APPLICATION NOTE

Wavelogic Encryption Solutions

Securing All In-flight Data, All the Time

Security has become a boardroom issue. A 2020 Thales Data Threat Report[1] revealed that 49% of global respondents' companies have been victims of a breach at some point in their history. More targeted industries such as healthcare, finance, government, and education report breaches far exceeding the average.

In addition to endangering customer information, data breaches impact an organization's bottom line. According to a global Ponemon study[2], approximately 25,500 records are exposed during every data breach, putting the cost of a single breach into the millions, in addition to the immeasurable loss of customer trust. This study also revealed that the average total cost of a data breach in the U.S. in 2019 was $8.19 Million. Again, this varies by industry; the cost per record lost in the healthcare industry is almost double.

But even as the threat of breaches rises, the traffic flow across the network is growing. Bandwidth demands continue to climb, necessitating a network that can elegantly scale to handle higher capacities with less operational complexity. Additionally, with the increasing sophistication and frequency of data breaches, no organization is immune to the ever-present threat of malicious attacks to collect sensitive and private information. Today's high-capacity networks require much more than high capacity bandwidth—they need a security strategy to protect all critical data, both at rest and in-flight, as it spans the globe traveling metro, regional, long-haul and submarine distances.

Designed to secure today's high-capacity networks, Ciena's WaveLogic™ Encryption cost-effectively enables a scalable, protocol-agnostic, ultra-low-latency encryption solution on the widely deployed 6500 Packet-Optical Platform. The solutions extends to Ciena's Waveserver® Family of high-capacity, compact, modular transport devices enabling cost-effective, secure Data Center Interconnect (DCI) applications. This always-on encryption combines ease of operation and administration to enable a simple-to-implement data protection strategy that leverages

Benefits

- Offers an ultra-low-latency, FIPS-compliant, encryption solution for highly secure and transparent end-to-end communications
- Scales with programmable WaveLogic coherent technology for flexible 100G to 400G wire-speed encryption
- Features protocol-agnostic encryption, offering flexibility to support a variety of services
- Leverages enhanced security features, including two distinct sets of keys for authentication and data encryption functions, with a fast encryption key rotation interval of seconds
- Integrates seamlessly into existing enterprise Public Key Infrastructures (PKIs) using X.509 certificate-based authentication
- Enables secure management of Encryption-as-a-Service capability by the end-user via an integrated management tool
- Delivers a field-proven encryption solution widely deployed across the globe in finance, legal, healthcare, military, utility, and government networks

1 https://cpl.thalesgroup.com/sites/default/files/2020-04/2020-data-threat-report-global-edition-infographics.pdf
2 Ponemon, IBM study: Cost of a Data Breach 2020: https://www.ibm.com/security/data-breach

Ciena's industry-leading WaveLogic coherent technology to deliver unmatched flexibility, performance, and the industry's first coherent 100G to 400G wire-speed encryption solution.

Encryption technology

Encryption is defined as the process of transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge, referred to as the key in cryptography. Essentially, this process locks down the network by encrypting this data, rendering it completely unusable to an intruder that retrieves it, or to anyone not in possession of the correct key to decipher the message.

There are many ways to encrypt data, defined by various standards that specify the encryption requirements of the supporting products and keys, and set a certification process for network equipment. Several standards-based encryption algorithms exist, including Advanced Encryption Standard (AES), which has various key sizes (56-, 128-, 256-bits) published by the National Institute of Standards and Technology (NIST). These standards are published as U.S. Federal Information Processing Standard (FIPS) publications. As an example, the AES-256 encryption algorithm was published as FIPS 197. In addition to algorithm-specific publications such as FIPS 197, NIST also publishes standards coordinating the requirements for cryptographic modules that include both hardware and software components in FIPS 140-2.

There are other similar frameworks used to certify encryption solutions. Another important standard is the Common Criteria (CC) for Information Technology Security Evaluation, which is an international standard (ISO/IEC 15408) for computer security certification. Common Criteria provides a means of ensuring that the process of specification, implementation, and evaluation of a network device, such as an network element in an optical network, has been conducted in a rigorous and standard manner. In Germany, the BSI, the German Federal Office for Information Security, issues security certifications that include certification against Common Criteria. BSI certificates based on Common Criteria are often used as a basis for local certification, which saves time and costs in the certification process. This set of standards and certification processes deliver service providers and end-users the assurance that the encryption solution has demonstrated compliance to the defined requirements by having successfully completed the rigorous laboratory testing and reviews mandated by the standards.

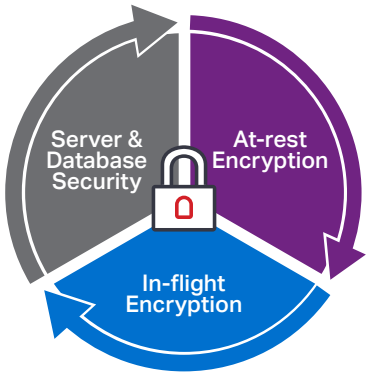

Figure 1. Encryption of in-flight data is part of a holistic security strategy

Securing today's networks

Encryption is widely used today to secure both at-rest and in-flight data. According to a Ponemon report on encryption trends, only 13 percent of global respondents have no encryption strategy.[3] Organizations of all sizes in every industry must go to great lengths to protect information stored in their data centers from unauthorized access. The impact and cost of a data breach cannot be ignored and has increasingly severe consequences to an organization, including degrading a company's reputation, criminal prosecution, expensive regulatory fines, and high customer churn.

A range of commonly used techniques exists today to protect at-rest data for secure servers, databases, routers, and switches by managing user access and credentialing. However, in today's web-scale networks, large amounts of critical data are in-flight as high-bandwidth communications occur beyond the walls of the data center, traversing a larger, potentially worldwide network. A comprehensive IT security approach must therefore encompass a robust in-flight encryption solution as part its holistic security strategy, as shown in Figure 1. By encrypting data as it leaves the security of the private cloud, operators can ensure this data is protected from unauthorized intercept as it traverses the network, crossing varying security levels as it reaches its destination.

While many organizations are adding in-flight data encryption to their security strategy, the focus traditionally has been on encrypting in-flight data at Layer 2 or higher. Although this may be a good option for some low-speed IT applications that are not data-intensive or time-sensitive, it is often not enterprise-wide and only encrypts IP application data. This operational model for deploying an encryption solution is quite cumbersome and costly, as shown in Figure 2, as it typically requires protocol-specific standalone encryption devices

3 Ponemon, Thales e-Security research report: 2018 Global Encryption Trends Study; April 2018; https://go.ncipher.com/rs/104-QOX-775/images/2018-nCipher-Ponemon-Global-Encryption-Trends-Study-ar.pdf

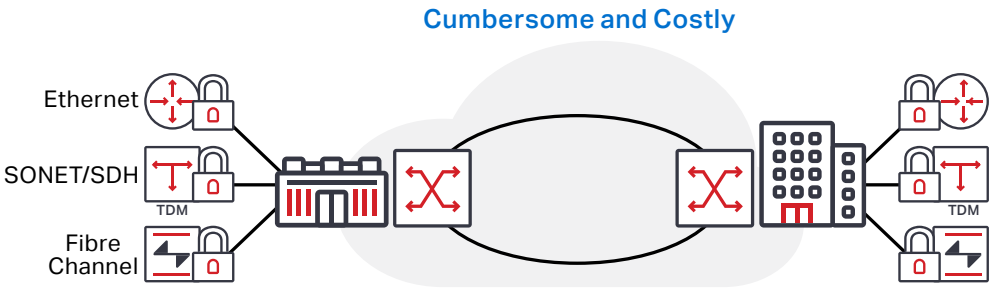

Figure 2. Traditional, protocol-specific encryption deployed in a multiservice network

and can contribute significant amounts of latency, impacting the application throughput and resulting in inefficient use of bandwidth. Furthermore, encryption key management and authentication across multiple independent devices is complex and labor-intensive, and end-to-end network troubleshooting is further complicated across many independent devices. Additionally, this approach leaves a gap in the organization's in-flight data protection strategy. While, traditionally, the risk of fiber-optic cable intrusion has not been a consideration in an organization's security strategy, the threat of optical cable infiltration to access the data it carries is real. Fiber-optic cables are typically very easily accessible and unguarded, and anyone with the right tools can tap a fiber-optic cable and collect data undetected for days, months, or even years. Deploying a transport-layer encryption solution protects all in-flight data, all the time, ensuring every bit is secure.

Data Security with Optical Encryption
Download infographic now

WaveLogic Encryption

As part of Ciena's multi-layer security approach that ensures the confidentiality, integrity, and availability of data in the network, Ciena's WaveLogic Encryption combines the proven encryption technology deployed on platforms that have a large global installed base with the proven reliability of the market-leading 6500 Packet-Optical Platform, deployed by more than 600 operators around the globe. Additionally, Ciena's WaveLogic Encryption capabilities extend to Ciena's Waveserver and Waveserver Ai stackable interconnect systems, enabling up to 1.2 Tb of wire-speed encryption capacity in 1RU for simple, rack-and-stack DCI applications.

Simple to deploy

With WaveLogic Encryption, operators can benefit from a solution that simplifies the deployment of encryption by integrating encryption functionality directly into the network element within the transport network. This approach reduces network complexity and eliminates the need to manage different encryption solutions for various applications, as shown in Figure 3. This operational simplification also extends to the management of the encryption solution, including a dedicated authentication and key management tool, and easy integration into existing enterprise PKIs.

The flexibility of the 6500 platform enables customers to select the optimal shelf size to best meet their site-specific capacity, space, and power requirements for cost-efficient transport of encrypted services. An additional key benefit is that the solution is fully protocol-agnostic, supporting a wide range of flexible clients, including Ethernet, SONET/SDH, Fibre Channel, and OTN, to address multiple applications among security-conscious customers.

Differentiate with encryption 24/7

Encryption is always enabled in Ciena's WaveLogic Encryption solutions, ensuring the highest level of security, as all network

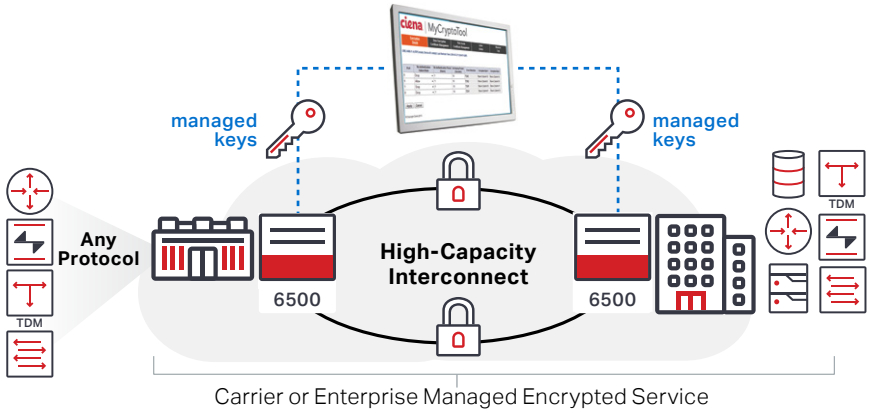

Figure 3. Ciena's 6500 WaveLogic Encryption solution

traffic is always encrypted. Although the ability to turn encryption on or off may seem like added flexibility, simple human error can result in sensitive traffic being sent over the network unencrypted. Operators can leverage a differentiated infrastructure that protects all in-flight data, all the time, as it spans the globe across metro, regional, long-haul, or submarine distances. Additionally, operators can increase revenues and customer retention by offering differentiated high speed Service Level Agreements (SLAs) leveraging encrypted services with ultra-low-latency connectivity and several path/equipment protection options.

Ironclad encryption

Ciena's WaveLogic Encryption is validated externally and independently certified by a third party to ensure it is implemented with industry-standard algorithms and advanced security features that include Common Criteria and FIPS certification. It provides a FIPS-certified AES-256 encryption engine with standards-based authentication mechanisms (such as X.509 certificates), enabling seamless integration into existing enterprise PKIs. Additionally, the 6500 hardware and software components of the cryptographic modules are compliant with FIPS 140-2 and full BSI certification under Common Criteria for Information Technology Security Evaluation, offering service providers and end-users the assurance that the encryption solution complies with all aspects covered by this comprehensive evaluation, including encryption algorithms, key exchange mechanisms, and user authentication.

For enhanced data protection, two distinct and independent sets of keys are used for authentication and data encryption functions, with a fast encryption key rotation interval of seconds instead of minutes. The AES-256 data encryption session keys are autonomously negotiated and rotated every second, independently on each line port, without impacting traffic or throughput, and without user intervention. Operators can deploy the next generation of public key cryptography algorithms with support for Elliptic Curve Cryptography (ECC), which provides a significantly more secure strategy than first-generation public key cryptography systems.

Programmable 100G to 400G wire-speed encryption

To meet the needs of today's high-capacity communications, Ciena's WaveLogic Encryption leverages industry-leading WaveLogic coherent technology to enable high-capacity, flexible, and customizable encryption solutions. WaveLogic 3 Extreme builds on the capabilities of WaveLogic 3 and provides extreme performance for all coherent networking applications through the use of additional modulations and enhanced mitigation of both linear and non-linear impairments. This cutting-edge solution provides software-programmable modulation to enable 100G wire-speed encryption with QPSK modulation, 150G wire-speed encryption with 8QAM modulation, and 200G wire-speed encryption with 16QAM modulation. WaveLogic Ai builds upon the best-in-class performance of WaveLogic 3, and uses an advanced, 400G-optimized engine to significantly improve transport economics: driving twice the capacity per channel, three times the distance at equivalent capacity, and four times the service density.

On the 6500, operators can integrate a WaveLogic 3 Extreme line module with encryption with any one of various client interfaces, to flexibly deploy a solution tailored to meet their specific traffic needs, be it 10G, 40G or 100G service transport. As demands increase, with this pay-as-you-grow modular offering, the same line module can be programmed to carry 200G of encrypted traffic simply by adding an additional client card. Additionally, operators can deploy high-capacity encrypted services across the network, leveraging the 6500's high-capacity hybrid packet/OTN fabric, maximizing the efficiency of network resources.

On the Waveserver, operators leverage up to 400 Gb/s of FIPS-certified, AES-256 wire-speed encryption line capacity in just 1RU and the flexibility to support a mix of 10GE, 40GE, and 100GE clients on the same device. Programmable modulation allows the Waveserver to optimize its wire-speed encryption line capacity for each application/need, enabling two 100 Gb/s, 150 Gb/s or 200 Gb/s wavelengths. To address ultra-high-capacity secure interconnect applications, operators can deploy Waveserver Ai to enable up to 1.2 Tb/s of encrypted capacity in 1RU, with the ability to support three traffic modules, each of which offers up to 400 Gb/s of encrypted capacity. Waveserver and Waveserver Ai provide highly secure, ultra-low latency, in-flight data protection across metro, regional or long-haul distances.

6500 10G wire-speed encryption

Operators can cost-effectively provide 10G encrypted services by leveraging the 4x10G Optical Transponder with encryption module. This single-slot module provides 40G of

High-capacity Wire-speed Encryption Modules Download data sheet now

wire-speed encrypted service capacity via four distinct 10G protocol-independent encrypted line ports, so customers can benefit from simpler network designs with integrated encryption capability in any 6500 chassis variant. The module offers enhanced security with its FIPS 140-2 Level 3-compliant design, providing protection against physical tampering of the card, with support for zeroisation. This ensures that all critical security information is erased upon detection of any physical tampering of the cryptographic module by setting all data to zero, even when the card is not plugged into the shelf.

Encryption management made simple

A best-in-class transport layer security solution would not be complete without a simplified, integrated encryption management approach. Partitioning encryption management from transport management allows added flexibility in an operator- or enterprise-maintained infrastructure. In either case, it is important that the 'owner' of the data—the end-user—maintain full control of the encryption security parameters associated with their critical data, issuing new keys or certificates as required by their security policies, while remaining aware of any security alarms and logs on an end-to-end basis.

Ciena's 6500 WaveLogic Encryption solution includes MyCryptoTool, a dedicated encryption management interface designed for distributed management of the network that enables the end-user/security officer to independently manage the security parameters and alarms of carrier-managed or enterprise-managed networks. MyCryptoTool is a simple-to-use interface that securely connects to the cryptographic module and provides mutual authentication, limiting access to authorized security personnel. In the event that the encrypted service is purchased from a service provider, the provider will manage the links and their provisioning, administration, and performance monitoring, just as in any other service, but will not have control or visibility of the encryption parameters. The same approach is valid when the encryption solution is deployed and managed by two different groups within the same enterprise or government agency.

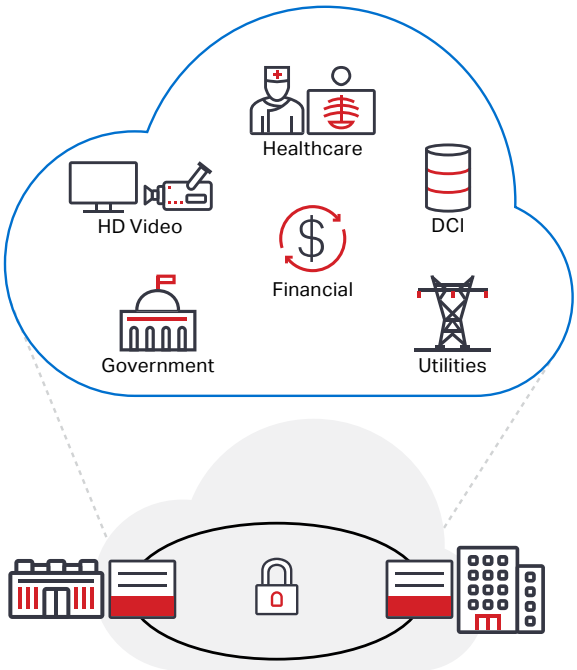

Figure 4. Examples of key WaveLogic Encryption applications

Key applications

Ciena's WaveLogic Encryption solutions are tailored to protect critical in-transit data in all of today's high-capacity applications. Key applications that would benefit from these solutions include:

- Enterprise DCI for high-capacity storage and data encrypted transport
- Government and institutions that require certified, secure, high-speed communications between different locations
- Healthcare applications with high-quality, low-latency requirements for secure, efficient, and timely collaboration between healthcare stakeholders
- Managed service applications
- Latency-sensitive applications, such as high-definition video or high-speed trading, that require a secure, ultra-low-latency transport solution
- Utilities that want to protect their critical communication infrastructures

Summary

As increasingly more sensitive information gets distributed across fiber-optic networks, today's high-capacity communications must deploy an IT security approach that encompasses not just server security and at-rest encryption, but also a robust in-flight encryption solution. Ciena's WaveLogic Encryption combines a high degree of flexibility and security, with ease of operation and administration, to enable cost-effective, scalable, wire-speed encryption solutions for securing all in-flight data, all the time, whether it is traveling across the street, across the city, across borders, or across the ocean.