

DTS DDoS multilayer protection

DDoS multilayer protection

Almost every business relies heavily on web-based systems, applications and services. With such reliance, however, the potential damage from DDoS attacks also increases. DDoS refers to a "distributed denial of service" and is classified by the BSI as one of the main cyber attack threats. In a DDoS attack, the resources of a network, service or application are overloaded by concentrated attacks. The intent is to harm, eliminate, infiltrate or even blackmail the target. An additional problem is the ever-increasing area for potential attacks resulting from outdated technologies, broadband expansion and the increased use of digitalized business processes and the internet in general. At DTS, we provide you with continuous protection against DDoS attacks as a managed service with our market-leading solution.

- BSI certification-based, multi-layered protection against DDoS attacks
- Market-leading technologies & protection mechanisms
- Defense against high-volume attacks
- Customized service modules & packages
- Optionally via a DTS data center, on-premises, cloud or as a hybrid combination
- DTS managed services

DDoS attacks can take place in very different ways. The spectrum ranges from high-volume to subtle attacks that are hard to detect. IT infrastructure devices, applications, security components or simply the entire bandwidth capacity come under attack. However, combinations of different types of attacks are becoming increasingly common. In general, the frequency of attacks and their ferocity are increasing enormously. If an attack has already been successful, a vulnerability is revealed. Then further attacks are to be expected.

Multi-level protection against all hazards

Only when a DDoS attack has been detected is actual protection possible. We offer you multi-layer protection as a solution. This is based on two cloud scrubbing centers in the EU and DTS's own scrubbing center. The 2.5 Tbps mitigation capacity that is made available in this way also protects against high-volume attacks. In addition, up to 14 cloud scrubbing centers can be used globally, for even higher traffic capacity. State-of-the-art protection mechanisms are applied: behavioral protection, real-time signature generation, challenge & response.

Behavioral protection applies specialized behavioral analysis to detect patterns and attacks, including for customized applications. The protection also applies to short, recurring burst DDoS attacks. This avoids false positives when defending against attacks. Real-time signature generation provides protection against new, changing attack types via signatures. These are based on a comparison with the behavior of normal data traffic. Automatic creation of signatures, plus subsequent refinement to prevent errors, takes a matter of seconds and is almost instantaneous. Challenge and response is an additional check of suspicious traffic according to query type before blocking.

A special engine as a mitigation platform against unknown attacks, automatic security updates with signatures of known attacks, identification and blocking of IP addresses of known attackers and geo-blocking of hostile origins complete the multi-layered protection to provide integrated defense.

Service modules

First, we enable DDoS protection using three standard data center services. These apply to nearly all customers in our DTS data centers with IT infrastructure that requires protection:

- DTS Light DDoS Multilayer Protection: Basic protection in the DTS scrubbing center according to "best effort"
- DTS Basic DDoS Multilayer Protection: Basic protection in the DTS scrubbing center, including defense against high-volume attacks in the cloud scrubbing centers according to "best effort"
- DTS Advanced DDoS Multilayer Protection: Dedicated protection, including defense against high-volume attacks in cloud scrubbing centers with scalable legitimate traffic sizes

On the other hand, we enable DDoS protection based on on-premises & cloud services. These apply to customers with their own IT infrastructure requiring protection on site, in hybrid environments on the customer's premises or in the DTS data centers:

- DTS Hybrid DDoS Multilayer Protection: Protection with our own scrubbing solution on-site, DTS service with individual rule sets & read rights, including cloud scrubbing centers with scalable legitimate traffic sizes
- DTS Always On DDoS Multilayer Protection: Permanent protection provided by cloud scrubbing center to defend against high-volume attacks, with scalable legitimate traffic sizes