

Fast, qualified help to ward off overload attacks

Ensure that it is always possible to access your company's online services, even if you are exposed to an overload attack. We clean the traffic on your Internet connection in our powerful cloud service. The goal is to mitigate the effect of the attack and allow legitimate traffic to pass as undisturbed as possible.

Cloud service the only opportunity for full protection

A Distributed Denial of Service (DDoS) attack results in the rapid collapse of the attacked infrastructure. Operation-critical processes are halted, which can result in large revenue losses or cause important community functions to go down.

Using the environment that is under attack to ward off an overload attack is more or less impossible. Protection must be located outside of your company. With Telia DDoS Protection, you can benefit from Telia's powerful, network infrastructure for identification of and resistance to attacks.

Attack cleaning

The initiative to start attack cleaning can come from us following an alarm from our monitoring system or from a customer initiated alarm. If we get a alarm from the DDOS-platform, we will call one of the appointed contact persons at your company to confirm any actions. You can also request attack cleaning.

Traffic to the protected object passes through our service platform and legitimate traffic is allowed to continue to your environment. The cleaning continues until the attack is believed to be over.



Free choice of protected groups

You define which objects in your IT environment will be protected by Telia DDoS Protection. All servers and applications that communicate via IP can be included, with up to 254 hosts per group of protected objects.

We handle the attack together

Our technicians will help you throughout the attack, and provide feedback per previously made agreements. The decision to change measures (to ward off the attack) is taken jointly, based on your input as the situation changes.

The measures are based partly on the results from our set-up of the protected groups and information gathered in conjunction with the attack. We analyze characteristics, methods, geographic origin, attacking IP addresses, etc.



Telia DDoS Protection

Useful information

What is included

- Set-up of up to five protected groups in conjunction with delivery.
- Four weeks (672 hours) of attack cleaning per year.
- Monitoring via traffic collection platforms at B2B Service FO (CMC), 24 hours a day, 365 days a year.
- Error notification, 24 hours a day, 365 days a year.
- Support during service hours, depending on the service agreement .
- Blackholing traffic from identified destinations (as per agreement).
- Redirection of incoming traffic and cleaning of DDoS traffic in network Telia platforms (as per agreement).
- Weekly reports with information about IP addresses via e-mail (as per agreement) in the event of an attack.
- Annual renewed set-up of protected groups .

What you need

To be covered by Telia DDoS Protection, the protected object must be connected to one of the following communications solutions from Telia:

- Telia Bredband Pro (former Telia ProLane)
- TeliaSonera Datanet with Internet connectivity

Monitoring

Once the delivery of Telia DDoS Protection is complete, the proactive monitoring begins. If CMC receives an alarm about abnormal traffic patterns to or from your Internet connection, a technician will contact one of your appointed contact persons at the provided telephone number to discuss the appropriate action. You can appoint several contact persons and rank them in priority.

Report a suspected attack

If you discover a suspected attack, you should report this via telephone to our support. The report can only be filed by earlier appointed contacts. Telia always call back, for authentication.

Reporting

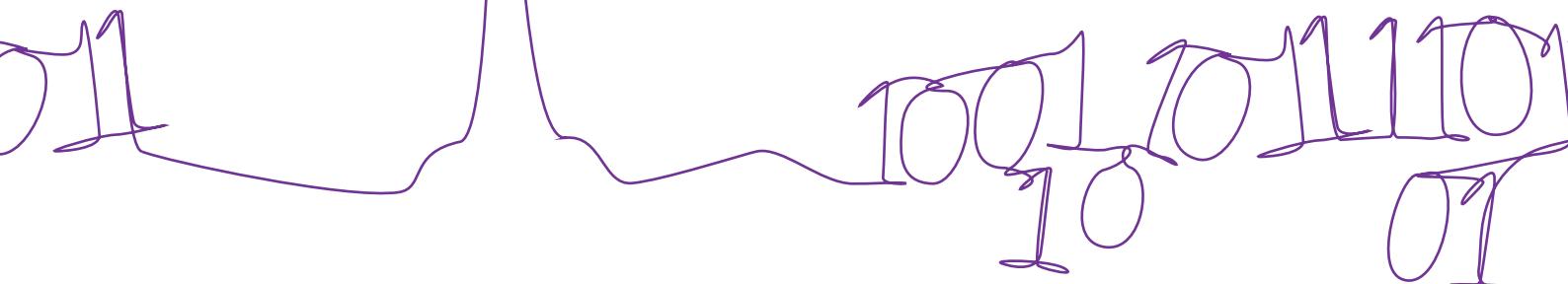
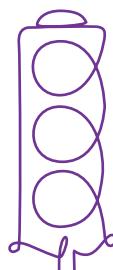
An alarm that initiates activation of functions in Telia DDoS Protection generates what is called a “trouble ticket” in Telia’s task management system. The tasks are listed with information about traffic patterns in your weekly e-mail report.

Service time

The service time for Telia DDoS Protection is the same as the level for the Internet connection the protected object uses. We recommend that you choose a service time that provides service 24 hours a day, 365 days a year. This is a prerequisite for you to be able to offer high accessibility to your protected objects, regardless of the time of day that an attack may start.

Service window

The service window for Telia DDoS Protection is the same as the level for the Internet connection the protected object uses.



Would you like to learn more about Telia DDoS Protection or place an order?
Simply fill in the form at www.telia.se/foretagskontakt and a salesperson will contact you. If you are in Sweden, you can also call: 90 400.