6 Must-Have SLA Metrics

The Service Level Agreement (SLA) is a crucial component of DDoS defenses. It is the contractual guarantee outlining what your DDoS mitigation provider will deliver and their obligation to remedy in case they do not meet those guarantees.

Many vendors make expansive claims about mitigation capabilities, but when it comes to contractual commitments, these claims vaporize into thin air. It is fair to say that DDoS protection is only as good as its SLA.

Use these six questions to evaluate how good DDoS protection is. Each SLA metric has a specific technical benchmark and defined business purpose. Not having one (or more) of these KPIs in your SLA document should cast doubt on your vendor's confidence in their own service, and ultimately the vendors' ability to protect your organization against DDoS attacks.

1 How Soon Can You Detect Attacks?

The first step in stopping a DDoS attack is recognizing that an attack is taking place. Many vendors will make bold claims on mitigation time, but the question is mitigation from when? The sooner an attack can be identified the sooner that attack can be mitigated. With a **Time-to-Detect** SLA, your DDoS mitigation vendor commits to how quickly they will detect an attack. Not including the Time-to-Detect leaves you exposed to the possibility that a DDoS attack could be well under way before it's noticed.

2 How Quickly Will You Let Me Know?

When something bad happens, you want to be the first to know about it. The **Time-to-Alert** SLA is crucial for ensuring that you're notified immediately if under attack. Failure to include this metric means that your mitigation provider does not commit to immediate notification of an attack, and puts the burden on you, your customers, or worse – your boss – to find out on their own.

3 How Swiftly Will You Divert?

For on-demand DDoS protection deployments, the time it takes the system to initiate diversion is a crucial step to quick mitigation. Any delay in diversion can result in needless downtime. The **Time-to-Divert** SLA commits to how fast a mitigation provider will initiate diversion once an attack has been detected. Not having this metric in the SLA likely means that the DDoS mitigation provider lacks the technology or processes to ensure fast diversion, leaving you exposed for longer periods.

4 How Fast Will You Stop The Attack?

Once an attack has been detected and diverted to your DDoS mitigation provider, the next question is how fast will it take to mitigate the attack The **Time-to-Mitigate** metric measures the speed with which DDoS mitigation vendors mitigate different types of attacks, based on attack characteristics. Although most providers provide this commitment, there are still many that do not. This is a key metric, and unwillingness to commit to mitigation time should cast serious doubt on their ability to stop attacks.

5 How Do You Measure Quality of Protection?

Apart from the time it takes to mitigate an attack, a key consideration is the quality of mitigation. Some vendors casually throw around the term 'mitigation', but when you read the fine print you learn that there is not much to back it up. The **Consistency-of-Mitigation** metric provides a baseline to calculate the effectiveness of mitigation, and how much bad traffic is allowed through. A high-level mitigation threshold will only allow less than 5% of attack traffic to go through. Not including a Consistency-of-Mitigation commitment in an SLA effectively renders Time-to-Mitigate commitments meaningless because vendors can pass almost anything for 'mitigation' and claim to meet mitigation SLAs.

6 How Reliable is Your Service?

Finally, when under attack, you want to be sure that your mitigation service will be available to take over. The **Service Availability** metric defines uptime requirements for service, and how much downtime will be tolerated on an annual basis. A high-quality service will commit to at-least 99.999% of uptime, which means only about 5 minutes of allowed downtime throughout the year. If an SLA does not include a Service Availability commitment, that should make you wonder whether it will be there in a time of need.

These six performance indicators are crucial to guarantee the effectiveness of DDoS protection. These metrics should be outlined in clear, straightforward terms inside the SLA document. If you don't see them – ask about how those guarantees are provided and what they commit to.

INDUSTRY-LEADING SLA FROM RADWARE

Radware has the industry's most expansive and granular service level commitments, ensuring the highest quality of DDoS protection. Radware's SLA provides individual commitments to Time-to-Detect, Time-to-Alert, Time-to-Divert, Time-to-Mitigate, Consistency-of-Mitigation and Service Availability SLAs.