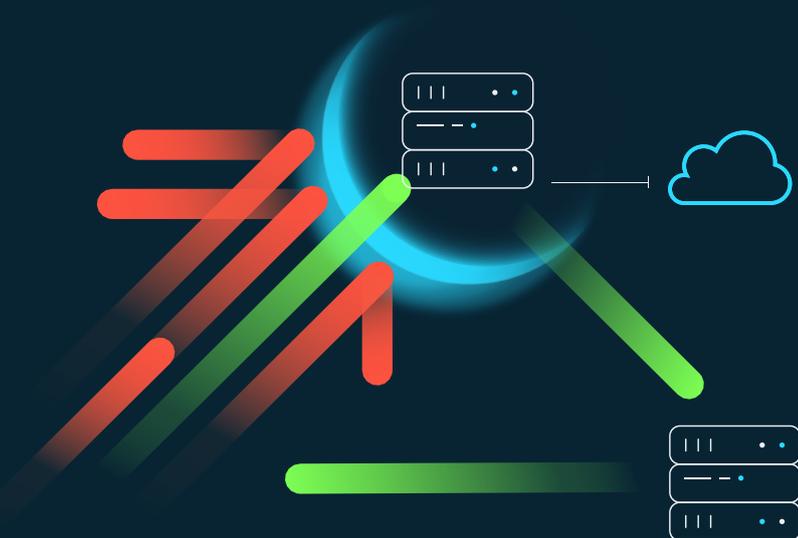


## PRODUCT SHEET

# Myra Cloud Scrubbing



**Benefit from certified protection for your data centers and IT infrastructures. The automatic traffic filtering of Myra Cloud Scrubbing prevents costly downtime and increases the uptime of your business processes sustainably.**

Volumetric DDoS attacks on IT infrastructures are increasing in frequency and strength year after year. Massive damage to operators is the result. According to an Allianz analysis, external events such as DDoS attacks account for 85 percent of global cyber insurance losses. Myra Cloud Scrubbing secures enterprise infrastructures from such threats at layer 3 and 4.

- **Qualified security for critical infrastructure**  
Highly efficient DDoS protection for mitigating a wide range of attack vectors
- **On-demand or always-on**  
Demand-driven Mitigation based on real-time monitoring or permanently active protection
- **Individual configuration**  
Thresholds, IP prefixes, measures, flow systems
- **Automatic or manual mitigation**  
You can trigger mitigation either automatically or manually via dashboard (WebGUI), API call or terraform provider.

## WHY MYRA SECURITY?

**Comprehensive certification**  
Our technologies, services and processes are regularly audited and certified to the highest standards.

**Made in Germany**  
As a company headquartered in Germany, Myra is legally compliant with the GDPR.

**Local 24/7 support**  
Get professional help from our IT experts from the Myra SOC (Security Operations Center).

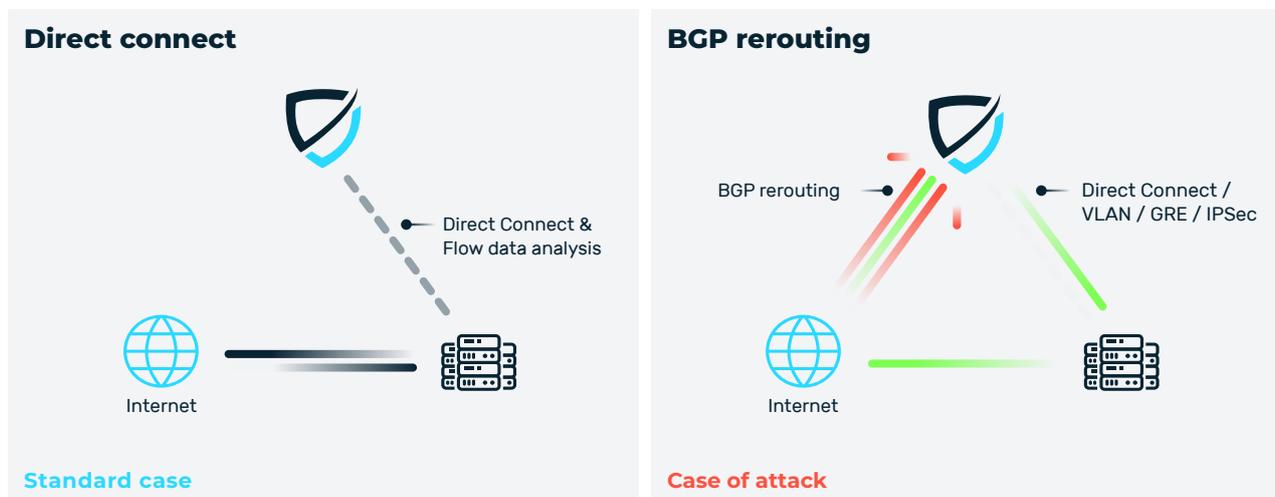
## This is how Myra Cloud Scrubbing protects your data centers

In the event of an attack, all traffic is redirected to the Myra infrastructure through an automatically triggered „more specific BGP announcement“. The Myra Scrubbing Center filters out and discards the malicious attack traffic, while the valid clean traffic continues to be delivered to the destination server. Once the attack is over, the BGP announcement is withdrawn. The data packets then flow directly to the customer infrastructure again and there is no more filtering by Myra.

## Identify and defend against attacks reliably – fully automated or manually

In on-demand mode, Myra Flow Monitoring monitors traffic flows in real-time. If the threshold values defined individually for the customer network are exceeded, mitigation can be initiated within a few seconds. Manual switching is also possible in the Myra Dashboard (WebGUI), via BGP announcement or via API call. This allows you to proactively secure online events, livestreams or traffic-intensive shopping events (Black Friday, Cyber Monday etc.) that are particularly worth protecting.

In the alternative always-on mode, every data packet always passes through the Myra infrastructure. This mode of operation is advantageous for responding instantaneously to attacks.



## Benefit now from the advantages of a customized DDoS protection for your infrastructure

### Stop DDoS attacks

Secure network and protocol-level protection for web infrastructures and data centers against volumetric attacks:

- Protection against ICMP flood, UDP fragmentation, UDP reflection, UDP amplification via DNS, NTP, rpcbind, SSDP, SYN flood, ACK flood, RST flood, and others
- Support for IP subnets from /24 for IPv4 and /48 for IPv6
- Flexible connectivity via Direct Connect, GRE tunnel, VLAN or IPsec

### On-demand or always-on

Myra offers a choice between flexible on-demand protection and permanently active always-on mode, with attractive cost models that require minimal configuration effort.

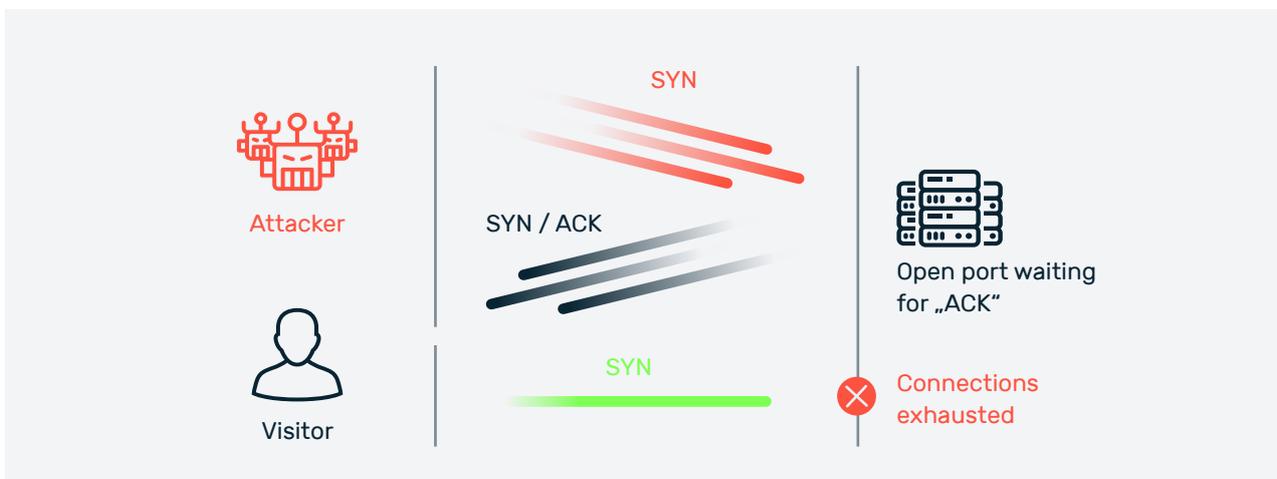
- No configuration effort in case of an attack due to API
- Real-time traffic analysis via flow monitoring with individually definable thresholds

## These attacks threaten your business at layer 3/4

All attacks on layer 3/4 stress the target either with very high bandwidths or immense packet rates. Legitimate accesses thus no longer find a data channel to establish communication.

### Example: SYN/ACK attack

In a SYN/ACK attack (or SYN and ACK floods), for example, a botnet controlled remotely by attackers floods a server with SYN packets. These are usually part of the so-called three-way handshake that occurs when a TCP connection is established between client and server. A SYN/ACK attack provokes mass half-open connections by sending many SYN packets but no ACK packets needed to fully establish a connection. As a result, no new connections can be established, and the website is no longer accessible.



Myra Cloud Scrubbing automatically detects SYN/ACK attacks as well as other DDoS attack types and filters the malicious traffic immediately. This means no additional load on your origin servers, even in the event of an acute attack.

## Providing transparent insights into DDoS defenses

In the event of an attack, the Myra SOC will inform you of the mitigation via ticket center or by telephone. In addition, you will receive an attack report (German and English) within 48 hours on weekdays, which will be provided to you via the ticket center.



### You will receive this information:

- Attacked domain(s)
- IP(s)
- Period
- Origin impact
- Attack type
- Peak bandwidth
- Peak packet rate
- Attacker details like attacking IPs / AS networks / countries / software stacks
- Applied treatment methods
- Recommended actions

## Key benefits and features at a glance



### Qualified security for critical infrastructure

Highly efficient DDoS protection for mitigating a wide range of attack vectors



### On demand operation

Fully automated mitigation with switchover times of a few seconds in the event of an attack



### Provider independent

Implementable in a short time, independent of existing infrastructure and provider



### IPv6 and IPv4

Protection for IP subnets from /24 for IPv4 and /48 for IPv6



### GRE

Universal traffic forwarding via GRE tunnel



### API

Optional automated or manual switching of subnets via API call



### VLAN

High-performance and flexibly configurable connection for the transmission of clean traffic



### Direct Connect

The direct connection between your infrastructure and Myra makes you independent of disturbances in the public network.



### Extensive peering options

Connection of your infrastructure to the most important data centers and Internet nodes



### IPsec (optional)

Encrypted forwarding of clean traffic for increased security requirements



### Flow monitoring

Real-time traffic analysis in own data center for individual mitigation configuration



### Myra Dashboard (WebGUI)

Fast and easy switching for subnets via a graphical user interface



### Reporting

Incident reports from Myra SOC with detailed information about incidents



## Industry-leading security, performance and compliance

- **BSI-KRITIS-qualified:** The BSI catalog includes 37 comprehensive criteria that DDoS providers must meet to qualify for the protection of critical infrastructure (“KRITIS”). Myra is one of the leading security service providers worldwide, meeting all 37 criteria.
- **Comprehensive certified quality:** ISO 27001 certification based on IT-Grundschutz, BSI-KRITIS certified, BSI C5 Type 2, DIN EN 50600 certified datacenters, PCI-DSS certified, IDW PS 951 Type 2 (ISAE 3402) audited service provider, Trusted Cloud
- **Special cluster for critical infrastructures:** GDPR-compliant, geo-redundant server infrastructure in Germany
- **Made in Germany:** full technical control, permanent development, 24/7 full service support

## BSI-certified IT security

Myra Technology is certified by the German Federal Office for Information Security (BSI) in accordance with the ISO 27001 standard based on IT-Grundschutz. In addition, we are one of the leading security service providers worldwide to meet all 37 criteria set by the BSI for qualified DDoS protection providers. We are setting the standard in IT security.



ISO 27001 BSI zertifiziert  
auf der Basis von IT-Grundschutz  
Zertifikat Nr.: BSI-IGZ-0479-2021



PCI DSS  
Certified



BSIG  
KRITIS-qualifiziert



GDPR  
compliant



BSI C5  
TESTAT TYP 2



Trusted  
Cloud  
SERVICE  
100%



ISAE 3402  
IDW PS 951  
TYPE 2



DIN EN 50600  
zertifiziert  
BETRIEBSSICHERES  
RECHENZENTRUM

Certified by the Federal Office for Information Security (BSI) in accordance with ISO 27001 based on IT-Grundschutz | Certified in accordance with Payment Card Industry Data Security Standard | Qualified for critical infrastructure in accordance with §3 BSI Act | Compliant with (EU) 2016/679 General Data Protection Regulation | BSI C5 Type 2 | Certified Trusted Cloud Service | IDW PS 951 Type 2 (ISAE 3402) audited service provider | DIN EN 50600 certified datacenters

## Myra Security is the new benchmark for global IT security

Myra monitors, analyzes and filters malicious Internet traffic before virtual attacks cause any real damage. Our certified Security as a Service platform protects your digital business processes from multiple risks such as DDoS attacks, botnets and database attacks.



Bundesministerium  
für Gesundheit



ITSG



msc  
Munich Security  
Conference



Barmenia  
EINFACH. MENSCHLICH.



DSV IT Service



BZgA  
Bundeszentrale  
für  
gesundheitliche  
Aufklärung

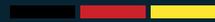


BIOSCIENTIA  
MEDIZIN. LABOR. SERVICE.



Liechtensteinische  
Landesbank 1861

Made in Germany



# Myra Security is the new benchmark for global IT security.

German technology manufacturer Myra Security offers a certified Security as a Service platform to protect digital business processes.

The smart Myra technology monitors, analyzes and filters harmful Internet traffic before virtual attacks can cause real damage.

**Request an individual security analysis now**

**Myra Security GmbH**



+49 89 414141 - 345



[www.myrasecurity.com](http://www.myrasecurity.com)



[info@myrasecurity.com](mailto:info@myrasecurity.com)