CORERO SMARTWALL® INTEGRATION WITH VERISIGN OPENHYBRID™ SOLUTION BRIEF

Cloud and Premise based hybrid DDoS detection, analysis and defense against the vast DDoS attack landscape based on open APIs

KEY BENEFITS

REAL-TIME DEFENSE

Corero Smartwall® Network Threat Defense System (TDS) integration with Verisign OpenHybrid™ provides customers with an always-on, hybrid DDOS protection solution. For Verisign and Corero customers, this integration combines on-premises technology from Corero Network Security to defeat sub-saturating DDoS attacks alongside cloud-based DDoS Protection Service from Verisign for high volume and complex application layer attacks that exceed the customer's network and resource capacity. Together, these solutions are designed to provide Internet-dependent organizations with scalable DDoS protection capabilities.

COORDINATED ATTACK MITIGATION

Verisign OpenHybrid™ enables interoperability between the Corero SmartWall Threat Defense System (TDS) and Verisign DDoS Protection Service through an easy-to-use set of open APIs. This integration enables the Corero SmartWall TDS device to signal threat information back to the Verisign DDoS protection cloud and provides customers with the benefits of both local on-premise mitigation and cloud-based DDoS mitigation for high volume and complex application layer attacks.

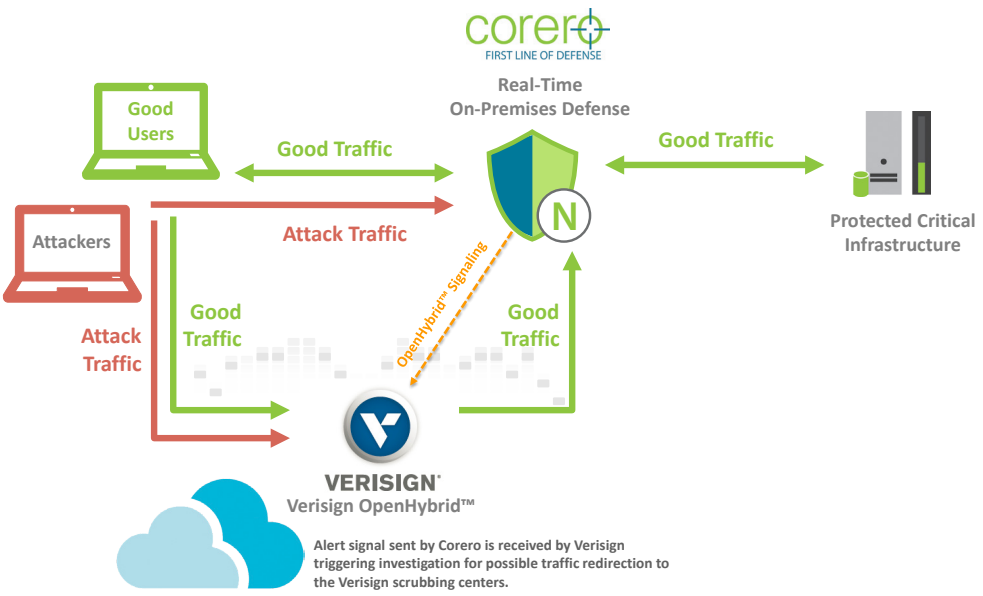
*For decades, online businesses have been tasked with defending against DDoS attacks. In today's Internet dependent world, those that rely on the Internet to conduct operations are increasingly concerned about the DDoS threat and the impact to their business, yet few have implemented a comprehensive solution to addresses the vast and adaptive DDoS attack landscape. With the size, frequency and sophistication of these attacks increasing, comprehensive DDoS protection has never before been in such high demand. Based on mitigations enacted on behalf of, and in cooperation with, customers of Verisign cloud based DDoS Protection Services, the average attack size mitigated by Verisign has grown in size by 245% from Q4 2013 to Q4 2014'**

MEETING THE DEMAND

The Corero SmartWall TDS is designed to detect and respond to a large spectrum of DDoS attacks; ranging from high volume denial of service attempts to blended multi-vector threats, as well as low and slow application layer attacks. Further, the solution detects, analyzes and responds to DDoS attacks by inspecting raw Internet traffic at line rate and identifying the threat within the first few packets of any given attack. At this stage of mitigation, the Corero do-no-harm approach to DDoS protection allows good user traffic to flow uninterrupted, while attack traffic is stifled immediately.

At the onset of a pipe saturating attack that exceeds the pre-defined attack threshold, Corero SmartWall TDS will leverage the Verisign OpenHybrid™ architecture to alert/signal the Verisign DDoS Protection Service to trigger a possible traffic redirection. With the Verisign DDoS Protection Service, customers benefit from a cloud-based DDoS protection platform and a dedicated team of technical experts who are continuously monitoring these signals and as well as customer's traffic flow to trigger appropriate mitigation responses. Verisign leverages its globally distributed network and dedicated DDoS mitigation centers to protect against high volume attacks such as DNS / NTP reflection or flood attacks. Additionally, for more complex application layer attacks such as SSL attacks or zero day attacks, Verisign utilizes its purpose-built mitigation platform, Athena, to deliver mitigation against a wide range of attacks.

JOINT DDoS PROTECTION SOLUTION FROM CORERO AND VERISIGN



Verisign OpenHybrid™ enables interoperability between the Corero Smartwall TDS and the Verisign DDoS Protection Service through an easy-to-use open API. DDoS signals from the Corero on-site device automatically generate alerts that can trigger a mitigation response from Verisign providing the customer with the combined benefits of both services. All alerts generated as a result of Verisign OpenHybrid™ signaling from the Corero appliances, and any associated mitigation event reporting, can be viewed in near real time on the secure Verisign DDoS customer portal.

As reported by the SANS Institute in early 2014, "DDoS mitigation solutions integrating on-premises equipment and cloud based mitigation architectures are nearly four times more prevalent than on-premises or services-only solutions. The growing sophistication of DDoS attacks and the sensitive nature of potential disruption to business services require both local and upstream protections that work in sync."

Corero Smartwall integration with Verisign OpenHybrid™ provides customers with the benefit of combining the resiliency and scale of cloud-based services with the real-time protection, sophisticated visibility, and the granular traffic inspection of on-premises solutions.

CUSTOMER BENEFITS

Always-on DDoS defense delivered via on-premise appliance(s)	✓
Protection against increasingly frequent partial pipe saturation attacks	✓
Superior mitigation for fully saturating, high volume, attacks that exceed network capacity	✓
Integrated solution with massive scalability	✓
Minimized operational involvement with attack re-direction to cloud, based on customer-defined thresholds	✓
Advanced real-time DDoS security event reporting and analytics on-premises, coupled with visibility of attack countermeasures applied in the cloud	✓
Next generation technology, built to grow with the needs of your business	✓

"DDoS is a complex problem to solve, but the hybrid approach to DDoS protection utilizes on premises defenses for complete traffic visibility, and real-time attack mitigation coupled with a cloud based solution for defeating full saturation attacks providing protection as needed, has become a more common strategy for the Internet connected business looking to eliminate the DDoS problem in their environment."

- JEFF WILSON, PRINCIPLE ANALYST, SECURITY, INFONETICS RESEARCH

*Verisign Distributed Denial of Service Trends Report Issue 4 – 4th Quarter 2014

ABOUT VERISIGN

Verisign, a global leader in domain names and Internet security, enables Internet navigation for many of the world's most recognized domain names and provides protection for websites and enterprises around the world. Verisign ensures the security, stability and resiliency of key Internet infrastructure and services, including the .com and .net domains and two of the Internet's root servers, as well as performs the root-zone maintainer functions for the core of the Internet's Domain Name System (DNS). Verisign's Network Intelligence and Availability services include intelligence-driven Distributed Denial of Service Protection, iDefense Security Intelligence and Managed DNS. To learn more about what it means to be Powered by Verisign, please visit VerisignInc.com.

ABOUT CORERO

Corero Network Security, an organization's First Line of Defense® against DDoS attacks, is a pioneer in global network security. Corero products and services provide Online Enterprises, Service Providers, Hosting Providers and Managed Security Service Providers with an additional layer of security capable of inspecting Internet traffic and enforcing real-time access and monitoring policies designed to match the needs of the protected business. Corero technology enhances any defense-in-depth security architecture with a scalable, flexible and responsive defense against DDoS attacks and cyber threats before they reach the targeted IT infrastructure allowing online services to perform as intended. 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