Can DDoS Attacks Be Stopped in ZERO SECONDS?

LETS BE CLEAR ABOUT TIME TO MITIGATE (TTM)

The traditional idea of TTM is that it should be measured in time to respond, not time to stop the attack. But that’s not what every vendor can or will operationalize (SLA) means.

Zero means different things to different vendors. Some require no delay at all, while others require just a few seconds. But even when it’s clear what the TTM means, there are many variations on the theme.

Let’s start with the basic definition of TTM: the time between when a DDoS attack is detected and when it is mitigated.

VENDOR A

Vendor A’s controls must be engaged in 5-10 minutes before malicious traffic is identified. This means that if an attacker starts an attack, the vendor must have controls in place to neutralize it within the time window. 

VENDOR B

Vendor B defines TTM as the time to apply mitigation countermeasures. In the event of a sustained DDoS attack, the vendor must be able to automatically neutralize the attack within 10 minutes.

VENDOR C

Vendor C commits to responding to a DDoS attack in under 5 minutes. This includes all manually configured mitigation and any automated detection and application to optimize response.

UNDERSTAND THE T&Cs

UNDERSTAND THE T&Cs

As a customer, you need to be clear about what each vendor’s TTM means. You also need to ensure that it aligns to your business needs.

Zero TTM means:

- Immediate blocking of malicious traffic
- Immediate identification of legitimate traffic
- Immediate neutralization of attacks

What are the consequences of downtime?

- 0:01: Your website is unavailable for 1 second, and you lose an opportunity to make a sale or complete a transaction.
- 0:10: Your website is unavailable for 1 minute, and you lose an opportunity to complete 10 transactions.
- 5:00: Your website is unavailable for 5 minutes, and you lose an opportunity to complete 300 transactions.

When Zero Means Zero Seconds

When an attacker starts an attack, your vendor must have controls in place to neutralize it within the time window. This means that when an attacker starts an attack, your vendor must be able to automatically neutralize the attack within 5 minutes.

Zero seconds means:

- Immediate blocking of malicious traffic
- Immediate identification of legitimate traffic
- Immediate neutralization of attacks

Strengthen Your DDoS Protection Today

Find out how Akamai can help you achieve zero second mitigation.