

Premium Network Assurance

InfoRelay's Network Assurance gives you confidence that your network is covered in the event of a malicious attack. The increase in severity and frequency of Distributed Denial of Service (DDoS) attacks is a growing problem that without the proper response procedures, can cost your business *millions*.

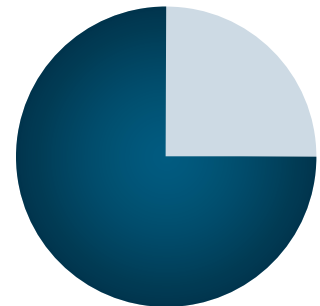
The Truth About DDoS

Distributed Denial of Service (DDoS) attacks are a growing problem for companies dependent on online systems. With the risk and size of attacks growing each year, the cost of incurring one can be devastating—amounting to millions in lost revenue.

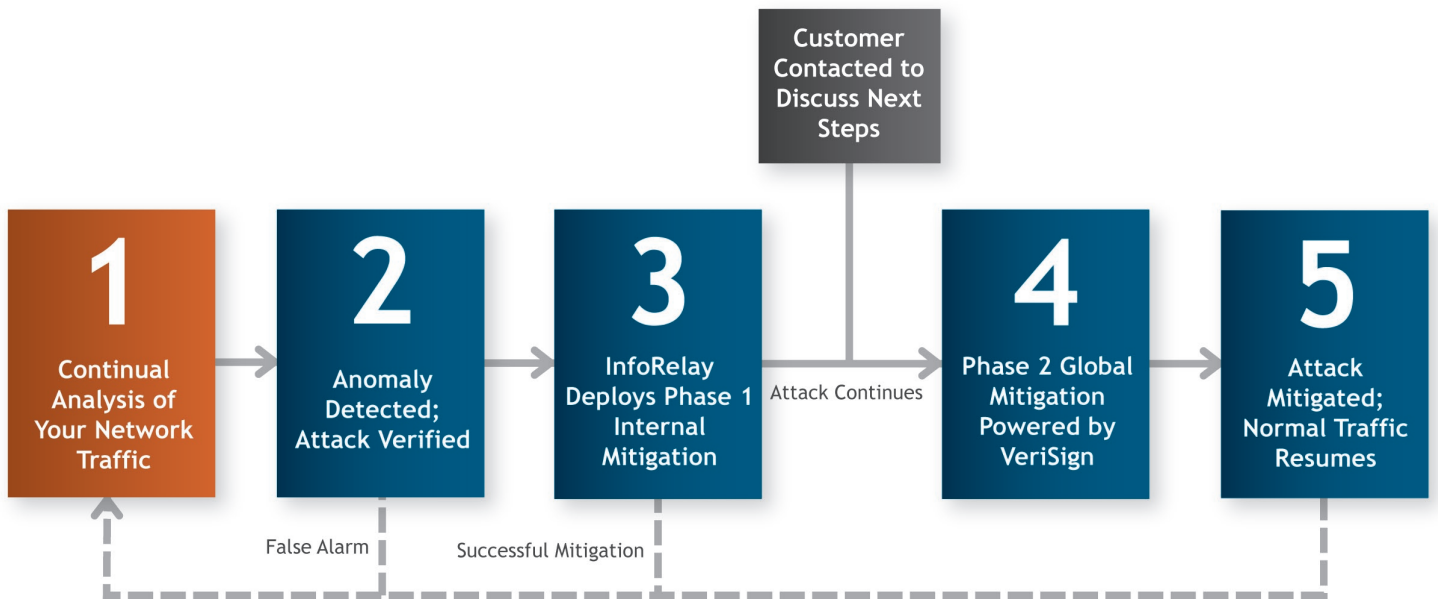
Today, perpetrators are using the help of compromised computers to form “botnets”, which are capable of launching large attacks powerful enough to bring down even the most sophisticated networks.

Here are some interesting facts:

- Arbor Networks recently revealed that a DDoS attack broke 100 Gbps for the first time; up 1000% since 2005¹
- 74 percent of 400 IT decision makers in the United States and Europe reported experiencing one or more DDoS attacks in the past year—even though they had some basic measures in place to prevent such an attack²
- Some reports estimate that more than 10,000 attacks occur each day³
- Many ISPs report attacks in excess of 10 Gbps³
- Anywhere between 4 and 6 million computers are actively used in botnets at any time³



74% of IT decision makers surveyed in the US and Europe reported experiencing one or more DDoS attacks in the past year²



How the Premium Network Assurance Plan Works

It Starts with Monitoring

Your traffic is continually monitored and analyzed 24x7 by trained technicians. Each customer is profiled so that their normal traffic patterns are identified and there won't be any false alarms. Traffic that exceeds the predefined thresholds of the customer's profile will automatically trigger an alert to a technician.

Phase 1: In-House Mitigation

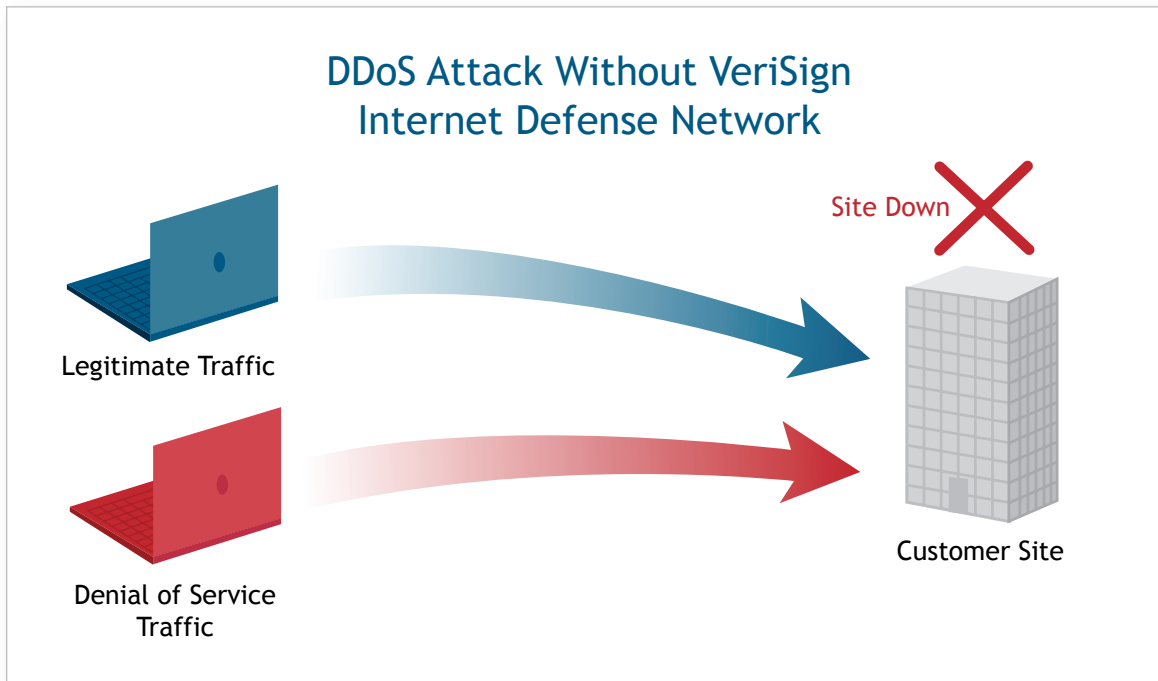
If a threat is detected and under 1 Gbps, we will initiate Phase 1 mitigation techniques with InfoRelay trained technicians, Top Layer and Cisco Premier-Grade hardware. We follow a standardized set of procedures when it comes to first mitigating attacks during Phase 1. If the attack is difficult to mitigate, utilizing more than 1Gbps, long-lasting or we are unable to resolve the issue within Phase 1, it can be escalated to Phase 2, powered by the VeriSign Defense Network. This decision will be placed on the customer.

If the client does not want to escalate the attack to VeriSign, we will continue to do our best to mitigate it in-house. If the client does choose to escalate the attack to VeriSign, a series of events will occur.

Phase 2: Mitigation Powered by the VeriSign Internet Defense Network

The internet traffic destined for the customer's site is off-ramped and redirected to VeriSign Internet Defense Network global scrubbing centers such that the traffic must pass through one of the VeriSign sites before being on-ramped again and reaching the customer's site. The traffic that passes through the VeriSign Internet Defense Network is filtered progressively to remove the DDoS traffic. As time goes on, the filters become more efficient by marking DDoS traffic in order to recognize it quickly.

How VeriSign Mitigation Works



Key Features of the Assurance Plan

- Ability to initiate Phase 2 mitigation, powered by the VeriSign Internet Defense Network
- Layered filtering of Internet traffic to ensure DDoS traffic is eliminated while valid traffic is delivered
- Continuous monitoring of your traffic
- Customer traffic profiling
- On-Demand mitigation
- Requires no customer premise equipment

What are the Benefits?

- 24x7 monitoring and support by our qualified technicians and security analysts.
- Efficient mitigation allows for minimal down time—potentially saving you millions
- Large capacity and scalability
- Global peering relationships allow for additional threat intelligence
- Escalation procedures are designed to detect, identify and mitigate issues as quickly as possible
- Peace of mind knowing that your business is protected

Get Protected Now!

Every year, cyber criminals are improving their skills and coming up with new ways to commit an attack. Don't let your business fall victim. Send an email to sales@inforelay.com or call us at (888) 55-RELAY or (703) 485-4600 now and ask about our Premium Network Assurance.

About InfoRelay

InfoRelay Online Systems, Inc. boasts a 15-year history of delivering enterprise-level managed services to businesses of all sizes. InfoRelay improves our clients' efficiency and profitability through the company's array of reliable products and services. By demonstrating unparalleled levels of responsiveness, concern, and overall service, InfoRelay establishes a unique trusting relationship with each client, allowing InfoRelay to act as a 24x7x365 extension of its clients' IT departments. For more information, please visit www.inforelay.com, follow InfoRelay on Facebook and Twitter, or call (703) 485-4600.

1 SecurityWeek.com, DDoS Attacks Exceed 100 Gbps, Attack Surface Continues to Expand, February 2011

2 Forrester® Consulting, The Trends and Changing Landscape of DDoS Threats and Protection, July 2009.

3 VeriSign, VeriSign Internet Defense Network Overview, 2011.

