



# ROBUST DEFENSES AGAINST THE DATA DELUGE

## DISARMING DDOS ATTACKS WITH DDOS PROTECT PRO

A distributed denial of service (DDoS) attack is an attempt to cause a server, a website, or other infrastructure components to negatively influence accessibility by flooding the target with traffic from multiple remotely-controlled sources. In the majority of cases DDoS is a means of blackmailing the company on the receiving end. As a result, assaults of this kind often go unreported.

Nevertheless, DDoS attacks are by no means uncommon. According to the German Federal Office for Information Security (BSI), they are still a serious risk in 2016, even the world-wide number of open servers is on a decline. The maximum bandwidth has grown since 2014. As a result, the BSI now views DDoS as one of the greatest threats to IT security.

Moreover, the cybercrime industry has recognized the “market demand” for this kind of “service”, taking the problem to a new level. In fact, DDoS attacks can now be purchased in underground forums at low prices – an (illegal) 24-hour onslaught costs as little as 50 Euros.

### EXCELLENT PROTECTION FOR ALL NEEDS

Basic firewalls or intrusion prevention systems (IPS) do not provide sufficient defense against DDoS attacks. The vectors are so sophisticated that existing security systems only offer limited protection, and only at application level. However, volume (i.e. flooding) attacks can quickly breach internal defenses. With DDoS Protect Pro, T-Systems offers a multi-tiered protection solution against DDoS attacks that can be tailored to individual customer requirements

#### DDOS PROTECT PRO

CLOUD WEB DDOS PROTECTION	BACKBONE DDOS PROTECTION	ON PREMISES DDOS PROTECTION
Automatic protection	Reactive protection	Automatic protection
Against complex & volume attacks	Against volume attacks	Against complex attacks
On web services	On internet access & bandwidth	On systems and applications
Out of the cloud for local and hosted systems	In the Telekom backbone for the internet access	On customer premise for local infrastructure

COUPLING:  
AUTOMATIC  
MITIGATION  
OF VOLUME  
DDOS-ATTACKS

## CLOUD WEB DDoS PROTECTION

Cloud Web DDoS Protection is a standardized cloud-based service. It establishes a strong first line of defense against DDoS and is suitable for any organization that operates a web server or online store – independent of its location.

### Scope:

- Protection of web services (web shops, websites, B2B portals) against application- and system attacks
- Web servers can be located in the customer's, or any service provider's, data center
- Internet traffic is routed via the Cloud DDoS Protection platform
- Standardized always-on service
- Rapid provisioning
- Price depends on bandwidth



## ON PREMISES DDoS PROTECTION

On Premises DDoS Protection offers more extensive defenses. T-Systems operates a dedicated solution for the customer. On Premises DDoS Protection not only identifies all types of DDoS attacks on both systems and applications, it also protects the local infrastructure.

### Scope:

- Detection of, and protection against, application-level DDoS attacks
- Safeguards the local infrastructure (web servers, firewalls, VPN gateways, DNS servers, e-payment systems, SAP, etc.)
- Application-layer (layer 7) protection
- Can be tailored to the customer's infrastructure
- Around-the-clock support from security experts at T-Systems
- Technology and defense mechanisms are regularly updated
- A choice of monitoring or blocking modes

## BACKBONE DDoS PROTECTION

Backbone DDoS Protection intercepts attacks before they can impact and overload the company's Internet connection. To use Backbone DDoS Protection, the customer must have Internet connectivity via T-Systems.

It can be difficult to differentiate between a legitimate spike in traffic and a DDoS-generated load. Backbone DDoS Protection is usually activated at the customer's request and does not block traffic automatically. To quickly invoke the service and defend against DDoS attacks, customers will have direct access to the 24/7 DDoS-Protect-Pro-Team.

### Scope:

- Protection of network and access bandwidth against volume attacks
- Security mechanisms include blackholing, filter lists, rate limiting(thresholding), and rerouting via mitigation systems.
- The customer contacts the Backbone DDoS-Protect-Pro-Team directly, and each individual case is examined jointly by both sides.
- Requires Internet connectivity via T-Systems (CompanyConnect, DeutschlandLAN Connect L, DeutschlandLAN Connect IP or IP Transit offerings)
- Rapid provisioning

## COUPLING OF BACKBONE AND ON PREMISES PROTECTION FOR MAXIMUM SECURITY

Customers who want to be on the safe side and build maximum protection for their systems and networks can chose T-Systems' optional combination of On Premises DDoS Protection and Backbone DDoS Protection. Both solutions together form a stern defense shield against all types of DDoS attacks. The reaction time to counteract volume attacks on the network infrastructure will be reduced to a minimum – gaining time that can be crucial to keep up services to customers.

### CONTACT

T-Systems International GmbH  
security-info@t-systems.com  
www.t-systems.com/security

### PUBLISHED BY

T-Systems International GmbH  
Hahnstrasse 43d  
60528 Frankfurt am Main  
Germany