



## DDoS Protection Buyer's Guide

Choosing the right solution to protect your company against Distributed Denial of Service attacks resulting in harmful business disruptions

## DDoS Protection Buyer's Guide

**Choosing the right solution to protect your company against Distributed Denial of Service attacks resulting in harmful business disruptions**

The products offered by DDoS service and solution providers sometimes differ considerably, so selecting a protection solution is often difficult. This Buyer's Guide tells you what to look for when choosing a DDoS protection solution and how your company can benefit from working with an external protection provider. It also provides information on the basic functions of modern DDoS protection solutions, which you should make a point of asking about with each provider.

### Content





Available DDoS protection solutions .....	3
CDN .....	3
Hardware appliances.....	3
Cloud-based DDoS protection .....	4
Cloud-native approach (AWS/Azure) .....	4
Hybrid protection .....	5
Routing solutions: Redirection of data traffic .....	5
DDoS protection via DNS forwarding .....	5
DDoS protection via Border Gateway Protocol (BGP) .....	6
Possible combinations: Web DDoS and infrastructure protection .....	6
Availability: Always-On or On-Demand .....	6
On-demand protection.....	6
Always-on protection .....	6
Filter options .....	7
Automation in attack detection and filtering .....	7
Protection for OSI layers .....	8
Service Level Agreements .....	9
SLA for protection bandwidth .....	9
SLA for time to mitigate .....	9
SLA for service uptime.....	10
Scalability of the overall solution .....	10
Multi-cloud support .....	11
Compliance.....	11
Dashboard with configuration options.....	11
Pricing & costs .....	12
Integrated platform for DDoS-related services .....	13
Support.....	13
Conclusion .....	13
About Link11 .....	14
Checklist .....	15

## Available DDoS protection solutions

Several approaches are used to protect organizations against DDoS attacks: CDN, hardware appliances, cloud-based and cloud-native DDoS protection, and hybrid protection solutions.








### CDN

A content delivery network (CDN) distributes website content to servers placed around the world. This basically means that requests do not have to be answered by the original server. This helps compensate for load peaks up to a certain level, such as those caused by high-volume DDoS attacks.

-  Provides protection against high-volume attacks
-  The protection level is determined by the maximum external connection
-  Not all attack types are covered
-  Many of the providers are in the USA and are therefore subject to the Patriot Act and other relevant legislation. This means they are obliged to hand over data to US authorities upon request. The compliance aspect was further intensified by the European Court of Justice's decision in July 2020 to end the EU-US Privacy Shield (see the "Compliance" chapter).

### Hardware appliances

In this protection method, a device (DDoS appliance) is installed in the company's infrastructure or the provider's backbone. This appliance monitors data traffic. In the event of abnormalities such as a sudden increase in data traffic, it limits the traffic or detects and blocks the attacker's requests. Some deployment models require manual intervention, either by the company's IT department or an external security service provider. This requires time and physical presence that cannot always be guaranteed in the age of COVID-19 and remote working.

-  Makes individual adjustments to customer-specific IT infrastructure and data traffic
-  Cannot provide protection against attacks that exceed the available Internet bandwidth (i.e., the protection level is determined by the maximum external connection)
-  Does not include machine learning to detect new attack vectors (see "Automation in Attack Detection and Filtering" chapter)
-  The solution is isolated and does not work in hybrid IT infrastructures that use one or more cloud services
-  High procurement (CapEx), operating, and personnel (Opex) costs for the company
-  Integration into existing IT infrastructures is complex
-  Many providers are based in the US, meaning they are subject to the Patriot Act and other legislation that obliges them to hand data over to the US authorities upon request. (See "Compliance" chapter)

## Cloud-based DDoS protection

The website's data traffic is routed through the DDoS protection provider's external filter. Attackers can be detected and blocked via a multilevel analysis of the requests. Only legitimate data traffic is forwarded.

- + Good attack detection of volume, application, and protocol attacks and unknown attack vectors
- + High-bandwidth strength
- + Virtually unlimited scalability
- + Quick and easy integration
- + Holistic protection of complex IT landscapes and a company's local, global, and cloud-based infrastructures
- + Redundancy
- The country's data protection standards must be observed
- Operated by third-party providers

## Cloud-native approach (AWS/Azure)

To ensure fast implementation, cloud-native DDoS protection solutions are delivered with a basic set of options and security settings. These are suitable for DevOps projects. In practice, however, cloud-native protection is often insufficient to ensure the integrity of applications and data in production environments. Since the user is responsible for security and data protection vis-à-vis third parties, extensive adaptations and in-depth security knowledge are necessary.

Security features provided as part of cloud computing solutions are not designed to avert targeted attacks or mega-attacks. What's more, the attacks often originate within the same cloud environment. However, most cloud providers do not offer transparent information about the level of protection they offer or options for individual security settings.

- + Good attack detection of volume, application, protocol attacks, and unknown attack vectors
- + High bandwidth strength
- + Scalability
- The solution is isolated and only alerts, protects, and reports on a platform-specific basis. Therefore, it requires very high administrative effort in multi-cloud scenarios (see "Multi-cloud Support" chapter)
- Protection is sometimes only available for some, but not all, of the services operated by the public cloud provider
- Lack of clarity regarding protection when attacks on a company's cloud IT originate from the same cloud environment. For an extra fee, alarm auditing is sometimes available
- Alarm auditing is sometimes only possible for an extra charge
- Cloud providers offer basic protection. Advanced protection is costly
- Cloud providers offer basic protection. Advanced protection is costly. Basic SLAs stipulate up to a 20-minute response time, if they stipulate a response time at all



- ➖ Lack of transparency regarding how the protection works (design authority)
- ➖ Limited logging and reporting
- ➖ No individual support
- ➖ The country's data protection standards must be observed

## Hybrid protection

A combined hardware and cloud protection solution provides comprehensive and integrated protection against combined application and network-level attacks.

- ⊕ Double protection
- ⊕ Protects the entire infrastructure
- ⊕ High bandwidth strength (but significantly limited in the hardware solution)
- ➖ High procurement costs (CapEx) for the appliance and running costs for the company (including personnel expenses)
- ➖ Complex to integrate into existing IT infrastructures
- ➖ Insufficient protection for public cloud services
- ➖ Little automation
- ➖ Latency and downtime in the event of an attack due to switching
- ➖ The country's data protection standards must be observed

## Routing solutions: Redirection of data traffic

DDoS protection can be implemented via DNS forwarding, or in the event of an attack, by routing data traffic via BGP to the protection provider or its scrubbing centres and filtering it. The structure of the company's IT systems is decisive when choosing between these two routing solutions.

### DDoS protection via DNS forwarding

This DNS protection solution aims to secure a company's web applications. There is no need to expand the server infrastructure, add bandwidth, or buy new router technology. The DNS protection solution can be implemented starting with just one IP address. It protects applications based on domain names from DDoS attacks on layers 3-7. To do this, the DNS A-record entries of the affected application are adapted, which redirects the data transfer to the scrubbing centre. The infected clients ask the DNS servers for the IP address, receive the IP address of the scrubbing centre through the DNS change, and therefore do not send the attack to the original server. The protection via DNS forwarding is active as soon as the change has been made on the DNS server.

## DDoS protection via Border Gateway Protocol (BGP)

The BGP variant provides comprehensive protection of the entire company network and therefore protects all elementary company applications such as mail, VPN, database servers, etc.

BGP DDoS protection can be used in a hot-standby mode, which maintains the normal data flow as long as no attack is underway. Data transfer is only routed through the scrubbing centre in the event of an attack. The filtered data packets are transmitted back to the customer network via a protected tunnel (VPN, IPsec, GRE). After the DDoS attack has been successfully averted, the data transfer is directed back via the original route.

Using a BGP solution requires a /24 or larger IP network for redirection. In addition, complete protocols can also be forwarded according to customer specifications. In the event of an attack, both the customer and the security operations centre can announce the network in a standby integration.

By adding monitoring of flow data from the customer's local routers, DDoS protection can be activated automatically and without manual interaction in the event of an attack.

BGP DDoS protection is also available in always-on mode. For details about permanent or temporary protection installations, see the chapter "Availability: Always-On or On-Demand".

## Possible combinations: Web DDoS and infrastructure protection

Companies' IT infrastructures are becoming increasingly complex and are often made up of different IT systems, from web servers, databases, and Internet telephony to cloud applications. To ensure maximum DDoS protection, a combination of DNS forwarding and BGP redirection is recommended. The decision regarding this should always be specific to the company and based on a thorough analysis carried out in conjunction with the commissioned DDoS protection provider.

## Availability: Always-On or On-Demand

Companies can choose whether the external protection solution should filter the data stream permanently (always-on) or only in the event of an attack (on-demand/standby).

### On-demand protection

With on-demand protection, data traffic flows to the company in the usual way but is constantly monitored (usually based on flow data). In the event of an attack, the company is automatically notified, and traffic is redirected to the scrubbing centre and filtered. Once it has been cleaned, the data traffic flows from the scrubbing centre back to the company through the GRE tunnel that has already been prepared. Because of the network switching, the protection takes effect with a few minutes' delay. When the attack is over, the network is switched back. If an attacker takes a shot at a company and attacks it repeatedly over a longer period of time, the network must be announced anew each time.

### Always-on protection

Intensified use of certain company services, such as increased VPN access while many employees work from home during the coronavirus pandemic, can create an increased need for permanent protection. The alternative to on-demand protection is to install permanent protection. With always-on protection – both via DNS forwarding and BGP redirection – data traffic is permanently routed through a scrubbing centre. This approach ensures that the company's IT is reliably protected 365 days a year, 24/7. At the same time, the permanent filtering and cleansing of data traffic relieves the burden on the company's own IT infrastructure.

On the other hand, DDoS protection providers should offer flexible deployment models. The combination of always-on and on-demand solutions helps to address the different protection needs of increasingly complex infrastructures. For example, organizations can choose always-on protection for their applications and combine it with event-driven, on-demand protection for email and database servers.

## Filter options

There are essentially two different methods for filtering traffic: filtering based on static heuristics, and filtering based on dynamic heuristics.

### Static analysis

Static filters use predefined rules (blacklist) to check data traffic. The blacklist contains filter rules for known forms of attack. If, when comparing the behavior patterns of certain requests, matches with blacklist heuristics occur, the traffic is classified as DDoS.

Typical static filter rules include:

- Protocol (TCP, UDP, ICMP etc.)
- TCP flags, ICMP type
- Source and destination IP
- Rate limit per IP or network area

Filtering DDoS traffic according to static rules is only as good as the blacklist on which it is based. If it does not contain a tailored, behaviour-based pattern for certain or new attacks, an attack cannot be detected as such.

### Dynamic analysis

DDoS attackers constantly identify new vulnerabilities and open services that can be misused for overload attacks. Recent Memcached and CLDAP attacks, as well as the emergence of the vectors WS-Discovery, Apple Remote Control, and DVR DHCPDiscovery, have shown that companies are constantly faced with new attack techniques.

The future therefore belongs to filter methods that proactively search for conspicuous but as-yet undefined behaviour patterns. In peaceful times, the protection solution first learns the legitimate traffic profile of a website or network and derives normal ranges from it (whitelist). Deviations and unusual behaviour patterns are automatically detected via machine learning and artificial intelligence (AI) before damage even occurs. (See chapter "Automation in Attack Detection and Filtering".) These dynamic patterns are in turn stored as new filter rules.

## Automation in attack detection and filtering

Human error is the most common cause of security problems. Due to the increasing number of alarm messages, important events can quickly disappear. To ensure real-time response and 100% attack detection for both known as well as new, as-yet unknown forms of attack, processes for fast and reliable analysis must be fully automated and based on artificial intelligence.

Workflow for manual defense against DDoS attacks	Workflow for automated defense against DDoS attacks
A security incident is detected and reported, for example, by sending an e-mail to the SOC	The incident is detected automatically
The SOC initiates the response to the incident	Mitigation is activated
The SOC completes its validation and the protection is activated	The system has now learned from this attack for the next attack

Ideally, the DDoS protection solution will use "learning" filtering processes that have been thoroughly calibrated based on legitimate website visitors. In this case, DDoS protection is not based on simple and static exclusion methods, but on sophisticated statistical behaviour models that immediately detect and lock out IPs that deviate from normal behaviour. This ensures a very low false positive rate. While a blacklisting approach was primarily chosen for DDoS protection in the past, whitelisting is becoming increasingly popular; it works, in a sense, by reversing the burden of proof. This means that everything that does not conform to the legitimate data pattern (whitelisting) is conspicuous and potentially threatening.

DDoS protection solutions should examine incoming traffic in a granular manner and provide each client with a digital fingerprint. This distinction is much more differentiated than identification by IP address. It also makes it possible for regular visitors to access the affected systems in the event of an attack without even noticing the filtering process. If known attack characteristics are identified in the fingerprint, the client is blocked at the first request.

As a downstream step, the incoming traffic should be analysed using machine learning and artificial intelligence and compared with historical data on known attack patterns. If the protection solution detects an attack, only this DDoS traffic is blocked in one of the worldwide filter clusters, while legitimate data traffic is allowed to pass. However, unlike a protection solution that focuses on distributing content, the load is completely removed from the traffic. This allows the entire filtering process to run in the background and remain hidden from users. To continuously improve attack detection, new attack patterns should be defined as dynamic filter rules and stored for future traffic analysis.

## Protection for OSI layers

In general, DDoS attacks can be broken down according to which level of the Open Systems Interconnection (OSI) model they attack. They are most frequently carried out at the network (level 3), transport (level 4), and application (level 7) levels. Efficient DDoS protection should therefore extend to layer 7.

### Application Layer (#7)

The challenge in detecting attacks is that DDoS traffic disguises itself as legitimate data traffic. It can try to overload CPUs and databases, for example, by carrying out DDoS attacks on login pages or through manipulated search queries on dynamic websites and feedback pages. However, if the DDoS protection solution performs deep packet inspection, the information can be used to filter traffic by using machine learning and artificial intelligence.

Examples: GET, TLS, HTTP GET, HTTP Post

### Transport layer (#4)

Volumetric attacks, also called floods, occupy bandwidth and slow down or stop the performance of web servers.

Examples: UDP floods, ICMP floods, SYN floods

### Transport layer (#3)

These are also volumetric attacks that attempt to overload the firewall's bandwidth and rate limiting.



## Service Level Agreements

Service standards (Service Level Agreement/SLA) are defined in several units. There are service categories for the level of protection, the response times of the defense, and for general network and service availability.

### SLA for protection bandwidth

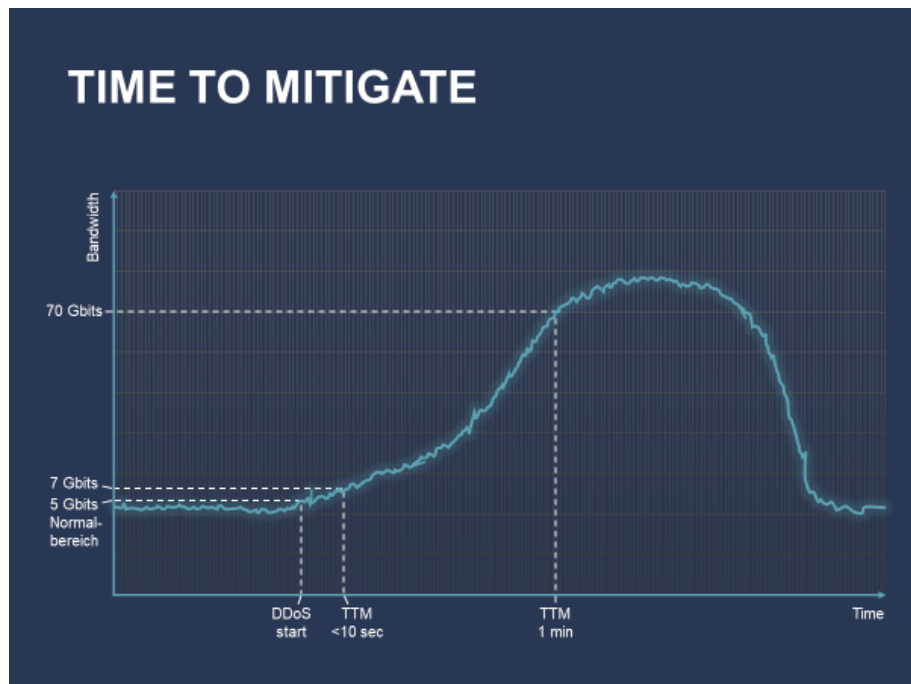
The attack volumes for DDoS attacks vary greatly and mostly depend on the attack vectors and amplification techniques used (reflection amplification attacks). The generated DDoS bandwidths have increased continuously over the last few years. While the average bandwidth of attacks was 2 Gbps in 2016, it had reached 5.3 Gbps by 2019. In addition to average bandwidth, the maximum attack volume of DDoS attacks has also increased. In 2018 it was 1.7 Tbps; in 2019, 1.3 Tbps, and in February 2020, 2.3 Tbps. In view of this development, 2 Tbps attacks threatened by internationally active and very aggressive DDoS blackmailers – such as the perpetrators of attacks in August and September 2020 going by the names of Fancy Bear and Armada Collective – should be taken very seriously.

The development of corporate broadband connections the world over has lagged behind the growth in attack volumes. Only one in six companies in the EU has an Internet connection of more than 100 Mbps. Most companies have connections with significantly less bandwidth. Companies seeking protection thus require a protection solution that can block attacks with a lot more volume than their own external connections. At the same time, the solution should be flexibly scalable to be able to cope with the ever-increasing number of attacks. Based on the largest known attack volume in Gbps as well as in packets per second (pps), the DDoS protection provider should guarantee a protection bandwidth of, for example, 10 Gbps, 50 Gbps, 100 Gbps, or 500 Gbps.

To protect against high-volume attacks, the DDoS protection provider should operate a worldwide network. A large external connection allows attacks of tens or hundreds of Gbps to be recorded and filtered. Globally distributing filter clusters also helps to filter attacks as close as possible to the source. The most significant source countries for DDoS attacks include the USA, China, Russia, and numerous South American and European countries.

### SLA for time to mitigate

Many online services and digital business models such as direct banking or logistics promise their users uninterrupted around-the-clock access. In terms of DDoS protection, this means 100-percent availability and performance. Therefore, every second counts when detecting and defending (time to mitigate/TTM) against an attack. The TTM begins when the first DDoS attack packet reaches the system and lasts until the DDoS protection solution starts scrubbing the traffic. Some providers only commit to a 'time to detection' (TTD) and make no definition for the second phase of the response time, the mitigation. For a company under attack, however, the only thing that counts is when the attack stops.



TTM differs greatly among protection solutions. It can take from 0 to a few seconds – in other words, real time – and up to 30 minutes or even longer. Time spans of several minutes are unacceptable here due to downstream effects such as the collapse of IP tunnels, server reboots, etc. Only countering attacks in real time can ensure that Internet connections will not become overloaded. The TTM should apply not only to volumetric attacks but also to attacks on APIs and applications at the application level (layer 7) (see the "Protection for OSI Layer" chapter). Because layer 7 attacks disguise themselves as valid packets, they are more difficult to detect and block. Defense guarantees with a service level agreement of 100 percent should also not only apply to selected attack techniques, but rather to all of them, including novel vectors.

## SLA for service uptime

Service uptime guarantees that the DDoS protection provider's infrastructure will remain available and that the customer will be protected without interruption. In a digitized world, there is zero tolerance for IT failures. Downtime not only damages a company's reputation; it also prevents sales and causes business interruptions. For this reason, companies should demand maximum service uptime from their DDoS protection provider. The industry standard for this is between 99.9 and 99.99%. If a company uses a DDoS protection solution via its hosting provider, the provider should guarantee service uptime.

## Scalability of the overall solution

It's becoming increasingly important for companies to invest in a DDoS protection solution that can grow linearly with the company's infrastructure. New locations in the global corporate network, expansion of applications, and increasing use of APIs are just a few of the many possible drivers that make it necessary to increase DDoS protection. In the case of appliance-based solutions, this means reinvestment in the form of procurement and sometimes requires a lead time of several months. Cloud-based protection, on the other hand, can be expanded quickly and flexibly to include new instances, without the need to purchase hardware. Costs are linear according to usage (see "Pricing" chapter).

In view of increasing attack volumes comprising several hundred Gbps, or as a response to acute incidents such as waves of blackmailing, you should also regularly review whether the booked protection bandwidth is still appropriate. DDoS protection from the cloud, which has sufficient resources with a worldwide network, can provide additional protection in the shortest possible time. Also, in the event of an acute attack, short-term scaling may become necessary. For example, if an attack exceeds the protection bandwidth, it must be possible to expand it quickly and at any time. Appliances are limited here by the maximum available external connection (see "Approaches to DDoS Protection" chapter).

## Multi-cloud support

Companies are increasingly relying on hybrid IT landscapes that consist of their own data centres, web services, and applications in the private and public cloud. To reduce risk, companies should strive for the same security standards across all of their digital work and business environments. The fact that each cloud follows different standards for DDoS protection can create complex distributed security problems in the multi-cloud. High administrative effort is accompanied by inconsistent protection, which weakens rather than strengthens IT security.

Complete DDoS protection solutions from a single source are a good way to reliably manage the complexity and high demands placed on availability and performance. Rolling out protection across all used cloud platforms is a proven method. From a technical, security, and compliance point of view, this results in consistent and reliable protection of the entire corporate IT environment. It doesn't depend on the cloud provider, is tailor-made for the company, and remains flexible for scaling in the cloud. Multinational companies with sites all over the world also benefit from low latency when protecting their infrastructures.

## Compliance

When securing digital business processes, companies must comply with various regulations at the national and international levels such as the GDPR and the German Federal Data Protection Act (BDSG). It's best to go with an all-round solution that ensures both DDoS protection and legal compliance. Problems often arise if the protection provider's server locations are located outside the scope of the EU's GDPR. If the protection provider commissions subcontractors, this can also raise compliance concerns, because if any of the protection solution's services are outsourced to external companies, this can reduce transparency enormously, especially with regard to compliance with legal requirements.

The European Court of Justice's decision in July 2020 to end the EU-US Privacy Shield has tightened the compliance requirements for DDoS protection solutions whose providers are not based in the EU area. CDN-based products often entail the transfer of metadata from the EU data protection zone to the US by default. What's more, service providers often store log files on U.S. territory and use them within their network operation centres (NOC) to extensively optimize the systems in use or to improve the classification of threat situations. Furthermore, the valuable metadata can also be incorporated into the work activities of centrally managed security operation centres (SOCs). They evaluate this to identify threats and fine-tune the relevant filters and protection mechanisms. However, the NOCs and SOCs are all too often located outside the EU, for example in the US. The problem of data transfer and storage often applies to providers of hardware appliances as well.

Companies that want to play it safe should entrust their data and IT security to a provider from Germany or Europe, which will allow them to rule out data transfers to the US from the beginning. The strict requirements of European and German legislators regarding data protection and data security provide the necessary security for data transmissions. In most cases, this also facilitates adherence to compliance requirements. To be on the safe side, choose a service provider without a branch office in the US to exclude any possible access by the US branch office. In addition to the legal aspects, EU suppliers without US branches may also benefit from technological advantages. What's more, they also have comprehensive and profound knowledge of the European market and the needs of their European customers.

## Dashboard with configuration options

Transparency and monitoring of website and network traffic should be ensured via a web-based dashboard. In addition to options for setting customized protection parameters, a dashboard allows for real-time analysis of data traffic and logs detailed information on averted DDoS attacks. Overall, a dashboard facilitates:

- Detailed reporting
- Configuration of the blacklist/whitelist
- Setup of the static filter rules
- Management of globally distributed protection infrastructures and different protection profiles
- An alert function
- Individual settings options

## Pricing & costs

Several pricing models are used to charge for DDoS protection services. With regard to investments, the consumption of IT security services is recorded in capital expenditure (CapEx) and operating expenses (Opex). Depending on the choice of protective solution, CapEx and Opex are in different proportions to each other and pose financial risks.

### Hardware appliance

- High CapEx and Opex
- Costly to purchase
- Subsequent costs of updating/exchanging the appliances every x years
- Additional procurement costs if the company grows and the new infrastructure requires protection
- Great need for specialized IT managers and support staff for maintenance and further development
- High investments in existing IT infrastructure (computer centres, servers, networks, data)
- Fees for training, support, and updates are usually also incurred

### CDN-based protection

- Low CapEx costs, high Opex expenditure
- When using CDN services to protect against DDoS attacks, no investment costs in hardware are incurred
- Billing is based on consumption: traffic flow rate per second (Mbit/s) or volume per month (Tbyte/month)
- Costs are considerably lower than those of a classic on-premise solution

### Cloud-native approach (AWS/Azure)

- Low CapEx percentage, also low Opex costs for standard protection
- Advanced protection against complex attacks only possible at extra cost
- Monthly billing
- Attacks are sometimes also invoiced (burst capacity)

### Cloud protection

- Low CapEx percentage, also low Opex costs
- By default, cloud protection is billed according to monthly or annual contracts
- Low capital commitment in the areas of hardware and software, depending on whether the DNS forwarding or BGP forwarding deployment model is used
- Minimal need for IT managers and support staff for maintenance
- Invoicing occurs according to actual usage, which is based, for example, on the guaranteed protection bandwidth, on clean traffic, or on the number of instances to be protected (IPs, websites, data centres)
- Fees for implementation and support may also be incurred
- Some providers charge additional fees if the attack exceeds a certain duration or a specified number of attacks. This makes it difficult for customers to estimate costs.

In addition to costs, flexibility must also be considered. Using DDoS protection from the cloud provides independence. The DDoS protection can grow flexibly with the company at a predictable monthly cost. In addition, there are short usage terms. Hardware solutions, which are considered as investments, only pay off after a longer period of time.

## Integrated platform for DDoS-related services

Combining DDoS protection with other IT security solutions can be useful for complete protection of performance and availability at the network and application levels. If a 360-degree approach is followed, security can be further enhanced by using a web application firewall or secure DNS services, for example. A fully integrated solution from a single vendor helps to close important security gaps. In addition, the more applications are combined in one management console (single pane of glass), the more efficiently they support the protection of networks and applications, because

- Services are coordinated and interlinked
- The applied protection functions can be extended as required
- Integrability with APIs makes integration into the company's existing IT infrastructure possible
- Less training and administrative effort (administration) is required).

Deciding on one platform makes parallel operation of several solutions, which is ineffective and often non-economical, a thing of the past.

## Support

Protection against DDoS attacks is only holistic when it is accompanied by expert, easily accessible support. Such support should offer:

- 24/7 availability
- Communication by telephone, e-mail or chat
- Service in the local language, via an assigned Customer Success Manager
- Reaction times or response times defined in the SLAs that range from 30 minutes to several hours.

In addition, support employees should help the customer set up the protection solution (e.g. in redirecting data traffic), provide guidance with the implementation, and proactively advise customers on the integration of the solution into the existing IT security infrastructure.

The support team should also be able to advise DDoS protection customers on how to handle DDoS extortion.

## Conclusion

DDoS attacks are an everyday threat for more and more companies. In times of increasing digitization and ever-larger IT infrastructures that are vulnerable to attack, companies must prepare for future attacks that will be even more high-volume and complex. The trend towards increased use of applications in the cloud offers further gateways to entry and will lead to a further alarming increase in DDoS attacks on layer 7.

For this reason, effective DDoS protection is essential. Knowledge of the threats and the various technologies available helps businesses help make informed decisions and find the best protection against known and future attacks.



## About Link11

Link11 is the leading European IT security provider in the field of cyber-resilience. The global protection solutions of the Cloud Security Platform are fully automated, react in real-time and defend against all attacks, including unknown and new patterns, in under 10 seconds. According to unanimous analyst opinion (Gartner, Frost & Sullivan) Link11 offers the fastest mitigation (TTM) available on the market. To ensure cyber-resilience, web and infrastructure DDoS protection, Bot management, API protection, secure DNS, zero touch WAF, secure CDN, and threat intelligence services, among others, ensure holistic and cross-platform hardening of corporate networks and critical applications. International customers can thus concentrate on their business and digital growth. Since the company was founded in 2005, Link11 has received multiple awards for its innovative solutions.

### Link11 GmbH

Lindleystraße 12  
60314 Frankfurt Germany  
+49 (0)69 - 264929777  
[info@link11.com](mailto:info@link11.com)

### UK & Ireland Office

+44 (0)203 - 8688711  
[info.uk@link11.com](mailto:info.uk@link11.com)

### Nordics & Baltics Office

+46 (0)85 - 250 05 71  
[info.nordics@link11.com](mailto:info.nordics@link11.com)

### BeNeLux Office

+31 (0)68 - 992 3607  
[info.benelux@link11.com](mailto:info.benelux@link11.com)

## Checklist

What are the points to consider when choosing a DDoS protection provider? The list of criteria will help you to assess the reliability and trustworthiness of various protection solutions. Please print it and fill it out.

Feature	Link11	Vendor 1	Vendor 2
Guaranteed protection bandwidth	✓		
Guaranteed defense time that includes all vectors and layers	✓		
Guaranteed availability (service uptime)	✓		
Availability as web protection/DNS forwarding	✓		
Infrastructure protection via BGP stand-by/on-demand	✓		
Infrastructure protection via BGP always on	✓		
Flexible combinations of web and infrastructure protection	✓		
Hybrid protection solution (cloud and appliance)	✓		
Static filter rules (TCP, UDP, ICMP, IPs, rate limits etc.)	✓		
Protection on layers 3-7	✓		
Dynamic filter rules (whitelisting based on AI)	✓		
Automated processes and filtering	✓		
Multi-cloud support	✓		
Integrated platform for DDoS-related web security services	✓		
SaaS commercial model reducing investment risks	✓		
Scalability of protection	✓		
Owned fully controlled worldwide filter network	✓		
GDPR compliant	✓		
Compliant with EU law (esp. Privacy Shield ECJ sentence)	✓		
Dashboard with configuration options	✓		
Easy implementation and setup service	✓		
24/7 service centre	✓		