cyberlink
SINCE 1995

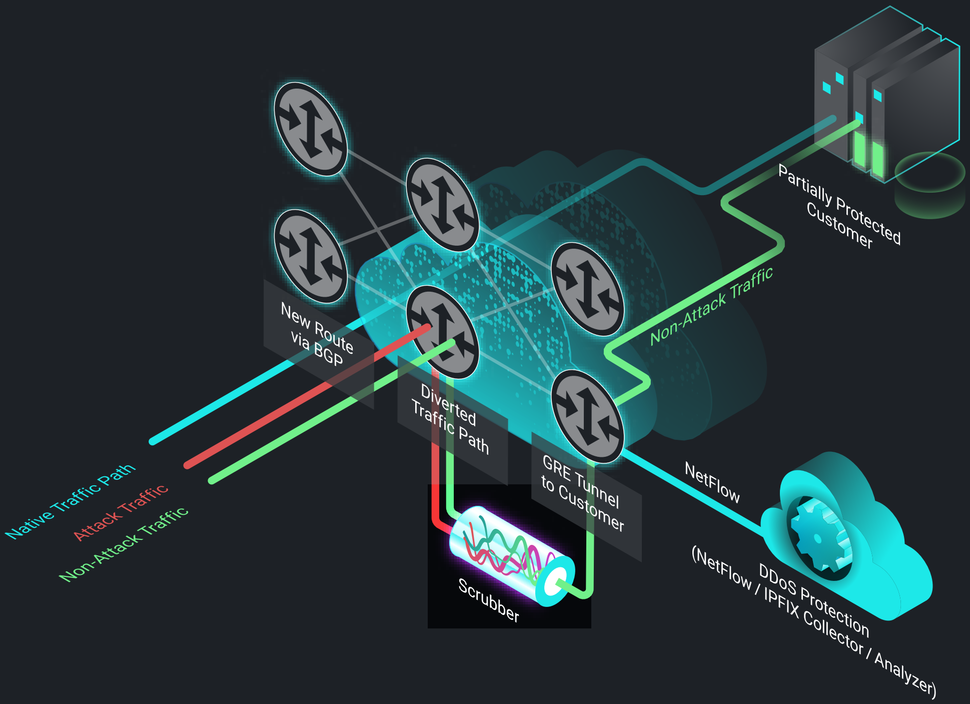
Bellerivestrasse 241
CH-8008 Zürich

+41 44 287 29 92
info@cyberlink.ch

DDoS Protection Service.

Reliable protection, even against multi-stage attacks.

2. BILANZ
Telekom-Rating 2025
Internet
Geschäftskunden
Cyberlink



Most people still associate the term "DDoS" with automated attacks using only one attack vector, namely volumetric attacks. Such attacks, which consume enormous bandwidth, are easy to identify and defend against. Cyberlink's DDoS protection provides additional, reliable protection, even against sophisticated multi-stage attacks.

Multi-vector attacks and adaptive DDoS attack techniques are becoming established.

In addition to the increasing number of brute force attacks with more than one attack vector, analyses have revealed something else. Hackers are increasingly turning to adaptive techniques that allow them to gain a more accurate picture of the respective security infrastructure. Using this profile, they then design a customized second and third attack, in which they specifically bypass the security levels of that particular company. Even though volumetric attacks remain the most common form of DDoS attack, mixed and adaptive forms of attack are also becoming established.

DSub saturating DDoS attacks – the smarter DDoS.

Intelligent DDoS attacks that work in a quasi "surgical" manner are a new development: 84% of the attacks observed last less than 10 minutes, 71.6% of them even between 0 and 5 minutes, and 93% require less than 1 Gbit/s (source: Corero Networks Inc). The attackers use just enough bandwidth to achieve their goal. Traditional solutions for defending against DDoS attacks overlook such attacks. Even if they are detected as attacks on the radar, they are often over before anything can be done about them. The attacks often follow a very typical pattern over time. And they are not without consequences.

So you need both. An immediate assessment of whether there is actually a security threat, as well as a long-term analysis of trends in order to be able to react to developments at an early stage.

Key Facts.

> Free DDoS protection for all Internet connections up to an attack volume equal to your bandwidth or max. 1 Gbit/s

> Additional DDoS protection up to an attack volume of several TB

> Real-time and fully automated protection

> Forensic analysis of previous attacks

> Personal service around the clock, including 24/7

The solution.

Nowadays, DDoS attacks can do much more than “just” interrupt services or make websites unavailable. For some time now, we have been observing a sharp increase in the number of short-term DDoS attacks that consume very little bandwidth.
We protect all our customers from this with our Basic DDoS protection. For high-volume attacks or support in analyzing attacks, we offer our customers comprehensive additional services with our Standard and Premium services.

With its fully automated DDoSP service,
Cyberlink protects both its own systems and customer connections from overload attacks. In this way,
Cyberlink can ensure that no unwanted data traffic reaches the Cyberlink backbone or end customers. The protection systems are installed in our data centers (EQ and IX) with geographic redundancy and are constantly monitored by Cyberlink. Incoming Internet traffic is checked and unwanted data packets are automatically removed.

Our DDoS protection services at a glance.

	Basic	**Standard**	**Premium**
Maximum attack bandwidths	Connection bandwidth (max. 1 Gbit/s)	Maximum Cyberlink Internet capacity	up to 1 TB
Availability	All Internet connections	All Internet connections	Datacenter Internet

Range of Functions.

Protection against DDoS attacks	✓	✓	✓
Installation obligation	✗	✓	✓
Personalized customer portal with real-time evaluation	✗	✓	✓
Forensic analyses by Cyberlink specialists	✗	optional	
Action taken if maximum attack bandwidth is exceeded	Access to IP address is blocked		Redirect to cloud service

Contract.

minimum contract term	none	none	none

Basic DDoS Protection Service.
This protection is implemented for all Cyberlink connections and is available to all customers free of charge. As long as the volume of a DDoS attack does not exceed the bandwidth of a customer's connection or 1 Gbit/s, the unwanted traffic is automatically cleaned up. If the volume of an attack exceeds the bandwidth of a connection or 1 Gbit/s, the data traffic is blocked for 15 minutes (Remote Triggered Blackholing, RTBH).

Standard DDoS Protection Service.
Cyberlink customers can optionally use advanced DDoS protection. In this case, all attacks are cleaned up as long as the total capacity of the Cyberlink perimeter to the Internet is not exceeded. If the volume of DDoS attacks exceeds Cyberlink's total Internet capacity, the attacked IP address (RTBH) is blocked. Customers who purchase this service receive access to an online portal where both real-time and historical information is available and attacks can be analyzed in detail.

Premium DDoS Protection Service.
In addition to standard DDoS protection, if Cyberlink's total capacity is exceeded, data traffic is redirected to an external scrubbing center operated by a specialized DDoSP provider and cleaned. This allows even terabit attacks to be repelled. It should be noted that such services may analyze and clean the data abroad, which typically results in delays (increased latency).

Additional services & alternatives.

SCION Internet.

Revolutionized Internet architecture for highly secure data exchange.

> **More about SCION.**

Private Network.

Your company locations, intelligently and securely connected.

> **More about Private Network.**

Virtual Private Cloud.

Take advantage of the synergy between the best internet and one of Switzerland's most advanced cloud services from a single source.

> **More about Virtual Private Cloud.**

Some of our customers.