staminus™
Communications

DDoS Mitigation
TREX

Start Here

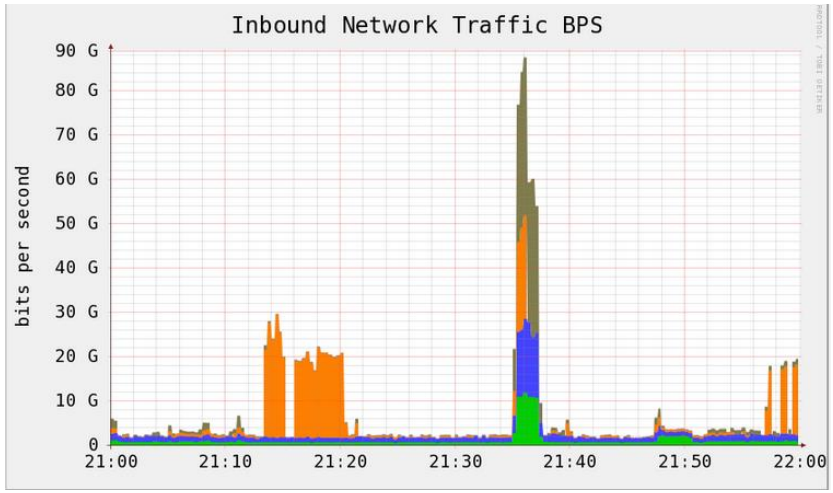
About Staminus

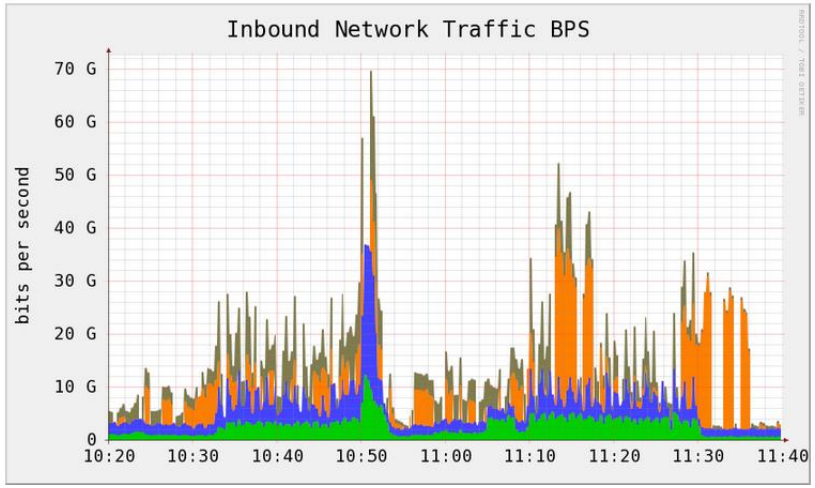
Founded in 1998, Staminus Communications provides revolutionary DDoS mitigation services to millions of users and thousands of companies around the globe.

Powered by an ever-expanding global network dedicated to DDoS mitigation and multiple patent-pending mitigation technologies, Staminus helps enterprises, ISPs, small and medium business, financial institutions, and even casual gamers protect their services' availability from DDoS attacks.

The Problem

Distributed Denial of Service Attacks





Why do people attack?

- Political Protest
- Business Espionage
- Disgruntled Employees
- To steal and sell private information
- To become Infamous on the internet
- Extortion

How easy is it to send an attack?

- 1/3 of all downtime incidents are attributed to DDoS Attacks
- You can buy and launch a week-long DDoS attack for under $150
- The black market is developing even easier ways to send attacks, such as mobile phone Apps to initiate launches.
- Its not a matter of if, but when.

+The Problem

The Real Costs of DDoS

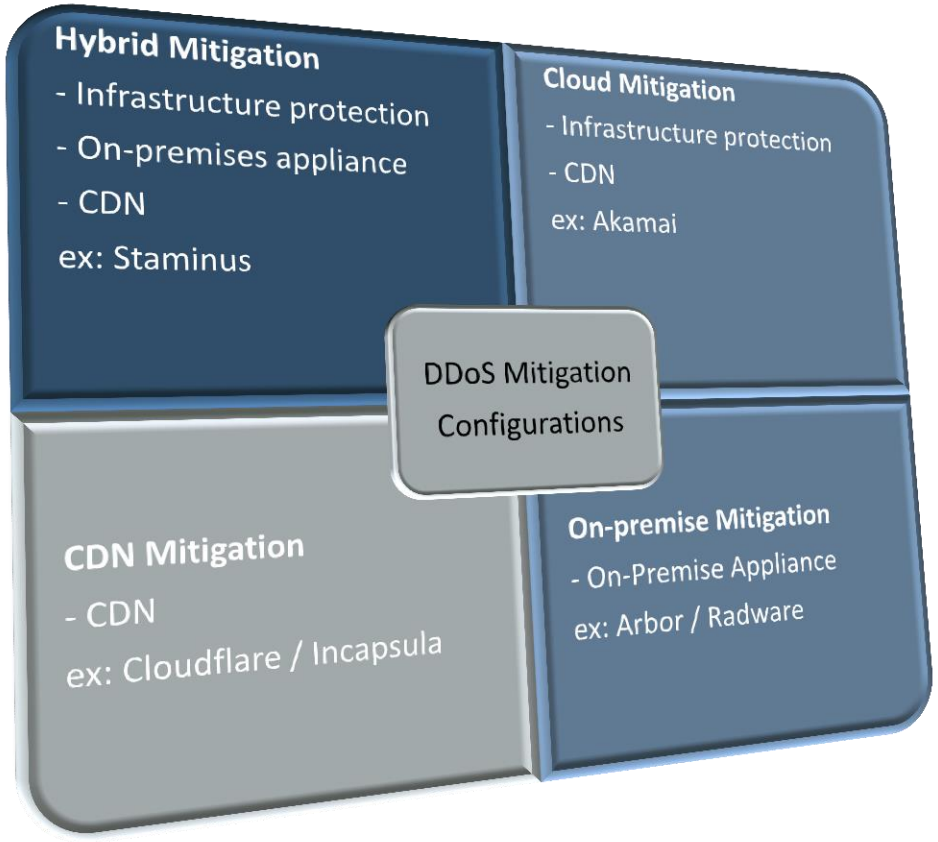
What if you were attacked tomorrow?

- Productivity Decline
- Lost Revenue
- Reputation Damage
- Customer Turnover
- Emergency Mitigation Costs
- Regulatory Actions or Lawsuits
- Cost or outside consultants
- Cover up for other cyber attacks

$10,000+ /hr

Average Loss of Revenue

Mitigation Configurations



- **Hybrid:** A hybrid solution is a combination of on premise mitigation box and remote cloud defenses. An on premise appliance provides defense against smaller volumetric attacks and application layer attacks. In volumetric attack situations, the cloud solution is able to divert the traffic into a scrubbing center before rerouting back to the customer network. True joint solutions have not been common. Cloud providers have been somewhat reluctant to move into the business of selling hardware.

Client Activation

Protection Options

On-Demand or Always-On

Customer IPs

BGP Announcement or Cross Connect

Client announces a /24 or larger prefix. In return we configure all global locations and client submits LOA for any prefixes in need of protection. Both Staminus and Client verify IRR and AS Set before BGP can go live.

Protection can be accessed through GRE tunnel, client provided physical connection, or private line.

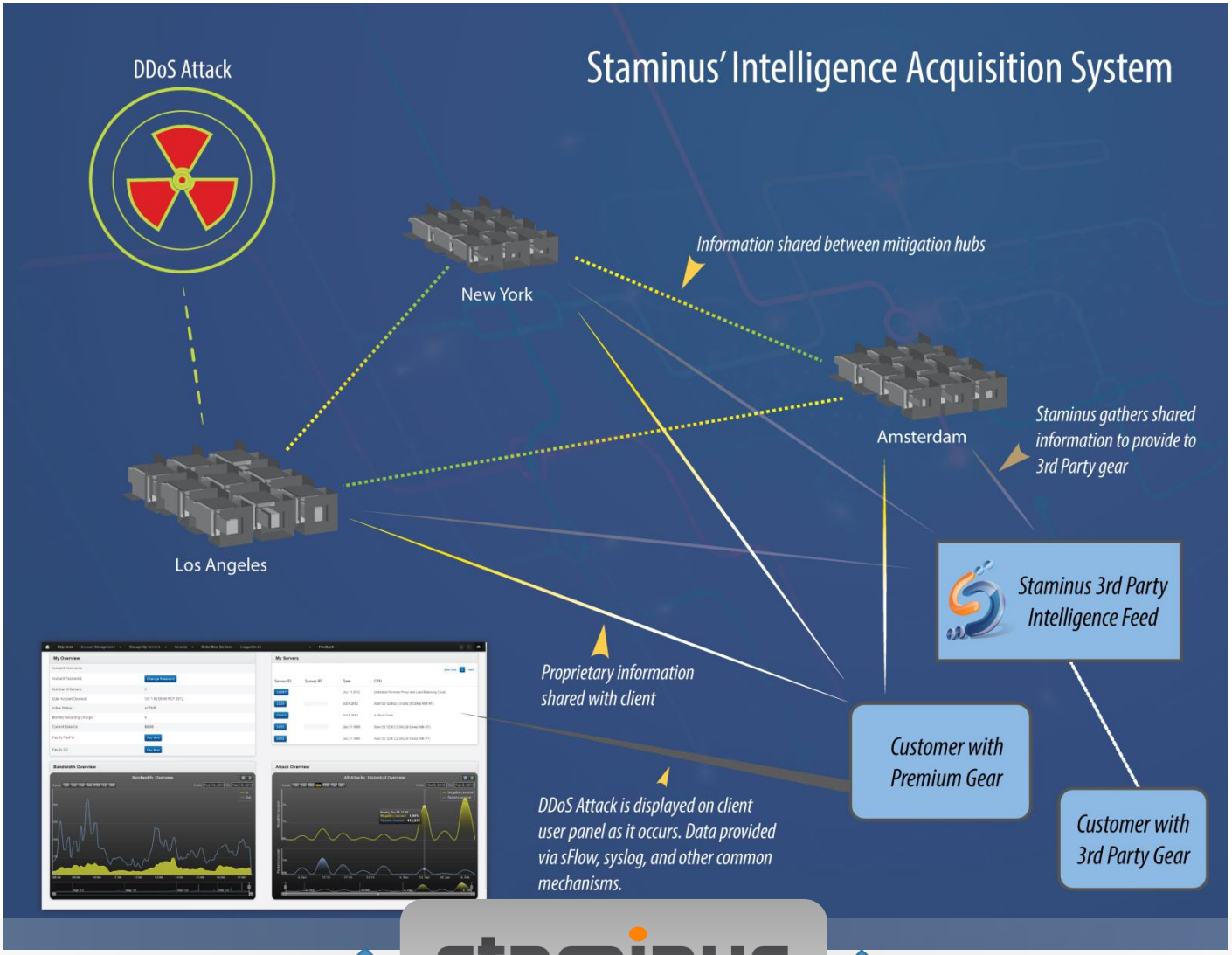
Staminus IPs

GRE or Reverse Proxy

Clients requiring /24 or smaller subnet protection can access Staminus Protected IPs via GRE Tunnel or Reverse Proxy for on-demand or always on protection.

SecureNet Configuration

Hybrid Solution Intelligence in Action



The Solution

Protection From All Attacks

Protected Layers

Broad Spectrum Mitigation

- HTTP(S) Header
- HTTP(S) POST Flood
- HTTP(S) POST Request
- HTTP(S) Get Flood
- HTTP(S) GET Request
- NTP Reflection
- DNS Amplification
- SSL Exhaustion
- TCP Flood
- Application Attacks
- SYN Flood
- UDP Flood
- Zero-Day Attacks
- Smurf Attacks
- Botnets

Plus Many More

Contact Us

For a free consultation

4695 MacArthur Court, 11th Floor
Newport Beach, CA, 92660

P. 1 866 323 8306
+1 949 202 5305
E. sales@staminus.net

Website
www.staminus.net/contact-us

Twitter
@staminuscomm

Facebook
Staminus