Product Brief

Cloud Connect Encryptor

Full customer control from security policy to key management

cpl.thalesgroup.com

THALES
Building a future we can all trust

High-speed encryption within the cloud; providing maximum data protection for cloud computing and storage. The Cloud Connect Encryptor from Thales is a high-performance solution that enables the secure movement of data to, from and within cloud infrastructure. It delivers FIPS certified end-to-end encryption of data among enterprise premises and cloud computing and storage services and features seamless integration of Thales hardware and software encryption appliances; creating a single, trusted platform for maximum data security.

A dedicated, mixed network encryption solution, the Cloud Connect Encryptor is designed to protect enterprise network links and cloud computing and storage services without compromising performance. Transport Independent Encryption (TIM) provides maximum security for all network types and topologies, without the performance penalties associated with IPsec and VPN, and without the vulnerabilities associated with dual-purpose network appliances.

Customer Convenience

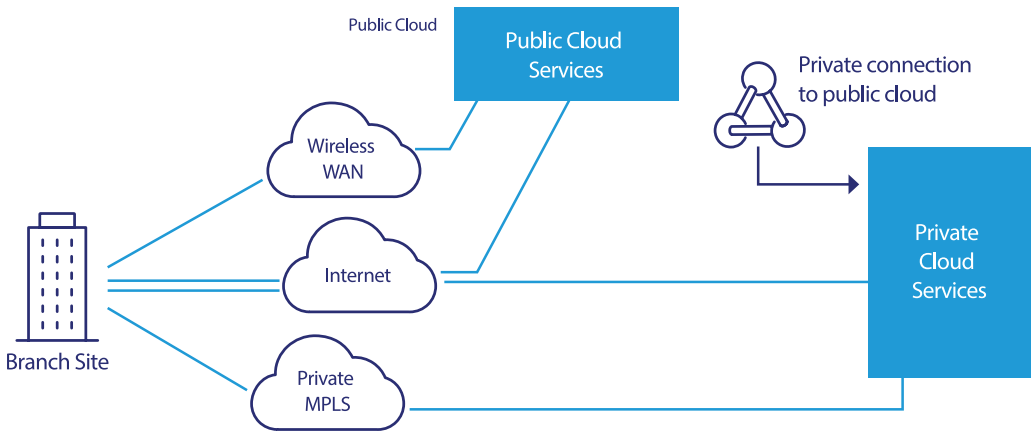
Customers already using Thales High Speed Encryptors for on-premises applications, such as data center interconnection, multi-location data links and other network security needs, can easily add the Cloud Connect Encryptor. As simple as adding another encryptor, the Cloud Connect Encryptor will expand data protection to/within/from the cloud for secure cloud computing and storage.

Shared responsibility

The cloud shared responsibility model means that while cloud providers are responsible for infrastructure security, customers remain responsible for their own data security. Customers are responsible for the security of data both in the cloud and as it travels to/from the cloud.

With the Cloud Connect Encryptor, customers can leverage the industry leading high-speed encryption platform as a unified, cloud-native solution to protect data as it moves across critical infrastructure (to and from data centres, office locations and cloud computing and storage service providers) and bring Thales' benefits of low-latency, tunnel free encryption to the cloud.

Most modern IT infrastructure comprises a complex mix of both public and private networks that are connected to both public and private cloud computing and storage environments. The challenge is to implement a solution that can meet the diverse security and compliance needs of these hybrid environments without compromising on performance or availability.



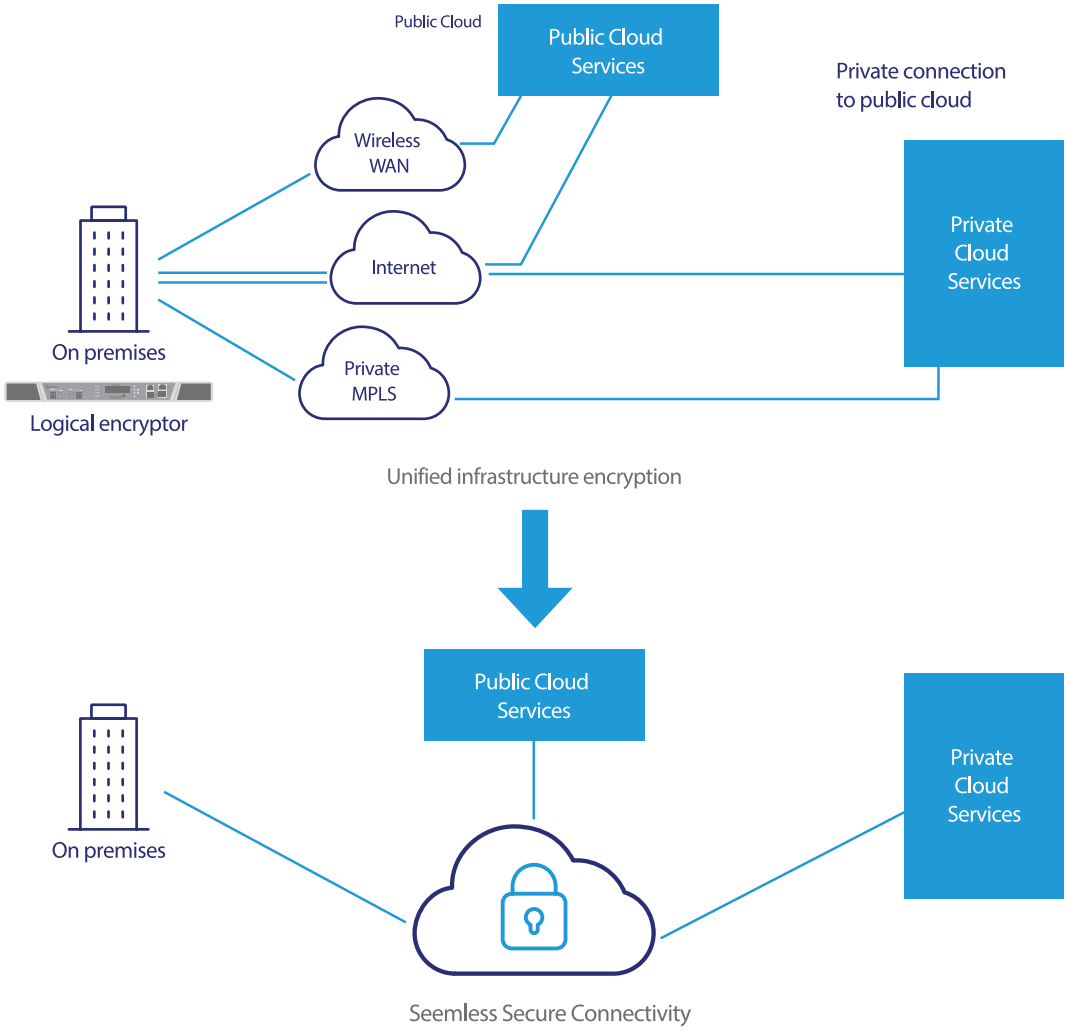
Cloud computing and Storage Services

Cloud Connect Encryptor supports Microsoft Azure and Amazon Web Services public cloud computing and storage.

Cloud Connect Encryptor's seamlessly integrated encryption platform is made up of dedicated physical and logical encryption. It enables multiple network layer security to/from, within and among multiple cloud computing and storage resources wherever they are located.

With the introduction of the Cloud Connect Encryptor, customers have a single, unified solution that can secure all touchpoints:

- High-speed data center interconnections
- Physical office to branch office connections
- Secure public cloud computing and storage access (single or multiple)



Thales Cloud Connect Encryptor

Key Features

The Cloud Connect Encryptor is a specific type of high-speed encryption (HSE) solution that is used to send encrypted traffic between a cloud solution provider and an office location over the public internet. It also enables encrypted traffic between Virtual Private Clouds (VPC) inside the cloud provider's network.

- Implemented as a cloud native Virtual Machine (VM)
- Supports Microsoft Azure and AWS (Amazon Web Services)
- Easy to deploy, scale and manage
- Ensures the authenticity, integrity and privacy of data transmitted:
  - to the cloud from on-premises
  - within a provider's cloud environment
  - between different cloud providers
- The Cloud Connect Encryptor authenticates and encrypts data in transit at one or more network layers. All VM-to-VM traffic within a VPC network and peered VPC networks is encrypted
- Encryption protects data if it is intercepted between site locations and the cloud provider or between cloud services
- Full interoperability with CN Series physical and CV Series virtualised encryptors with HSE physical and virtual appliances

Technical Information

- Transport Independent Mode
  - Encrypts traffic at Layers 2, 3 and 4
  - Efficient tunnel-free encryption
- DPDK accelerated
- Software requires minimum 4 vCPUs and 2Gb RAM
- Supports AWS Gateway Load Balancer
  - Uses GENEVE encapsulation for high-performance connections to virtual encryptors in AWS
  - Allows greatly increased secure traffic volumes in/out of AWS
  - Allows horizontal elastic scaling and load balancing across a fleet of virtual encryptors

About Thales

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world, rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centres to devices and across networks. As the global leader in data security, identity & access management, and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us