TIME TO MITIGATE THE RISKS OF DELAYED TTM

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

Let’s be clear about Time to Mitigate (TTM). TTM is a service-level agreement (SLA) that every vendor publishes. It sounds simple:

But that’s not what every vendor can deliver, and don’t expect Gartner to clearly mean.

Akamai has the fastest TTM in the industry, with a powerful combination of threat researchers, and leading-edge defensive technologies. Akamai’s security operations command center (SOC) executes these steps:

In the event of a sustained DDoS attack:

- Detect attack
- Analyze threat vectors
- Block attack
- Neutralize shifting attack vectors
- Mitigate attack

What are the consequences of downtime?

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Time to Mitigate (TTM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor A</td>
<td>0:01</td>
</tr>
<tr>
<td>Vendor B</td>
<td>0:10</td>
</tr>
<tr>
<td>Vendor C</td>
<td>5:00</td>
</tr>
</tbody>
</table>

Akamai’s Time to Mitigate (TTM) is calculated by the number of seconds it takes to get your brand back online, from the moment an attack is confirmed.

Can DDoS Attacks Be Stopped in Zero Seconds?

Zero means it’s Not Possible. "Zero" means the attack has already caused damage, and your brand is down. DDoS attacks are not stopped in zero seconds. There is no committed service-level agreement (SLA) that says mitigation starts and when your assets or applications are protected. It’s your responsibility to make sure that your mitigation controls are always-on, always-up, and always-understanding of the attack.

Understand the T&Cs

- Vendor A’s controls must be deployed and applied within minutes
- Vendor B’s T&Cs define TTM as the time to deploy a mitigation control—a manual, customized defense approach
- Vendor C commits to automated detection and defensive techniques to neutralize shifting attacks

A Zero TTM Defensive Initiative

Zero doesn’t mean your business can be exposed to the dangers of unmitigated DDoS attacks.

Evaluate Your DDoS Posture

- On average, your users cannot detect or differentiate between legitimate and malicious traffic within seconds.
- Malicious DDoS traffic is orders of magnitude larger than legitimate traffic.
- If your vendor cannot identify and neutralize shifting attack vectors within seconds, your business will experience downtime.

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

STRENGTHEN YOUR DDoS PROTECTION TODAY

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

Learn More