



Joint Solution Brief

Real-time DDoS Detection and Mitigation with Corero Network Security and Gigamon

The Challenge

Disruptions to Internet-facing services due to Distributed Denial of Service (DDoS) attacks can cripple operations, negatively impacting customers and resulting in major financial losses for service providers, hosting providers and online enterprises.

Integrated Solution

Integrated with the Gigamon GigaSECURE® Security Delivery Platform, the Corero SmartWall® Threat Defense System (TDS) gains intelligent insight into traffic to detect and mitigate DDoS attacks in real-time and maintain availability of Internet-connected infrastructures, applications and services.

Joint Solution Benefits

- Automatically detect and surgically remove DDoS attack traffic while maintaining full connectivity.
- Aggregation, filtering and distribution of relevant traffic to the Corero SmartWall Threat Defense System accelerates processing throughput and helps ensure analysis of only traffic that provides security value.
- The GigaSECURE Security Delivery Platform inline bypass functionality supports failover protection and maintains traffic continuity for Corero in the event of a network outage or tool failure.
- SSL decryption allows for protection from encrypted sessions.

Introduction

Large-volume Distributed Denial of Service (DDoS) attacks may dominate headlines, but it's the short, frequent, low-volume sieges that continue to make up the majority of attacks. Though smaller, they can still knock firewalls and intrusion prevention systems (IPSs) offline to let attackers infiltrate networks, install malware and exfiltrate data. In other words, a flicker of an Internet outage may seem inconsequential, but it could be a sign of hackers testing for vulnerabilities and experimenting with new techniques prior to deploying them at an industrial scale.

As the leader in high-performance, automatic, scalable DDoS defense for internet service providers (ISPs), hosting providers and online enterprises, Corero Network Security provides dedicated technology for real-time mitigation of a wide variety of DDoS attacks.

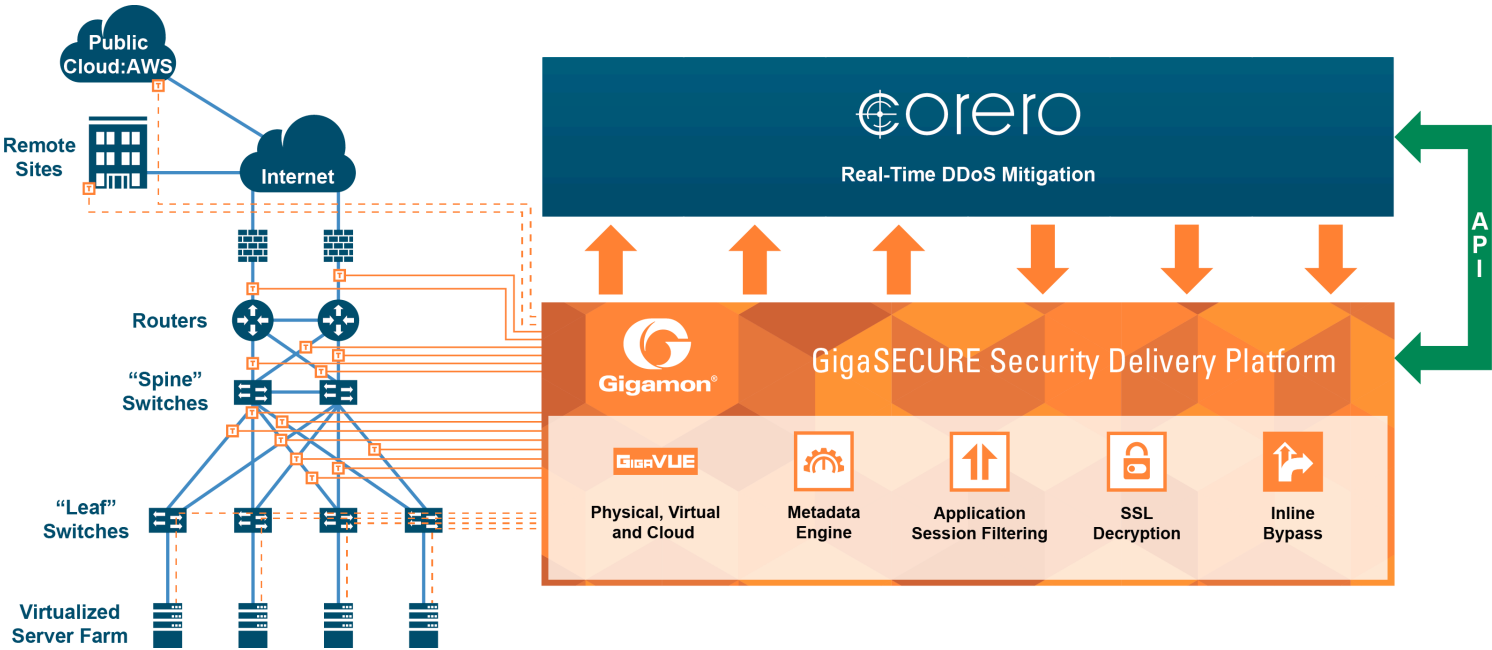
The Gigamon and Corero Network Security Joint Solution

Interoperable with the Gigamon GigaSECURE Security Delivery Platform, the SmartWall TDS gains the visibility required to automatically detect and surgically remove DDoS attack traffic while maintaining full connectivity so that legitimate user traffic flows uninterrupted. At the same time, the solution's robust reporting and analytics, powered by Splunk, can transform sophisticated DDoS event data into easily consumable dashboards for use in gauging product performance and proving value and return on investment.

Key Gigamon solution features that augment the value of Corero technology deployments include:

Traffic filtering: The GigaSECURE Security Delivery Platform sends specific traffic or sessions – such as HTTP, HTTPS and email – to the Corero SmartWall TDS for inspection and elimination of bad DDoS traffic.

Aggregation to minimize tool port use: The GigaSECURE Security Delivery Platform can aggregate links with low traffic volumes before sending them to the Corero solution to minimize the number of ports required. By tagging the traffic, the GigaSECURE Security Delivery Platform helps ensure that the traffic source can be identified.



Load balancing to spread traffic across multiple devices:

When traffic flows are larger than a single tool can handle, the GigaSECURE Security Delivery Platform can split the flow across multiple tools while helping to ensure sessions are kept together. This also facilitates incremental tool growth rather than rip-and-replace upgrades by allowing new devices to be added to those already connected.

Inline bypass for efficient and resilient deployment:

The GigaSECURE Security Delivery Platform inline bypass functionality provides physical bypass traffic protection in the event of power loss and logical bypass traffic protection in the event of an inline tool failure. Any number of Corero devices can be deployed to mitigate DDoS traffic – regardless of the speed and utilization of monitored network connections – or moved in and out of line at the touch of a button.

SSL decryption: Real-time SSL decryption integration increases traffic visibility for the Corero solution.

Learn More

For more information on Corero and Gigamon solutions, contact:

