

Encrypted wavelengths accelerate and protect the application-driven network

As enterprises undergo digital transformation, cutting-edge applications and massive workloads are generating huge amounts of data that must be moved between geographically distributed data centers and cloud environments. Because consumers of that data expect a high level of reliability and performance, enterprises are rearchitecting their networks and deploying fiber optic links to increase data speeds not only in the core network, but at the edge as well.

Content

Security challenges..... 2

Protecting data in motion:
Optical layer encryption..... 3

The CenturyLink solution 4

Conclusion 5

The journey to digital transformation is far from complete. According to a recent survey, 62 percent of IT leaders say digital transformation is very important but only 25 percent say it's widely adopted.¹

At the same time, cyber attacks are increasing in number and variety. Phishing, ransomware, virus and distributed denial of service (DDoS) attacks are multiplying, and malicious actors are sometimes using them in combination to circumvent defenses in new and destructive ways.

The increase in threat activity is driving up costs. Not only are many organizations paying ransomware fees, but many are paying legal settlements to customers whose credit cards and personally identifiable information (PII) have been compromised.

¹CenturyLink and TechTarget, *Make Your Enterprise Network a Top Priority for Hybrid IT*, 2016.

The cost of protecting data is increasing. Organizations are implementing defense in depth strategies, including encryption for data both at rest and in transit. According to Gartner, “through 2020, driven by the increasing risk of a data breach, more than 50% of enterprises will purchase enterprise-wide encryption products, which is a significant increase from fewer than 20% today.”²

Corporate leaders are aware of the dangers, but must weigh difficult choices between the cost of protection and their ability to carry out strategic business transformation initiatives.

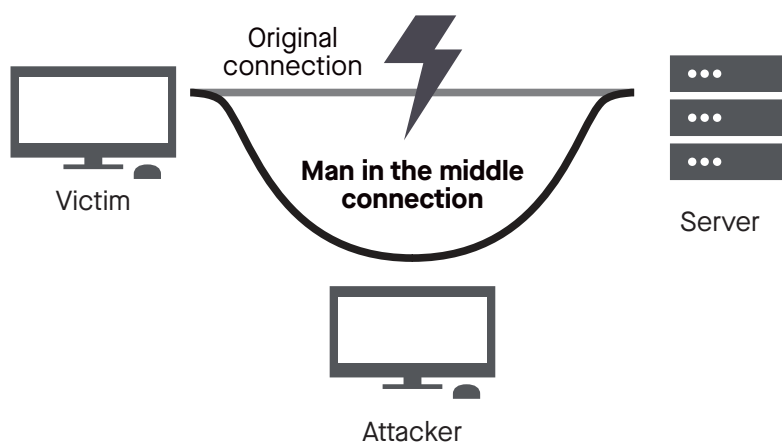
Security challenges

Moving data across global networks is essential for many digital strategies, but doing so exposes the data stream to such threats as man in the middle (MITM) attacks. In these attacks, an actor makes it appear to both parties that a trustworthy connection has been established between them. When data is sent, it is intercepted by the actor, although both parties believe that nothing is amiss. The use of cloud-based services increases MITM vulnerability. Each time data is sent to and from those services, it leaves an organization’s network, exposing it to malicious actors.

Although every organization must protect its data, organizations in fields such as financial services, health care, utilities and government face particular challenges. These organizations not only handle proprietary internal data, but also handle PII from a multitude of customers.

Because many of these organizations are in highly regulated industries, they must conform to guidelines and periodically perform compliance audits. In health care, Health Insurance Portability and Accountability Act (HIPAA) regulations mandate that patient information be safeguarded. In financial services, Payment Card Industry (PCI) guidelines specify how credit card data must be protected. Companies doing business in Europe must comply with the General Data Protection Regulation (GDPR), which is designed to shield PII. And companies in regulated industries bear the burden of higher costs. The average cost per record in highly regulated industries is 20 percent higher than the average, according to a recent Ponemon Institute study.³

Federal government agencies, meanwhile, are subject to technology regulations including the Federal Infrastructure Processing Standard (FIPS), Critical Infrastructure Protection (CIP) and Common Criteria (CC) for Information Technology Security Evaluation, all of which contain rules for implementing data security measures.



A MITM attack diverts traffic to a malicious actor, while making the connection appear trustworthy to victims.

²Gartner, *Prioritize Enterprise wide Encryption for Critical Datasets*, June 28, 2017.

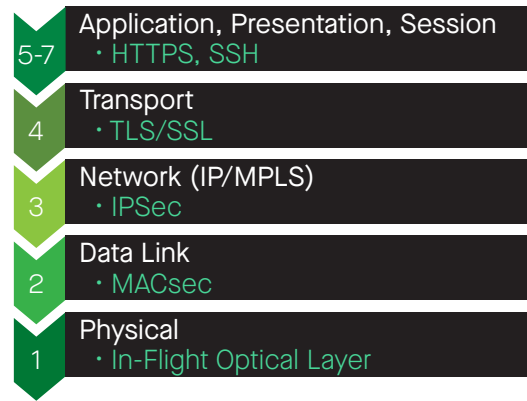
³Ponemon Institute, LLC, sponsored by IBM, *Cost of Data Breach Study*, 2016.

Protecting data in motion: optical layer encryption

To protect data in flight, many organizations have deployed VPN technology, including the IPsec encryption protocol suite. Although effective in protecting data, IPsec, which operates at the network layer (Layer 3), is complex and significantly enlarges the header of Ethernet packets. Implementing IPsec also requires the deployment of complex key management technology that can present management challenges to many organizations. And IPsec implementation typically requires the use of a dedicated encryption engine.

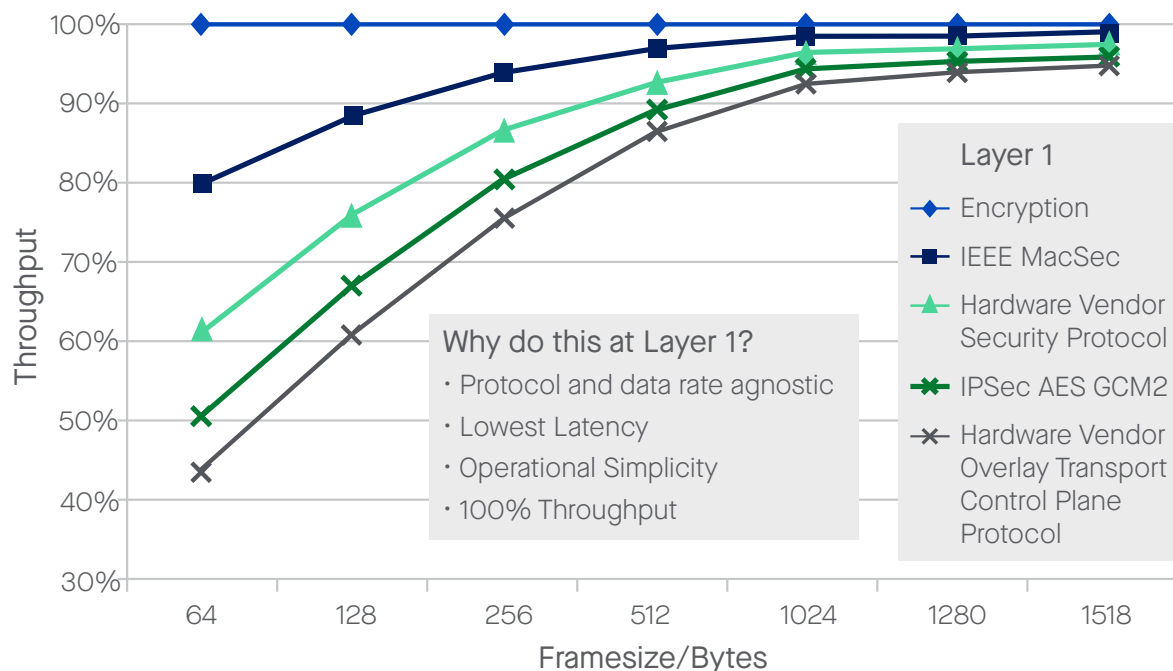
Another security protocol suite, MACsec, may be used in addition to IPsec. Less complex than IPsec, MACsec works at the media access control (MAC) layer (a sublayer of the data link layer, which sits between the physical layer and the network layer).

The increased packet size required by IPsec, with or without MACsec, generates bandwidth inefficiency, which is multiplied as data quantities increase, leading to network performance degradation and unacceptable levels of latency. As enterprises increase bandwidth to overcome these problems, costs also increase, which can throw budgets out of alignment and adversely impact corporate financial results.



There are many reasons to protect data in flight at the physical layer.

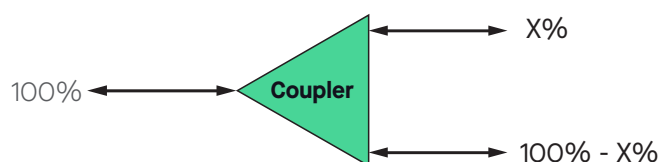
Despite these challenges, organizations are unlikely to do away with VPN technology and its encryption protocols. But to improve performance and cut costs when moving large amounts of data between enterprise and cloud-based data centers, organizations should consider replacing VPN and IPsec technology where possible with wavelength encryption across fiber optic networks.



Encryption may be implemented in any of several different layers.
Wavelength encryption at the physical layer requires very small overhead and latency.

Wavelength encryption works at the physical layer (Layer 1), with very small overhead and latency that can be measured in nanoseconds (billionths of a second). In contrast, the overhead and latency introduced by IPsec is measured in milliseconds (thousandths of a second). As a result of this performance advantage, wavelength encryption delivers significantly lower cost per encrypted bits per second than IPsec. In addition, it is possible to implement wavelength encryption through protocol agnostic, general purpose hardware, rather than a dedicated encryption engine. This also simplifies deployment and generates savings.

Companies often believe the encryption of Layer 1 traffic over fiber is unnecessary because in the past, fiber was difficult to reach and the technology to tap into it was prohibitively expensive. But tapping equipment is now cheap and easy to access, and the knowledge of how to tap fiber links has become widespread. Demonstration videos are widely available, featuring experts like well-known hacker Kevin Mitnick.⁴



However, organizations deploying wavelength encryption until now have been faced with the challenges inherent in a do-it-yourself solution. Typically, this includes buying the dense wavelength division multiplexing (DWDM) encrypted waves platform and the associated key management tools, then deploying, managing, maintaining and upgrading the resulting infrastructure.

The CenturyLink solution

CenturyLink® Encrypted Wavelength Service delivers these key benefits:

- Low-latency and low overhead with line speeds up to 100G bit/sec
- Purpose-built key management portal that remains under customer control
- Certified compliance with regulatory guidelines such as FIPS 140-2 and CC EAL-2, in 2018
- CenturyLink's bookended encrypted wave service mitigates the deployment of special purpose on-premises equipment
- Provide clients with a monthly operating expense, rather than a large capital expenditure

⁴YouTube, Kevin Mitnick explains how to hack fiber optic and steal sensitive data, August 28, 2015.



Conclusion

In the era of digital business, organizations are sending and receiving greater quantities of data than ever. This data often must be sent between widely separate data centers, both on-premises and in the cloud, across the globe. With security threats such as MITM attacks increasing, encryption in transit is essential, but the IPsec and MACsec protocol suites can be expensive and unwieldy. In contrast, wavelength encryption provides low-cost, low-latency security to protect 100 percent of its data using in-flight encryption for data moving across wide-area fiber connections.

Customer segments such as healthcare, financial, government, retail, utilities and cloud service providers are often faced with increasing compliance and regulatory challenges. As a result, these organizations should be seeking to make their security strategies more comprehensive and will need to seriously consider optical layer encryption for its data center applications.

In the coming years, as more clients adopt this approach, data encryption for wave services is likely to become a standard expectation, especially for high-speed data center connectivity.

In order to meet these increasing security threats and compliance challenges, customers should consider providers with a global wavelength footprint to serve their locations as well as an integrated secure key management tool to simplify network operations and promote business growth.

For additional information, go to:

centurylink.com/en/products/wavelength

This document is provided for informational purposes only and may require additional research and substantiation by the end user. In addition, the information is provided "as is" without any warranty or condition of any kind, either express or implied. Use of this information is at the end user's own risk. CenturyLink does not warrant that the information will meet the end user's requirements or that the implementation or usage of this information will result in the desired outcome of the end user.

Services not available everywhere. CenturyLink may change or cancel products and services or substitute similar products and services at its sole discretion without notice. ©2019 CenturyLink. All Rights Reserved.