

# NETWORK SECURITY

SOLUTIONS BRIEF



## IN THIS ISSUE

- 3 FortiGuard Labs Threat Research**  
By: Fortinet
- 5 Fiber Assurance Solutions**  
By: Adtran
- 12 SASE Transitions**  
By: Enterprise Management Associates, Inc. and Juniper Networks
- 17 The Security Gap Threat to Rural Broadband Success**  
By: A10 Networks
- 20 Wavelogic Encryption Solutions**  
By: Ciena
- 26 Flexible, Scalable DDoS Protection**  
By: Corero

## INTRODUCTION

The estimates are stunning. By 2030, the number of global Internet of Things (IoT) devices is set to nearly double to more than 29 billion by 2030. The expectation is we will have more than 20 connected devices per human by that same time. Our increasingly digitalized and connected world will have a profound impact on a wide range of applications at home and work, including several use-cases in healthcare, government, transportation, and energy, among others.

And as we rapidly move to an environment that is permanently online, protecting the integrity of your network from cyber threats and denial of service attacks is critically important. Without the proper protection, your business and customers are vulnerable to data breaches and loss of intellectual property and financial risks inherent with not protecting your data.

More specifically, new research by the Ponemon Institute and IBM Security revealed that the global average cost of a data breach reached \$4.45 million and the costs of avoiding law enforcement after a ransomware attack have increased by \$470,000.

Looking across industries at 553 organizations impacted by data breaches that occurred between March 2022 and March 2023, not only did the healthcare sector see a 53% jump in breach costs since the COVID-19 pandemic, but health data breach costs reached nearly \$11 million.

The security of your network should encompass many priorities including the prevention of unauthorized access to network resources; detection and preventing cyberattacks and security breaches in progress; and ensure that authorized users have secure access to the network resources needed.

From the network core to service delivery edge, Netceed offers a wide range of tailored products, materials, and solutions backed by more than 30 years of expertise and technical performance.

Our comprehensive portfolio of passive materials, active equipment, and tools, through strong, long-lasting relationships with industry-leading partners, is comprised of more than 90,000 SKUs available from nearly 1,500 global sourcing and supply partners. We also provide a wide range of value-added services including CPE refurbishment and repair, integration, outsourced procurement, and logistics solutions supported by our global team of service delivery experts.

Our robust portfolio of solutions to meet your network security deployments. A10 Networks, Adtran, Ciena, Corero, Fortinet, and Juniper Networks are just a sample of recognized leaders in this space. The accompanying content chronicles a small sample of products and resources available to our customers. Please contact us today to learn more about our complete network security portfolio or visit us at [www.netceed.com](http://www.netceed.com).





# FORTIGUARD LABS THREAT RESEARCH

**BY: DOUGLAS JOSE PEREIRA DOS SANTOS**  
Cybersecurity Strategist, Fortinet

## Key Findings from the 1H 2023 FortiGuard Labs Threat Report

In our 1H 2023 Threat Landscape Report, we examine the cyberthreat landscape over the year's first half to identify trends and share insights with security professionals, enabling them to enhance their security strategies and better prioritize patching efforts. The report findings reflect the collective intelligence of FortiGuard Labs, drawn from Fortinet's vast array of sensors that collect billions of threat events observed worldwide during this same period. Below are key takeaways from the report.

### 1H 2023 Threat Report: A Summary

In the year's first half, we observed significant activity among advanced persistent threat (APT) groups, a rise in ransomware frequency and complexity, increased botnet activity, and much more. And while attack volume isn't entirely on the continual upward climb we've seen in the past, we're witnessing breach attempts become more sophisticated and targeted.

As cybercriminals continue to advance their tactics, the good news for security practitioners is that much of the malicious activity observed is familiar, giving leaders and their teams ample opportunities to implement effective defense strategies.

## Ransomware Becomes More Sophisticated and Targeted

While ransomware has existed for decades, we've witnessed threat actors using more-sophisticated and complex strains in recent years to infiltrate networks, largely thanks to the expansion of Ransomware-as-a-Service (RaaS) operations. Ransomware volume certainly isn't slowing down, either, with ransomware activity ending 13 times higher at the end of 1H 2023 compared to the start of the year. Yet the number of enterprises detecting ransomware on their respective networks is declining: 13% in 1H 2023 compared to nearly 25% five years ago. Unfortunately, this isn't cause for celebration, as it indicates bad actors carrying out more targeted attacks using highly adaptable playbooks.

In several previous reports, we discussed wiper malware, a highly destructive attack technique that "wipes" data from infected systems. While we observed a surge in wiper use in early 2022, mainly in conjunction with the Russian-Ukrainian conflict, wiper malware attacks slowed in the first half of 2023.



## **Malicious Actors 327x More Likely to Exploit Top Vulnerabilities**

Since its inception, Fortinet has been a core contributor to exploitation activity data supporting the Exploit Prediction Scoring System (EPSS). Many vulnerability management teams use EPSS to help prioritize their remediation efforts. But EPSS can also help us track the progression of vulnerabilities from initial disclosure to the outbreak of exploitation in the wild.

Our latest report analyzed six years of data spanning more than 11,000 published vulnerabilities for which our sensors detected exploitation. We sought to determine how long it takes for a vulnerability to move from initial release to exploitation, whether vulnerabilities with a high EPSS score get exploited faster, and whether we could predict the average time-to-exploitation using EPSS data.

Our analysis shows that the top most exploitable vulnerabilities, as identified by EPSS, are 327 times more likely to be attacked within a week than others on your radar. Using EPSS data in this way can serve as an early warning system.

## **Nearly a Third of APT Groups Were Active in 1H 2023**

For the first time in the history of our Global Threat Landscape Report, we tracked the number of active APT groups. Our research shows that of the 138 cyberthreat groups identified by MITRE, 41 (30%) were active during the first half of the year. Based on our malware detections, Turla, StrongPity, Winnti, OceanLotus, and WildNeutron were the most active. Yet over the past six months, APT-led threats impacted only a small subset of all organizations, indicating that APT endeavors remain highly targeted... at least for now.

## **Unique Exploits, Malware Variants, and Botnet Activity on the Rise**

In this year's report, we examined longer-term trends regarding unique exploits, malware variants, and botnet activity to give us a greater perspective on today's threat landscape.

Our data shows that the count of unique exploit detections is up 68% over the past five years—a sign that attackers are multiplying and diversifying their exploits. However, we also observed a 75% drop in exploitation attempts per organization and a 10% dip in severe exploits, both of which signal that cybercriminals increasingly carry out more-targeted attacks. Malware families and variants have exploded over the past five years, up 135% and 175%, respectively. We also observed more active botnets (+27%) and a higher incidence rate of botnet infection among organizations (+126%). What's most concerning about botnets is that they have become more persistent over this period, spending more time "lingering" on networks before they're detected and blocked.

## **Protect Your Organization from an Increasing Array of Threats**

Threat actors won't be slowing down anytime soon, particularly as organized cybercrime groups make it even easier for them to achieve a quick payday. However, there are numerous actions organizations can take today to better protect their networks from these adversaries.

Sharing and utilizing threat intelligence has never been more important to combat the ever-increasing sophistication and volume of cyberthreats. Additionally, understanding attack flows—from initial entry points to post-exploitation activities—is vital to creating effective cybersecurity strategies. Finally, there's no better time to implement new security technologies and reassess your team's processes and playbooks. Developing and maintaining a comprehensive defense strategy is crucial to protecting enterprise networks today and in the future.

# FIBER ASSURANCE SOLUTIONS

BY: ADTRAN

## Creating more value from your fiber plant

Fiber is the established choice for connecting core sites. Now, it's also becoming the dominant medium for access to enterprises, public buildings and cell sites. The communication and data services transported over those fiber networks are crucial for our working environments and our social lives. Network unavailability caused by damaged fiber can create major problems and even threaten the operation of critical infrastructures. Immediate action is indispensable.

Field forces need to be able to distinguish between issues caused by active devices and those caused by passive cables. In-service fiber monitoring solutions are the most efficient way to identify the root cause of link outages. This enables targeted action for highest service availability.



## Time for change

The value of proactive, in-service fiber link monitoring is clear. It simplifies failure isolation, enabling fiber network providers to take immediate, targeted action, while also preventing false alarms and unnecessary truck rolls. This shortens the repair cycle, reduces the unavailability of a fiber link and also speeds up installation and commissioning of fiber services.

Why have service providers been reluctant to implement in-service fiber monitoring solutions until now? Previous fiber monitoring systems were optimized for reactive fiber measurement rather than in-service monitoring. Test equipment is typically designed for portability. It frequently fails to meet the cost and availability requirements of in-service monitoring solutions. Now, the latest innovation with optical components and digital signal processing has provided the basis for economically feasible, in-service fiber monitoring systems.

In case of network failures, time is of the essence. Fiber monitoring enables fast failure isolation and rapid restoration of services. Higher network availability is a major benefit for customers, enabling them to meet stringent business continuity requirements. As well as fiber degradation, insertion of bending couplers for eavesdropping can be identified by analyzing real-time attenuation data.

## Who benefits from fiber monitoring?

### 1. Dark fiber providers

Fiber providers can offer a higher value service, providing real-time fiber integrity information.

### 2. Dark fiber customers

Fiber monitoring enables fast root-cause failure analysis, shortening repair cycles and detection of fiber tapping events.

### 3. Communication service providers

Fiber failures are located without additional truck rolls, allowing efficient and targeted action.

### 4. Mobile network operators

Transparent, non-intrusive monitoring of fiber links opens up the possibility of connecting mobile cell sites with any radio access technology.

## Fiber link monitoring saves the day

A broken or accidentally disconnected fiber can disrupt mission-critical and revenue-generating services. Fiber network providers frequently operate under stringent service level agreements (SLAs). Their business depends on the ability to detect and isolate any problem in the network quickly and precisely. There's no room for doubt and inefficiency. Fiber link monitoring provides accurate real-time information, minimizing downtime and maximizing the value of fiber infrastructure.

## Simple and efficient

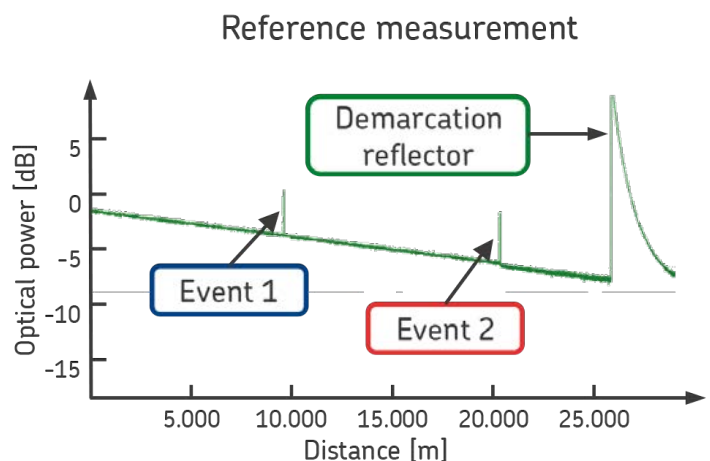
Scattered and reflected light from measurement signals is used to calculate the loss profile of a fiber link in real time. With such precise information, the operational team can immediately identify and locate any problem on the link. An optical measurement signal is generated and coupled into the fiber. Analyzing the reflected light provides detailed information about the loss profile and disturbances on the link.

The loss profile, shown in the diagram, clearly indicates the location of the demarcation reflector as the end-point of the fiber, which frequently also represents the service demarcation. There's no interaction between the measurement signal and the user data. Fiber monitoring is fully transparent to user services.

ALM, our advanced fiber monitoring solution, dramatically alters how operators monitor their fiber networks. This new technology is the most cost-efficient professional fiber assurance product available on the market. Its core purpose is to proactively monitor fiber plants and help operators to resolve any issues before they impact services. With the Adtran ALM, operators are able to pinpoint faults and eliminate any wasted repair efforts.

## Bringing light into the dark

Why can you see a beam of light shining through fog? It's because light scatters as it passes through diffusing media or hits a reflective surface. The same principle applies to fiber monitoring. A test signal is sourced into a single mode fiber and the scattered, reflected light is analyzed. This enables network operators to identify fiber disturbances caused by micro-bending or water diffusion, increased attenuation from splices or fiber connectors, and broken fibers or disconnected patch cables.



## ALM at work

Our ALM is a unique plug-and-play fiber assurance device for proactive fiber monitoring. It enables operators to supervise their critical fiber infrastructure with minimal and simple additions to their existing network. The optical measurement signal generated by our advanced link monitoring solution is coupled into a single mode fiber and reflected back at the demarcation point. This test signal does not interfere with user traffic on the fiber, enabling fully non-intrusive monitoring of the fiber plant.

The seamless integration into our Ensemble Controller SW for management and control offers a range of sophisticated functions including advanced alarm management and reporting, trouble-ticket handling and a view of the entire network status.

### Why proactive fiber monitoring?

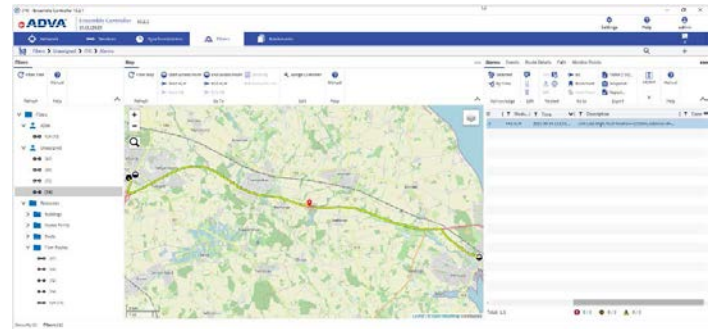
1. Degradations are identified before services are affected.
2. Precise root-cause analysis avoids unsuccessful repair attempts.
3. Localizing failures shortens repair cycles.
4. Real-time information assures service quality.
5. Maintenance-free demarcation does not consume power.

## Fits all your applications needs

Due to its innovative multifunctional design, our ALM is the ideal solution for any fiber monitoring application. Procedures for continuous in-service monitoring, fast fault localization and accurate detection of small changes in fiber infrastructure can be set up quickly, involving only a few mouse clicks. Its multifunctional test capabilities enable our ALM solution to accurately locate faults on access, core or backhaul links within distances of 300km and beyond.

It can test up to 64 fiber services with a very short scanning cycle of only 2 to 5 seconds per active link. And it quickly detects intrusions that threaten network integrity, regardless of whether the services and applications provided on top of the dark fiber service utilize uncolored, CWDM or DWDM optics. What's more, our ALM device comes in a compact and versatile housing.

## Geographic information system (GIS)



Service providers and their customers require full visibility of network integrity. They need to be able to direct field forces precisely to the location of a fiber failure. Geographic information systems combine fiber monitoring data with geographic information of cable routes. A graphical user interface shows a fiber map and clearly indicates locations of any faults or anomalies. There is no easier and faster way for repair teams to identify the position of a fiber break.

Our Ensemble Fiber Director builds on real-time data from our advanced fiber monitoring solution ALM. It further enhances the spatial resolution by correlating the measurement data with the location of connectors and splices in the network. This calibration assures highest precision in real world applications. The Ensemble Fiber Director is part of the Ensemble Controller solution, which provides easy operation as well as simple integration into customer`s business support system With extensive customization options as well as immediate notification capabilities, fiber operators can further optimize their operational processes and thus offer more stringent SLAs to increase customer satisfaction.



## Solution components

### 1. Monitoring unit

Our ALM monitoring unit calculates a loss profile of the monitored fiber link by analyzing the reflected measurement signal.



### 2. WDM coupler

The test signal operates at a wavelength distinct from the user traffic. A WDM coupler combines both signals on the supervised fiber.



### 3. Demarcation reflector

A passive demarcation reflector defines the service handoff point. It does not consume power and can be applied even under harsh environmental conditions.



## Applying fiber link monitoring

There are good reasons for communication service and dark fiber providers to monitor their fiber asset with advanced link monitoring. The system is simple to install and operate. It assures service quality with real-time information on fiber integrity. Field forces can locate fiber incidents and initiate immediate counter-action. There's no need for additional truck rolls for fault analysis. What's more, dark fiber customers have a means to differentiate between problems on their premises and fiber failures.

## Improving service quality

Service providers want to maximize the value of their fiber asset. By providing real-time information on fiber integrity, latency and attenuation, they can offer high-value advanced services.

Customers benefit from this information in various ways. Network failures are remotely detected and isolated based on a comprehensive set of real-time information, without additional onsite visits. This avoids time-consuming fault isolation and shortens repair cycles as counter measures can be initiated immediately.

Proactive fiber monitoring also detects malicious attacks on a network as coupling devices for eavesdropping cause additional attenuation that can be detected on the loss profile of the fiber link.

### Essential use cases

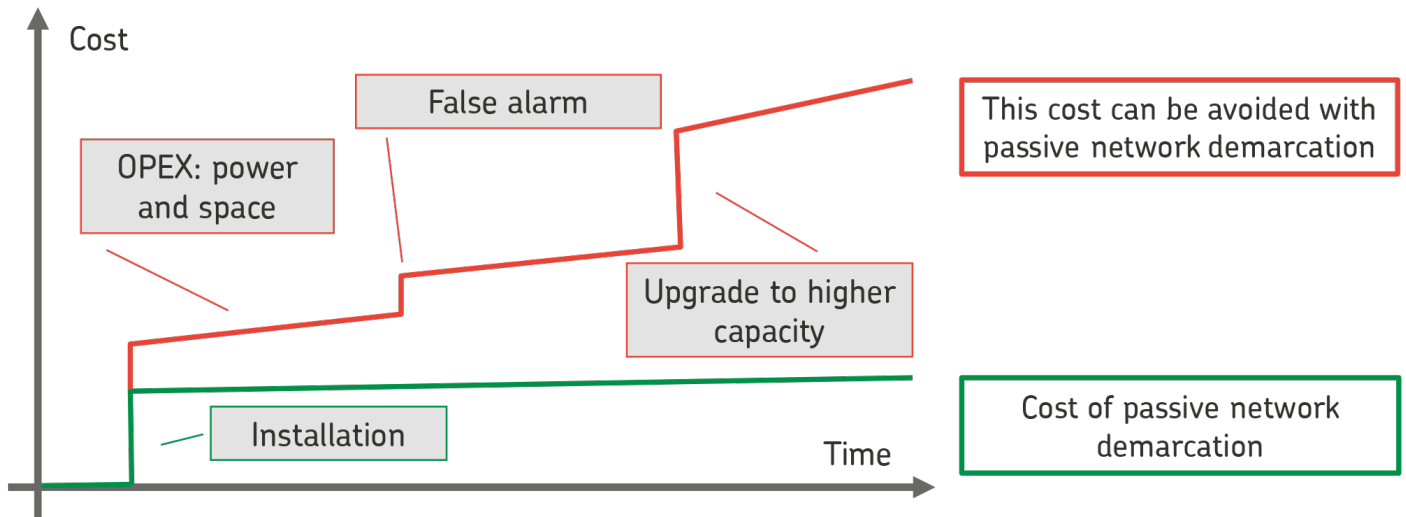
- 1. Supervised dark fiber services:** higher value with better SLAs
- 2. Service-agnostic demarcation:** change services without site visits
- 3. Monitoring layers in isolation:** immediate fault isolation for shorter repair cycles
- 4. Securing a fiber link:** protect against eavesdropping
- 5. Sensor networks:** monitor sites without power supply



## The merits of passive demarcation

Today, active demarcation devices are installed at a service hand-off point on the customer premises. The very same information can also be gained by monitoring services at the central office, if fiber integrity can be assured.

Hence, central service monitoring in combination with fiber link monitoring is an interesting alternative to active demarcation devices. Passive demarcation has obvious cost advantages, as shown in the cost curve. It compares the cost of our demarcation solution including installation with an active demarcation device that has higher first-in cost, adds operational cost for power and space as well as upgrade cost from the introduction of new services.



*The diagram highlights the significant OPEX advantage of passive versus active demarcation. Passive demarcation assures availability of the fiber link at lowest cost. On the other hand, active demarcation can provide additional OAM information and resiliency by local switching.*

## Monitoring network layers independently

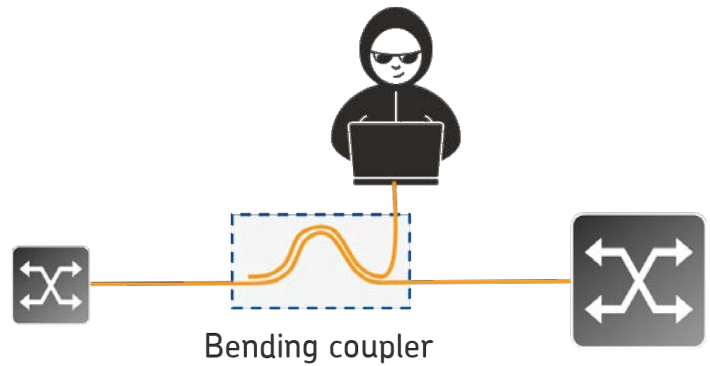
There are various problems that can disturb a network connection. There might be a failed interface card, a dirty fiber connector, a misconfigured router or a broken fiber. If the problem is analyzed by a network management system optimized to control an active network element, all problems look very similar and the operator cannot differentiate between them and identify the root cause, let alone the location of the problem. This is where monitoring of the physical transmission media comes in. Results from fiber link monitoring enable a service provider to immediately understand the root cause of a problem.



## Securing a connection with link monitoring

Fiber optical transmission systems are potentially at risk of being intercepted. An attacker might introduce a bending coupler or a splitter into a fiber link in order to gain access to the optical signal and to the user data being transmitted. The insertion of those coupling devices adds attenuation at a discrete point on the link. Such suspect signatures can be used to detect malicious attacks.

When an attacker introduces a coupler into a fiber link, the additional loss can be detected by a link monitoring system. This improves the integrity of fiber links and secures communication against eavesdropping.

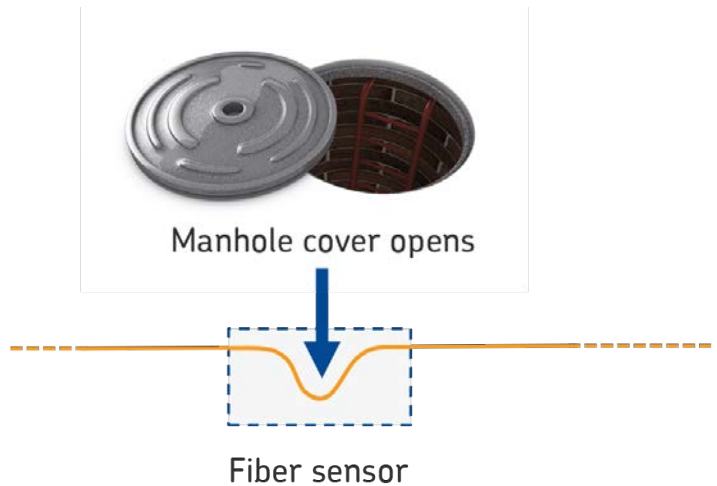


*Unmasking an attacker with real-time monitoring of fiber loss*

## Securing a site with link monitoring

Some sites along a fiber link need to be monitored but have no available power. In cases like this, such as manholes that need to be managed and controlled, active devices can't gather local information and transmit it to a central control site. Vandalism is often reported, ranging from removing a cover to cutting through cables. To minimize negative impact, immediate action needs to be taken.

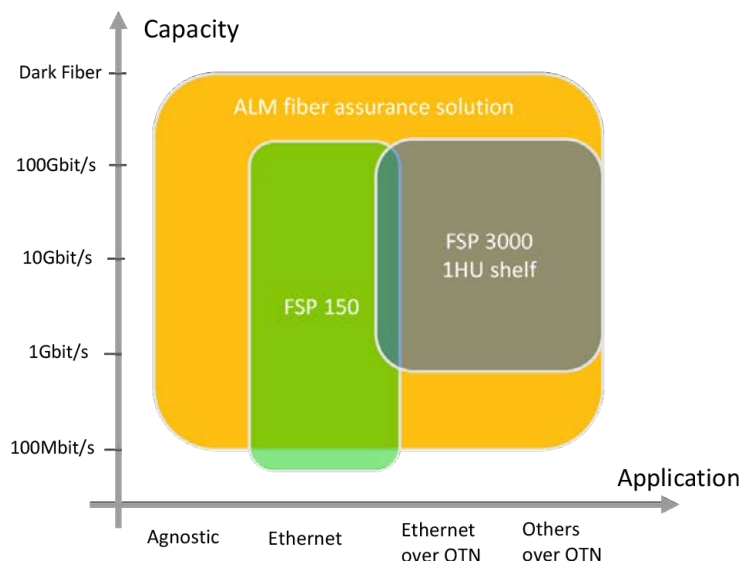
If a service provider wants to monitor such sites, there's a simple solution: applying fiber sensors in combination with link monitoring solutions. Fiber sensors transform mechanical stress into attenuation, which can be measured remotely. There's a wide range of sensors for monitoring torsion, temperature and humidity for deployment at remote sites. In most cases, a spare fiber will be used to access these passive sensors.






*Passive, remotely monitored fiber sensors for measuring pressure, humidity and temperature*

## A range of different devices or a single assurance solution for all services? Your choice

Today's communication networks are built on a connectivity infrastructure applying a range of interfaces, such as OTN for high-capacity, fixed bandwidth connectivity, Ethernet for packet connections, CPRI in the mobile fronthaul network or 5G-SDI for 4K native video signals. Each interface comes with different service assurance capabilities and different management tools. In consequence, service providers will apply a range of demarcation devices aligned with the needs and capabilities of different services. Fiber link monitoring minimizes the range of network demarcation devices needed. And, as fiber monitoring is agnostic to the communication service, a single assurance technology can be applied with any technology.



	Product	Application
	FSP 150 ProNID family	Ethernet and IP service demarcation over Ethernet, MPLS and IP networks with a rich set of OAM functions
	FSP 3000 (1HU chassis)	SDH, OTN, Ethernet, 3G-SDI, transparent bitrate over OTN networks featuring OTN OAM
	ALM, Ensemble Fiber Director	Service-agnostic, non-intrusive link monitoring using a passive demarcation reflector; Ensemble Fiber Director eases operation with map-based GUI

Adtran offers a rich set of network demarcation devices, which can be applied in a wide range of applications. Our ALM device complements the solution portfolio with a service agnostic monitoring technology that does not require an active component at the remote end. The table provides an overview of the different demarcation technologies complementing our proactive fiber assurance solution.



# SASE TRANSITIONS ARE HARD, BUT THERE ARE WAYS TO MAKE THEM LESS PAINFUL

**BY: PAULA MUSICH**

Enterprise Management Associates, Inc.  
and Juniper Networks

In early 2020 many organizations were already well along in their digital transformation initiatives, but the rush to support users now working from home put those projects into overdrive. It also spurred greater interest in the emerging set of solutions described as Secure Access Service Edge, or SASE (pronounced sassy). When it comes to SASE adoption, the most difficult part of the journey in moving from separate, on-premises-based networking and security stacks to a largely cloud-based service is in the transition. The convergence of networking and security that forms the centerpiece of a SASE service has a number of implications that, when planned well, can make that transition significantly less painful.

Like a mantra, nearly all SASE providers murmur the phrase single policy engine when discussing the advantages of their SASE solution. That single policy engine may apply to all of the functions covered by their service, but it doesn't take into account the fact that there are still legacy security (and networking) technologies in use within new SASE customer environments—and those are governed by separate policy management systems. Inherent in any architectural shift is the need to manage new services or applications in parallel with legacy systems. This increases complexity, which was already an ongoing issue for security operations teams trying to manage a large number of best-of-breed security tools that offer little in the way of integration.

## Introduction

Although the market for converged networking and security services for remote users (better known as SASE) is relatively nascent, the need to better support changing network traffic patterns has been building over several years. As enterprises engaged more cloud services and as users more frequently needed to access the services and applications necessary to do their jobs from any location, the legacy architectures that required sending traffic through a centralized data center for inspection and policy enforcement before it reached its destination no longer fit the bill. This evolution only accelerated in 2020 as IT teams scrambled to quickly support work-from-home initiatives. In research conducted on SASE interest and usage in the second half of 2020, Enterprise Management Associates found that among respondents whose organizations were in the midst of adopting a SASE solution, at least half indicated that the COVID-19 global pandemic had accelerated their SASE engagement.

What constitutes a SASE service varies from one SASE provider to another. Most higher-layer networking and security functions are typically executed in the cloud. At minimum, a SASE service should provide SD-WAN, SWG, CASB, ZTNA, FWaaS, the ability to identify sensitive data (including encrypted data) and malware, and consistency in line-rate operations at the network's edge and from the cloud.



Beyond those core capabilities, some enterprises looking to adopt a SASE service may also seek to incorporate web application and API protection, remote browser isolation, recursive DNS, network sandbox, API-based access to SaaS for data context, and support for managed and unmanaged devices. Still others may look for Wi-Fi hotspot protection, network obfuscation, legacy VPN, edge compute protection, and UEBA. Given the complex mix of capabilities that can make up a SASE service, and given the different approaches each SASE provider takes in creating their service, embarking on a SASE engagement can be daunting. Following are seven tips to help make transitioning to SASE less risky and ensure engagements are more successful.

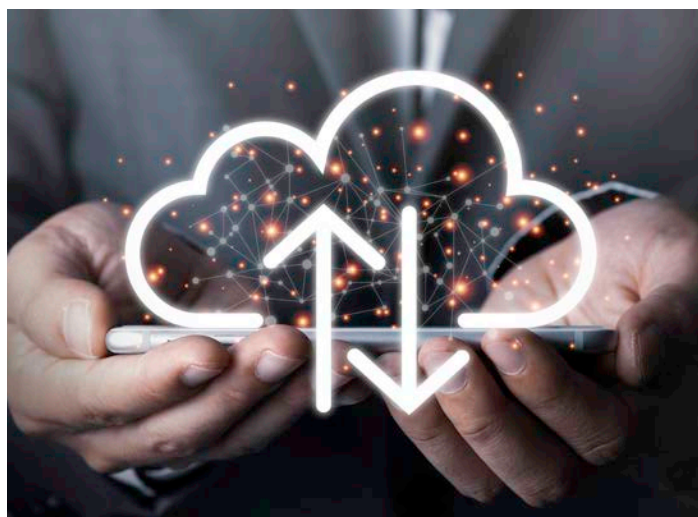
## 1. Starting Down the SASE Path

Where and how organizations begin their SASE journey will vary from one enterprise to the next, depending on each's unique business requirements. Like any new technology adoption process, it's best to start with smaller projects and specific use cases as an enterprise looks to deploy elements of a SASE solution. Early SASE adopters often urge those starting a SASE deployment to gradually transition by replacing existing on-premises equipment, such as firewalls or secure web gateways (SWG), as their contracts near expiration. Starting with a small site can be a good place to gain experience in crafting policies. These can be geared toward specific use cases that represent the organization's business priorities. Some organizations will start with use cases, such as an MPLS replacement project, while others will start with an initiative to replace edge firewalls or VPN infrastructure with cloud-based security. Still others may start with transitioning SWG functionality from legacy gateway appliances located in branch offices and other remote locations to cloud-based web filtering.

The types of organizations that will find it easier to engage SASE service providers include newer technology companies born in the cloud and smaller companies that don't have as much legacy baggage as larger organizations. For the latter type of organization, overcoming inertia will be a bigger barrier to adoption, involving a longer education period.

For existing security and networking software or appliances that won't be replaced or that don't have near-term contract expirations, it's also important to consider where and how those can be redeployed. Are there some locations within the organization that require more in-depth, best-of-breed functionality than what a chosen SASE provider offers? Or are there locations that require greater performance than is available from the SASE provider's nearest point of presence? At the same time, does a prospective SASE provider offer integration with any of the existing security tools that will be redeployed to other locations?

In getting started with a SASE project, there is one other key consideration in planning for converged networking and security services: what will the workflows look like for team members responsible for managing a SASE deployment? Which existing security and networking processes should remain in place, and what has to change to ensure efficient and secure operation?



## 2. SASE Migration: It Takes Two to Tango

Converging networking and security functions into a single service requires close collaboration between networking and security teams. Although EMA research suggests that networking teams predominantly represent early SASE adopters, input and guidance from the CISO's team should be incorporated from the get-go.

Large organizations looking to adopt SASE services should consider creating a dedicated team that draws on both networking and security practitioners, and that team should be assigned common objectives and goals to ensure a successful deployment. Given the borderless nature of SASE architectures and changing network traffic patterns as they move toward a range of cloud services, including security team members with more expertise in cloud security will bring vital insights to a SASE engagement. Their thinking has already moved beyond outdated notions of perimeter security and protecting a private, centralized data center where all enterprise traffic is aimed. At the same time, security practitioners involved in SASE migrations will need to elevate their focus from low-level security tool configuration and deployment to a higher-level business risk focus that takes into account the identity of users, devices, and applications.

SASE will ultimately require a change in culture, and IT executives can help to foster greater collaboration and trust by creating common incentives for SASE deployment teams that help to break down different IT silos. IT executives should lead by example to change culture from the top down.

One other thought about organizational challenges in adopting a new SASE service: any service under consideration should support multi-tenancy and role-based access control to enable more technical operations team members to perform their work without stepping on each other's toes.



### 3. Don't Let Policies Get Lost in Translation

One of the potential benefits of SASE is having centralized, role-based policies that can streamline operations, but the security industry in general has never taken into account what it takes to get there. SASE is no different, and many SASE providers—especially in the early days of the market—are typically not focused on playing nice with established policies, processes, and workflows. Centralized policy management is a misnomer if it does not combine the management of SASE services with remaining, on-premises networking and security functions. As networking and security teams assess potential SASE providers, it's important to look under the hood to determine how easily existing policies can be migrated to the new service while minimizing the opportunity for errors in the process.

As they transition to SASE services, larger organizations will want to use on-premises policy management tools and leverage an instance in the cloud. What's key to reducing operational complexity is to be able to synchronize both on-premises versions and cloud instances rather than requiring administrators to establish policies and manage them separately. Synchronization should be multi-directional so that any configuration or policy changes made within individual network security devices (such as firewalls or web proxies) that affect other devices in the network are propagated across the network, rather than having to be redone in the cloud instance or on-premises policy engine.

At the same time, prospects should also peer into the provider's architecture to gauge whether the provider started with a clean slate or whether they created their service via multiple acquisitions and/or through OEM relationships. The latter enables a best-of-breed collection of network and security services, but it requires solid integration among technology partners to ensure good orchestration across different service-chained policy engines and effective data sharing to reduce operational friction. The former can increase operational complexity, which can slow the migration and obviate any capex savings.

In planning a SASE transition, it's also important to keep in mind how policies need to change as enterprises move from heavy branch architectures, in which more security and networking functions are processed locally, to thin branch architectures, in which more functions are executed from the cloud. It will be critical to plan how access policies need to change to reflect the new architecture without changing the intent of existing policies as a result of human error. At the same time, policy decisions should be informed by greater context, such as the sensitivity of data users wish to access, the location and device from which they wish to access data, and whether a payload appears to be potentially malicious based on correlated threat intelligence.

#### 4. Follow the App

One of the top benefits of a SASE architecture is that it frees applications from the confines of private data centers, enabling them to reside where it works best for the business. This is because with SASE, the perimeter where policies are applied becomes the identity of entities, whether those are devices, users, or applications, rather than the traditional DMZ. As applications migrate from private data centers to the cloud as part of organizations' digital transformation initiatives, and as cloud applications or workloads move, it's important to consider how adaptable the SASE provider's policy engine is. How much effort is required to ensure that the correct policies are applied to applications as they move from private data centers to a cloud provider's facilities? Do administrators have to manually reconfigure policies to move with those applications, or can those policies automatically be applied to the application in its new location? Is it possible to tag applications based on their identity and other contextual information so that policies automatically move with those applications? SASE services that deliver that level of integration and automation can help to reduce the time it takes to successfully deploy a SASE service by reducing the complexity surrounding its deployment. It also reduces day-to-day operational overhead as organizations move applications to meet changing business requirements.



#### 5. Identity Needs Context

With SASE identity, the new perimeter becomes a multi-dimensional construct. No longer just a MAC and IP address, identities include richer context to enable the enforcement of more fine-grained policies. As IT teams tackling SASE projects look at identity, they need to think beyond basic usernames and passwords stored in an Active Directory vault. For human users, identity information should go deeper to include the user's role, department, main geographic location, and the primary devices they use to access enterprise digital resources. This greater level of identity information, coupled with real-time contextual data, allows security practitioners to create policies that better match the changing network traffic patterns SASE is intended to serve. Policies can be tailored to better address changes in location, types of network connections being used, applications that users want to access, and more. The application of security controls and higher-layer network services, such as quality of service, can vary depending on whether the user is requesting access from a coffee shop or an airport Wi-Fi network, versus a branch office or headquarters' enterprise network. Policy decisions will also vary based on whether the application to which the user is requesting access is an enterprise CRM system, enterprise email, or financial application.

The concept of identity also applies to different device types and applications. Beyond just servers and laptops, devices can include an increasingly broad array of OT and IoT devices, such as industrial control systems or smart refrigerators. SASE services should be able to gather details on devices to create a profile that governs policy decisions regarding the types of activities and levels of access they are allowed. The more granular the identity information, the more effectively the entity can be secured and compliance mandates met.

Understanding context is especially critical for applications and workloads located in the cloud, whether it is a SaaS, PaaS, or IaaS service. As IT teams evaluate SASE providers, they should ensure that the provider leverages the APIs of the cloud providers most important to their organization to be able to inspect out-of-band activity associated with their cloud usage.

## **6. You Can't Secure What You Can't See**

SASE service providers are no different than many legacy network and application security providers. They all promise some form of single-pane-of-glass management. That may be true for all of the SASE functions that they directly support, but more often than not, it does not extend to legacy security appliances still in use within the organization. For multi-vendor SASE providers that work with a range of different partners to deliver a service-chained series of SASE functions, the ability to provide a single policy engine and management interface is limited by how well they integrate with those partners. This can increase operational complexity and greatly limit visibility into the customer's network traffic handled by products and services from the different partners, which makes it more difficult for security teams to spot malicious traffic or investigate an incident.

Observability into changing network traffic patterns from a centralized management interface is another key capability that can affect the successful rollout of a SASE service. The ability to detect and block malicious traffic does not end at the boundary between SASE-provided network and security services and services that internal security controls still support.

With users in a constant state of motion, connecting at different times from different locations, and cloud-based workloads and applications being spun up and down on a continual basis, with new locations coming online, maintaining visibility to determine what activity is legitimate and what is malicious is a big challenge. This raises the questions: is a prospective SASE provider's security monitoring capability up to the challenge? Can it correlate threat intelligence generated by not only its own monitoring capability, but from intelligence gathered by other security tools in use within the organization? Can it fill in the blanks between seemingly unrelated but anomalous activity to show the timeline of an attack as it progressed along the kill chain?

## **7. SASE Partner, not Product Pusher**

As IT networking and security teams prepare for a SASE deployment, many will likely look to their SASE provider for advice and help in making the transition to a new architecture. What educational tools do they offer to help architects and operations professionals wrap their arms around how to deploy and manage their new SASE services? Are strategic planning services and deployment services options available? Does the provider have a customer success team to help ensure the deployment meets its objectives? What does the provider offer in the way of migration services? If there is no customer success team, is there an option of having a dedicated support engineer to assist with onboarding of the SASE service? Once onboarded, what type of support does the provider offer if or when problems arise that require help to determine the root cause? This is especially critical for SASE solutions that draw on best-of-breed services from different vendors so customers are not subjected to finger-pointing between technology integration partners. The selected SASE services provider should have a stake in the customer's success, given the relative immaturity of the market.



# THE SECURITY GAP THREAT TO RURAL BROADBAND SUCCESS

BY: A10 NETWORKS

## What utility co-ops need to know about DDoS attacks and how to protect their broadband investment?

Spurred by government funding, utility co-ops are spending millions to build-out fiber networks that provide high speed connectivity to unserved and underserved communities – to bridge the digital divide. However, there is another gap – the security gap that is equally important. That investment and the high-speed experience it delivers can be stopped dead in its track when your network is subjected to DDoS attacks. DDoS attacks can disrupt availability to your entire subscriber base or target specific, often critical, organizations such as hospitals and schools.

A comprehensive strategy for DDoS detection and mitigation will help co-ops create a sustainable business that meets the higher expectations of post-pandemic subscribers and entice new business prospects to your community. High speed and low price are no longer sufficient differentiators.

So, what is a DDoS attack and what can utility co-ops and other regional ISPs do?

### DDoS Attack Trends

Initially, hacking was a challenge, just something to do because it could be done. Next came political hacktivism and targeting websites to support a pet cause.

Motivations have now evolved — or devolved — to one of humankind's oldest motivators: greed.

Today's hackers are largely in it for money: Shaking down companies with DDoS for Bitcoin threats and ransomware, and disgruntled workers extorting protection money from former employers. Small-to-mid-sized companies (SMB) are particularly attractive for extortion-based DDoS attacks, while large companies — with their security expertise, deep-pocketed resources, and bandwidth to spare — are more resilient in the face of extortion threats. DDoS attacks, often combined with ransomware, have surged in the last couple of years and comprise over 60% of all security incidents, according to Verizon. Every year, the size, duration, and frequency of DDoS attacks increase. The average attack costs \$20-40,000 per hour.

Today, largely due to the inexpensive availability of DDoS attack tools on the dark web and the over 15M DDoS weapons available to attackers, DDoS attacks can be launched by anybody from anywhere to anywhere. For example, In November 2021, Microsoft mitigated a DDoS attack targeting an Azure customer with a throughput of 3.45 Tbps and a packet rate of 340 million PPS – believed to be the largest DDoS attack ever recorded. According to Microsoft, this was a distributed attack originating from approximately 10,000 sources and from multiple countries across the globe, including the

United States, China, South Korea, Russia, Thailand, India, Vietnam, Iran, Indonesia, and Taiwan.

Most DDoS attackers would prefer to stay out of the headlines, so they target smaller, less defended organizations. Despite media attention relative to large volumetric attacks, 90% of DDoS attacks are under 10 Gbit/s, and the average is only 115 Mbit/s.

These smaller DDoS attacks may not even be detected by Tier 1 carriers. However, for a typical co-op or regional ISP serving 50,000 subscribers or homes, a 10 Gbit/s level attack can significantly impact service quality or availability. In that scenario, a 1 Gbit/s attack could take out IT services for an ISP's downstream customers, like a small hospital or school.

### **Anatomy of the DDoS Attack – the basic**

There are multiple types of DDoS attacks targeting different vulnerabilities in protocols, applications, and networks, but here is an overview of the most common categories:

#### **Volumetric Attacks, Reflected and Amplified**

Volumetric attacks overwhelm internet service provider networks or downstream enterprise customer websites with huge traffic flows, thus throttling the traffic handling capacity of a victim's network connections. Large volumes of traffic gridlock targeted internet access networks with junk traffic, thereby preventing legitimate users from getting through. These attacks deliver large packets directly from botnets or leverage reflection and amplification to deliver indirect traffic swells.

- **Reflected Attacks**

In what are known as reflected attacks, perpetrators use a victim's spoofed IP addresses to mask the source of their attacks, bouncing requests off third parties and thus tricking targeted servers into sending their responses back to the victim. As such, reflected volumetric attacks really have two victims of their bandwidth-consuming attacks: the target and innocent bystanders. Attackers, however, only need a small amount of bandwidth to achieve their results.

- **Reflected Amplification Attacks**

Here attackers send reflected queries to a victim calling for an enormous volume of responses to amplify the effect of reflection. For instance, using the victim's spoofed IP, the attacker might query thousands of open DNS resolvers from the pool of millions of available DNS servers armed with large amplification payloads. These small, spoofed DNS queries result in thousands of large responses directed at the victim. Attackers can also exploit NTP, SNMP, and other protocols and services that answer authenticated spoofed requests and have large payloads that can be delivered directly.

### **Application Attacks: Chewing Up System Resources**

A DDoS attack targeting the application layer is sophisticated and subtle, not a brute force assault that relies on massive data flows to take down its victim. The objective is to exhaust the victim's resources at the application layer.

The most common DDoS application attack is HTTP flood. Here, the attacker's mission is to send an HTTPGet or Post request guaranteed to make a targeted web server do lots of work, chew up lots of resources, and ultimately time-out. When it does, the requests of legitimate website users go unanswered. It doesn't take a lot of bandwidth; an unusual, complex query can do the trick.

For instance: An attacker might send a GET request to a travel application, say Expedia, looking for daily flights between San Jose and Beijing with a stopover in Zurich. The travel site queries dozens of individual airlines, the little ball spins, and spins as the session times out, and the site goes down. Or, an attacker sends a POST request for a massive quantity of records, e.g., all IP addresses associated with Google. In a short time, the web server gets bogged down servicing bogus requests.

### **Diversion, Subversion and Smokescreens**

DDoS attacks are often launched for reasons that go beyond merely shutting down a website or disrupting network availability. Increasingly, and especially during multi-vector attacks, perpetrators, typically

nation-state actors or commercial spies, launch their attacks to distract attention and create a smokescreen to mask nefarious activities, including:

- **Reconnaissance** — to scope out an organization's security posture and defense mechanisms, probe for vulnerabilities, and lay the groundwork for cybercrime.
- **Malware** — to infect networks with viruses and other malware (e.g., ransomware, keyloggers) that can be used to perpetrate criminal activities and further distract an organization's threat detection and mitigation capabilities.
- **Data Exfiltration** — the ultimate objective of a diversionary DDoS attack may be to steal confidential data, sensitive PII, valuable IP, or other proprietary information; when the DDoS attack has subsided, the criminals are already gone.

## The Changing Role of ISPs

Most ISPs host scores and scores of users and domains. Historically, their DDoS defenses have been focused on protecting their own infrastructure, not necessarily their downstream customers. For smaller DDoS attacks, the attack traffic may well be “under the radar” of many ISPs, effectively leaving important enterprise or critical community organizations to fend for themselves against the attack. If it is a large volumetric attack, once the attack traffic is identified and to protect its general network availability, the ISP will often route all inbound traffic to the victim to a black hole (dropped) until the attack subsides. While the ISP succeeds in preserving its own network, it also effectively assists the attacker in the attacker's goal – to disrupt the service of the downstream target.

Today, many ISPs are re-evaluating the level of protection they offer their downstream customers and either upgrading their DDoS defenses as a differentiator or offering more robust DDoS protection as a fee-based service to those customers.

## Next Steps for Stronger DDoS Protection

While cybersecurity challenges may seem daunting to regional ISPs, many of whom have only 1-2 people on their IT security staff, the industry is slowly

recognizing the importance of including cybersecurity in their rural broadband buildout strategies and providing more resources to assist.

- Cybershare is a small broadband provider information sharing and analysis center (ISAC), administered by NTCA and developed from a pilot program supported by a 2019 grant from the National Institute of Hometown Security.
- ISAAC (Information Sharing and Analysis Centers) helps critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards.
- CISA (Cybersecurity and Infrastructure Agency) has published a set of “Cyber Essential Toolkits,” which outlines many of the steps that can be taken and provides resources for evaluating cyber risks.

There are many actions that even the smallest ISP can take to thwart a good number of attack vectors, including doubling down on basic security hygiene and eliminating the use of default passwords, keeping security patches up to date. Other actions include:

- Create an attack mitigation plan— because it's not if, but when you will be attacked.
- Prepare for multi-vector attacks and watch out for the growing prevalence of IoT threats Cloud scrubbing is an essential element of volumetric defense, but not a panacea.
- Collaborate with your industry to collect and correlate threat intelligence and look for ways to make it actionable.
- Protect your customers and tenants from collateral damage. When DDoS attacks come, watch your back door for other security threats. Provide options to your customers for the level of protection they need.

Overall, security investment must be prioritized within the various initiatives intended to bridge the digital divide and extend broadband to unserved/underserved communities. Ransomware and other cyber threats render the infrastructure of critical services, such as hospitals, unusable, regardless of broadband access.





# WAVELOGIC ENCRYPTION SOLUTIONS

BY: CIENA

## Securing All In-flight Data, All the Time

Security has become a boardroom issue. A 2020 Thales Data Threat Report<sup>1</sup> 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. In the 2023 IBM Ponemon Institute report, it states that the average cost of a data breach on a global basis is \$4.45M where the average cost of a data breach in the U.S is \$9.48M<sup>2</sup>. 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 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.



## 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

## 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 a 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.

## Securing today's networks

Encryption is widely used today to secure both at-rest and in-flight data. According to the 2022 Ponemon Institute report, "extensive use of encryption can help lower the average cost of a data breach by \$252,088.<sup>3</sup> 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.



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

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 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.

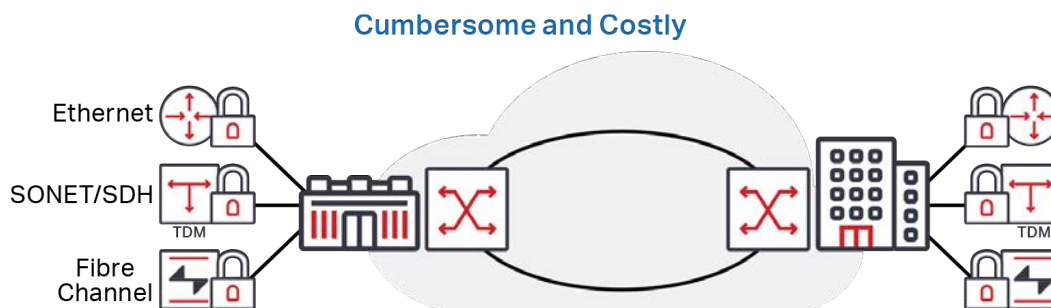


Figure 2. Traditional, protocol-specific encryption deployed in a multiservice network

## 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.

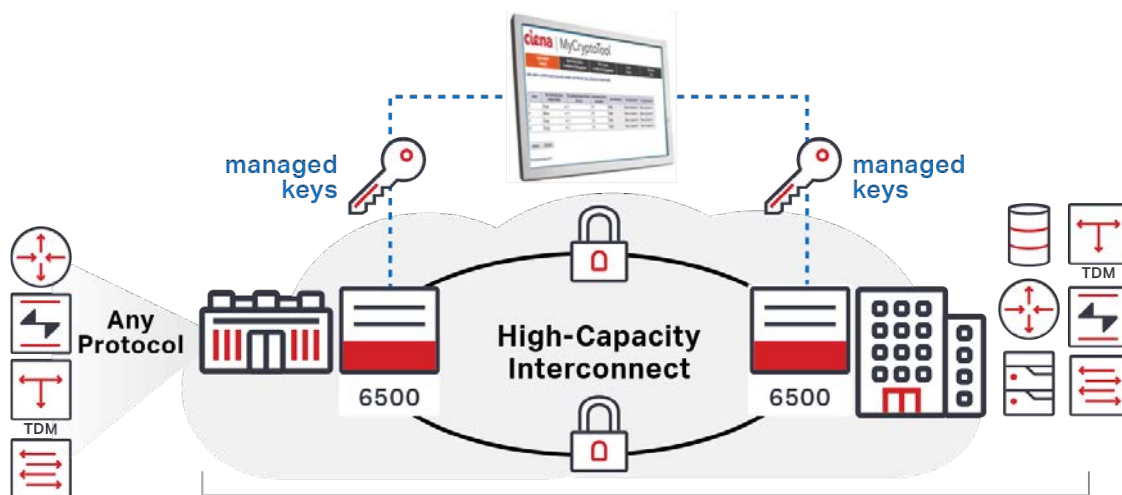
### Simple to deploy

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 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.



Carrier or Enterprise Managed Encrypted Service

Figure 3. Ciena's 6500 WaveLogic Encryption solution

## 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-highcapacity 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 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.

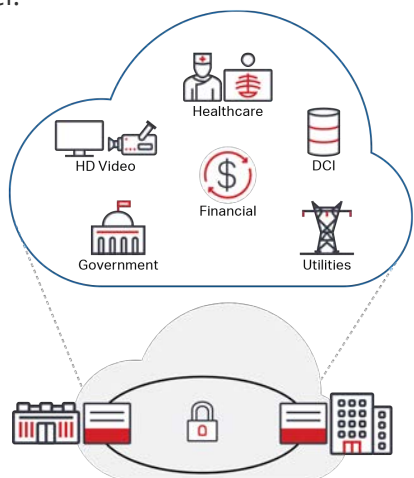


Figure 4. Examples of key WaveLogic Encryption applications

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.

## 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.

1 <https://cpl.thalesgroup.com/sites/default/files/2020-04/2020-data-threat-report-global-edition-infographics.pdf>

2 IBM Security: Cost of a Data Breach Report 2023; <https://www.ibm.com/security/data-breach>

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>

# FLEXIBLE, SCALABLE DDoS PROTECTION

BY: CORERO



Your customers demand quick, smooth and continuous digital experiences. However, the threat from evolving cyberattacks, like distributed denial-of-service (DDoS) attacks, makes maintaining service availability challenging. Even for well-resourced teams, comprehending the variety of protection options against these attacks can be overwhelming. It's an even tougher challenge when dealing with tight timelines, limited budgets and not enough staff.

## Highlights

**Flexible:** Modular DDoS protection platform, highly adaptable to changing network environments.

**Customization:** Can be customized to meet the specific needs of an organization.

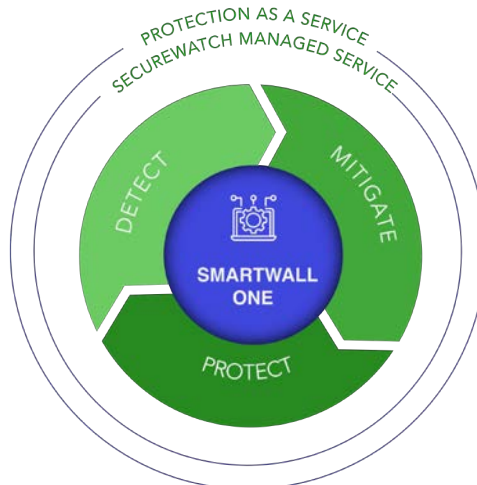
**Scalable:** Can scale up or down as needed to meet the demands of an organization.

**Cost-effective:** Organizations can choose the modules they need, reducing the cost of unnecessary features.

## The Corero SmartWall ONE Platform

These are the reasons why we've designed our SmartWall ONE DDoS protection platform around the principles of modularity and flexibility. We believe that a DDoS solution shouldn't just be effective. It should be tailored to your unique needs, fitting seamlessly into your existing network infrastructure, offering a simple approach to enhancing your security posture. What sets SmartWall ONE apart is its ability to adapt.

Whether you're just starting to build your DDoS defenses or looking to strengthen an established system, SmartWall ONE is ready to meet you where you are now and grow with your business. This platform aims to serve as a partner in your DDoS journey, providing the support you need today and preparing for the challenges you may face tomorrow.



## Detect

DDoS detection is the first step to achieving full DDoS protection. Our approach utilizes packet header and payload inspection to detect malicious traffic, as well as aggregated traffic monitoring to identify known and previously unknown attack traffic patterns.

## Mitigate

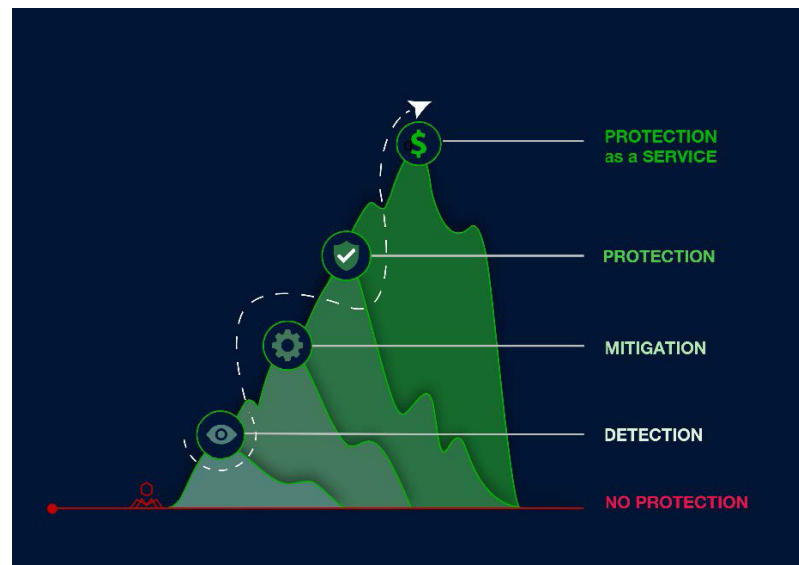
The goal of DDoS mitigation is to lessen the impact of an attack. SmartWall ONE intelligently and responsively employs the correct mitigation method to defend against the attack while protecting operations.

## Protect

DDoS protection represents the final, ongoing stage in the DDoS defense journey. While detection focuses on identifying a DDoS attack and mitigation is about reducing its impact, protection is all about implementing intelligent, automatic countermeasures that accurately separate DDoS traffic from good traffic to maintain service availability.

## DDoS Protection that Pays for Itself

DDoS protection-as-a-service (DDPaaS) is a service model that enables you to provide your customers with robust defenses against DDoS attacks. You can offer continuous monitoring and threat intelligence updates, helping your customers stay abreast of emerging DDoS attack trends. With the automated nature of SmartWall ONE and the backing of our industry experts, we reduce the burden for you to offer a DDoS protection-as-a-service. This not only enhances their security posture but also elevates their trust in your services. By offering DDPaaS, you position yourself as a proactive service provider that goes beyond providing internet services and ensures that your customers' network infrastructure is secure, resilient, and trustworthy.



## SecureWatch Managed Services

We understand that businesses like yours face unique challenges. Balancing the demands of providing top-tier services with the realities of limited budgets, staffing, and resources is no small feat. That's why we've tailored our optional SecureWatch Managed Services to address these very challenges.

SecureWatch Managed Services represent a comprehensive set of services designed to optimize configuration, monitor network activity, and respond effectively to mitigation needs. Handled by our seasoned security operations center team, this service operates around the clock to ensure you're always protected.

What makes SecureWatch stand out is that we take the time to understand your security policy requirements and business objectives. Consequently, each SecureWatch service plan is tailored to the specific needs of each SmartWall ONE customer. With SecureWatch, you're not just enlisting a managed service, you're enhancing a partnership that respects your unique requirements and business goals.

“ GARR values the automated, hands-off efficiency of the Corero solution, which frees up staff to work on other tasks. Thanks to the Corero solution, we operate more efficiently. So, we estimate that we're saving about 20% in terms of staff time dedicated to network security. It's clear that no human, or even a team of ten security analysts, could react quickly enough to manage these sophisticated DDoS attacks.” - Massimo Carboni, CTO of GARR



## YOUR ONE-STOP SHOP

Worldwide telecom & broadband partner for deployment of next generation networks and technological value-added services.



**\$2 Billion+**  
in sales revenue  
globally



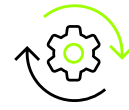
**19,000+**  
customers  
worldwide



**90,000+**  
SKUs of network  
materials



Nearly  
**1,500**  
global sourcing and  
supply partners



**19**  
countries of  
Netceed's  
best-in-class  
operations



**1 million+ sq ft**  
of warehousing and  
storage capacity  
domestically



**1,800+**  
experienced and  
dedicated team  
members dedicated  
to customer  
satisfaction &  
reliability



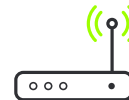
**600,000+**  
network product  
deliveries per year,  
and counting



**80+**  
locations globally  
comprised  
of corporate  
offices, logistics &  
distribution centers,  
production centers,  
and on-site sales



Distributing  
**8 million+**  
miles of fiber  
annually



Refurbished over  
**6.5 million**  
CPE units last  
year, helping our  
customers go green  
and reduce capex



Supplying  
**70+**  
carriers in Europe,  
Middle East,  
and US