HOW TO GUIDE

SELLING DDoS PROTECTION AS-A-SERVICE

THIS PRACTICAL GUIDE FOR SERVICE PROVIDERS EXPLAINS EVERYTHING YOU NEED TO KNOW ABOUT DDOS DEFENSE AND HOW TO MAXIMIZE THE BENEFITS OF DDOS PROTECTION AS-A-SERVICE FOR DOWNSTREAM TENANTS.

CONTENTS

Introduction

Distributed Denial of Service (DDoS) attacks are a major cybersecurity threat to Service and Hosting providers' infrastructure, as well as to their customers. Few providers offer sufficient protection to defend against DDoS attacks, so those that implement robust defenses are able to more effectively keep their infrastructure running optimally and gain a competitive advantage in the marketplace due to the extra security measures they have taken.

Providers who are automatically protected against DDoS, in real-time, aren't just differentiating themselves from the competition by prioritizing their customers availability and internet resiliency, but they can also generate incremental revenue by offering protection as a value-add service

This "How to Guide" includes everything a provider needs to know when it comes to DDoS defense; from understanding the current DDoS threat landscape and choosing the right solution, down to choosing how to structure and charge for the service. This guide is designed to help providers maximize the value of their DDoS protection and uncover what strategy best suits the needs of the provider.

The Growing DDoS Threat

DDoS attacks continue to rise in size, frequency and complexity, impacting the security and availability of the Internet. The latest breed of multi-vector volumetric DDoS attacks, including flood, reflection, amplification and state-exhaustion, requires mitigation in seconds, not minutes. These increasingly sophisticated cyber-threats have the potential to challenge traditional security defenses and compromise networks.

DDoS attacks have evolved considerably from when they were mostly the preserve of teenagers coding in their bedrooms to cause mischief and disruption. DDoS attacks have now become an easy method of cyber-attack, that just about anyone can launch. The rise of DDoS-for-hire botnets has caused an explosion of attacks, partly due to their cheap price point – they can be launched for just a few dollars – but also because there is virtually no technical barrier to entry because they require no coding knowledge. While the cost of launching an attack has reduced significantly, the costs incurred by the victims for lost revenue and reputation are increasingly significant. Imagine how many customers an online store could lose if a DDoS attack takes its website offline, for even a few minutes of trading.

Aside from DDoS-for-hire services, Ransom DDoS extortion campaigns have also become a common tool in the cyber-threat arsenal, and one of the easiest ways for an attacker to turn a quick profit. When service availability is threatened, the victim company needs to consider the potential loss in downtime, revenues and brand damage. When faced with these costly implications, you can understand why some organizations choose to pay the ransom in hope of circumventing an attack. Unfortunately, in most cases, this is futile: the promise of withholding attacks after the payout is often empty.

All of this makes for an extremely concerning future for the DDoS attack landscape. With Ransom DDoS attacks and DDoS-for-hire services evolving so quickly, and the capacity for future botnet-driven DDoS attacks growing incrementally, organizations must stay ahead of the game and take steps to ensure they stay protected. The best way for organizations to mitigate DDoS attacks is to get protected by the latest generation of always-on, real time, automatic DDoS protection.

Overview of DDoS Defense for Providers

Distributed Denial of Service (DDoS) attacks are a major cybersecurity threat to Service and Hosting providers' infrastructure, as well as their customers. However few providers offer sufficient protection to defend against these attacks. Those that do implement robust DDoS defenses are able to keep their infrastructure running optimally and gain competitive advantage with these added security measures.

Real-time DDoS protection has become more critical now than ever before. Expectations for Internet response and resilience comes down to seconds, not minutes. When the Internet goes down, organizations that rely on Internet services go down with it. DDoS attacks are one of the most serious and common threats to business continuity. Downtime and internet disruption can impact brand reputation, customer trust and revenue. To avoid damage to reputation and brand, provider customers are looking for protection that keeps up with the evolving DDoS threat. For providers, this is an opportunity to offer the latest generation of DDoS protection for their customers - gaining new value-add service revenue in the process.

LEGACY DDoS PROTECTION IS NOT EFFECTIVE

Today's networks require precise, rapid enforcement of mitigation policies against DDoS attack traffic. Legacy out-of-band, on-demand, DDoS scrubbing centers and cloud services introduce what are now viewed as unacceptable delays between the start of an attack and when the actual remediation efforts begin. This legacy approach is also typically resource-intensive and expensive for providers because it requires many highly trained personnel to monitor traffic 24/7. It is also prone to error, since security analysts can't react fast enough to modern multi-vector DDoS attacks that are typically short in duration, small in volume and hard to distinguish from legitimate traffic. These short, sub-saturating, attacks are cause for concern, because they still result in poor network performance and inability to access applications and services, which can lead to lost revenue, and reputation damage to organizations that rely on the Internet to do business.

A NEW APPROACH TO DDOS DEFENSE

Corero SmartWall is an innovative solution to DDoS protection, using real-time, automatic mitigation technology to enable DDoS protection at your full edge bandwidth, scaling to tens-of-terabits where previously only partial scrubbing capacity was feasible. It's a flexible solution, designed for both physical and virtual deployments, as services migrate to support the needs of 5G-enabled environments.

Providers can take a proactive stance against attacks with Corero's automatic and dynamic DDoS protection capabilities. When a business is under attack, these mechanisms automatically trigger, and operate autonomously. The detection-to-mitigation timeline is reduced to seconds, or even sub-second. That's because it eliminates the requirement to manually analyze events, and can avoid the need to reroute traffic (good and bad) in order to remove the DDoS packets.

CHOOSING THE RIGHT DDoS DEFENSE SOLUTION

Many commercial solutions are available for organizations to defend against DDoS, but not many of them fully protect against these attacks and prevent the downtime associated with them. Many DDoS mitigation solutions use legacy approaches and require manual intervention that can take minutes and, sometimes, even tens-of-minutes to block an attack, resulting in downtime for providers and their customers. When shopping for a DDoS mitigation solution, organizations should choose one that protects, not just mitigates attacks, and does so automatically, in real-time, to prevent any possible downtime and maintain business continuity when targeted by an attack.

To ensure the fastest most accurate DDoS protection, Corero's solution is designed to be deployed on-premises, at the edge, between the Internet and the network. This first-line-of-defense approach prevents outages by inspecting packets at line-rate and blocking attacks in real-time, while allowing legitimate traffic to flow. Corero's SmartWall solution eliminates the need for manual intervention saving providers time, money, and resources. Corero's on-premises defense enables complete and total protection and provides comprehensive visibility into DDoS security events. Additionally, the archived security event data enables forensic analysis of past threats for compliance reporting.

To enhance protection, Corero also offers a hybrid combination of on-premises appliances, with a cloud scrubbing service to deliver protection against the whole spectrum of attacks for organizations irrespective of their available Internet bandwidth. In the event of a massive volumetric attack which saturates Internet links, the solution can engage the cloud defenses to soak up the attack. Meanwhile the on-premises solution mitigates any other attacks and any residuals not blocked when the cloud scrubbing is active. A key benefit of the hybrid approach is that the on-premises devices heavily reduce the number of times an organization switches over to the cloud, which lowers costs and delivers a real-time, comprehensive and consistent defense.

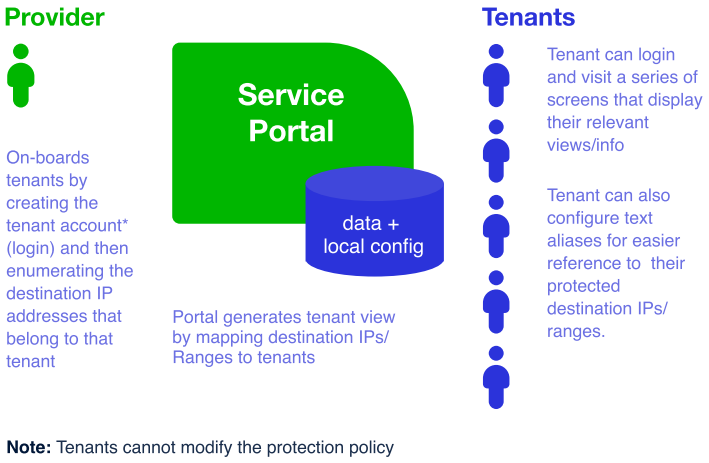
The only way to have confidence in your ability to prevent downtime from damaging DDoS attacks is to invest in an automatic, always-on defense solution. With Corero's SmartWall® DDoS protection, providers can protect themselves and their customers by offering clean transport, with enhanced security SLAs.

MONETIZING YOUR DDOS SOLUTION AS A SERVICE

Corero enables providers to easily deliver award-winning real-time DDoS protection as a premium security service to their customers.

Providers can:

- Monetize their DDoS protection, offering tiered levels of protection to tenants that deliver increasing value.
- Structure their value-add service to suit the service model
- Manage tenants centrally with our multi-tenant portal.



Note: Tenants cannot modify the protection policy

Corero's Service Portal enables providers to define and enforce the required service levels. Each tenant customer can be easily configured to deliver the level of service they are paying for.

The SmartWall Service Portal enhances Corero's award-winning real-time protection with extensive multi-tenancy and service delivery capabilities, including:

- DDoS attack monitoring dashboards globally, and per customer
- Role-based access for provider and tenant customer users
- Scheduled DDoS attack reporting and real-time alerting
- Tenant customer life-cycle management

This web application portal enables providers to onboard tenant customers, define and assign DDoS protection service levels and view attack dashboards for each. Protected customers can login to their own view, to access DDoS attack reporting and analytics, and understand the value of the DDoS protection they are receiving.

From: Provider <DDoS.Protetion@YourProvider.com>
Date: Monday, June 28, 2021 at 11:07 AM
To: Tenant <Admin@TenantCustomer.com>
Subject: DDoS Event Alert

DDoS Event:

Tenant: Demo Tenant

Attack ID: 78dad4d01c06eefd72e0277e14da30c22d1f8c4b

Attack Description: UDP Reflection from SSDP (1900) to multiple services

Attack Status: completed

Attack Start Time / Attack Event Time: 11 Jun 2021 21:06 UTC / 11 Jun 2021 21:22 UTC

Attack Duration: 960 seconds

Technical Details:

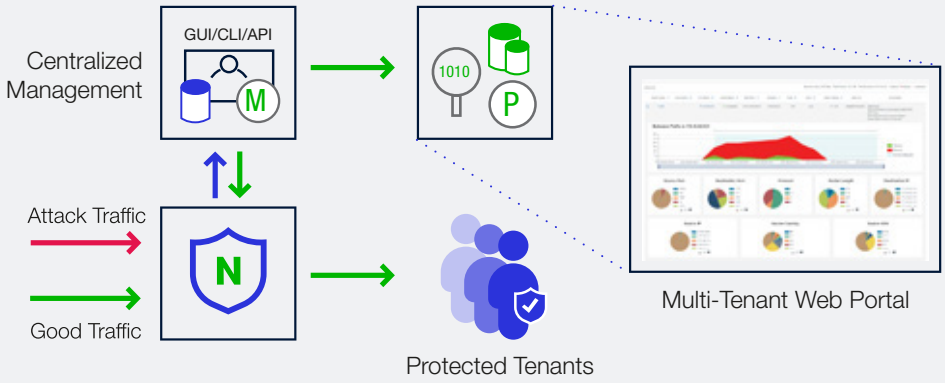
Attack IP: 172.16.4.80

Attack Max Bitrate: 203 Mbps

In the event of a DDoS attack, the affected tenant receives an automated alert, either by email or Slack and Teams notification.

Alerts are sent instantaneously and include information about each event such as attack ID, duration, and start time. Tenants can clearly see what attacks have been blocked, and are reassured that the attack has been automatically mitigated. It is also followed up with a corresponding notification when an attack finishes.

FIGURE 1
Providers can protect from DDoS attacks and offer as a service to tenants



N Network Defense Device | **M** Provider Service Management | **P** Service Portal

Structure your value-add service in a way that best suits your business needs.

Below are some examples of how a provider can offer their value-add DDoS protection service:

Customer is Unsubscribed and Provider offers basic protection – up to, say, 1Gb/s attacks

» They are under attack but not over service threshold

SmartWall Action:
Attack is automatically mitigated

» They are under attack and over current service threshold

SmartWall Action:
Choice between automatic mitigation and system alerts to upsell service level, or blackhole during attack

Customer purchased enhanced protection at $/month - up to, say, 100Gb/s attacks

» They are under attack, but the traffic volume is over the service threshold

SmartWall Action:
Choice between automatic mitigation and system alerts to upsell service level, or blackhole during attack

Customer purchased complete protection at $$$/month – Unlimited DDoS protection

» They are under attack but not over service threshold

SmartWall Action:
Attack is automatically mitigated

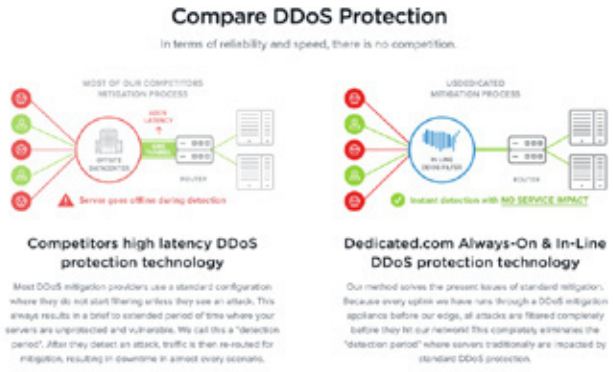
» Tenant is under attack AND links are saturating

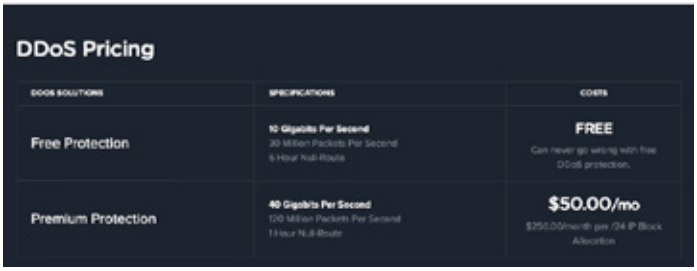
SmartWall Action:
Swing traffic to cloud scrubbing service or upstream Null-Route target to prevent impact to other tenants

ECONOMIC BENEFITS OF DDOS PROTECTION AT SCALE

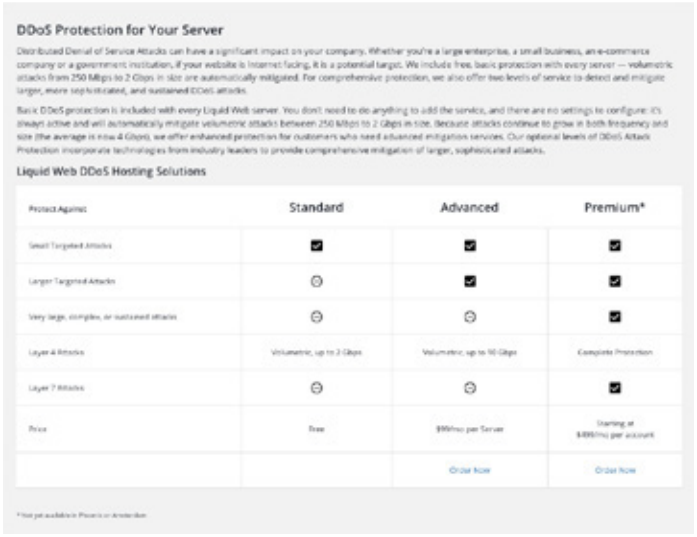
Below are some examples of Corero provider customers and how they structure the value-add service for their customers:

DEDICATED





LIQUIDWEB



Dedicated and Liquid Web are cloud and infrastructure hosting providers. They deliver a tiered DDoS protection offering to tenants, and blackhole traffic for attacks over capacity, depending on what their customer has chosen for protection.

Providers also benefit from SmartWall's local and upstream signaling capabilities which provides the flexibility needed to deal with attacks that threaten to take all their customers offline, without resorting to blocking all traffic (good and bad) to the target. The result is no downtime for the customer and peace of mind knowing that bad traffic stays out and good traffic remains flowing to keep all customers online.

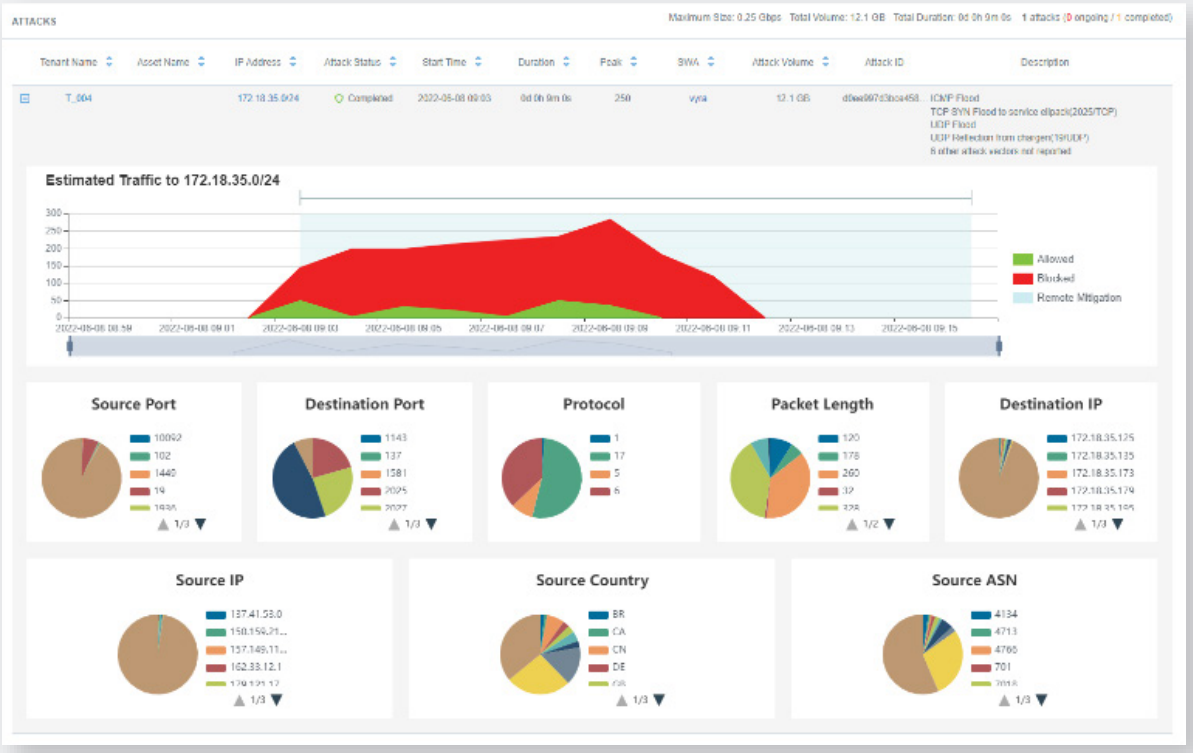
> Don't pay for downtime – keep customers online while maximizing ROI by delivering a highly effective and automated value-add service.

Many organizations struggle with how to extract meaningful real-time information on DDoS attacks. Historically, without significant investment into analysis tools and expert security staff, only minimal visibility into these classes of security events has been available. Oftenproviders and their customers are left to pick up the pieces after the damage of the DDoS attack has occurred.

Corero offers a new approach where providers and their customers can benefit from granular DDoS event data that complements their security event monitoring practice. SecureWatch Analytics delivers unprecedented DDoS visibility without requiring dedicated security analysts to sift through reams of unintelligible log data. It transforms the sophisticated Corero DDoS event feeds into dashboards of actionable security intelligence.

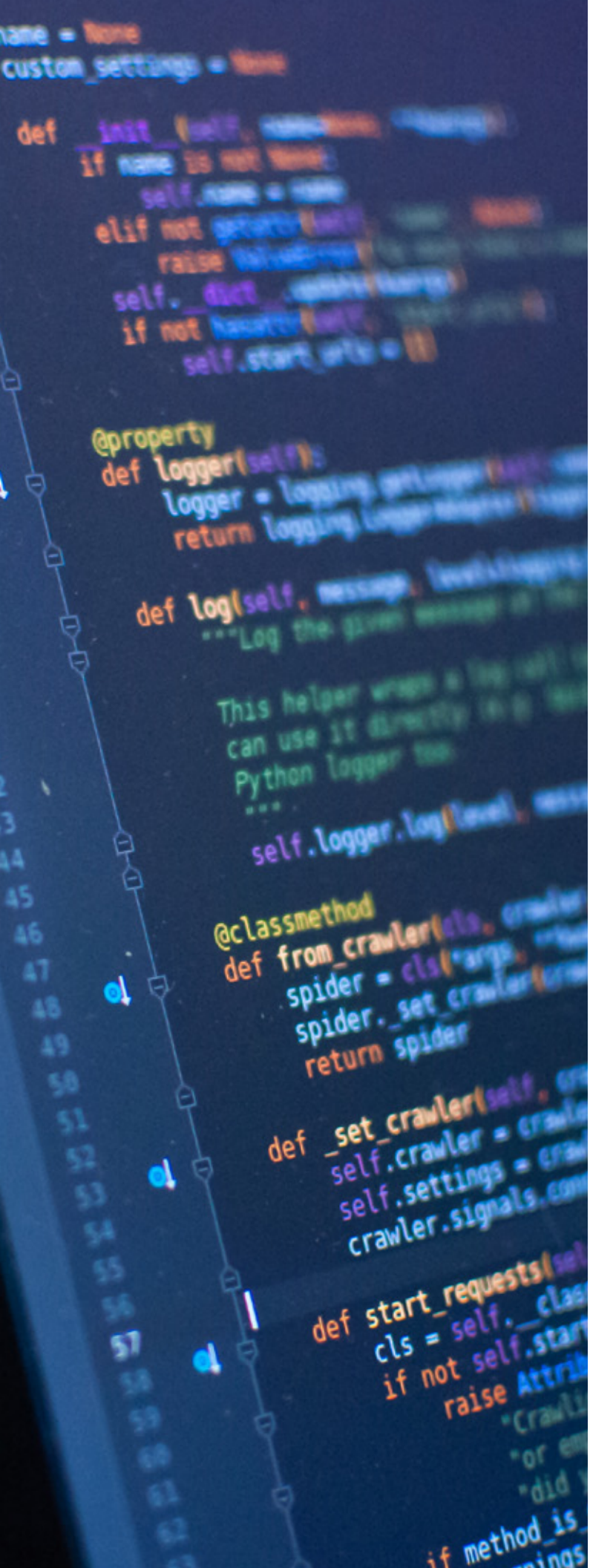
With Corero's SmartWall® DDoS protection, providers can offer cleaner transport, enhanced security SLAs, and benefit from greater visibility, reporting and forensic-level analysis. Providers can offer baseline DDoS mitigation services to all customers, but for those customers who place a premium on high availability they can create value-added options and build incremental revenue streams while strengthening their brand.

FIGURE 2
Tenant Portal shows real time DDoS attack analysis and reporting



FLEXIBLE PROCUREMENT MODELS

Corero SmartProtect also includes the flexibility for providers to purchase real-time DDoS mitigation in a way that aligns to their business model. Options include a traditional CAPEX model where costs are met up-front, or an OPEX model where costs are spread evenly over multiple years.



DEPLOYING AND MANAGING YOUR SOLUTION —

How you deploy DDoS protection is influenced by the topology of your IT environment. The type of organization, number of locations, geographic distribution, network topology and aggregate Internet bandwidth, all influence the techniques required to provide the most effective DDoS protection. Corero's three pillars for delivering effective real-time DDoS protection are:

- **SmartWall Threat Defense System**
  (TDS) appliances deployed in the incoming data path.

- **SmartWall Threat Defense Directort**
  (TDD) controlling intelligent network edge infrastructure devices capable.

- **» SmartWall Threat Defense Cloud**
  (TDC) for a hybrid combination of on-premises and cloud protection.

Whether you deploy TDS and/or TDD on-premises protection, SmartWall delivers fast, automatic, surgical protection against damaging volumetric and state exhaustion DDoS attacks. Combining this with TDC, ensures SmartWall delivers the most effective protection against DDoS attacks of all sizes. In the vast majority of cases, always-on protection alone at the network edge is the best option with the lowest latency and little to no downtime.

Corero's SmartWall solutions can be centrally managed through the CMS (Central Management Server).
The CMS can send operation, forensic, and event data to SIEMs via syslog messages and allows for programmatic control via Integrated JSON-Based REST API.

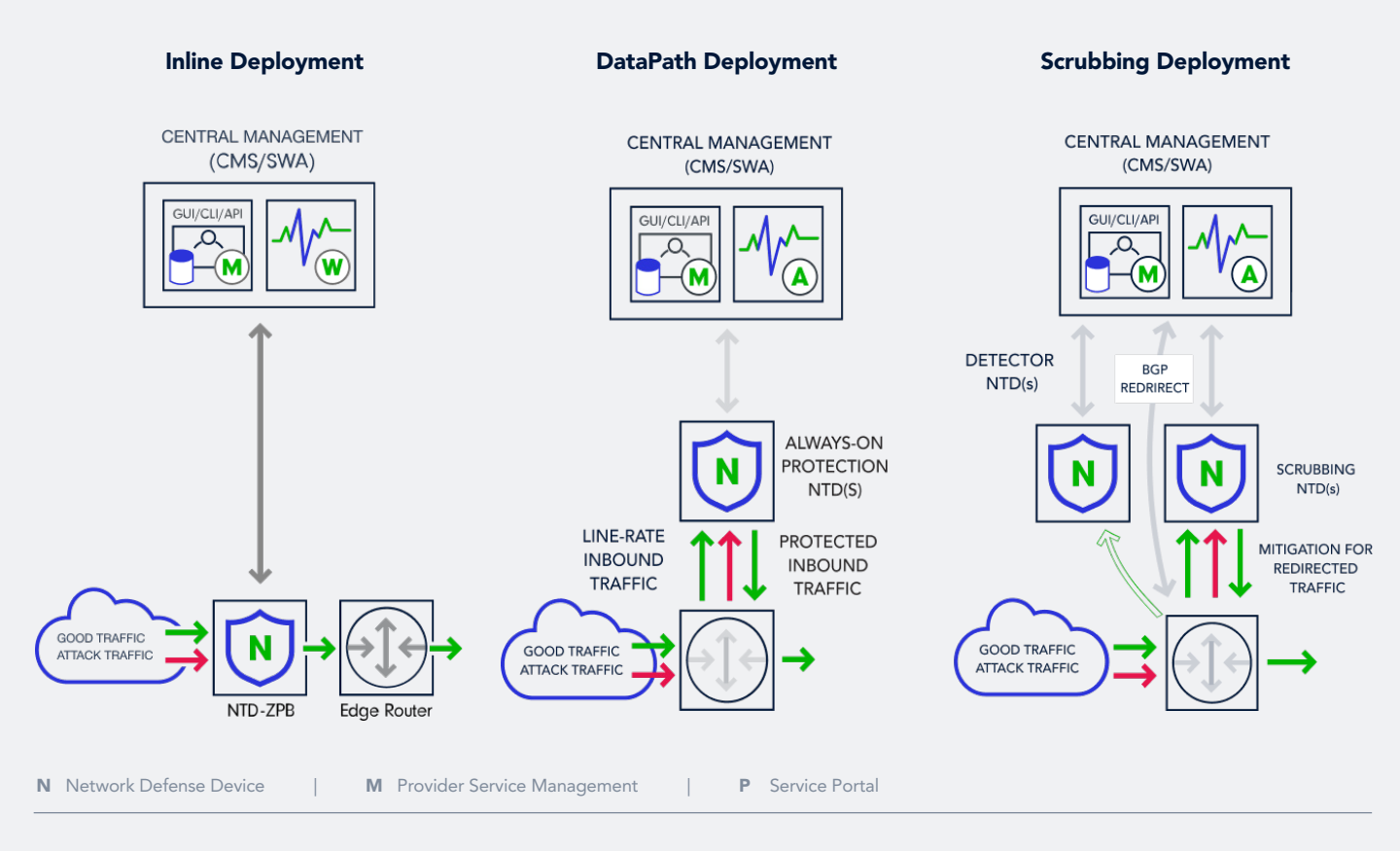
DDOS PROTECTION
WITHOUT THE HASSLE —

Whether you are experienced with DDoS protection, or not, Corero's SecureWatch Managed Services let you outsource all, or a portion of your SmartWall deployment to our experts – so you can focus on what you do best.

Corero's SmartWall solution automatically blocks over 98% of attacks, eliminating the need for on-site DDoS experts. For cases where further analysis is required to determine if an attack was missed or it was in fact some other traffic anomaly, Corero's SecureWatch Managed service delivers 24x7x365 support. In fact, 70% of SecureWatch calls are confirmed as being network issues, by our experts, and not DDoS events, which is critical information when it comes to tracking down true root causes.

SecureWatch Managed Services are a comprehensive suite of configuration optimization, monitoring and mitigation response services. This round-the-clock service, delivered by Corero's highly experienced Security Operations Center, is tailored to meet the security policy requirements and business goals of each SmartWall customer that engages in a managed service plan. Corero customers receive expert DDoS services, starting with an organization-specific implementation, continuing with round-the-clock monitoring, and immediate and effective mitigation and response, in the event of an attack. As DDoS threats continue to grow, there is an increasing shortage of trained cybersecurity professionals to defend against these threats. Investing in Corero's SecureWatch Managed Service plan will bridge that gap and allow providers to focus on critical business needs.

Customers choose a managed service plan that most effectively meets their ongoing mitigation needs. A dedicated technical account team works closely with each customer to ensure successful deployment, DDoS defense planning, rigorous monitoring and alerting, and swift response and successful follow-through. If, at any time, a provider customer is facing a particularly challenging attack, an ad-hoc service is available from Corero's SOC, at a daily rate that is available upon request.



MARKETING YOUR VALUE-ADD DDoS SERVICE

With SmartWall, providers are able to easily offer their DDoS protection as-a-Service to their downstream customers in a variety of ways:

1. Providers can offer DDoS protection included with their standard service offering, or

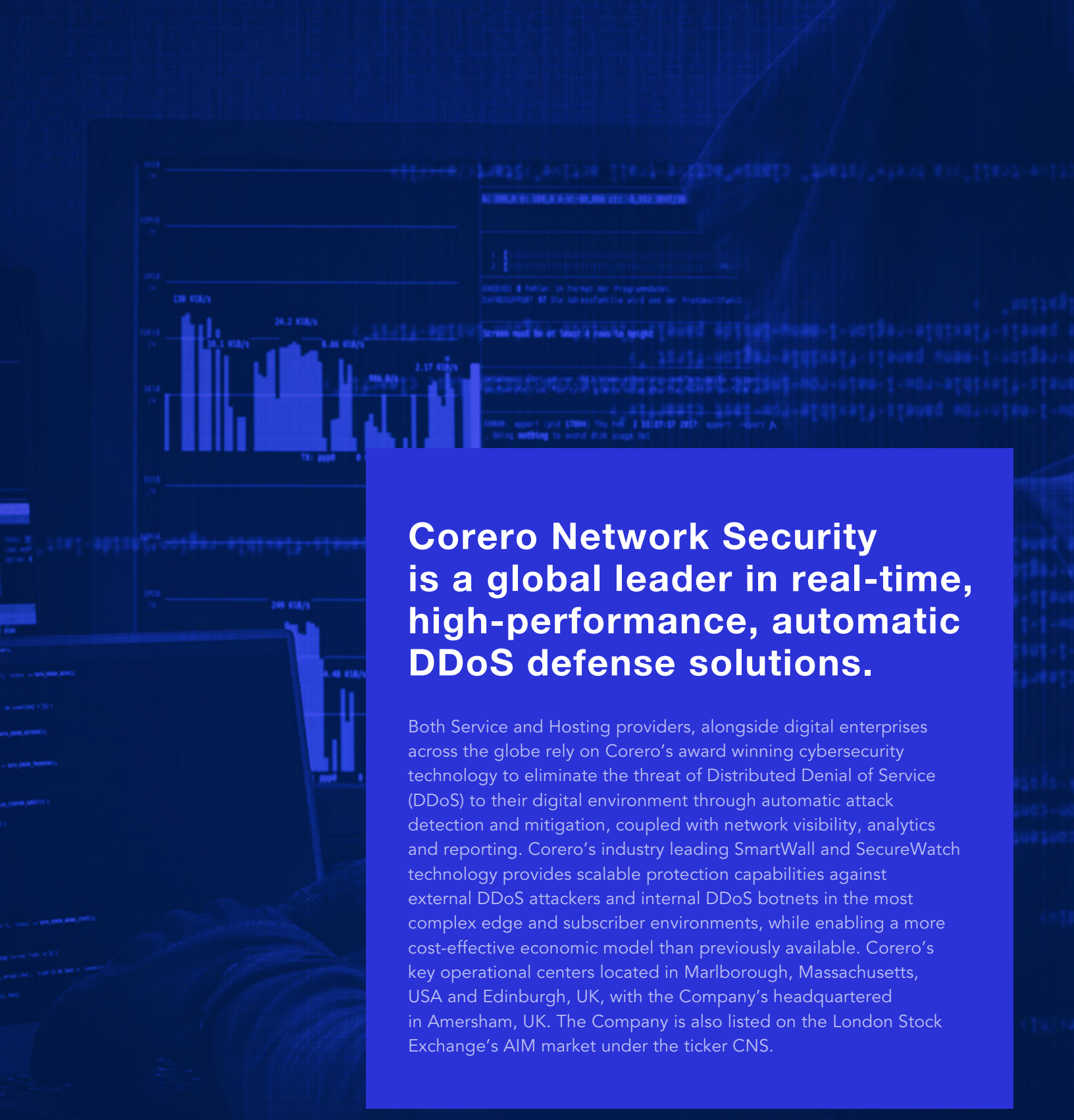
2. Optional add-on DDoS protection services, according to customer's subscription level. SmartWall's multiple service delivery options make it easy for providers to maximize their investment and deliver protection that best suits their business needs along with the needs of their customers.

We have produced a variety of collateral aimed at supporting your marketing of the DDoS Protection service:

» **Infographic** to share with prospects and customers that provides a high-level overview of why choosing a provider with DDoS protection enables customers to have the highest levels of availability

» **Solution Brief** to educate prospects and customers on the value of DDoS protection when it comes to choosing a provider to ensure uptime

» **Brandable tenant user guide**



Corero Network Security is a global leader in real-time, high-performance, automatic DDoS defense solutions.

Both Service and Hosting providers, alongside digital enterprises across the globe rely on Corero's award winning cybersecurity technology to eliminate the threat of Distributed Denial of Service (DDoS) to their digital environment through automatic attack detection and mitigation, coupled with network visibility, analytics and reporting. Corero's industry leading SmartWall and SecureWatch technology provides scalable protection capabilities against external DDoS attackers and internal DDoS botnets in the most complex edge and subscriber environments, while enabling a more cost-effective economic model than previously available. Corero's key operational centers located in Marlborough, Massachusetts, USA and Edinburgh, UK, with the Company's headquartered in Amersham, UK. The Company is also listed on the London Stock Exchange's AIM market under the ticker CNS.

US HEADQUARTERS info@corero.com **EMEA HEADQUARTERS** info_uk@corero.com

corero.com