



### Highlights

- Blocks L3-L7 DDoS and advanced targeted attacks
- Eliminates attacks that degrade or disable the IT infrastructure
- Ensures the unimpeded flow of legitimate customer traffic

### How to build your First Line of Defense today

**Step 1** — Select the correct capacity or protection cluster of DDS devices depending on the size and number of Internet connections.

**Step 2** — Install Corero DDS unit(s) in front of your firewalls as a First line of Defense.

**Step 3** — Configure and deploy defense policy based on your organizations web presence.\*

**Step 4** — You are protected! Observe continuous reporting or receive alerts of detection and control of unwanted traffic including attempted DDoS attacks.

\*Optional SecureWatch® service provides Corero Security expertise to optimize this process.



## New IT Infrastructure Perimeter - the First Line of Defense - Protects Where Firewalls Cannot

Corero's award-winning First Line of Defense solutions are real-time network attack prevention devices that redefine the perimeter of your network. They protect your IT infrastructure against sophisticated Distributed Denial of Service (DDoS) attacks, application downtime, server targeted threats, information theft and other emerging network attacks before those threats reach your firewall.

Cyber criminals/hacktivists have reached a level of complexity that firewall technology cannot protect against. While firewalls are designed to, and still do, protect networks from a variety of security issues, there are gaping holes when it comes to DDoS and malicious server targeted attacks. With attacks on the rise, such as the recent DDoS attacks against major U.S. financial services institutions, Corero has created a solution, the DDoS Defense Solution (DDS) that protects existing network and security investments and optimizes their performance by blocking not only against DDoS attacks but unwanted and malicious traffic before it enters the network. DDS does this while allowing revenue generating customer traffic to flow unimpeded to its intended destination.

These attacks happen every day.

If availability of basic services such as your website, and online sales are crucial to conducting your business then you are a potential target of cyber criminals and terrorists, regardless of your organization's size.

**First Line of Defense**

- Stop DDoS Attacks
- Protect IT Infrastructure
- Eliminate Costly Downtime

While it appears due to intense media coverage that victim organizations are high asset targets, do not be fooled. Every organization is within reach. Cyber criminals routinely scan the Internet for vulnerable organizations with security holes and then cheaply, easily and remotely take them down. If you don't plug the hole you likely will be hit again.

DDoS and malicious server targeted attacks result in loss of profits, damaged reputation, reduced productivity, and costly downtime. A sustained DDoS attack on a high transaction site can cost you over \$1million in as little as 24 hours.

Corero's new perimeter solution detects and stops bad traffic before it reaches your IT infrastructure, allowing your firewalls, Intrusion Prevention System (IPS) and other devices to perform their intended functions. As a result you eliminate downtime, your IT infrastructure operates more efficiently, and the performance of your network applications and servers are improved.

## Traditional Solutions Fall Short

While firewalls serve many purposes, they do not have complete L3-L7 protection. Designed to monitor regular levels of traffic and stop small amounts of stateful attacks, stateful firewalls fail when under extreme volumetric attacks. These traditional DDoS attacks are called network-layer attacks and are common.

### Firewalls

The firewall is an important cornerstone of any network's security and often is an organization's initial protection against Internet-based threats.

Firewalls also are often the first point of failure during a DDoS attack. This will take your site offline until the attack stops and the firewall is reset. Worse yet, some firewalls become overwhelmed and are then used as smokescreens to let more insidious attacks penetrate the network and steal information.

Cyber criminals/terrorists know firewalls are vulnerable and are now leveraging that very same firewall technology that is used to protect organizations to bring them down.

Because firewalls aren't designed to inspect all application content, an attack from an allowed IP address or port often can simply pass through a firewall undetected. This creates several problems as routine network protocols must be allowed through to facilitate certain functions such as Domain Name System (DNS) resolution.

The inability to inspect all packet content also makes firewalls ineffective against today's increasingly sophisticated and destructive application-layer DDoS attacks. Application-layer attacks, which use little bandwidth and establish legitimate connections with the target server, again go undetected by firewalls.

If request traffic is exceptionally high, the firewall has no choice but to perform rate limiting, that is, assigning more or less bandwidth to a particular connection. This will block legitimate customer traffic but it will not specifically block an attack. Rate limiting is not discriminating. It simply limits how much traffic is allowed through the firewall and that results in legitimate customer requests as well as malicious requests being denied access.

### Intrusion Prevention Systems

IPS solutions typically work in tandem with firewalls to provide greater network security. Most IPS maintain large databases of known attack signatures which must be regularly updated.

IPS solutions utilize pattern matching techniques similar to anti-virus products but have no ability to block attacks, including zero day, for which they have no signature. The attackers know

these weakness and use them to their malicious advantage. By simply manipulating a few characters in a header or payload, an attack can easily pass through today's signature-based technology and compromise network services.

### ISP and Cloud-Based DDoS Defense Solutions

DDoS attacks range from the very high volumetric attacks that fill your Internet pipes, to the most common attack seen today; the low and slow application-layer DDoS attack that shuts down web services and critical applications.

Cloud-based solutions only combat a small sample of DDoS attack vectors while ISP services simply black-hole route, throwing out the good traffic along with the bad. Additionally, most ISPs reserve the right shut down access to the targeted system or network, shutting you down to contain your DDoS attack and preserve the ISPs bandwidth to protect their other customers.

Network-layer brute force or volumetric attacks are easily blocked in the cloud due to their attack nature. However, in order to detect low and slow application-layer DDoS attacks and specially crafted packet attacks this requires significant amounts of deep packet inspection which cloud-based DDoS services do not provide.

### First Line of Defense Provides Total Protection

To stop today's DDoS and advanced targeted attacks you need to deploy a security solution that detects and stops these attacks at the gates to your organization.

Corero's DDS is a purpose built in-line networking appliance that combines full L3-L7 DDoS protection and deep packet inspection at the perimeter of your network, stopping network, application layer, and other advanced targeted attacks before they reach your firewall and/or IPS.

Taking an inspect, detect and protect approach, Corero's DDS, an organization's first line of defense, uses both signature matching as well as protocol behavioral analysis techniques to safeguard against known and yet to be discovered, zero-day attacks.

**Inspect  
Detect  
Protect**

An on-premises solution, Corero gives you complete control over detection and response, based on your policies, business practices, and application environment.

Centered on intelligent behavioral analysis, Corero uses an adaptive, patented DDoS defense algorithm to ensure your business continues as usual – blocking malicious incoming requests without impacting legitimate traffic flow to your organization's protected servers.

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

**EMEA Headquarters**  
68 King William Street  
London, England  
EC4N 7DZ  
Phone: +44 (0) 207.959.2496