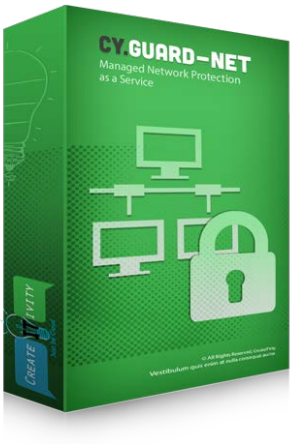
CY.GUARD-NET

Managed Network Protection as a Service

Overview



CY.GUARD-NET enables you with remote DDoS protection through Reverse Proxy or GRE Tunnel for any server or service, anywhere in the world. Powered by SecurePort:Global, the most advanced automated Global DDoS Mitigation solution in the world which enables the system to operate independently of any third-party solutions, as well as retaining full redundancy rather than relying on any single network provider. It is a culmination of over 15 years of continuous research and development and is still updated daily to stay two steps ahead of malicious attacks. Be at peace knowing your network is safe and secure 24/7/365.

Key Features & Benefits

- **Fully Automated DDoS Mitigation** – CYGUARD-NET automatically mitigates any attack without outside intervention. Other DDoS solution require manual activation and adjusting that results in unwanted downtime.
- **Complimentary Clean Traffic** – Other DDoS Mitigation providers charge you an arm and a leg for increased clean bandwidth and port speed. All CYGUARD-NET solutions come with 100Mbps clean bandwidth and a 1Gbps port at no additional charge. Stop worrying about insane overage fees or not having enough capacity to support your service and start focusing on what really matters to your business.
- **Global DDoS Mitigation Network** – With mitigation centers around the globe, CYGUARD-NET is powered with true global mitigation and redundancy allowing DDoS attacks to be mitigated worldwide near their points of origination allowing us to mitigate the largest DDoS attacks in the world. In additional, global mitigation centers gives you the lowest possible latency to keep your service running at peak efficiency.
- **The Performance** – CYGUARD-NET is powered by Rapid Detection Engine which is an all-inclusive security platform that is parallel scalable, redundant and resilient. It provides active and unobstructive latency-free protection from all attacks including SYN, HTTP GET & POST, ICMP, and UDP floods.
- **How It Works?** – Incoming data packets are initially inspected for “spoofing” using a proprietary detection technology. Normal traffic patterns are analyzed and stored as a baseline. Anomalies from the baseline are extracted from the dataset and applied to the IPS, NBA, and Reputation Engine database in order to determine which packets are legitimate. The Analysis Engine generates abnormal traffic signatures to mitigate only unwanted traffic. Normal traffic continues unimpeded by the traffic mitigation module.