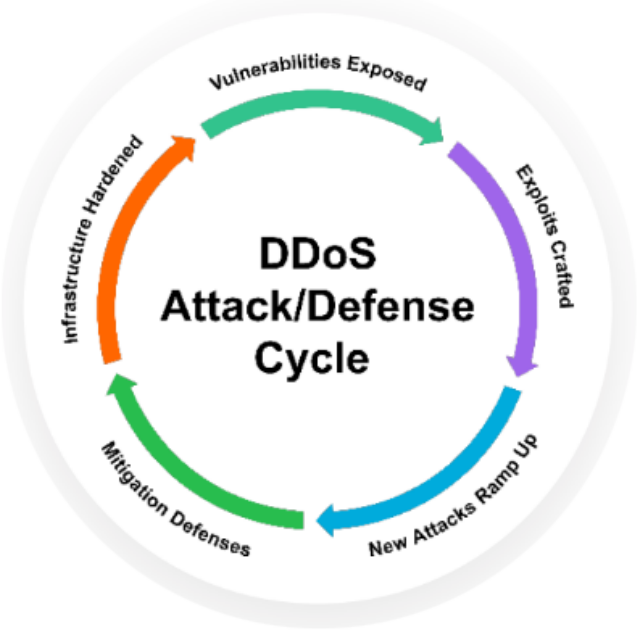
SmartWall® DDoS Protection

ZCorum™

The vast majority of DDoS attacks are small (less than one gigabit per second and less than ten minutes in duration).

But without dedicated always-on DDoS protection in place, these daily attacks, which impact business continuity and result in slow applications and failed services, can get attributed to some other IT issue. When in fact, they are preventable.



Real-Time DDoS Protection

Corero SmartWall® leads the industry with real-time, automatic, protection that keeps DDoS attacks at bay, without the downtime associated with other solutions.

SmartWall uses a patented, and automated, multi-stage detection and mitigation pipeline to ensure the highest possible protection is achieved while ensuring legitimate traffic is not impacted by damaging false-positives, or a significant increase in latency.

Unlike other DDoS protection solutions, SmartWall's Deep Packet Inspection looks into every bit of the packet header, plus the first 128-bytes of the payload, to deliver the most advanced DDoS attack detection, with surgical mitigation.

Features:

Real-Time Response
Detection and mitigation in seconds, rather than the minutes or tens of minutes taken by legacy solutions, ensuring online business continuity.

Clear, Actionable Intelligence
Comprehensive visibility with reporting and alerting for clear, actionable intelligence on the DDoS attack activity across the network.

Automatic Mitigation
Accurate automatic mitigation delivers lowest TCO and enables your IT and security teams to spend more time defending against other threats.

Highly Scalable
Flexible and highly scalable deployment options from the latest infrastructure-based enforcement, to inline and cloud.

Flexible Deployment Options

SmartWall is built on three key pillars of protection; physical and virtual appliances deployed in the network's Internet data path, central intelligence that can power the line-rate filtering capabilities of the latest generation of network infrastructure devices and cloud-based mitigation for hybrid protection.

Appliances
SmartWall TDS protects inbound connections with always-on appliances that block DDoS attack packets.

Infrastructure
SmartWall TDD protects inbound connections by enabling edge devices to block DDoS attack packets.

Cloud
SmartWall TDC protects inbound connections from saturation by blocking larger DDoS attack cloud packets.

SmartWall SecureWatch® Visibility

For all SmartWall deployments, SecureWatch analytics instantly shows the size and volume of packets in the attack, with granular visibility into every DDoS vector used, right down to the data in the packets themselves, if needed.

Contact Us

ZCorum
4501 North Point Parkway, Suite 125
Alpharetta, GA 30022
1-800-909-9441

ZCorum.com
Facebook.ZCorum.com
Twitter.com/ZCorum