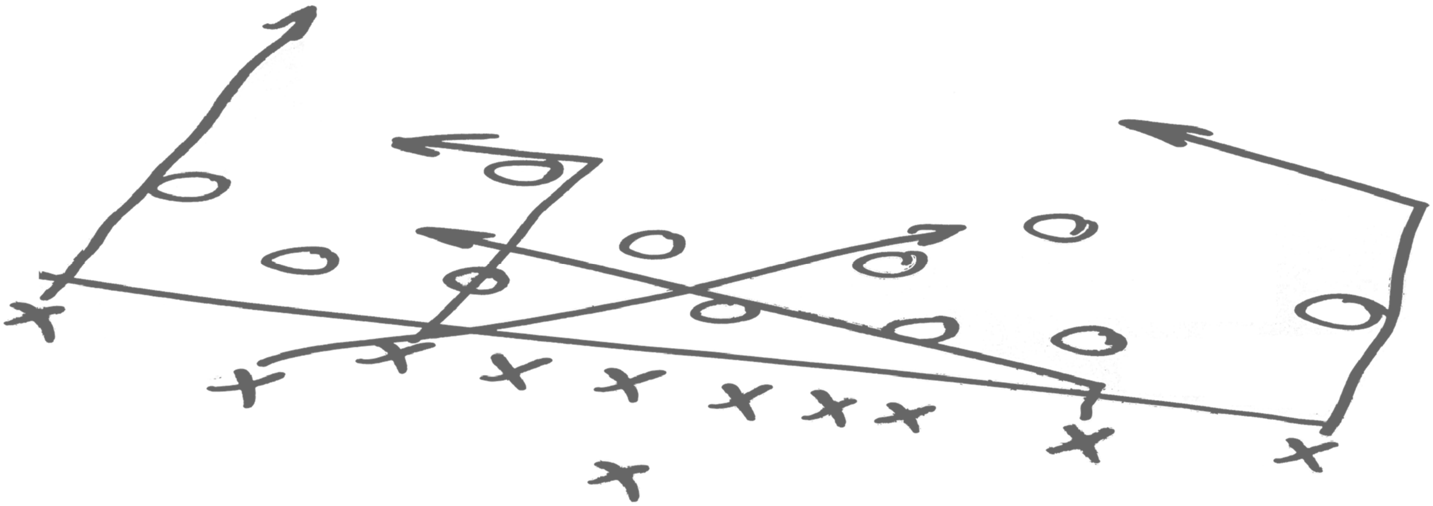
DDoS Managed Security Services Playbook



INTRODUCTION

Distributed Denial of Service (DDoS) attacks are major threats to your network, your customers and your reputation. They can also mask other security threats and are often used as a distraction while critical data is being exposed through other channels occupying your security staff's time and taking their attention away from the real attack happening elsewhere in your environment.

As a service provider, your customers count on you to provide them with the best service possible. Today that formula must include real-time DDoS protection. Simply blackholing offending traffic or relying on your upstream providers to take action is not enough to keep your customers' online applications working and not enough to protect your SLA's

The Corero MSSP (Managed Security Service Provider) program allows you to either 1) add the highest level of DDoS protection with cost-effective deployment models, further enabling additional revenue streams, or 2) increase the price premium you charge over competitors who lack sufficient DDoS protection.

THE FIRST LINE OF DEFENSE

The Corero SmartWall® Threat Defense System (TDS) is a purpose-built family of network security appliances that is designed to meet the needs of service providers.

These appliances deliver comprehensive threat defense services in simple scalable deployments with higher performance, greater reliability and broader functionality than previously possible.

Each SmartWall TDS appliance provides 10Gbps full-duplex or 20Gbps unidirectional performance in a ¼ wide, 1 RU form factor. (½ RU when passive optical bypass is used). Together these appliances protect your total network, 10Gbps at a time.

The SmartWall TDS appliance provides continuous visibility and security policy enforcement for inspecting traffic, detecting threats and blocking attacks.

It is capable of automatically mitigating a wide range of DDoS attacks while maintaining full service connectivity and availability to avoid impacting legitimate traffic. The SmartWall TDS is designed to handle volumetric network-based DDoS attacks or floods, reflective amplified spoof attacks, like DNS and NTP attacks, as well as application layer attacks that are typically too low to be detected by out of band solutions—such as slow loris, slow read etc.

In addition, the solution continuously records traffic and simultaneously retrieves specific historical packet captures for subsequent analysis of network packets, flows and trends over time. It provides the raw data for detailed visibility into detected threats and anomalous usage patterns, enabling robust network forensic analysis for regulatory compliance, corporate security incident response and law enforcement reporting.

The SmartWall (TDS) eco system is centrally managed through the Corero Management Server (CMS), minimizing IT overhead, speeding deployment and streamlining provisioning into your environment.

Corero also offers multiple integration options for configuring, controlling and monitoring the SmartWall TDS. This includes a flexible browser-based GUI, a full SSH CLI and a powerful REST API that supports open integration with existing management frameworks and seamless integration with Security Information and Event Management (SIEM) and operational Intelligence solutions, such as Splunk.

DEPLOYMENT SCENARIOS

Service Providers choose from one of two deployment scenarios; **Total Defense or Targeted Defense.**

The choice is to either protect the entire service provider environment, in which case sufficient SmartWall TDS appliances are purchased to cover the entire peering bandwidth of the service provider; or to protect specific parts of the network while allowing the remaining network traffic to pass around the SmartWall TDS appliances and into the network as usual.

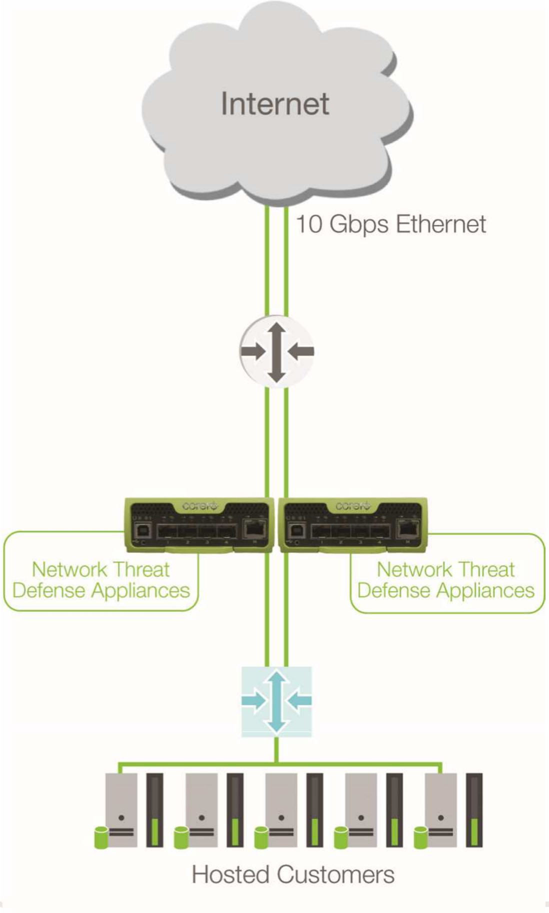
The **Total Defense** deployment scenario has the benefit of the simplest solution to manage and operate and does not preclude the provider from having multiple levels of chargeable service in their offering.

The **Targeted Defense** approach allows the provider to be a bit more selective as to where the protection is deployed, and who receives the benefits of the defense mechanism.

TOTAL DEFENSE

By far the easiest and most powerful deployment of the SmartWall TDS is to install the appliances on each inbound traffic link into your network. As each SmartWall TDS appliance is a transparent Layer-2 device, they do not change the network topology in this configuration, and require no management to determine which traffic should flow through them; your total network is protected up to the capacity of your peering links.

Active/Active High-Availability


Internet
10 Gbps Ethernet
Network Threat Defense Appliances
Network Threat Defense Appliances
Hosted Customers

The appliances can be installed either in front of or directly behind your peering edge routers and will work together with your existing link protection mechanisms to offer a fully active-active DDoS defense. This means that the loss of any link (due to the potential power failure) is no worse than the loss of a link due to any other failure today, there's no negative impact on your network reliability; only a new layer of defense against DDoS attacks.

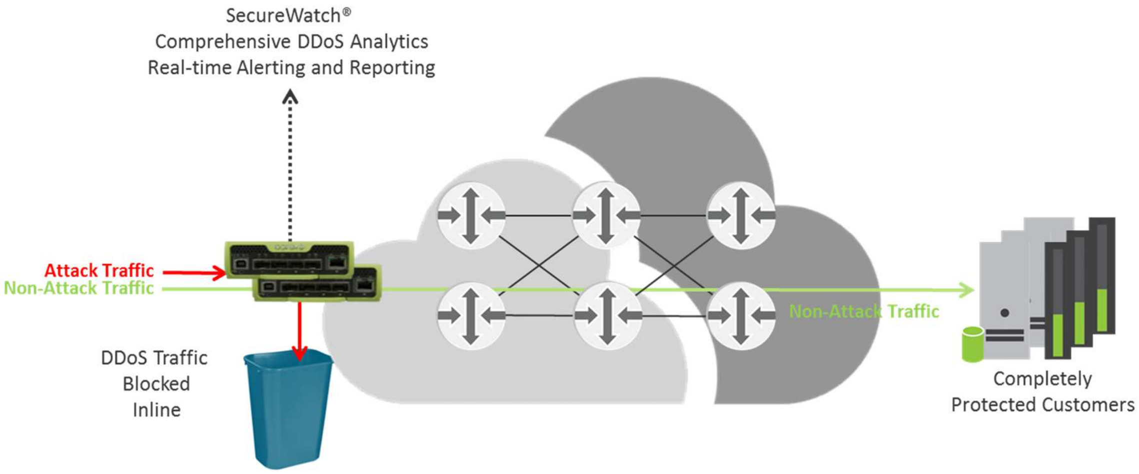
By installing the SmartWall TDS appliance in front of your peering routers you can also defend your router from the effects of attacks; this is very useful if your peering router is connecting to several different networks.

Capacity planning in this configuration also does not have to account for the total scrubbing capacity available. Because each link is naturally limited by the 10Gbps port speed, and the SmartWall TDS appliances are each capable of processing a full 10Gbps of traffic, there's no danger of ever running out of capacity.

This means that your total DDoS solution is uncontended and fully guaranteed.

Management is made simple because even though the Total Defense solution may result in a large number of units across multiple sites, they are all managed as a single system through the CMS and the attack mitigation features are automated to a great extent, meaning there is minimal support intervention once the Threat Defense System is deployed in your environment.

Lower speed links (<10Gbps) can also be consolidated via a suitable switch before being passed through the SmartWall TDS appliance and then broken out and returned to their original paths after passing through, so as to limit the number of appliances required to protect the environment.



TARGETED DEFENSE

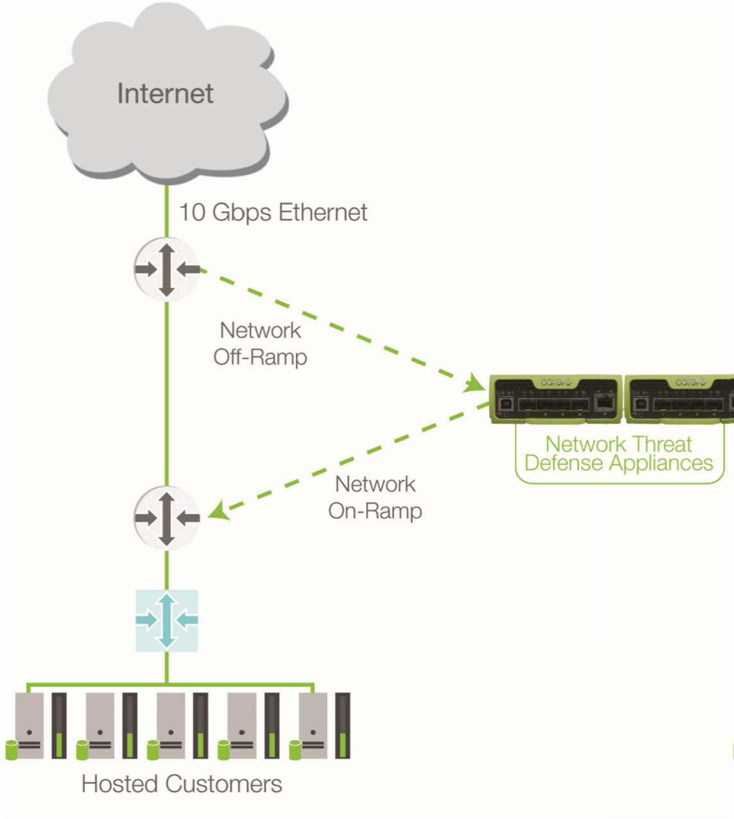
The Targeted Defense approach is most similar to other DDoS mitigation providers "Scrubbing Center" approach. The disadvantage of having to first detect the attack, then forward the traffic into the Scrubbing Center (usually a manual operation) mean that this approach often results in at least some downtime and service impact. While it is possible to use the SmartWall TDS appliances in the same type of configuration, because they are transparent Layer-2 devices on the network, it's far easier to simply "switch" traffic onto the SmartWall TDS appliances by changing the physical port used between hops in the network, without any requirement to change the network topology or routing.

This can be accomplished via many different means from both routers and switches; identifying traffic by IP mask, VLAN or any other means and then adjusting its physical path accordingly to either bypass or enter the SmartWall appliance on a link-by-link basis in the perimeter of the network.

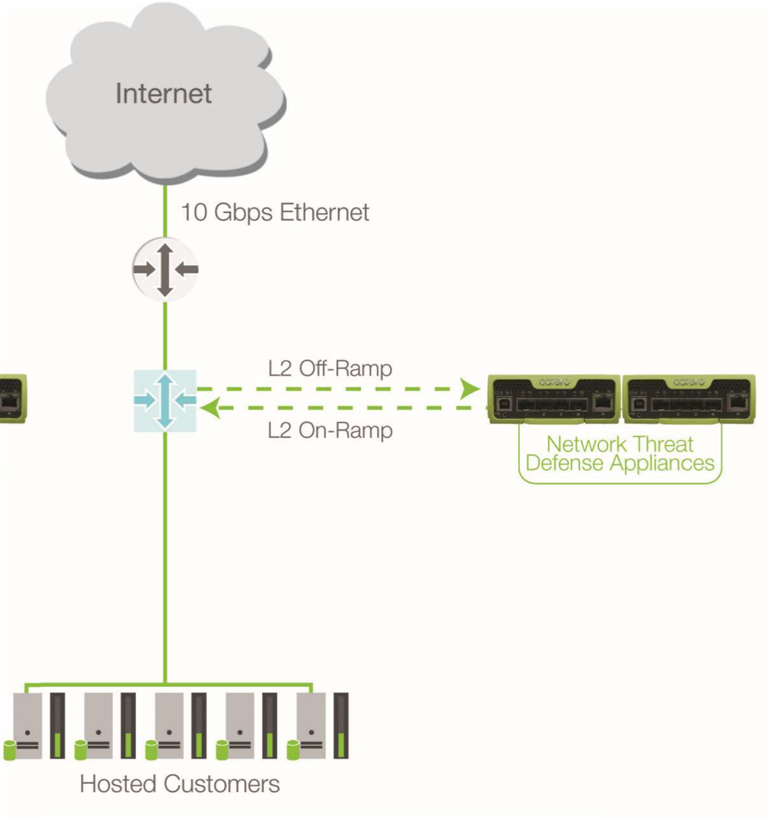
When required, the "off-ramp" link through the SmartWall TDS appliance can also be protected by a passive optical bypass module which will ensure that traffic over that link continues to flow, even in the event of the failure of the device. As the resulting bypass traffic is no-longer clean, it can be sent into another SmartWall TDS appliance or redirected into the network via another path for further control to be applied.

Scaling the solution is as simple as adding more SmartWall TDS appliances (one per 10Gbps network path) and then using the same link-bonding or load-balancing technologies currently in use. Because the SmartWall TDS appliances are totally transparent and operate at Layer-2, there is no need to make any structural changes to the network.

Scrubbing Traffic in a Routing Scenario



Scrubbing Traffic at Layer 2



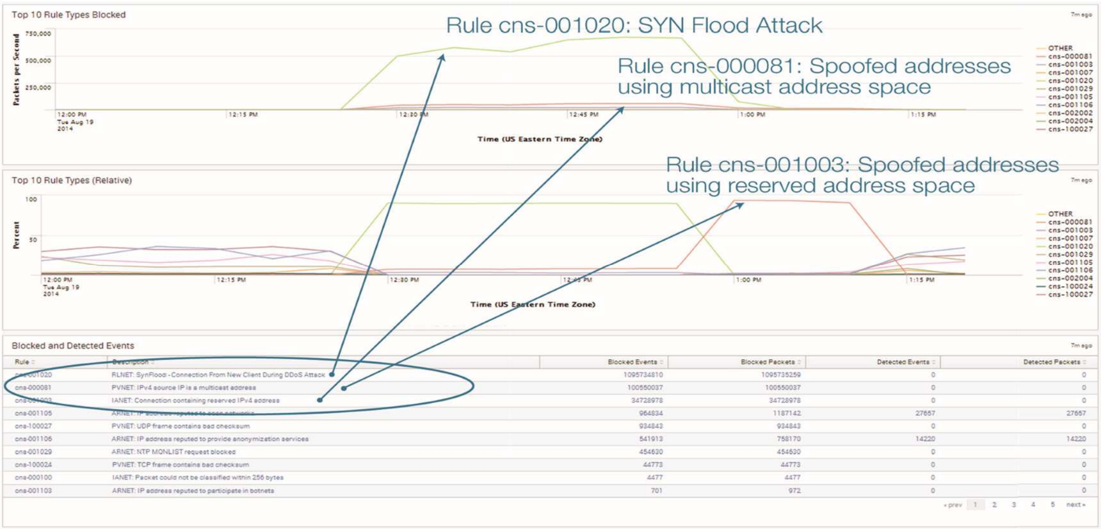
GAINING VISIBILITY INTO DDOS ATTACKS

The SmartWall TDS also offers comprehensive visibility into DDoS attacks and cyber threats that can be accessed via a flexible GUI, a powerful CLI and a full REST API suitable for being integrated into existing operational support system (OSS) infrastructure. This means that providers can potentially reduce to a single pane of glass for automated provisioning and reporting of events and alarms, and develop their own web portals, apps and tools to share monitoring and DDoS mitigation information with end customers under their own brand and identity.

Corero also offers SecureWatch® Analytics, a powerful web-based security analytics portal that delivers comprehensive and easy-to-read security dashboards based on DDoS tailored security feeds from Corero First Line of Defense products. Large hosting providers and their enterprise customers can benefit from the targeted granular DDoS event data they have been lacking that complements their security event monitoring practice. All users benefit from the turn-key analytics portal that delivers unprecedented DDoS and cyber threat visibility without requiring dedicated security analysts to sift through reams of unintelligible log data. SecureWatch Analytics is powered by Splunk, and it provides a portal that transforms the sophisticated Corero security feeds into dashboards of actionable security intelligence, exposing:

- Reflective amplified DDoS attacks
- Targeted application layer attacks
- Under the radar low and slow attacks
- Victim servers, ports, and services
- Malicious IP addresses and botnets

Security Visibility



Blocked and Detected Events

7m ago

Rule	Description	Blocked Events	Blocked Packets	Detected Events	Detected Packets
cns-001020	RLNET: SynFlood - Connection From New Client During DDoS Attack	1095734810	1095735259	0	0
cns-000081	PVNET: IPv4 source IP is a multicast address	100550037	100550037	0	0
cns-001003	IANET: Connection containing reserved IPv4 address	34728978	34728978	0	0
cns-001105	ARNET: IP address reputed to scan networks	964834	1187142	27657	27657
cns-100027	PVNET: UDP frame contains bad checksum	934843	934843	0	0
cns-001106	ARNET: IP address reputed to provide anonymization services	541913	758170	14220	14220
cns-001029	ARNET: NTP MONLIST request blocked	454630	454630	0	0
cns-100024	PVNET: TCP frame contains bad checksum	44773	44773	0	0
cns-000100	IANET: Packet could not be classified within 256 bytes	4477	4477	0	0
cns-001103	ARNET: IP address reputed to participate in botnets	701	972	0	0

« prev 1 2 3 4 5 next »

Providers can also utilize the capabilities of the SmartWall TDS to capture packet flow data to disk at 10 Gbps line rates to gain forensic visibility into network traffic. It provides line-rate network traffic capture to support deeper visibility into DDoS attacks and cyber threats. Providers can use the data to feed historical analysis of cyber threat activity, including identification of attack vectors, fingerprinting attacker identity, and breach characterization, as well as intelligence gathering for preparation against emerging threats.

CREATING ADDITIONAL REVENUE STREAMS

Once the technical deployment is out of the way, the real opportunity with the SmartWall Threat Defense System is in its ability to generate additional revenue for the operator. Most providers will use a combination of revenue protection with paid premium service as their business model for DDoS defense.

By offering a basic level of DDoS protection to all of your customers, you demonstrate that you are a conscientious and premium provider. This has proven to allow providers to maintain a price premium over competitors that do not offer DDoS protection, thereby helping you avoid price erosion in the competitive market of network and hosting services. This basic free protection usually consists of temporarily blocking IP addresses which are under attack while allowing all other network services to continue as usual.

To extend upon this basic protection and give customers the option to receive full DDoS mitigation where no good traffic is blocked and all services work as normal, an additional fee is usually charged. Corero's market studies have shown target price points as shown in the following chart:

Clean Traffic Amount	Monthly RRP (North America) Dedicated Scrubbing Capacity
0-5 Gbps	$2,000.00 per Gbps
5-10 Gbps	$1,750.00 per Gbps
10-20 Gbps	$1,500.00 per Gbps
>20 Gbps	$1,250.00 per Gbps

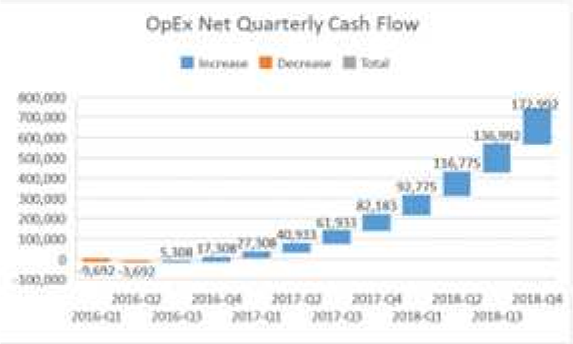
This can be a tremendous stream of additional revenue for your business. The typical ROI for an MSSP joining the Corero MSSP program is less than 6 months!

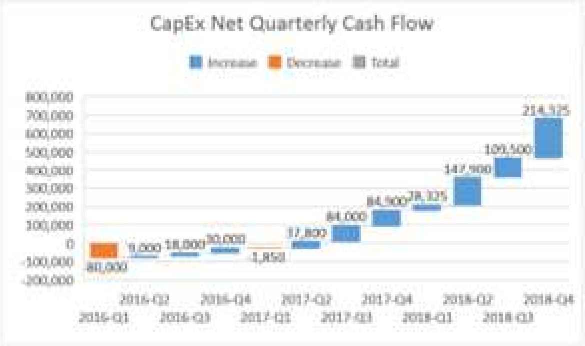
The Corero MSSP program offers flexible choices for both purchase and rental of the SmartWall appliances to suit both large and small service providers.

Depending on their deployment model, providers have the choice to match customer clean bandwidth 1:1 with DDoS mitigation capacity or tohandle customers as they may well do presently for many of their network services. The latter can be accomplished with the understanding that not all customers will be impacted at any given time, and that a lesser investment means a lower possible end-user price and greater adoption rates.

Service Provider Business Case

A small MSSP who may start with only 2 units servicing small clients averaging 0.5 Gbps of clean traffic can find themselves in profit on the CapEx plan in less than 6 months and achieve margins >60% in 3 years.





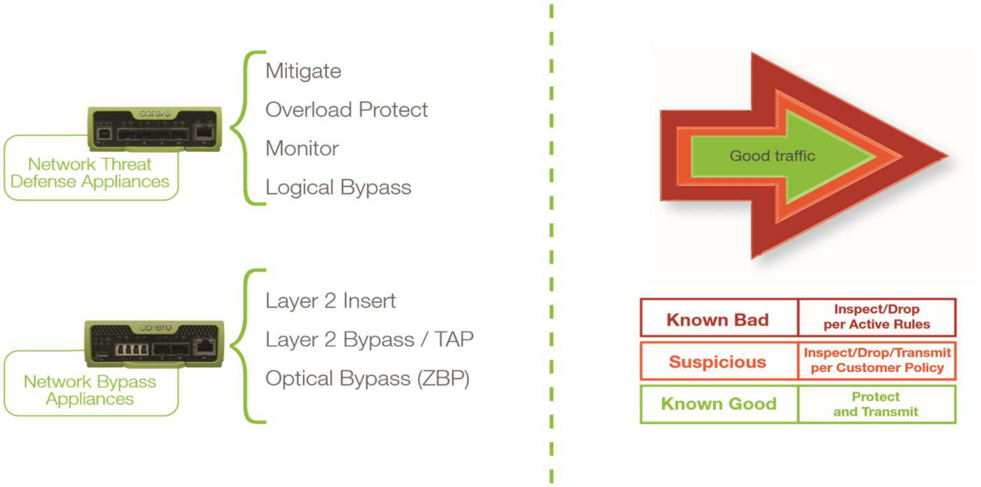
By choosing the OpEx route the same small MSSP is in profit by month 3 and achieving >60% margin in 2 years.

.

DO NO HARM

When providers implement steps for DDoS protection, false positives are always a concern. One of the failings of traditional scrubbing center deployments is that they have not been architected with sufficient performance capabilities to execute their duties at line rate. They have been relegated to scrubbing center deployments where the solution can do the least amount of damage in the event of false positives. Providers should invest in a DDoS defense solution that is designed to never drop good traffic. Corero has architected the SmartWall TDS to allow the highest possible performance for DDoS attack and cyber threat protection without incurring any false positives. Providers need to have these capabilities in place to differentiate between good and bad traffic, and respond accordingly—always allowing the good traffic to pass un-interrupted.

Do-No-Harm Architecture



Known Bad	Inspect/Drop per Active Rules
Suspicious	Inspect/Drop/Transmit per Customer Policy
Known Good	Protect and Transmit

Do-no-harm protection ensures good traffic will always get though

The Corero SmartWall TDS can be deployed inline or as an out-of-band scrubbing solution to offer hosting providers and data center operators DDoS attack mitigation and protection against a continuously evolving spectrum of DDoS attacks. Hosting providers and data center operators can enhance defense-in-depth security architectures with an additional layer of security capable of inspecting traffic arriving from the Internet at line rate, in real time.

ABOUT CORERO NETWORK SECURITY

Corero Network Security is the leader in real-time, high-performance DDoS defense solutions. Service providers, hosting providers and online enterprises rely on Corero's award winning technology to eliminate the DDoS threat to their environment through automatic attack detection and mitigation, coupled with complete network visibility, analytics and reporting. This next-generation technology provides a First Line of Defense® against DDoS attacks in the most complex environments while enabling a more cost effective economic model than previously available. For more information, visit www.corero.com.

Corporate Headquarters
1 Cabot Road
Hudson, MA 01749 USA
Phone: +1.978.212.1500
Web: www.corero.com

EMEA Headquarters
Regus House, Highbridge, Oxford Road
Uxbridge, England
UB8 1HR, UK
Phone: +44.0.1895.876579