LINK11

# How Secure Is the Cloud?

## A COMPREHENSIVE REALITY CHECK

www.link11.com

## How Secure is the Cloud? A Comprehensive Reality Check

**The use of the cloud has become part of everyday life in many companies around the world. It makes the networking of sites and systems easier, creates more flexibility and reduces costs. However, if the subject of security is underestimated, this very beneficial invention can quickly become a curse that shakes a company to its core.**

The use of cloud services has become established in companies. According to information from the "Cloud-Monitor 2019" report by industry association Bitkom and consultancy company KPMG, two out of three companies now rely on cloud computing.[1] Internationally it is even higher: 94 percent according to the "RightScale 2019 State of the Cloud Report" by Flexera. There are many arguments in favor of the cloud.[2]

But on the other hand, the growing dependence on cloud applications also has associated risks. A cyber attack on a business-critical application could, in a worst case scenario, lead to the entire organization coming to a standstill.

## Dependence on the Cloud has its own Risks

It is in the nature of things that the connection to the public network is a favorite target for denial of service attacks. Just like companies, cyber criminals have long discovered the advantages that the cloud offers. Likewise, they simply rent computing capacity from public cloud providers and use it for their purposes.

There is a particular risk of distributed denial of service (DDoS) attacks, which target the connection to the cloud or systems connected via the cloud. The disruption of internet access or the weakening of systems has damaging and expensive consequences:

- Operations are interrupted: access to important systems is impossible. If, for example, the telephone system depends on the cloud, it will not be possible to contact the company.
- Delivery targets are not met: applications in the cloud are sometimes used to control production. Any disruption of the regulated procedure manifests itself as interruptions or as deadlines and delivery quantities not being achieved.
- Productivity is disrupted: employees working within the company or externally cannot access applications or data, resulting in severe productivity disruption.

The consequences of the disruptions for the company are always the same: the image of the company is damaged from the perspective of customers, suppliers and business partners. The outages result in direct and indirect loss of money, for example due to lost sales or recovery efforts.

The potential magnitude of such cloud outages was demonstrated spectacularly in October 2019, when DDoS attacks partly caused outages with Amazons S3 offer (Simple Storage Service).[3] Many companies that use this infrastructure could not be reached for hours. Some estimates place the combined losses for all the companies at over 100 million US dollars.

In the past, particularly spectacular attempted attacks on companies and governmental institutions were often based on botnets, which incorporated components of the IoT. The H1 2019 DDoS report by the Link11 Security Operation Center (LSOC) found that cloud servers were involved in at least every third DDoS attack (39 percent). In comparison, in the first half of 2018, this number was only 26 percent.[4]

Careful considerations have made attackers change their approach in this way. Whereas routers or surveillance cameras are usually connected with only a few Mbps, the cloud instances generally offer considerably larger bandwidths of between 1 and 10 Gbps. The associated attack volumes can therefore be up to 1,000 times higher than with individual IoT devices.

In many companies, security concepts do not keep pace with these latest developments. Often CIOs, CDOs and administrators depend on the traditional firewall systems at the strategically important handover points between internal structures and the internet, or rely on concepts such as demilitarized zones.

## Traditional Security Concepts do not provide Sufficient Protection

The easiest way for companies to defend themselves against the particularly feared DDoS attacks seems to be to block cloud services, if the attacks are from Amazon or Azure. As the companies often access these services themselves, this would also interrupt their own connection and business processes would come to a standstill.

With a Web Application Firewall (WAF), legitimate cloud traffic can be put on a whitelist. To maximize its benefits, the traffic would have to be analyzed as early as possible. However, the firewall lies behind the wide area network (WAN). It can be blocked by the attacks before any filtering has even taken place.

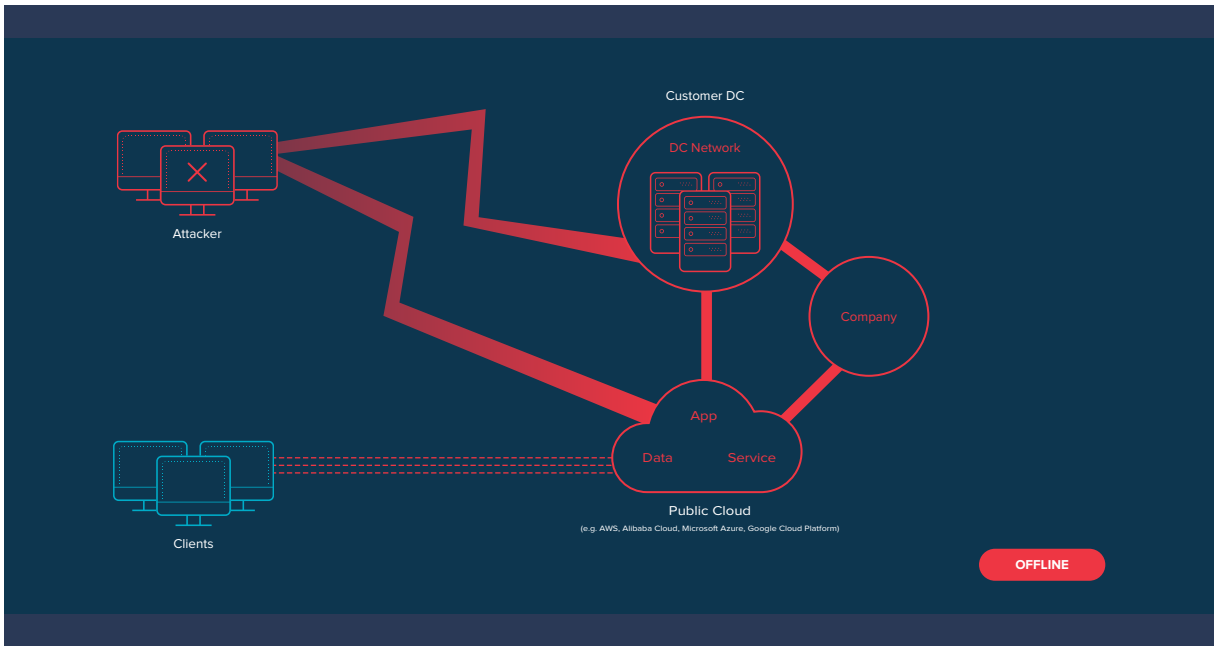
If a system instance running in the cloud is attacked from the same environment, all measures taken in the data center remain completely ineffective, because the requests do not even reach the company firewall. The shop – hosted via virtual machine on Azure or Amazon – or the CRM go offline or are so impaired that it is no longer possible to work effectively.

If companies rely on measures against DDoS attacks using their own dedicated hardware appliances in addition to the web application firewall, their filter mechanisms only work as long as the external connection is not overloaded. Most companies use connections in the range of 1 to 10 Gbps. In the past, however, Link11 has increasingly detected attacks in the three-digit Gbps range. Appliances are outgunned by these kinds of bandwidth-heavy attacks directly from the cloud.

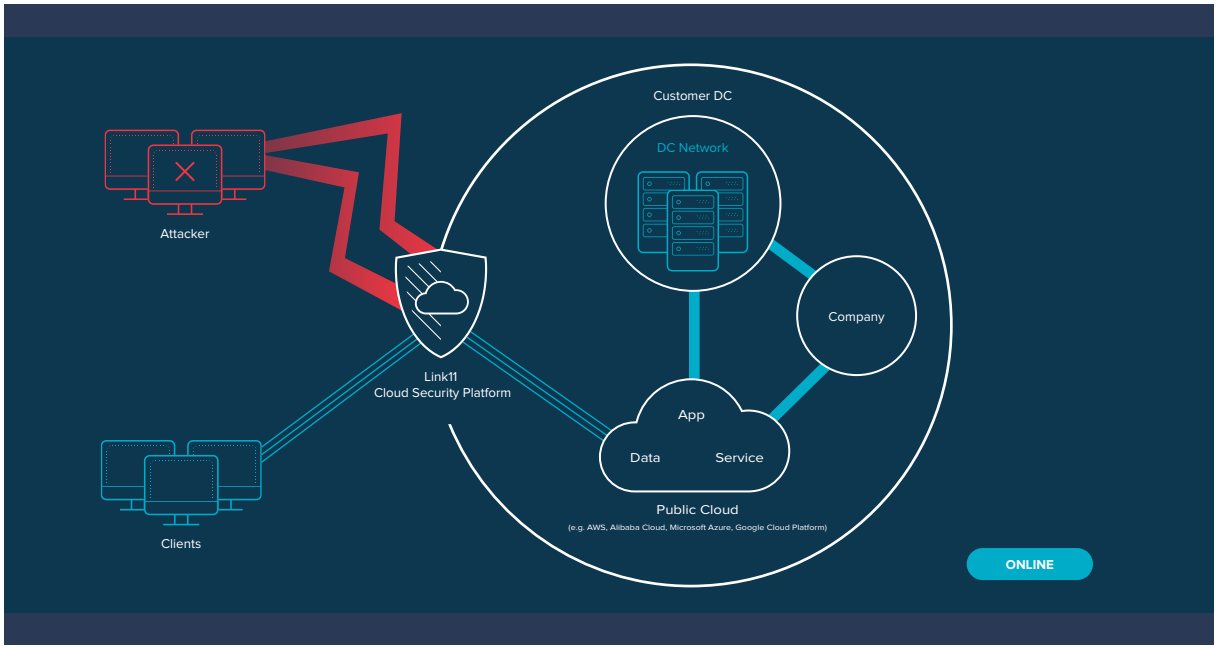
Large organizations that handle a lot of traffic via the cloud can establish direct connections with the cloud provider. However, such a dedicated private cloud connection (private peering) is only viable for very few companies. Nevertheless, even this connection has weaknesses without the use of additional security mechanisms. An attack from the same cloud environment can clog the connection with illegitimate data packets.

## Protection Against DDoS Attacks on Businesses with Virtual and Local IT Systems

Trends in computing show a movement away from the private cloud and toward the public cloud, where data, services and applications are stored externally on a cloud provider's servers. These servers are networked with the company's local IT. For this reason, a successful DDoS attack against just one part of this infrastructure can also damage all of the company's other systems and platforms.




Continuous monitoring of the entire virtual and local IT infrastructure as well as real-time traffic filtering is the best protection against DDoS-related failures. In this process, data traffic is routed through an external filter cluster. In the Scrubbing Center, attacker traffic is separated from legitimate client access.



## How Modern Security Concepts from Link11 Avert the Dangers

The increasing complexity of attack scenarios pushes simple rule-based systems, which work with whitelists, to their limits. Solutions that also use artificial intelligence provide up-to-date protection. Thanks to machine learning during the ongoing analysis of traffic, knowledge is built up about the communication profile of the permitted traffic. Deviations from this normal state are detected reliably and quickly. The technology also enables interventions with higher granularity. Traffic identified as threatening can be filtered out of the overall traffic, without interfering with the legitimate traffic.

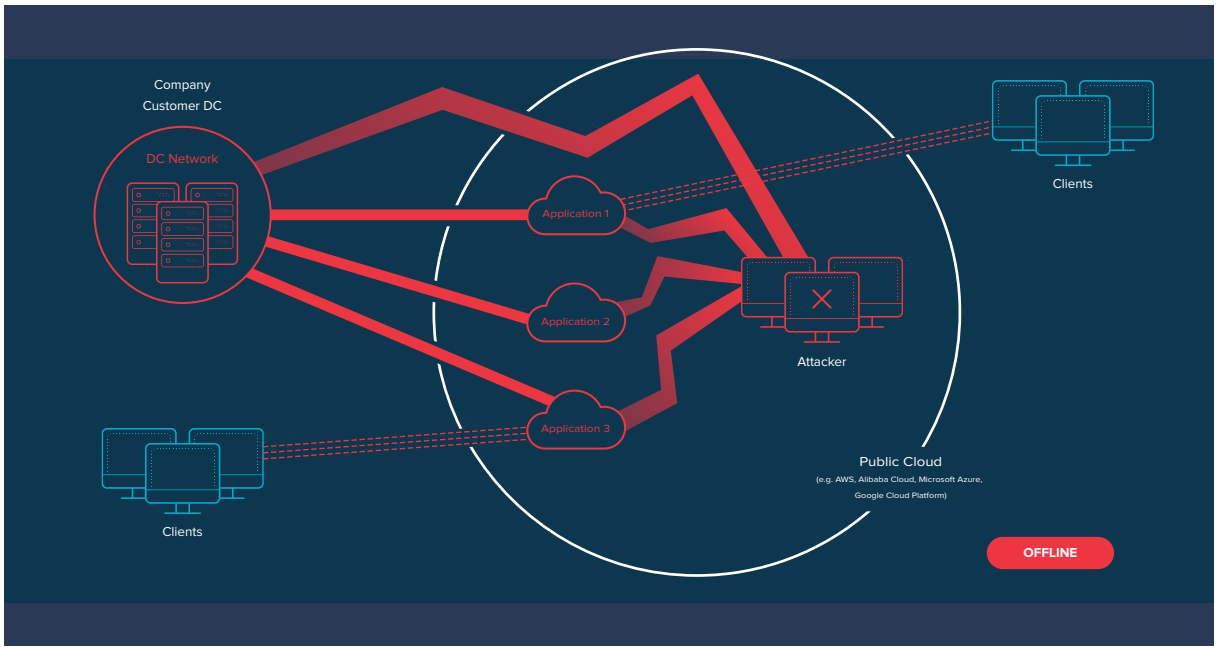
The Link11 external cloud filters work according to this principle and complement the standard protection from major cloud providers.

Separate cross-connects are maintained with the major cloud providers. Filter rules are processed in external systems, without restricting the bandwidth available to the company. This removes any potential weaknesses of private peering established by the company, because the filtering is completely external.

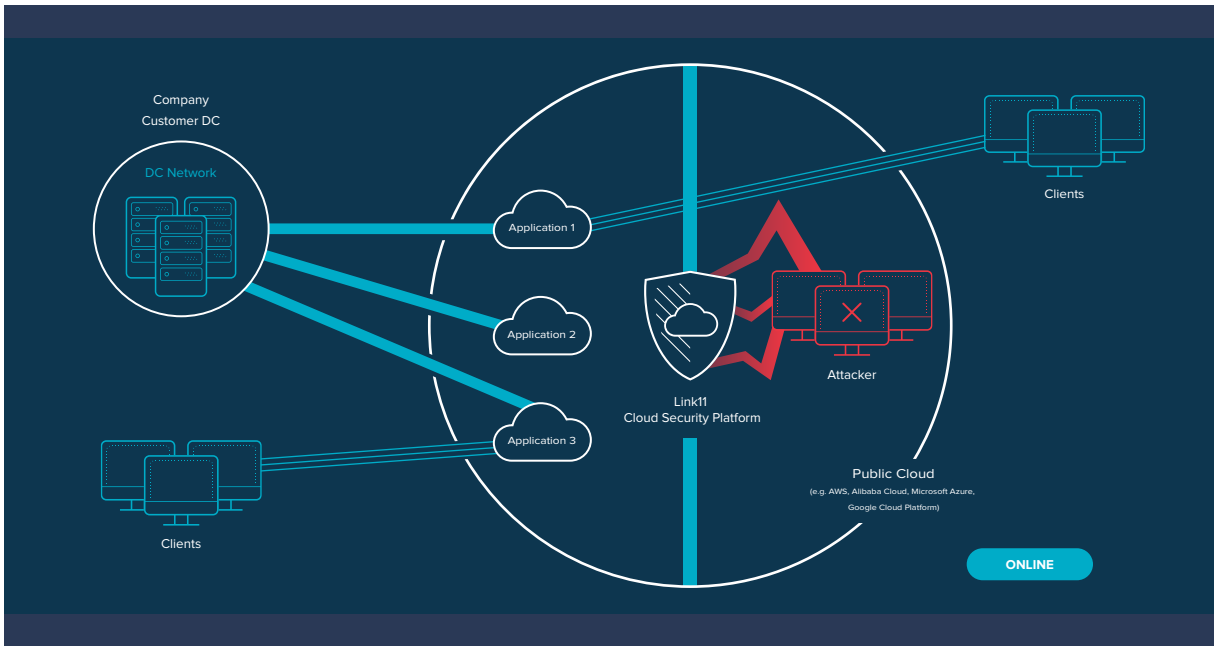
The protection is scalable and is adjusted in the event of a severe attack. Unlike other solutions, external DDoS filtering offers an additional advantage: the company´s WAN does not have to be made public. It is concealed by the upstream filter. This prevents or impedes further attacks.

## Efficient Protection Against DDoS Attacks from the Cloud

It's not only businesses that have been discovering the advantages of cloud computing: criminals are also employing modern cloud solutions. They generate the instances and bandwidth they need to launch DDoS attacks by using hacked accounts with public cloud operators. Attacks that use corrupted cloud instances can target every part of a company's hybrid IT infrastructure.




Again, the easiest solution for fending off DDoS attacks from the cloud to the cloud might appear to be simply blocking cloud services. However, since companies use these services for their own operations, an interrupted connection would mean that business processes are brought to a standstill. This problem is solved by using a cloud filter to scrub DDoS attack traffic from the cloud. With this solution, both the company's cloud-based services and its local infrastructure remain accessible.



## Conclusion

More and more business-critical processes are ending up in the cloud. The number of apps and devices connected to it will continue to grow in the coming years.

This not only requires a strategy to deal with the business aspects and process optimization. A security strategy that also considers the latest threat scenarios is essential as well.

Companies should therefore draw on external advice in order to explore how cloud-based security solutions help to minimize the risk of attacks. AI-based systems promise effective protection that outperforms conventional solutions by far.

## Sources


[1] KPMG und Bitkom: Cloud-Monitor 2019: Public Cloud und Cloud Security sind kein Widerspruch, June 2019
https://hub.kpmg.de/cloud-monitor-2019

[2] Rightscale: 2019 State of the Cloud Report from Flexera, February 2019
https://info.flexera.com/SLO-CM-WP-State-of-the-Cloud-2019

[3] The Register: Amazon is saying nothing about the DDoS attack that took down AWS, but others are, October 2019
https://www.theregister.co.uk/2019/10/28/amazon_ddos_attack/

[4] Link11: DDoS Report 1st half-year 2019, September 2019
https://www.link11.com/en/downloads/ddos-report-1st-half-year-2019/


## About Link11

Link11, headquartered in Germany, is a leading IT security provider that ensures cyber resilience. The company's protection solutions run fully automated, in real time and get better with every attack thanks to AI algorithms and machine learning. Even unknown attack patterns are mitigated in under 10 seconds. According to a report by Gartner, Link11 has the fastest time to mitigate (TTM) on the market. Alongside Link11's DDoS Protection for Web and Infrastructure, the advanced protection solutions Zero Touch WAF, Secure DNS, Secure CDN, Bot Mitigation, API Protection and Threat Intelligence are designed to strengthen cyber resilience as part of the integrated cloud security platform. International customers benefit from a 360° protection and maximum performance.
Since the company was founded in 2005, Link11 has received several awards for its innovative solution and strong growth.