

Corero DDoS Provider Evaluation Assessment

Corero has developed an evaluation assessment to help you align your experience and understanding of DDoS attacks to the most appropriate DDoS mitigation provider.

DDoS Security Client Assessment Sheet

If you are thinking about reviewing your existing DDoS security tools, can you answer these questions about your own organization? An online version of this assessment guide can be found at: go.corero.com/online-ddos-assessment

| | Questions | Context and Response | |
|---|---|------------------------------|-------------------|
| 1 | Existing Provider | Concerns and Needs | |
| 2 | Do you have dedicated internal specialists | Network Security | Yes/No – Examples |
| | | Incident Response | Yes/No – Examples |
| 3 | Have you experienced a DDoS incident? | Yes/No/Unknown | |
| 4 | If ‘Yes’ to Q3, what type(s) of incidents have you needed to respond to? | Small (<10Gbps) | Yes/No – Examples |
| | | Large (>10Gbps) | Yes/No – Examples |
| | | Short (<10 minutes) | Yes/No – Examples |
| | | Long (>10 minutes) | Yes/No – Examples |
| 5 | If ‘No’ or ‘Unknown’ to Q3, what type(s) of DDoS incidents do you believe would harm your company the most? | Small (size) | Examples |
| | | Large (size) | Examples |
| | | Short (duration) | Examples |
| | | Long (duration) | Examples |
| 6 | What % of DDoS attacks are you experiencing? | Small (size) | % of 100% |
| | | Large (size) | % of 100% |
| | | Short (duration) | % of 100% |
| | | Long (duration) | % of 100% |
| 7 | Have you experienced diversionary DDoS attacks, coinciding with other cyber-incidents? | Yes/No/Unknown – any context | |
| 8 | If ‘no’ or ‘Unknown’, to Q7, would you like to have your network monitored for the presence of DDoS? | Yes/No/Undecided | |
| 9 | Do you have a preference where you would run your DDoS mitigation tools? | On-Premise | Yes/No/Undecided |
| | | Cloud | Yes/No/Undecided |
| | | Hybrid (On-Premise + Cloud) | Yes/No/Undecided |
| | | Service Provider | Yes/No/Undecided |

DDoS Security Vendor Capability Assessment Sheet

If you are thinking about interviewing a potential new or existing vendor of DDoS security.

An online version of this assessment guide can be found at: go.corero.com/online-ddos-assessment

| | Questions | Context and Response |
|---|--|--|
| 1 | Is the vendor business focused mainly on DDoS mitigation? | Yes/No/Unknown any context |
| 2 | Does the vendor have technical support coverage in your region? | Yes/No/Unknown locations and residence of 24 x 7 support |
| 3 | Can you engage directly with the vendors engineering and product leaders? | Yes/No/Unknown who, roles and how |
| 4 | Does the vendor allow you to evaluate (Proof of Value) the DDoS protection solution to ensure it meets your needs? | Yes/No/Unknown implementation time and duration of PoV |
| 5 | Does the vendor allow you to purchase full DDoS mitigation capabilities independent of your network capacity? | Yes/No are there any exceptions? |
| 6 | Does the vendor pricing model align to your purchasing requirements? | Yes/No how can you purchase perpetual/subscription (monthly, quarterly, yearly) |
| 7 | What are the baseline support services provided with the DDoS solutions? | 9 x 5, 12 x 7, 24 x 7. What if any additional costs need to be paid to increase the baseline levels of support? |
| 8 | Can you engage with the vendor's reference customers in region/vertical? | Yes/No/Unknown any context/evidence |

DDoS Security Vendor Technical Excellence Assessment Sheet

An online version of this assessment guide can be found at: go.corero.com/online-ddos-assessment

| | Questions | Context and Response |
|----|---|---|
| 1 | Can the vendor offer 'real-time' TTM, <1 second, for known and unknown attack types? | Yes/No/Unknown any context/evidence that explains the architecture involved |
| 2 | What is the operational time to deploy the vendors 'real-time' offering? | Installation/connections/policies all active |
| 3 | Can the vendor offer 'On-Demand' DDoS mitigation? | Yes/No/Unknown any context/evidence |
| 4 | What is the operational time to deploy for their 'on-demand' service? | Yes/No/Unknown any context/evidence |
| 5 | Can the vendor offer a hybrid DDoS mitigation architecture? | Yes/No/Unknown any context that describes operational architecture |
| 6 | Can the vendor offer a managed DDoS service? | Yes/No/Unknown any context that describes operational architecture and responsibilities of alert mitigation |
| 7 | Does the managed DDoS provider allow you to update protection policies? | Yes/No/Unknown any context that describes operational management |
| 8 | Can the vendor offer manual and automated traffic re-routing to a local scrubbing center? | Yes/No/Unknown any context that describes operational architecture, control of re-routing and responsibilities of alert mitigation |
| 9 | What line speed can the vendor support without redirecting to a scrubbing center? | Yes/No/Unknown any context that describes architecture capability and performance |
| 10 | Does the vendor provide syslog output, for consumption by other security systems, such as an SIEM? | Yes/No/Unknown any context that describes integration with SIEM and other decision analysis tools |
| 11 | Does the vendor protect volumetric and state-exhaustion DDoS attacks at Layers 3, 4 and 7 by default? | Yes/No/Unknown any context |

DDoS Security Vendor Technical Alliances Assessment Sheet

An online version of this assessment guide can be found at: go.corero.com/online-ddos-assessment

| | Questions | Context and Response |
|---|--|---|
| 1 | How open is the technology to enabling integration with existing systems, including REST APIs for system and policy control? | Yes/No/Unknown any context that describes architecture capability and integration controls |
| 2 | What technology relationship does the vendor have with their cloud scrubbing operator? | Context that describes any vendor contractual agreements |
| 3 | What is the primary business of the vendor's cloud scrubbing partner? | Cloud /Outsourcing /Security Provider / MSSP / Hosting Provider / Dedicated Scrubbing |
| 4 | Do the vendor's managed services providers use their [vendor] DDoS tools for their own operations? | Yes/No/Unknown any context |