est la seule défense possible contre une nouvelle attaque de l'homme du milieu (Man in the middle). »

C'est dans cette optique que Colt a lancé sous l'appellation Colt Ethernet Encryption une nouvelle fonctionnalité majeure qui vient enrichir ses services **Ethernet Line**. Cette fonctionnalité complète l'offre de **produits de cybersécurité** conçus par Colt pour répondre aux besoins croissants des entreprises en quête de solutions de sécurité réseau capables de repousser les menaces croissantes tout en se conformant aux nouvelles réglementations en vigueur.

Chiffrement Ethernet Line : une solution simple et active en permanence

Disponible en Europe, en Amérique du Nord et en Asie pour les circuits Ethernet Line locaux, nationaux ou internationaux, cette solution assure un chiffrement de bout en bout, avec à la clé un débit élevé jusqu'à 10 Gbits/s, des clés managées par Colt et une assistance assurée 24/7 par l'équipe Service Assurance de Colt. Le chiffrement des circuits Ethernet Line convient à toute entreprise amenée à traiter des informations sensibles :

- les institutions financières qui souhaitent assurer un haut niveau de protection à leurs filiales et guichets automatiques ;
- les places boursières qui requièrent un chiffrement de haute qualité assorti d'une latence extrêmement faible pour traiter leurs transactions et offres d'achat ;
- les services gouvernementaux dont les données acheminées sur le réseau doivent être protégées contre les attaques lancées par d'autres États, et qui s'appuient sur un chiffrement de haute technologie pour assurer une protection maximale ;
- l'industrie des services publics, où les données critiques sont envoyées par des stations déportées ;
- toute entreprise faisant des affaires au sein de l'UE, ou qui reçoit des commandes de l'UE : institutions financières, agences de location de voitures, détaillants ou compagnies aériennes.

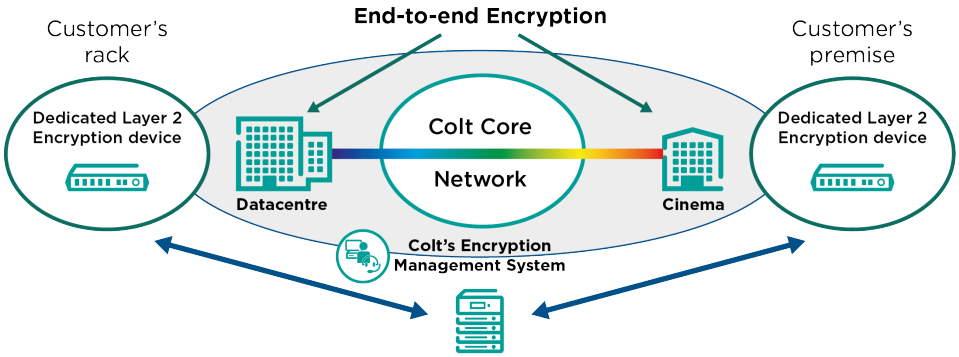


Festival international du film de Berlin (Berlinale)

Depuis 2009, Colt est partenaire pour le cinéma numérique de la **Berlinale**, fournissant au festival berlinois des services réseau à très haut débit (jusqu'à 10 Gbit/s) et un accès Internet permettant une transmission de données de haute qualité. En 2019, cette manifestation a accueilli 22 000 visiteurs professionnels dont plus de 3 500 journalistes venus de 82 pays, et vendu environ 335 000 billets aux festivaliers, ce qui représente la fréquentation la plus élevée, tous festivals de cinéma annuels confondus. Cette année, Colt a déployé sa solution de chiffrement Ethernet Line Encryption sous la forme d'une démonstration PoC opérationnelle en temps réel.

L'objectif de cette solution était de sécuriser un circuit Ethernet Line 1G entre le data centre dont dispose Colt à Berlin, site de la Berlinale, et une salle où un film était projeté. Le contenu hébergé sur les serveurs de la Berlinale a été transmis au cinéma au format DCP (Digital Cinema Package) et chiffré « en vol » afin d'éviter toute fuite. En effet, bon nombre de films sont projetés à Berlin en avant-première mondiale. Le chiffrement était non seulement effectué au niveau de la couche physique du data centre, mais également lors de la transmission des contenus sur le réseau afin d'assurer une approche holistique.

Colt a ainsi fourni un chiffrement de pointe sans pénaliser les performances du service Ethernet, avec seulement 11 µs de latence supplémentaire ajoutées à chaque extrémité.

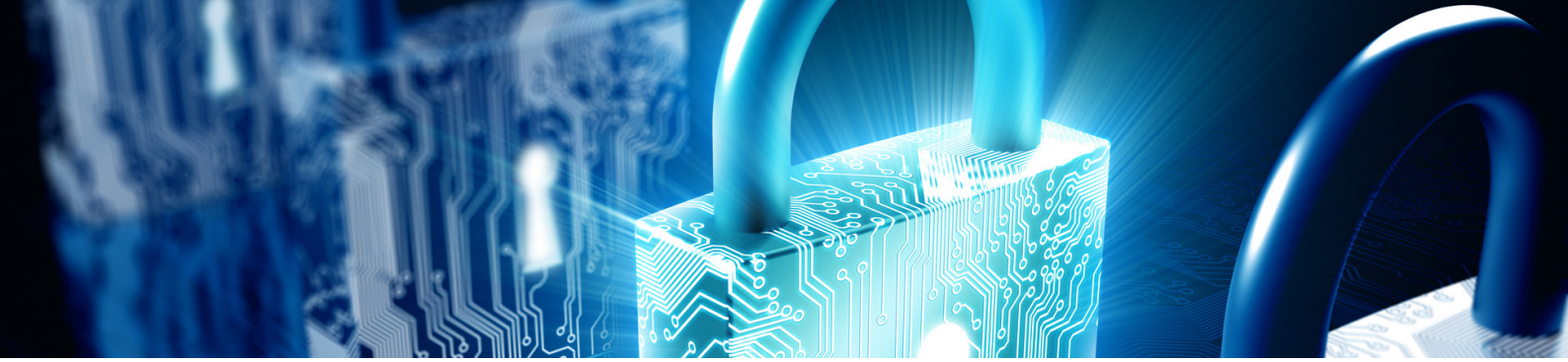


Autres exemples d'utilisation du chiffrement Ethernet Line :

Une compagnie d'assurance-maladie opte pour une solution IP-VPN sécurisée

Le problème : l'entreprise compte 152 succursales qui doivent se conformer aux réglementations européennes telles que le RGPD, à la norme PCI-DSS (Payment Card Industry Data Security Standard) relative à la sécurité des paiements effectués par carte bancaire (PCI DSS), ainsi qu'à la loi américaine Sarbanes-Oxley (SOX), pour transmettre les données personnelles des patients aux data centres. Le réseau de l'entreprise doit supporter une architecture redondante.

La solution : la société a pu peut transmettre des données à des débits mixtes (10/50/100 Mbits/s) grâce à des services IP-VPN MPLS standard. L'infrastructure couvre 152 sites supportant trois réseaux WAN distincts. Tous les sites disposent de ports 1 GbE, et le service de chiffrement emprunte des tunnels MACsec+ configurés pour répondre aux réglementations en vigueur. La trame Ethernet étant entièrement chiffrée, toutes les données qui circulent sur le réseau sont protégées.



Une société de services financiers disposant d'un réseau mondial

Le problème : les services financiers couvrent un large éventail d'activités (banque commerciale, banque de détail et banque privée, gestion d'actifs, investissements et gestion immobilière), ce qui implique le stockage et le transfert d'informations hautement confidentielles.

La solution : outre l'obligation incontournable de protéger des données hautement sensibles, la société devait également satisfaire aux exigences réglementaires du RGPD. Un réseau d'entreprise de couche 2 sécurisé lui permet de proposer une connectivité hybride qui couvre une bande passante de 10 Mbits-1GbE-10GbE. Toutes les connexions sont protégées par un chiffrement MACSec+ en couche 2, avec en prime une bande passante maximale doublée d'une faible latence.

Pouvez-vous compter sur vos applications pour chiffrer vos activités ?

Les nouveaux risques que soulève l'informatique quantique pour les méthodes de chiffrement traditionnelles menacent de rendre obsolètes bon nombre des techniques de chiffrement actuellement utilisées. Longtemps considérés comme une possibilité distante de plusieurs décennies, les ordinateurs quantiques seront probablement une réalité au cours des cinq prochaines années : depuis cette année, IBM propose d'ailleurs un ordinateur quantique accessible sur le cloud.

Les applications et les services en cloud sont des solutions à base de code qui s'appuient sur des développeurs tierce partie dotés dont l'expertise en matière de chiffrement est variable. « Parmi les 20 000 fournisseurs de services en cloud actuels, seuls 10 % respectent les bonnes pratiques industrielles pour chiffrer les données « au repos » et autres contrôles de sécurité de niveau professionnel ». Un employé lambda utilise activement 36 services cloud. Pour les entreprises, il est très difficile de valider individuellement chacun de ces services de chiffrement. La meilleure solution consiste à encapsuler les données en mouvement dans un environnement de chiffrement en réseau. Les protocoles de communications sécurisées IPSec forment une méthode de protection réseau traditionnelle qui n'a pas été conçue pour gérer les environnements de cloud moderne dont les besoins en matière de latence et de bande passante sont critiques.

De nouveaux standards sont actuellement développés pour faire face à cette menace et devraient commencer à voir le jour à partir de 2022, de sorte que tout dispositif de chiffrement déployé aujourd'hui devra pouvoir être mis à niveau dans quelques années. Actualisés sur site, les produits de chiffrement de réseau ADVA sont conçus pour supporter la puissance de traitement supérieure qui sera alors nécessaire.

Powered by colt IQ Network

Pour plus d'information :
www.colt.net/fr

Tél : 0800.949.944
E-mail: sales@colt.net

ADVA™