Can DDoS Attacks Be Stopped in ZERO SECONDS?

LET'S BE CLEAR ABOUT TIME TO MITIGATE (TTM)

TTM should be finite, right? The time between when a DDoS attack starts and when your assets or applications are protected.

But that's not what every vendor service-level agreement (SLA) actually means. You need to understand exactly when the clock starts and stops.

BEWARE OF THESE COMMON VENDOR SCENARIOS

VENDOR A

Vendor A's controls must analyze a traffic surge for 5+ minutes before confirming a DDoS attack.

The :10 TTM SLA only starts after the attack is confirmed.

VENDOR B

Vendor B's T&Cs define TTM as the time to deploy a mitigation control – a response.

There is no committed SLA to stopping the attack.

VENDOR C

Vendor C commits to automated detection and mitigation in its TTM SLA.

Manual, customized defensive techniques to stop sophisticated attacks are not a part of that SLA.

UNDERSTAND THE T&Cs

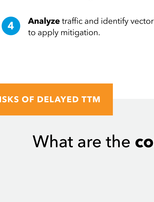
Be **skeptical** of language like:

… time to respond …

In the event of a sustained DDoS attack …

… post detection …

AKAMAI'S TIME TO MITIGATE



When **Zero Means Zero** Seconds

Our proactive mitigation controls are designed to drop DDoS attacks, protecting you before you even knew you were under attack. That's the power of the Akamai Intelligent Edge Platform.

TIME TO **Detect Attack** + TIME TO **Apply Mitigation Controls** + TIME TO **Block Attack** = **Best-in-Class Time to Mitigate**

8 STEPS FOR DDoS MITIGATION

Akamai has the fastest TTM in the industry, with a powerful combination of threat researchers, incident managers, security architects, and cutting-edge defensive technologies. Akamai's Security Operations Command Center (SOCC) executes these steps:

1. **Detect** an attack early with always-on DDoS monitoring.
2. **Alert** customer using established runbook.
3. **Manage** customer traffic with always-on facilitated routing.
4. **Analyze** traffic and identify vectors to apply mitigation.
5. **Fine-tune** applied mitigations to optimize between false positives and false negatives.
6. **Identify** new attack vectors.
7. **Analyze** traffic and identify emerging vectors to continuously apply mitigation.
8. **Optimize** applied mitigations to neutralize shifting attacks.

THE RISKS OF DELAYED TTM

What are the **consequences** of downtime?

0:01

At 1 second, your web-facing assets or applications become unavailable.

0:10

At 10 seconds, customer friction increases and employee productivity diminishes.

5:00

At 5 minutes, your brand reputation is damaged and revenue is lost.

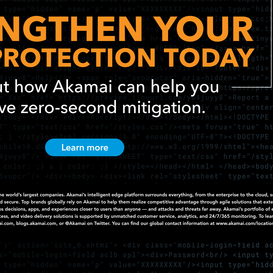
EVALUATE YOUR DDoS POSTURE

- How quickly can your vendor detect an attack?
- Would your critical applications be available?
- Would you suffer from collateral damage?
- Would legitimate users be impacted?
- How quickly can your vendor apply mitigation countermeasures?
- How quickly can your vendor start analyzing traffic?

AKAMAI THREAT INSIGHTS

Bigger, More **Complex**, and More **Dangerous**

DDoS attacks are growing to record sizes. In 2020, we observed increasingly large and complex DDoS activity; the number and combinations of attack vectors are unprecedented.



Effective defense requires the combination of a proven platform, seasoned professionals, and refined processes and techniques.

Time to mitigate should mean how quickly malicious traffic is identified *and* blocked, without impacting legitimate traffic and users.

In the end, protecting mission-critical applications, infrastructure, and brand reputation is the true measure of success.

STRENGTHEN YOUR DDoS PROTECTION TODAY

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

Learn more

Published 11/20