DDoS (Distributed Denial of Service): What it is, warning signs, and how to defend fast

Gridinsoft Help Center

What it is

How it works

- Network floods: overwhelm bandwidth (UDP/TCP floods).
- Protocol tricks: exhaust servers/load balancers (SYN, ACK, ICMP).
- Application hits: target URLs/APIs that are expensive to serve (HTTP GET/POST).
- Amplification: abuse open services (DNS/NTP/memcached) to multiply traffic.

Signs you'll see

- Site/API is slow or unreachable; timeouts climb
- Spikes from a few regions or thousands of odd IPs
- Infrastructure OK, but one URL or endpoint pegged at 100%

Defend smart (before it happens)

- Use a DDoS-capable CDN/WAF in front of everything public.
- Turn on rate limiting, challenge pages, and bot filtering.
- Lock down amplifiers you control (no open resolvers); prefer anycast edge protection.
- Create an emergency profile: cached pages, maintenance mode, and API allowlists.

If you're under attack

- Activate DDoS mode on CDN/WAF; raise challenges/rate limits for hot paths.
- Block/shape by ASN/geo/signature; throttle or drop obviously bad traffic.
- Protect the origin: only allow CDN IPs; increase autoscale limits temporarily.
- Communicate: status page and brief updates reduce support load.
- Capture evidence: traffic samples and logs help tune long-term rules.