



The DDoS Protection-as-a-Service Buyer's Cheat Sheet

10 Questions Business and Product Leaders Need to Ask Vendors

As a service or hosting provider, pricing pressures on your core offerings make it hard to increase revenue and stand out from the competition.

If you're not careful, you can end up in a race to the bottom because it is hard to differentiate. So, savvy business and product leaders look to value-added services to move the needle for their business in a significant way.

DDoS Protection

One area to consider, that feeds directly into your core business and can help you strengthen your brand and bottom line, is DDoS protection. Whether massive or small, DDoS attacks hit home for service and hosting providers by impacting uptime. Cementing your reputation for great uptime on your core offerings is a first level of competitive differentiation that you can achieve simply by deploying DDoS protection-as-a-service. But it has to be the right solution – enabling you to address your customers’ needs while complementing your existing business model.



If you’re evaluating DDoS protection solutions to enhance your core offerings, here are 10 questions to ask vendors to ensure you’re getting the product efficacy and sales support required to achieve your goals.

Product efficacy



How accurate is your detection?

Answer: Real-world DDoS attacks are multi-vector, change frequently, and come in all sizes – from volumetric attacks to quick strikes.

Solutions that identify known DDoS attacks based on real-time full traffic visibility and proactively updated detection rules offer more accurate detection than traditional methods. To identify unknown DDoS attacks, capabilities that behaviorally analyze traffic anomalies across your infrastructure and leverage the latest threat intelligence research to dynamically characterize traffic as malicious help you keep pace with evolving and new attacks.



How effective is the protection?

Answer: In addition to having accurate detection, you also want a solution that defends against malicious traffic comprehensively and quickly, without impacting good traffic.

Solutions that can automatically block a wide range of DDoS attacks, without requiring the intervention of security analysts or network operators, can stop attacks within milliseconds. Legitimate traffic must be able to flow uninterrupted, enabling services and applications to stay online, while DDoS traffic is surgically removed before it has the chance to cause any damaging effects.



What level of availability can we expect for our customers?

Answer: As a strategic differentiator, DDoS protection leads to better availability, which is enhanced by higher accuracy and faster speed to blocking. With a high-performing, best-of-breed solution, you should expect zero interruption in service delivery due to DDoS attacks.

To provide that level of confidence, a DDoS protection solution should keep you informed of attacks – what was blocked and when – through live and historical reporting and analysis tools. And if something isn't working as expected or questions arise, you need to know that there is someone you can talk to who can provide answers fast.



Sales support for DDoS protection-as-a-service



Is the DDoS protection solution easy to monetize?

Answer: The point of adding DDoS protection-as-a-service is to grow revenue. So, you need to make sure the vendor has the perspective of helping you make money from the solution, in addition to protecting your infrastructure. Look for language on the website and in collateral to get a sense of whether they are just focused on the technology side or also on the business side.

Choose a vendor with tools that make it easy to manage tenants and demonstrate value to them. This should include capabilities to easily onboard, update, and set service levels for tenants and show them when there is an attack and that they are being protected.



How should we structure our offering?

Answer: Vendors that view DDoS protection as a revenue opportunity for service and hosting providers, must have a flexible solution that can adapt to your business model, and should be able to provide guidance on how to structure your offering.

For example, you may want to be positioned as a premium service provider with DDoS protection built-in to the cost. Or, you may choose to include a base level of protection by default with options for additional levels of protection based on attack size. Or, offering a la carte options may work best for your customers and business model. However you decide to structure your DDoS protection service, the tenant customer portal must be very flexible to support the approach that maps to your business model.



How can the solution help us achieve the differentiation we need to drive our revenue goals?

Answer: Differentiation is driven by offering a best-of-breed service so that you can assure customers that you're keeping attacks away and availability up. Your objective is to meet your customers' needs and attract new customers with protection that is worthy of the additional investment – no question.

The combination of high product efficacy and great visibility for tenant customers will deliver availability guarantees that result in an attach-rate which enables you to make a good margin and achieve your revenue goals. Push vendors to show you they have what it takes to make that formula work for you.



What capabilities do you offer that make it easy to deliver the service?

Answer: Managing per-tenant policies, providing per-tenant views, and generating alerts and reports are prerequisites for efficient and effective service delivery. Ask vendors if they offer an integrated tenant customer portal that can be branded as your own, what information tenants can see, and how they will know when to go to the portal.

Tenants must be able to see only their traffic in their context and receive automatic notifications of attacks they were defended from via email and other channels of their choosing. Customized dashboards and reports should provide additional attack details and be easy to share with the rest of their security and business team to strengthen overall security posture.



What business and marketing support can you provide?

Answer: You shouldn't have to be a security expert to offer a value-add DDoS attack protection service that you can run on your network. When you make that investment, the vendor should have marketing materials to help you launch and grow that part of your business.

Ask if they have user guides for how to structure and market offerings and, in addition to a branded tenant portal, ready-made end-user tenant collateral that you can easily customize for your brand. This could include executive reports and explainers on why service availability should matter to users and their business. Your success is their success so this type of marketing support should be available to you.



How can your product help me generate incremental revenue?

Answer: Access to prospecting tools to help you find the subset of your tenants that are more likely to value the service, will help you increase revenue.

A picture is worth a thousand words. So, capabilities like a provider portal to help you identify the tenant customers best suited to the service, as well as the ability to run reports to show those tenants the type and volume of DDoS attacks they are experiencing are extremely powerful sales tools. As your business grows, the portal must allow for tens of thousands of users, so you can optimize service delivery at scale, continue to drive more revenue, and completely offset the initial protection investment.



How long will it take to realize a return on my investment?

Answer: Ultimately, how quickly you achieve a return on your investment (ROI) is dependent on how you offer the service and your customer base. An adaptive solution that helps to ensure the highest levels of availability for your customers, with the visibility they need to understand the value being delivered, will accelerate ROI.

Additionally, you will more likely be able to accelerate ROI when you can leverage a tool that will help you identify and prospect tenants. Understanding how price sensitive your customers are and underscoring that you have a premium service that will guarantee them uptime, will also impact the speed at which you can realize ROI.

DDoS protection-as-a-service is a great way to complement your existing core offerings and differentiate from your competitors, but it requires finding the right partner and solution for you.

If you're satisfied with the answers you receive to these questions, ask the vendor if you can speak with other service providers who have deployed their DDoS protection-as-a-service, and get a demo or see if a free trial is available.



Like what you've read?

Contact us and we'd be happy to dig deeper into these answers and show you how our DDoS protection-as-a-service is a great way to complement your existing core offerings, differentiate, and drive revenue growth.

[Speak with a Specialist](#)

Visit corero.com to discover how we can safeguard your business.