



VERISIGN™

DATA SHEET

# VERISIGN® DDOS PROTECTION SERVICES OVERVIEW

THE INCREASING FREQUENCY AND SEVERITY OF DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS ARE RAPIDLY CHANGING THE FACE OF NETWORK SECURITY. VERISIGN DDOS PROTECTION SERVICES PROVIDES A RELIABLE CLOUD-BASED APPROACH TO DDOS MONITORING, DETECTION, AND MITIGATION.

DDoS attacks continue to emerge as a growing threat to online business. Based on a recent survey conducted by Verisign, over one-third of outages experienced by organizations were the result of DDoS attacks. As a result, DDoS protection has become one of the top security and business continuity issues for any online organization. However, the common approach of stopping DDoS attacks at the network border has become an expensive and typically ineffective solution.

Verisign® DDoS Protection Services provide organizations with a reliable and scalable DDoS protection strategy. As a trusted partner, Verisign helps companies stay online without having to invest in the massive infrastructure to do so.

## DDOS ATTACKS: A GROWING THREAT

DDoS attacks intentionally deprive legitimate users of Internet resources, typically by overloading a network with a flood of data packets from multiple sources. Attackers usually create the denial of service condition by either

consuming server bandwidth or by impairing the server itself.

Today, malevolent actors are enlisting the help of compromised computers to form “botnets” capable of launching major attacks against unsuspecting victims. Estimates suggest that anywhere between 8 and 10 million computers are actively used in botnets at any time. These botnets harness the processing power and bandwidth of thousands of compromised computers to bring down the largest and most sophisticated networks. Some reports estimate that more than 10,000 attacks occur each day with recent reports of attacks reaching over 100 Gpbs.

## OVERVIEW

Verisign DDoS Protection Services help organizations reduce the risk of catastrophic DDoS attacks by detecting and filtering malicious traffic aimed at disrupting or disabling Internet-based services. Unlike traditional security solutions, the Verisign DDoS Protection Services filters harmful traffic upstream of the

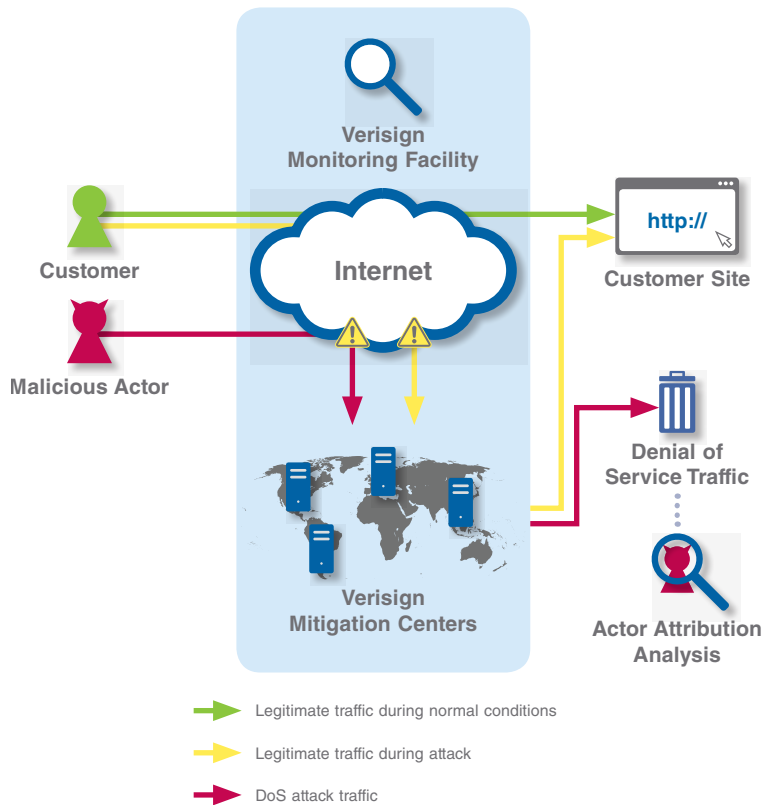
organizational network or, in the cloud.

Verisign DDoS Protection Services combine the security from Verisign's world-class traffic analysis and detection platforms with the flexibility of utilizing the mitigation components only when required. When an event is detected, Verisign will work with the customer to redirect Internet traffic destined for the protected service to a Verisign DDoS Protection Services site. The redirection happens “in the cloud,” swinging attack traffic to Verisign before it can overwhelm or otherwise harm the customer network. As Verisign monitors and analyzes traffic pattern data, the 24x7 security team begins “scrubbing” redirected traffic through the use of world-class mitigation technologies. Malicious traffic is progressively blocked while filtered traffic is sent to the customer's network, thus helping the customer sustain normal business operations.



VERISIGN™

## How the Verisign DDoS Protection Services Works



### KEY FEATURES

- Always-On Monitoring
- On-Demand Mitigation
- Easy Set-Up and Configuration
- Choice of DNS or BGP Traffic Off-Ramping
- Tunneling, VPN, or Direct Connect\* Traffic On-Ramping Options
- Detailed Event Reporting and Analysis
- Secure Customer Portal
- Requires No Customer Premise Equipment\*\*

\* Available in certain areas

\*\* If VPN is not required

## SERVICE COMPONENTS

### Monitoring

Monitoring customer traffic is critical to identifying and mitigating attacks in their infancy. Verisign collects traffic flow data from the customer's Internet-connected routers. Samples of the customer's Internet traffic are incorporated into Verisign's correlation engine for threat detection, alerts, and reporting. The frequency of packet

sampling can be tailored based on customer size, type, and router performance.

Packets are classified and analyzed by correlating a number of fields contained in the headers of the sampled packets. The packets are then broken down into categories and correlated using advanced heuristics to profile normal versus anomalous traffic patterns.

Customer traffic is monitored by Verisign's 24x7 Security Operations Center. Customer-specific alerts enable trained security experts to immediately identify nascent potential attacks. Additionally, customers can monitor their own traffic and alerts via a secure online portal.

### Threat Detection

Identifying potential events in their



VERISIGN™

early stages is critical to mitigating them before they can impact organizations. As such, Verisign continually looks for new methods to identify and classify malicious activity. Threat detection is composed of two primary components: signature analysis and dynamic profiling.

- **Signature Analysis** - Signature analysis, or misuse detection, looks for predefined deviations that are signs of a DDoS attack. Verisign uses a combination of industry best practices and proprietary intelligence to identify these signatures. Since attacks are always evolving, lessons learned from mitigating them feed into ongoing research and development to help identify new threat signatures.
- **Dynamic Profiling** - Because all customers are different and attack profiles are constantly changing, it is vital that Verisign understands each customer's "normal" traffic patterns. To do so, Verisign works with the customer to establish a dynamic profile of its Internet traffic. Deviations from the established customer profile that exceed predefined thresholds automatically activate an alert for Verisign 24x7 security teams, enabling Verisign to respond to new and one-of-a-kind attack profiles.

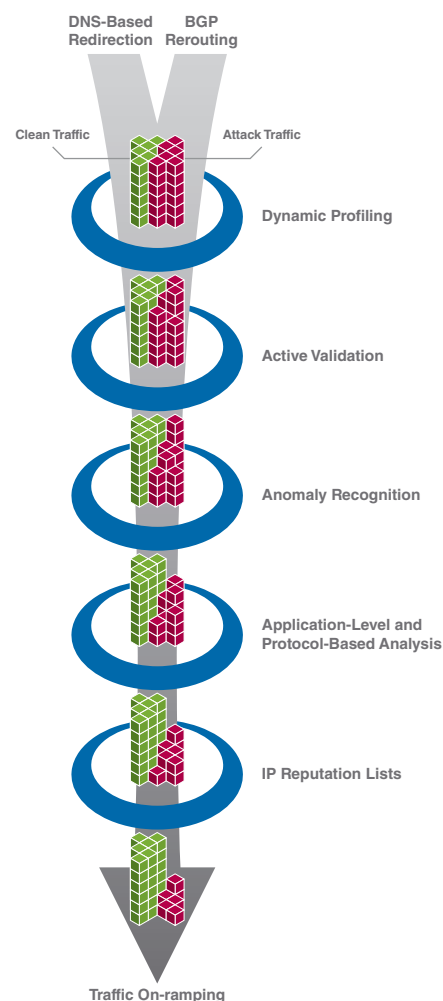
### Mitigation

Verisign establishes event mitigation procedures with the customer to fit the customer's service model. Mitigation is composed of three components: off-ramping, filtering, and on-ramping. Because timeliness

is critical to protecting customer services, Verisign works extensively with the customer during the initial set-up and testing phases to ensure a seamless implementation of all three components.

- **Off-Ramping Traffic** - Verisign security experts redirect Internet traffic destined for the customer directly to Verisign. Off-ramping occurs when a potential attack warrants traffic redirection. Verisign offers several methods for off-ramping traffic, including BGP announcements or changes to customer domain name system (DNS) records. Optimal solutions vary by customer and depend upon the size of the customer network, the types of services they utilize, and a host of other considerations.
- **Filtering** - Verisign employs a layered approach to traffic filtering that progressively enhances rule sets over time. Since blocking all traffic to a customer accomplishes the same goals as a DDoS attack, Verisign helps legitimate traffic reach its intended destination. Over time, state-of-the-art filtering technology increases the level of filtering to progressively block more malicious traffic. Filters are applied at various layers of the OSI stack. Although some attacks can be mitigated by implementing filters at the network layer, complex attacks now require analysis and filtering up through the application layer. Verisign is able to complement commercially available products with custom, in-house development

### A Layered Approach to Filtering



to create a world-class DDoS mitigation solution.

- **On-Ramping Traffic** - Once traffic is "cleaned," Verisign redirects it back to the customer's network. Verisign network architects work with the customer to establish the



**VERISIGN™**

best method for redirecting clean traffic back into its network, such as GRE tunneling, establishing a VPN, or directly connecting to a site.

### **Reporting**

Because understanding a customer's traffic is the first step in protecting critical services, Verisign provides detailed reports on customer traffic statistics to enable informed decisions. Examples include traffic summary reports, application reports, protocol reports, and event reports.

### **SUMMARY**

As malicious actors relentlessly pursue new means to sharpen their craft and avoid detection, the threats to organizational networks grow exponentially. Botnets composed of hundreds of thousands of compromised devices provide the foundation for tools that can inflict devastating attacks that not only impact revenue but damage company reputations and reduce customer confidence. Simply stated, threats are evolving at an extraordinary rate – and so too must security solutions.

Verisign DDoS Protection Services is a product of this security evolution. By mitigating threats closer to the core of the Internet, Verisign is able to effectively and efficiently mitigate some of the world's largest attacks. At the same time, Verisign is able to

quickly react to defend against the rapidly changing environment. As a proven leader in protecting critical Internet infrastructure, Verisign now provides that experience and technology to help organizations guard their own Internet assets.

### **ABOUT VERISIGN**

Verisign is the trusted provider of Internet infrastructure services for the digital world. Billions of times each day, companies and consumers rely on our Internet infrastructure to communicate and conduct commerce with confidence.

### **LEARN MORE**

For more information about Verisign® DDoS Protection Services, please contact a Verisign representative by phone at 866-367-0095 or 1-703-948-4140, by email at [insidesales@verisign.com](mailto:insidesales@verisign.com), or visit us at [www.verisigninc.com/ddos](http://www.verisigninc.com/ddos).

---

### **KEY BENEFITS**

#### **Massive Capacity and Scalability**

Sites are over-provisioned and globally distributed to protect against the largest DDoS attacks.

#### **Global Peering Relationships**

Our relationships with carriers, ISPs and other network service providers around the world provide an additional level of threat intelligence.

#### **24x7 Management, Monitoring and Support**

Verisign security analysts are available 24x7 to identify and mitigate events.

#### **Lower Costs**

Since no on-premises equipment is required, customers save time and money through operational efficiencies, reduced support costs, and economies of scale.

#### **Trained and Dedicated Professionals**

Certified security professionals undergo extensive training and rigorous background checks.

#### **Responsiveness**

Customer-specific escalation procedures are designed to detect, identify, and mitigate issues.

#### **Progressive Filtering**

Verisign network teams work with the customer to adjust filtering levels. As attack vectors are more clearly identified, Verisign filtering becomes more comprehensive.

---

[VerisignInc.com](http://VerisignInc.com)

© 2011 VeriSign, Inc. All rights reserved. VERISIGN and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign, Inc. and its subsidiaries in the United States and in foreign countries. PMS is a trademark of Pantone, Inc. All other trademarks are property of their respective owners.