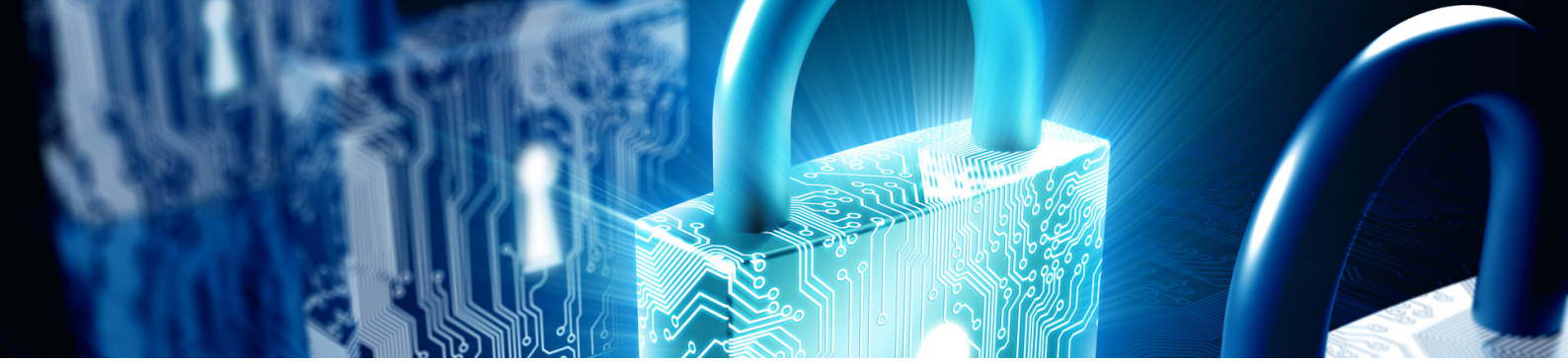
colt

Vincere la sfida della sicurezza Ethernet

www.colt.net/it

ADVA™



Si prevede che il traffico IP globale andrà a triplicare nel corso dei prossimi 5 anni, con un numero sempre maggiore di informazioni riservate e sensibili salvate e inviate. La virtualizzazione dei data centre ha creato un ambiente in cui i parametri di protezione non sono più sotto il controllo dei proprietari dei dati, in quanto gli Interexchange Carrier (IXC), i numerosi hosting cloud e gli algoritmi di Least Cost Routing diventeranno nuovi touch point nel trasporto dei dati, tutti esposti a minacce di sicurezza sempre nuove. Questi nuovi rischi hanno generato un aumento della frequenza, della gravità e dell'impatto delle violazioni dei dati.

L'anno scorso, l'Unione europea ha adottato il Regolamento Generale sulla Protezione dei Dati (GDPR), che ha avuto importanti conseguenze per qualsiasi organizzazione che offra beni o servizi in UE. Il GDPR si applica a qualsiasi azienda che riceve dati nel corso delle proprie normali attività (come i provider di servizi cloud e i data centre), indipendentemente dal fatto che l'azienda o i dati si trovino nell'UE. Quasi tutti i data centre o le imprese che gestiscono dati, o che comunque sono presenti sul web, possono essere ritenute responsabili di una violazione delle informazioni di un cittadino dell'UE. Le sanzioni sono molto severe, pari al 2-4% del reddito annuo globale o a 20 milioni di euro, a seconda di quale sia la cifra maggiore tra le due.

"Nell'aprile 2018, presso un Interexchange Carrier di Chicago, alcuni pirati informatici hanno deviato il traffico da un servizio cloud ad un sito in Russia e violato la crittografia di un'azienda di cripto-valute. Gli hacker sono riusciti ad accumulare milioni di sterline nel loro portafoglio informatico. Questo evidenzia il problema del trasporto dei dati attraverso la rete, in quanto un server di terze parti, presso un Interexchange Carrier, non disponeva di una sicurezza adeguata ed è stato utilizzato per l'attacco. La sicurezza di alta qualità è l'unica difesa per i nuovi attacchi man-in-the-middle."

Poiché le autorità di regolamentazione globali stanno rispondendo all'urgente necessità di sicurezza delle informazioni, le aziende devono adottare una strategia coerente e olistica su tutta la loro infrastruttura tecnologica. Questo rende la rete un elemento chiave per garantire la sicurezza di qualsiasi azienda.

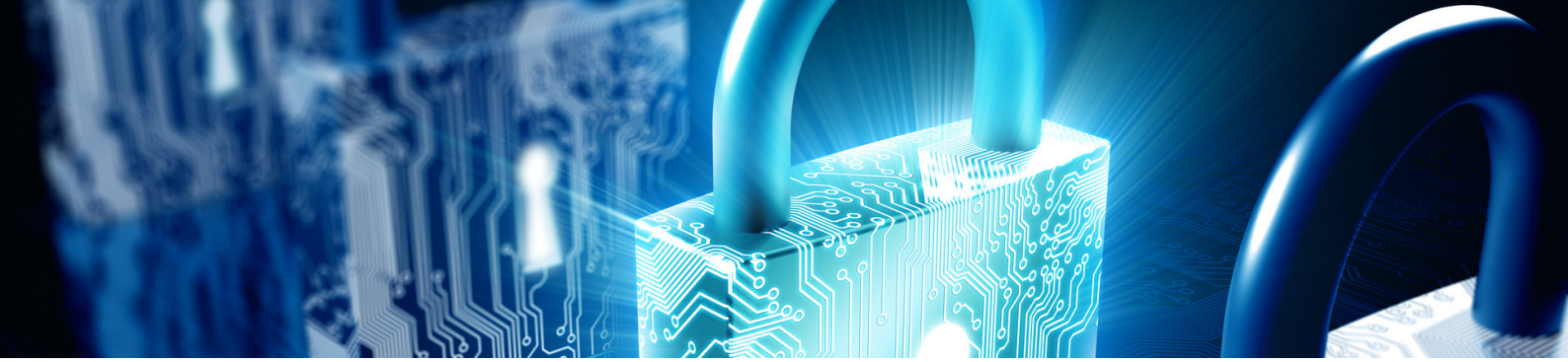
Ecco perché Colt ha lanciato Colt Ethernet Encryption, una nuova importante funzionalità add-on per i servizi Ethernet Line, che va ad integrare il Cybersecurity Programme di Colt, progettato per rispondere alla crescente necessità di soluzioni efficaci per la sicurezza di rete, viste le crescenti minacce e i nuovi requisiti normativi.

Ethernet Line Encryption: facile e sempre attiva

Disponibile in Europa, Nord America e Asia per circuiti Ethernet metropolitani, nazionali o internazionali, la soluzione fornisce una crittografia end-to-end con prestazioni ad alta velocità fino a 10G, chiavi gestite da Colt e supporto 24/7 fornito dal team di Service Assurance di Colt.

La crittografia della linea Ethernet è importante per qualsiasi azienda che gestisce informazioni sensibili, come:

- Istituzioni finanziarie che desiderano fornire una protezione di alta qualità alle filiali e agli sportelli automatici.
- Piazze borsistiche che necessitano di una crittografia di alta qualità e a bassissima latenza per le transazioni e le offerte
- Servizi governativi che devono garantire che i dati trasportati in rete siano protetti dagli attacchi di governi stranieri e che, per garantire il massimo della protezione, devono fare affidamento sulle tecniche di crittografia più avanzata
- Il settore delle utility, dove i dati critici vengono inviati da siti remoti
- Qualsiasi azienda che opera all'interno dell'UE o che dispone di una sede o di un'agenzia che accetta ordini dall'UE, come istituzioni finanziarie, agenzie di noleggio auto, rivenditori o compagnie aeree

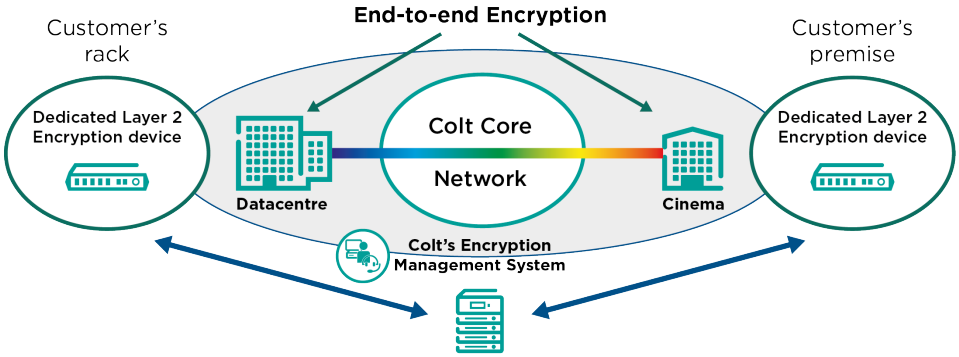


Il festival internazionale del cinema di Berlino

Dal 2009 Colt è Digital Cinema Partner della Berlinale e fornisce servizi di rete con larghezze di banda fino a 10 Gbit/s e accesso a Internet per una trasmissione dati di alta qualità. Nel 2019, il festival ha accolto 22.000 visitatori professionali, tra cui oltre 3.500 giornalisti provenienti da 82 Paesi, e ha venduto circa 335.000 biglietti per i partecipanti al festival, la più grande affluenza di pubblico di qualsiasi festival cinematografico annuale. Quest'anno Colt ha implementato una nuova soluzione live di Ethernet Line Encryption.

L'obiettivo era quello di garantire un circuito Ethernet da 1G tra il data centre Colt di Berlino, in cui sono in hosting i contenuti della Berlinale, e una sala cinematografica in cui veniva proiettato un film. I contenuti presenti sui server della Berlinale sono stati inviati alla sala in formato Digital Cinema Package (DCP) e criptati "in flight", per evitare qualsiasi perdita di dati, in quanto molti dei film proiettati all'evento sono anteprime mondiali. Questa crittografia non era quindi garantita solo a livello fisico all'interno del data centre, ma anche durante la trasmissione in rete per garantire un approccio olistico.

Colt è stata in grado di fornire una crittografia di ultima generazione, riducendo al minimo l'impatto sulle prestazioni del servizio Ethernet, con 11 µs di latenza extra ai due estremi della rete.

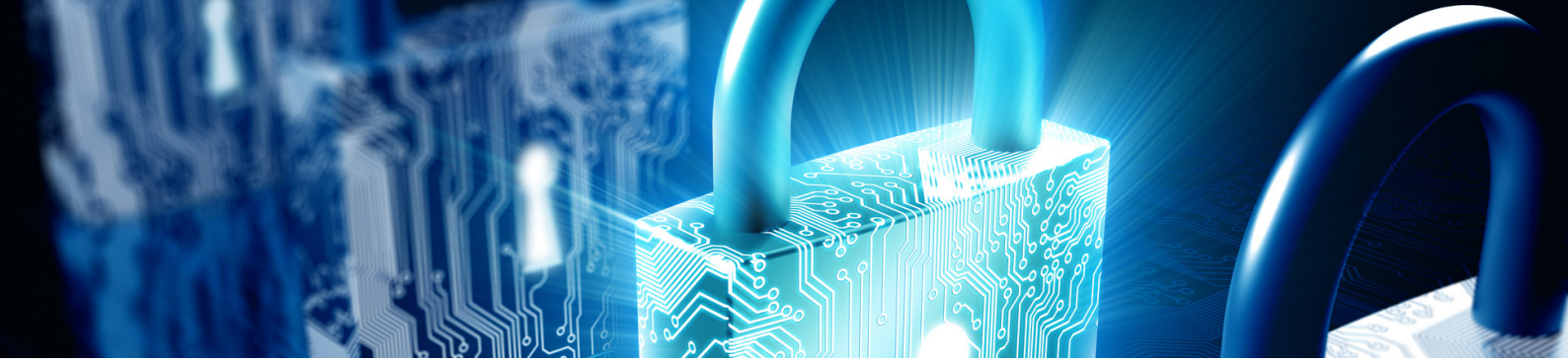


Altri casi d'uso di Ethernet Line Encryption

Azienda di assicurazione sanitaria con un'IP-VPN sicura

Problema: L'azienda in oggetto ha 152 filiali che devono soddisfare le normative UE come il GDPR, il Payment Card Industry Data Security Standard (PCI DSS) e la Sarbanes-Oxley Act per la trasmissione delle informazioni sui pazienti ai data centre. La rete aziendale deve supportare un'architettura ridondante.

Soluzione: L'azienda in oggetto è riuscita a supportare una capacità di dati mista di 10/50/100 Mbit/s attraverso servizi MPLS IP-VPN standard. La rete ha 152 siti che supportano tre diverse WAN. Tutti i siti hanno porte da 1GbE e il servizio di crittografia opera utilizzando tunnel MACsec+, configurati per essere conformi alle normative. Poiché l'intera infrastruttura Ethernet è crittografata, tutti i dati che attraversano la rete sono protetti.



Società di servizi finanziari con una rete aziendale globale

Problema: I servizi finanziari coprono un'ampia gamma di attività, tra cui: banca commerciale, retail e private banking, asset management, investment banking e gestione immobiliare. Tutti questi servizi implicano la conservazione e il trasferimento di informazioni altamente riservate.

Soluzione: Oltre all'evidente necessità di proteggere dati altamente sensibili, l'azienda doveva anche soddisfare i requisiti normativi del GDPR. Una rete aziendale con un layer 2 sicuro consente di fornire una rete diversificata che include larghezze di banda che possono variare da 10Mbit, a 1GbE e fino a 10GbE. Tutte le connessioni sono protette con la crittografia MACSec+ di layer 2, che garantisce la massima larghezza di banda con bassa latenza.

Ci si può fidare delle applicazioni per fornire la crittografia?

Per quanto riguarda i metodi di crittografia tradizionali, i nuovi rischi derivanti dall'informatica quantistica minacciano di rendere obsolete molte delle attuali tecniche di crittografia. Un tempo si pensava che i computer quantistici fossero lontani anni luce, ma ora si ritiene che saranno probabilmente disponibili entro i prossimi cinque anni. Infatti, a partire dal 2019, IBM lancerà un computer quantistico in modalità cloud.

Le applicazioni e i servizi cloud-based sono soluzioni basate su codici che si affidano a sviluppatori esterni, con un'ampia gamma di competenze in materia di crittografia. "Considerando i 20.000 servizi cloud attualmente in uso, solo 1 provider su 10 segue le migliori pratiche a livello di crittografia dei dati "a riposo" e di altri controlli di sicurezza di livello aziendale". Un dipendente medio, quando lavora, utilizza attivamente 36 servizi cloud. Per un'azienda, diventa quindi un problema enorme riuscire ad autorizzare ognuno di questi servizi di crittografia. La migliore pratica consiste nell'incapsulare i dati in movimento in una crittografia di rete protettiva. Il protocollo IPSec è stato un metodo efficace per proteggere la rete, ma non è stato progettato per supportare il moderno ambiente cloud, in cui i requisiti di latenza e larghezza di banda sono critici.

Nuovi standard sono attualmente in fase di sviluppo per rispondere a questa minaccia e inizieranno a essere disponibili nel 2022, per cui qualsiasi dispositivo di crittografia utilizzato in questo momento dovrà essere aggiornato. I prodotti di crittografia di rete ADVA saranno aggiornabili "sul campo" e sono progettati per supportare la maggiore potenza di elaborazione richiesta.

Powered by colt IQ Network

Per maggiori informazioni
visita www.colt.net/it

Tel: 800 909 319
E-mail: sales@colt.net

ADVA™