Secure high-speed connectivity

Protecting critical data in motion without compromise

ADVA™
Optical Networking

Data security is a growing concern

Enterprises of all sizes are adopting cloud-based applications, in which company data constantly interacts with customers, partners and suppliers and where the cloud architecture takes on an important role. As a result, more and more sensitive data is flowing outside of the traditional enterprise perimeter.

Cloud and distributed server, storage and backup systems are gaining more traction in almost every industry vertical. With sensitive data increasingly being sent to the cloud, IT professionals must reconsider data security. Insufficient data protection can put a company's ultimate value at risk. At the same time, cybercrime and cyber-espionage is set to intensify, and the regulatory environment consequently demands more focus on data security.

Securing data in motion is critical

Fiber-optic networks provide the physical infrastructure to transport important and large volumes of data over metro and long distances across the globe. They have long been considered the fastest and most secure method of moving information.

With cybercrime and espionage on the rise, fiber-optic networks have become increasingly vulnerable and all industries are falling victim. Industry research reports conducted by organizations such as the Ponemon Institute underline that the financial consequence of a cyber-attack is worsening and securing data in motion must be considered in the security plans for every organization. Focusing on the security of enterprise internal network resources alone is no longer sufficient.

Big data faces big challenges

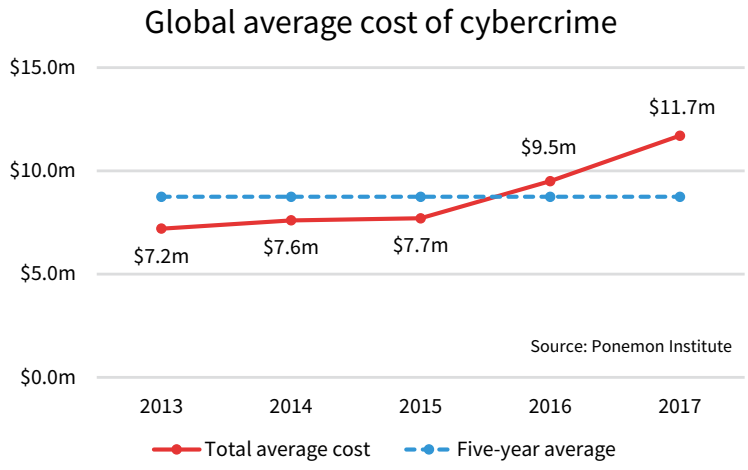
Encryption is the most effective way to increase the level of security and safeguard external network connections against unauthorized access. Network infrastructure solutions providing secure and scalable connectivity between points of presence and cloud locations are therefore at the heart of every data security architecture.

With encryption becoming a core capacity for organizations to safeguard sensitive assets and sustain compliance with regulatory mandates, the availability of secure and easy-to-operate high-speed transmission solutions is elementary to building a sustainable security foundation.

Protecting data wherever it is in the network

Securing data in motion by encryption at the connectivity network layer ensures superior network performance, simplifies network operations and reduces the overall cost of data protection. Data encryption at the lowest network layer also protects data at all layers in the network stack, as everything must flow through the connectivity layer before going anywhere else.

ADVA offers field-proven and widely deployed optical and packed-based solutions for site connectivity and access to the cloud. The ADVA ConnectGuard™ security portfolio is designed to safeguard traffic on any connectivity network layer while ensuring confidentiality and integrity with the highest transmission performance.



Your data has never been so vulnerable

Optical networking for secure communications

Data security is not a single feature but rather an increasingly important set of technologies used to safeguard private data sent across both public and private networks. The proliferation of data requiring protection means there is more data at risk of being compromised than ever before. The innovative ADVA ConnectGuard™ Optical technology available on the FSP 3000 platform enables data to be transported securely with the highest performance and lowest cost.

Encryption at the speed of light

ADVA ConnectGuard™ Optical network encryption is optimized for high-speed data center interconnect and enterprise connectivity applications requiring maximum data security on the network when connecting dispersed locations. It provides a transparent, wire-speed service using Advanced Encryption Standard (AES). Dynamic key exchange and a strictly separated encryption domain manager make the solution compliant to the most stringent regulatory requirements.

Hardware-based network encryption delivers maximum efficiency at ultra-low latency and carries a wide variety of protocols including Ethernet, Fibre Channel and InfiniBand in mission-critical applications. ADVA ConnectGuard™ Optical on the FSP 3000 guarantees optimum network security, highest availability and complies with national and international security standards such as requirements defined by the German Federal Office for Information Security (BSI) and Federal Information Processing Standards (FIPS).

Secure business continuity and disaster recovery

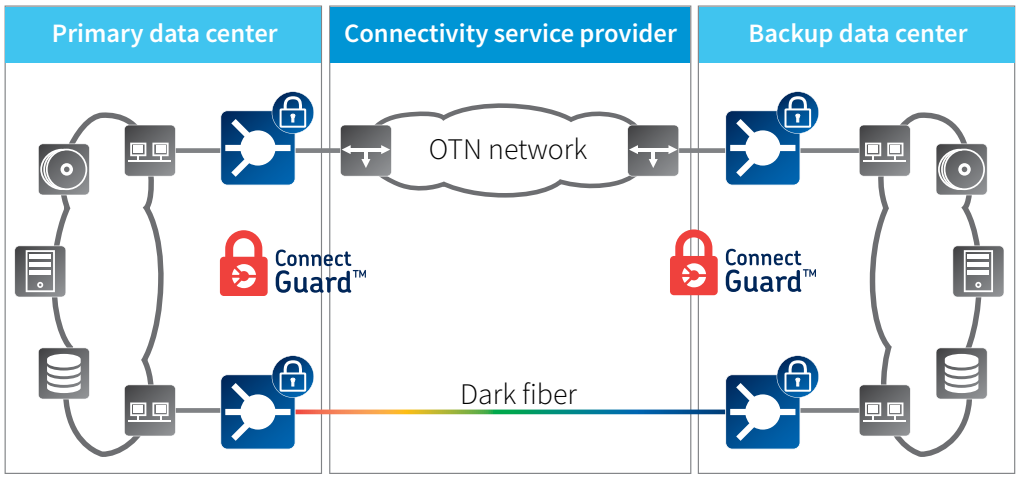
With General Data Protection Regulation (GDPR) and other regulatory requirements taking effect in 2018, an increasing number of industry verticals such as the financial sector, healthcare, government agencies and military institutions, require maximum network security when transmitting private information between data centers for disaster recovery and business continuity operations.

ADVA ConnectGuard™ Optical physical layer encryption is the safest method to protect information and guarantee data integrity with regards to latency and throughput. Network encryption on the physical layer is as powerful as it is reliable to securely connect high-performance data centers and maintain superior application performance for all networking protocols.

Secure managed wavelength services

With an increasing number of enterprises focused on regulatory compliance and placing more value on the security of their intellectual property, there is significant growth of interest in high-speed, secure data connectivity services provided by managed service providers.

ADVA ConnectGuard™ Optical simplifies the deployment of secure optical transport services for enterprises by combining market-leading optical transport with powerful encryption on a single, integrated infrastructure. Strictly separating management of the encryption domain from network management enables managed service customers to control their own encryption domain and provides them real-time awareness of potential security alerts.



Our FSP 3000 with ConnectGuard™ encryption is proven and certified for maximum security

Secure data transmission over Carrier Ethernet

Carrier Ethernet networks can be secured and encrypted without any loss of speed and performance. Compared to IPsec, Carrier Ethernet encryption is better suited to modern virtual private network environments, is simpler to administer, scales to larger settings and can boost network performance by up to 50%.

ADVA ConnectGuard™ Ethernet technology available on the FSP 150 platform provides network service providers plenty of opportunity for differentiation through service security in addition to end-to-end service level agreements and bandwidth on demand. For enterprises and government institutions, ADVA ConnectGuard™ Ethernet enables the transformation of traditional Carrier Ethernet leased lines into secure and encrypted connectivity.

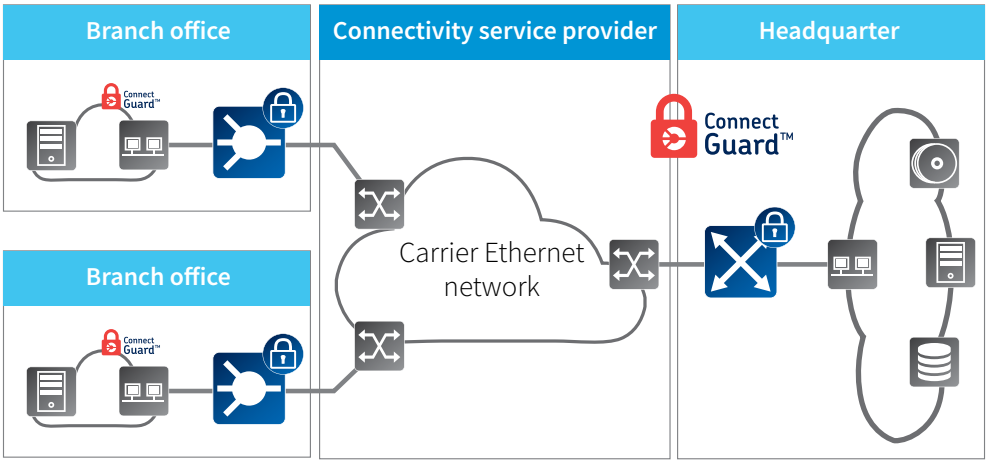
Assurance and control at Layer 2

The introduction of virtual private Carrier Ethernet services enables separation and isolation of data by a tag or a label that network elements utilize for data forwarding. Although the individual enterprise sees a logically private network service, that service still runs on a shared infrastructure. A virtual private network service is misleading in the sense that it is not a synonym for data security.

By enhancing the market-leading FSP 150 Carrier Ethernet access platform with ADVA ConnectGuard™ Ethernet encryption, service providers and enterprises now can deploy intelligent Carrier Ethernet services compliant to MEF CE 2.0 while guaranteeing end-to-end data security. In contrast to traditional Ethernet encryption appliances, ADVA ConnectGuard™ Ethernet can actively benefit from all service assurance and testing functionalities available on the FSP 150. Performance testing at service turn-up and pro-active in-service monitoring can dramatically increase reliability of secure connectivity services between enterprise locations.

ADVA ConnectGuard™ Ethernet benefits

- Encrypted Carrier Ethernet services at 1Gbit/s and 10Gbit/s line speed
- Port- and VLAN-based security domain assignment compliant with MEF CE 2.0
- Complete set of Carrier Ethernet CFM and OAM functions for service monitoring and testing
- Advanced cryptographic methods including dynamic key exchange and tamper protection



With ConnectGuard™ Ethernet, our FSP 150 transforms traditional Carrier Ethernet into encrypted connectivity

Secure cloud connectivity

Multi-cloud environments provide enterprises the ability to mix and match private clouds with multiple public clouds. The “multi” in multi-cloud raises the importance of securing connectivity between and among those clouds. The “cloud” aspect also adds complexity to achieving that security. You can’t march into a data center owned by AWS, Azure or IBM and demand to install your encryption appliance to protect your links. A new approach is needed.

Security in a virtualized world

As enterprises move applications to the cloud, they often employ the internet for connectivity. Using the public internet for transmission of sensitive corporate data opens the door to a new set of attacks. As a result, enterprises are looking to encrypt data in motion to prevent unwanted loss of confidential information.

Today, enterprises mostly use dedicated encryption appliances. However, appliance-based encryption is typically not suitable for cloud applications, because it can’t be placed in a public data center. Any encryption solution today must address hybrid cloud and multi-cloud applications.

Current best practices are insufficient

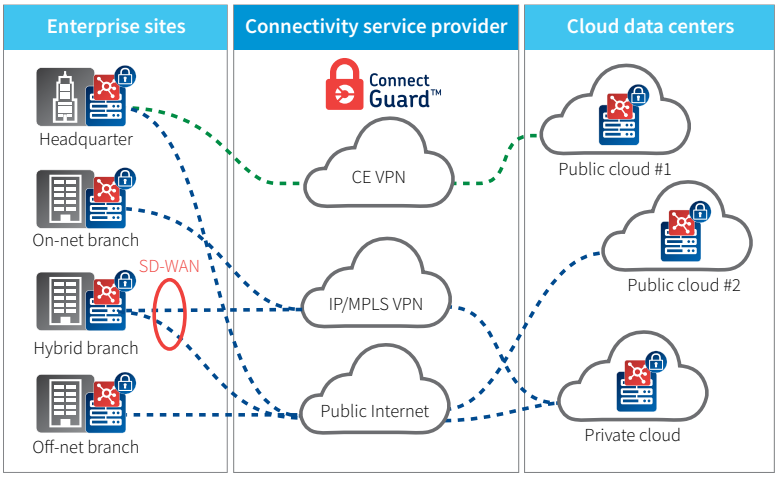
For encrypted data in motion using internet connections, the current best practices are insufficient. One option is to use IPsec encryption in the cloud infrastructure, but IPsec is inefficient. It incurs the further penalty of increased bandwidth used due to encapsulation, especially for bridged traffic and increased cloud compute usage for IPsec itself. Relying on application-level security is another option, but it puts the onus on developers, who may not be security experts, to adhere to security standards.

Bringing the cloud to the telco network

Ensemble’s secure cloud connectivity provides an alternative approach to address the encryption challenge. ConnectGuard™ Cloud is a purely software-based method of encryption. Enterprises can address site-to-site and site-to-cloud encryption requirements with a single solution, whether the endpoints are small branches, headquarters sites or data centers. Security can now be maintained whether the transport is on-net or off-net, public or private, or at Layer 2 or Layer 3.

ConnectGuard™ Cloud harnesses the power of NFV to extend networking, simplify operations and maximize choice. It extends encryption into the cloud and small branches by leveraging low-cost universal CPE (uCPE) platforms. It provides a cloud-native virtualized solution for encrypting WAN connections from 10Mbit/s on low-end platforms up to 10Gbit/s.

Virtualized encryption that can have virtualized endpoints enables deployment as a virtual machine in all popular public clouds for secure links from the enterprise to one or more clouds in parallel. In addition, the cloud deployment is within the Layer 2 broadcast domain of the enterprise’s cloud applications, not at some distant VPN gateway location, guaranteeing end-to-end encryption. Fast turn-up and low cost is provided by zero touch provisioning (ZTP), eliminating errors and the need for on-site support.



Scalable virtualized encryption protection at a fraction of the bandwidth and latency costs of IPsec

Scalable security domain management

Complementing connectivity networks with sophisticated security controls brings a set of technology and process management challenges that make it difficult for network administrators to provide a consistent approach to both network and security management. What's more, deploying, managing and maintaining security technology in an environment driven by headcount reduction and redirection dramatically increases the potential for human error, which can lead to security exposures and incidents.

To counter security management challenges faced by organizations today, operators and administrators need to focus on making encryption of data in motion and its management as simple and scalable as possible while implementing robust security architecture.

Effective, simple and affordable

In-depth end-to-end visibility is fundamental to help administrators with rapid detection and troubleshooting of security events. Our ADVA ConnectGuard™ Management solution provides advanced, end-to-end security management that facilitates event management and reporting, delivering an overview on priority security aspects that an administrator needs to be aware of.

All key features of ADVA ConnectGuard™ Management are designed for simplicity and efficiency, ensuring that organizations can effectively defend themselves against today's advanced threats. The user-friendly and flexible design of authentication and key management procedures helps organizations benefit from its options for security management and supports the deployment of all ADVA ConnectGuard™ technologies across large-scale networks.

Openness for a secure world

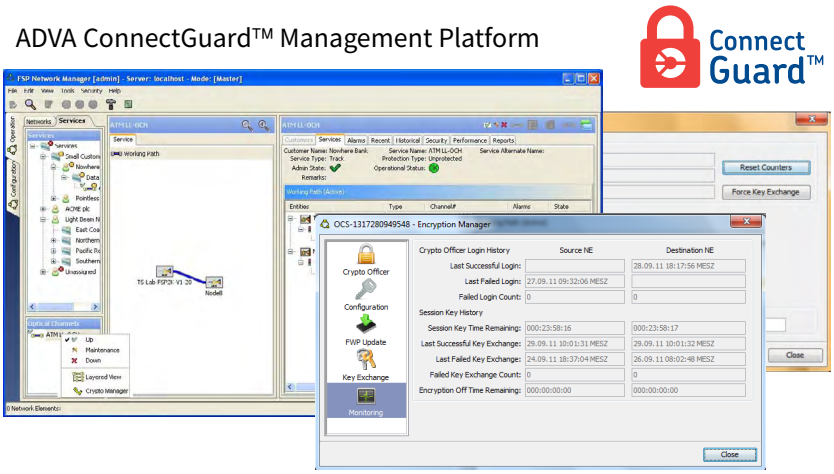
Our ADVA ConnectGuard™ solutions support extensible communication protocols such as Key Management Interoperability Protocol (KMIP) for simplified interfacing with external key management platforms and deeper integration into Public Key Infrastructure (PKI). Depending on an enterprise's needs, key lifecycle processes can be centralized if required or remain fully automated and integrated on any ADVA ConnectGuard™ encryption platform.

Enabling encryption as a service

ADVA ConnectGuard™ Management revolutionizes the delivery of encryption as a service. Partitioning encryption management from connectivity management allows added flexibility in either an operator- or enterprise-maintained infrastructure.

Strict role partitioning from encryption management by complete separation of privileges between administrators from the connectivity domain and those from the security domain helps security departments maintain full control of the security environment and comply with national and international regulatory requirements such as GDPR.

ADVA ConnectGuard™ Management Platform



A firm foundation for secure authentication, provisioning and configuration of network security

Secure connectivity across all networks

ADVA ConnectGuard™ provides a comprehensive state-of-the-art security infrastructure for all connectivity applications as an integrated, ready-to-run and fully automated solution. Our extensive ConnectGuard™ Optical solution on the FSP 3000 for disaster recovery and business continuity applications, ConnectGuard™ Ethernet on the FSP 150 for protecting data transported via Ethernet against espionage and manipulation and our ConnectGuard™ Cloud technology fully integrated with the Ensemble Connector for virtualized, cloud-based applications are designed to meet highest security requirements.

All ADVA ConnectGuard™ implementations operate transparently to the network infrastructure, which ensures that data is encrypted without impacting network performance and enables easy integration into any existing network.

Don’t leave your sensitive data unprotected

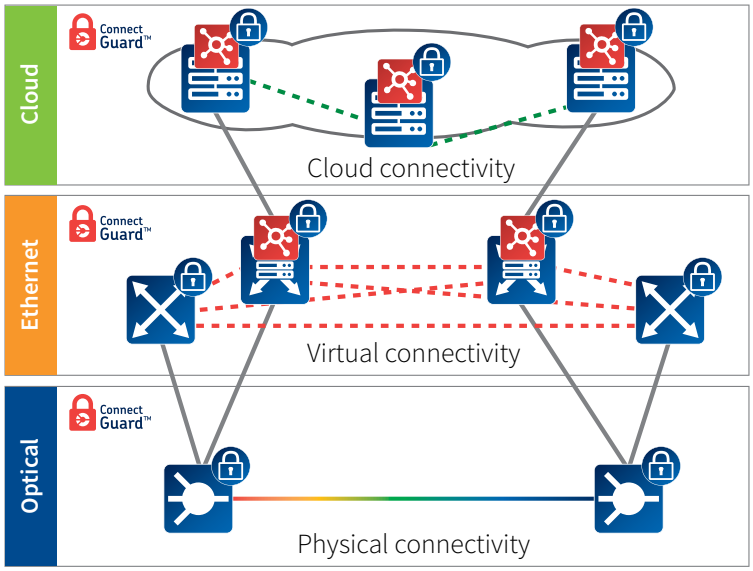
With our ADVA ConnectGuard™ encryption solution, your organization is empowered to meet immediate data protection and business needs now, while investing in a hardware- or software-based connectivity platform that provides robust security and the scalability you need to build a trusted framework for the future.

Strong authentication, flexible key management and high-performance encryption help to secure and control access to your high-value information. ADVA ConnectGuard™ ensures that your sensitive data in motion is never at risk.

Unmatched security and versatility

Whether you need to protect your intellectual property, your business is subject to regulatory requirements or you wish to strengthen your security architecture overall, ADVA ConnectGuard™ offers you the flexibility to secure your enterprise connectivity across all networks.

Our choice of integrated hardware implementations and software-based virtualized encryption helps to secure your big data frameworks and ensures secure migration of sensitive information to the cloud. Strict partitioning of encryption management from connectivity management ensures that your designated security officer will be the sole owner and manager of encryption keys and policies.



Effective protection of cloud and site-to-site connections against eavesdropping at all speeds

For more information
ADVA Optical Networking SE
Campus Martinsried
Fraunhoferstrasse 9 a
82152 Martinsried / Munich
Germany

ADVA Optical Networking North America, Inc.
5755 Peachtree Industrial Blvd.
Norcross, Georgia 30092
USA

ADVA Optical Networking Singapore Pte. Ltd.
25 International Business Park
#05–106 German Centre
Singapore 609916

Version 05 / 2018

About ADVA Optical Networking
ADVA Optical Networking is a company founded on innovation and driven to help our customers succeed. For over two decades our technology has empowered networks across the globe. We're continually developing breakthrough hardware and software that leads the networking industry and creates new business opportunities. It's these open connectivity solutions that enable our customers to deliver the cloud and mobile services that are vital to today's society and for imagining new tomorrows. Together, we're building a truly connected and sustainable future. For more information on how we can help you, please visit us at: www.advaoptical.com.

ADVA™
Optical Networking