# Distributed Denial of Service Protection

**Distributed Denial of Service (DDoS) attacks can strike at any time and compromise your user/customers' experience and can often shut down networks completely, resulting in lost productivity, revenue and costly bandwidth charges. Segra's DDoS protection service employs a multi-layered approach to DDoS defense to ensure your organization is safeguarded from both complex, stealthy DDoS attacks, and large saturating attacks.**

DDoS protection appliances are located at high-volume entry points on the Segra core network where attacks are most likely to occur, such as public transit connections, and automatically inspect all traffic as soon as it arrives immediately discarding malicious packets while sending legitimate packets to their destination. During this process, other network services continue to operate without interruption, even latency sensitive applications like voice and video.

## Customer Benefits

**Service Availability**
DDoS attacks aim to overwhelm a server, service or network with excessive traffic, causing legitimate users to be unable to access the services. This can lead to significant downtime and disruption of operations.

**Reputation Damage**
Frequent or prolonged service outages can damage a company's reputation, leading to a loss of customer trust and potential long-term harm to the business.

**Financial Impact**
Prolonged downtime can result in substantial financial losses, not only from lost business but also from the costs associated with mitigating the attack and restoring services.

**Security Breaches**
While the primary goal of a DDoS attack is to disrupt services, it can also be used as a smokescreen for other malicious activities, such as data breaches or malware infections.

**Operational Efficiency**
Ensuring that services remain available and operational is critical for maintaining business continuity and efficiency.

## Types of Attacks

- **Volumetric Attacks:** These attacks flood a target's infrastructure with massive amounts of traffic (measured in bps/pps), leveraging easily accessible and high-bandwidth connected devices to form increasingly powerful botnets.
- **TCP State-Exhaustion Attacks:** Exhaust protocol resources in servers, load-balancers, firewalls and routers by exploiting stateful nature of TCP protocol.
- **Application Layer Attacks:** 'Low & slow' attacks that stealthily exhaust application resources as opposed to flooding a targets network.

## Features

- Continual threat definition and behavior updates ensure the system's protection analytics are never caught off-guard by an unfamiliar mode of attack.
- As your business grows and your needs change, the system's scalable architecture adapts to provide the right level of defense no matter what.
- Infected traffic is identified and mitigated; ordinary traffic keeps flowing with minimal latency.

Let's create winning connections together.

**SEGRA**.COM • 833.**GO.SEGRA**