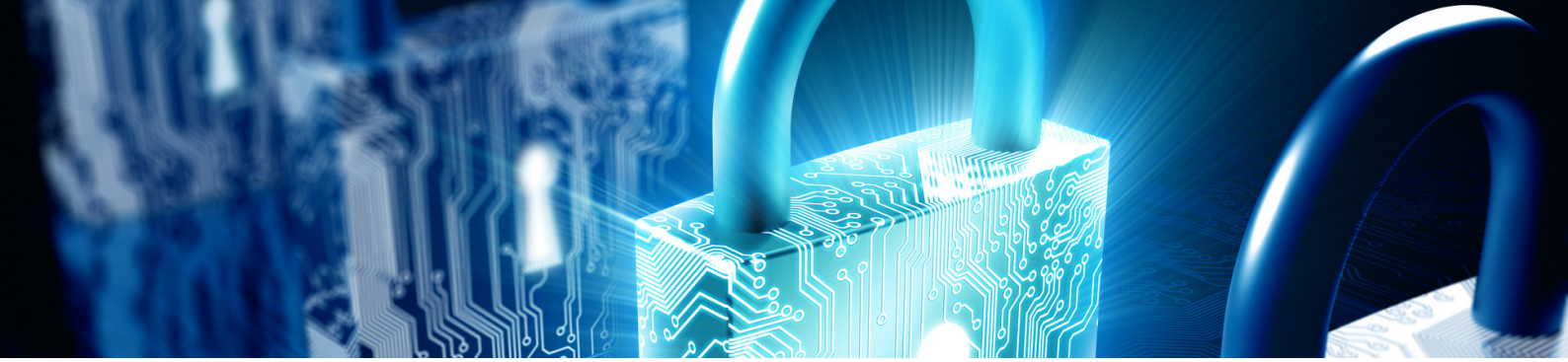
colt

Meeting the Ethernet security challenge

www.colt.net

ADVA™



Global IP traffic is predicted to increase threefold over the next 5 years, with more and more confidential and sensitive information now stored and transmitted. Data centre virtualisation has created an environment where protection parameters are no longer within the control of the data owner - interexchange carriers, multiple cloud hosts, and least-cost-routing algorithms add to the touch points in data transportation where security risks can be higher. These new risks have seen an increase in the frequency, severity and impact of data breaches.

Last year the European Union implemented the General Data Protection Regulation (GDPR), which impacts any organisation that offers goods or services in the EU. GDPR includes any third-party that receives data through the ordinary course of its operations (such as cloud providers and data centres), regardless of whether the company or data is in the EU. Almost any data centre or company that processes data, or has a web presence, can be held liable for a breach of information of an EU citizen. The fines are severe, either 2-4% of global annual revenue or 20 million Euros, whichever is higher.

"In April 2018 at a carrier Interexchange in Chicago, hackers diverted traffic from a cloud service to a site in Russia, including breaking the encryption of a crypto-currency company. The thieves had amassed millions of pounds in their cyber wallet. This highlights the problem of data being carried across the network, as a third-party server at the interexchange company did not have proper security and was used for the attack. High quality security is the only defense for new man-in-the-middle attack."

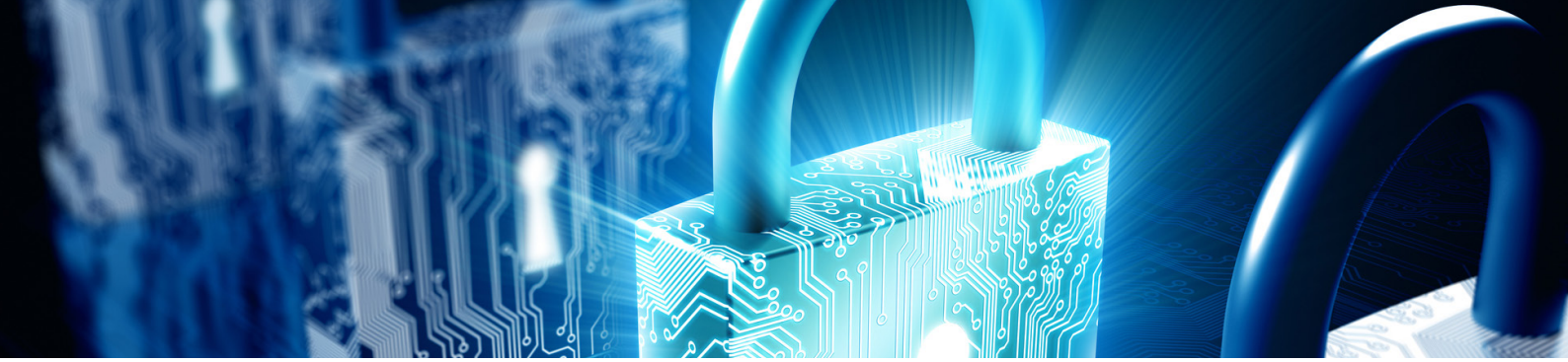
As global regulators address the pressing need for information security, businesses need to adopt a coherent and holistic strategy across their technology infrastructure. This makes the network a key element to secure for every company.

That's why Colt has launched Colt Ethernet Encryption; a significant new feature add-on for Ethernet Line services. It complements Colt's Cybersecurity Programme, designed to address the growing need for effective network security solutions, driven by increasing threats and new regulatory requirements.

Ethernet Line encryption: easy and always-on

Available in Europe, North-America and Asia for Metro, national or international Ethernet Line circuits, the solution provides end-to-end encryption for high speed performance up to 10G, keys that are Colt managed and 24x7 support from Colt's Service Assurance team.
Ethernet line encryption is relevant for any business dealing with sensitive information, such as:

- Financial institutions that wish to provide high quality protection to ATMs and branch offices
- Stock exchanges that need high quality and extremely low latency encryption for transactions and bids
- Government services that need to ensure the data carried in the network is protected from attacks from foreign governments and relying on state-of-the-art encryption to provide protection
- The utility industry, where critical data is sent from remote stations
- Any company that does business in the EU or has a storefront that accepts orders from the EU, such as financial institutions, car rental agencies, retailers or airlines

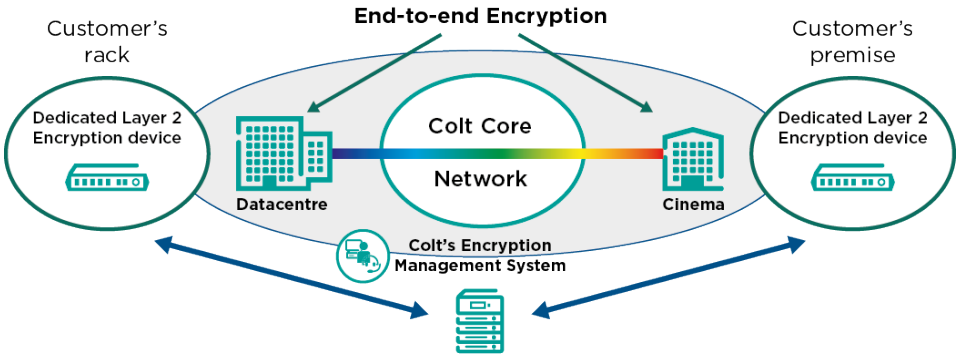


Berlin International Film Festival (aka Berlinale)

Since 2009, Colt has been a Digital Cinema Partner of the Berlinale, providing network services with high bandwidths of up to 10 Gbit/s and internet access to enable high-quality data transmission. In 2019, the festival welcomed 22,000 professional visitors including over 3,500 journalists from 82 countries and sold around 335,000 tickets to festival goers – the largest public attendance of any annual film festival. This year Colt deployed a live proof-of-concept for Ethernet Line Encryption.

The goal was to secure a 1G Ethernet Line circuit between Colt's Data centre in Berlin, where Berlinale is hosted, and a cinema where a film was displayed. The content hosted on the Berlinale servers was sent to the cinema in Digital Cinema Package (DCP) format and encrypted in flight, to avoid any leaks as many of the films shown at the event are worldwide previews. This encryption was not just at the physical layer in the data centre, but also when transmitted over the network to ensure a holistic approach.

Colt was able to provide state of the art encryption while minimising impact on the Ethernet service performance - just 11 µs extra latency was added on each end.

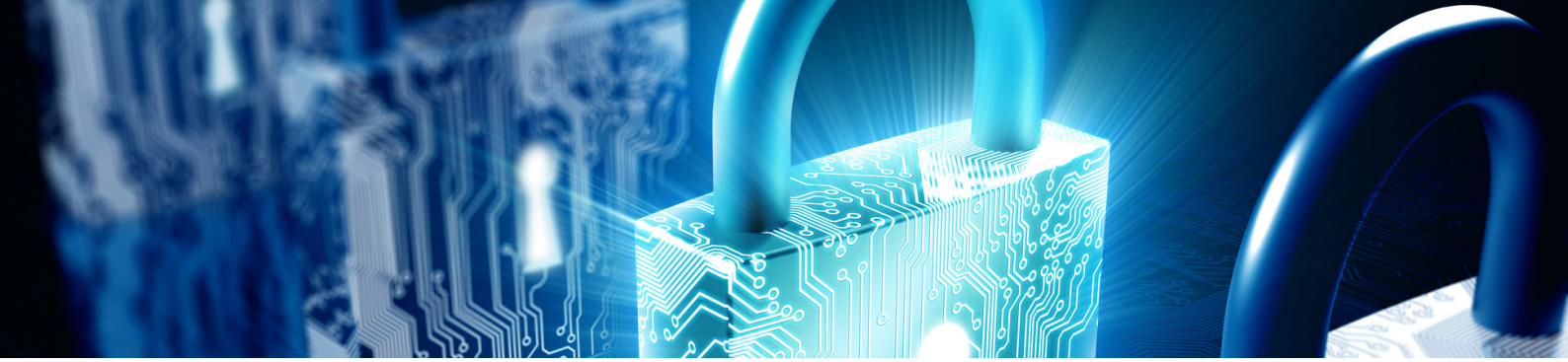


Other Ethernet Line Encryption use cases

Health insurance company with a secure IP-VPN

Problem: The Company has 152 branch offices that must meet EU regulations such as GDPR, the Payment Card Industry Data Security Standard (PCI DSS) and Sarbanes-Oxley (SOX) for transmitting patient information to data centres. The company's network has to support a redundant architecture.

Solution: The Company was able to support the mixed data capacity of 10/50/100 Mbit/s through standard IP-VPN MPLS services. The network has 152 sites supporting three separate WANs. All sites have 1GbE ports and the encryption service operates using MACsec+ tunnels, setup to meet compliance regulations. Since the entire Ethernet Frame is encrypted, all data flowing through the network is protected.



Financial service company with a global corporate network

Problem: Financial services cover a wide range of activities including; commercial, retail and private banking, asset management, investment banking and real estate management. All of these involve the storage and transfer of highly confidential information.

Solution: Besides the obvious need to protect highly sensitive data, the company also had to meet the regulatory requirements of GDPR. A secure layer 2 corporate network allows them to provide a diverse network that includes 10Mbit-1GbE-10GbE bandwidth. All connections are protected with layer 2 MACSec+ encryption, which guarantees maximum bandwidth with low latency.

Can you rely on applications to provide encryption?

New risks to traditional encryption methods from quantum computing threaten to render many of today's encryption techniques obsolete. Quantum computers were once thought to be decades away but are now likely to be available in the next five years – as of 2019 IBM now offers a cloud-based quantum computer.

Applications and cloud based services are code based solutions that rely on third party developers with a variety of expertise on encryption. "Of the 20,000 cloud services in use today, only 1 in 10 of the providers follow the industry's best practice of encrypting data at rest and other enterprise-grade security controls." The average employee actively uses 36 cloud services at work. It is an overwhelming problem for an enterprise to be able to validate each of these services encryption. The best practice is to encapsulate the data-in-motion in a network protective encryption. IPSec has been a legacy method of providing network protection but is not designed to support the modern cloud environment where latency and bandwidth requirements are critical.

New standards are being developed to meet this threat and will start to be released in 2022, so any encryption device deployed today must be able to upgrade. ADVA networking encryption products will be field upgradeable and are engineered to support the higher processing power that will be required.

Powered by colt IQ Network

For more information
visit www.colt.net

Tel: +44 (0)20 7863 5510
E-mail: sales@colt.net

ADVA™