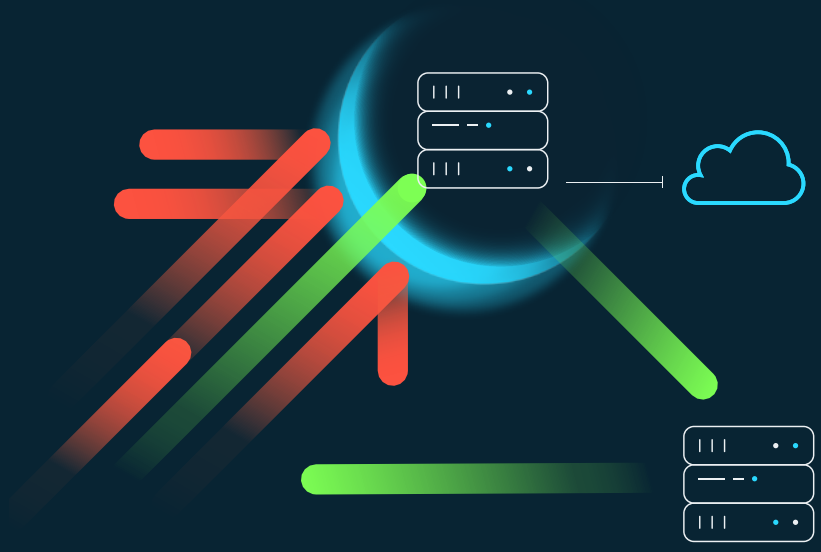
MYRA

PRODUCT SHEET

Myra Cloud Scrubbing



Profitieren Sie von zertifiziertem Schutz für Ihre Rechenzentren und IT-Infrastrukturen. Die automatische Traffic-Filterung des Myra Cloud Scrubbing verhindert kostspielige Betriebsausfälle und steigert die Uptime Ihrer Geschäftsprozesse nachhaltig.

Großvolumige DDoS-Angriffe auf IT-Infrastrukturen nehmen Jahr für Jahr in Frequenz und Stärke zu. Massive Schäden für die Betreiber sind die Folgen. Laut einer Analyse der Allianz verursachen externe Ereignisse wie DDoS-Attacken 85 Prozent der globalen Cyberversicherungsschäden. Das Myra Cloud Scrubbing sichert die Infrastrukturen von Unternehmen vor solchen Bedrohungen auf Layer 3 und 4.

- **KRITIS-qualifizierte Sicherheit**
  Hocheffizienter DDoS-Schutz zur Mitigation verschiedenster Angriffsvektoren
- **On-demand- oder Always-on-Betrieb**
  Bedarfsgerechte Mitigation auf Basis von Echtzeit-Monitoring oder permanent aktiver Schutz
- **Individuelle Konfiguration**
  Schwellenwerte, IP-Präfixe, Maßnahmen, Flow-Systeme
- **Automatische oder manuelle Umschaltung**
  Auslösen der Mitigation wahlweise automatisiert oder manuell per Dashboard (Web-GUI), API-Call oder Terraform-Provider

WARUM MYRA SECURITY?

Hochzertifiziert
Unsere Technologien, Services und Prozesse werden regelmäßig nach höchsten Standards auditiert und zertifiziert.

Made in Germany
Myra ist ein rechtssicher DSGVO-konformes Unternehmen mit Hauptsitz in Deutschland.

Lokaler 24/7 Support
Professionelle Hilfe durch unser IT-Expertenteam aus dem Myra SOC.

So schützt das Myra Cloud Scrubbing Ihre Rechenzentren

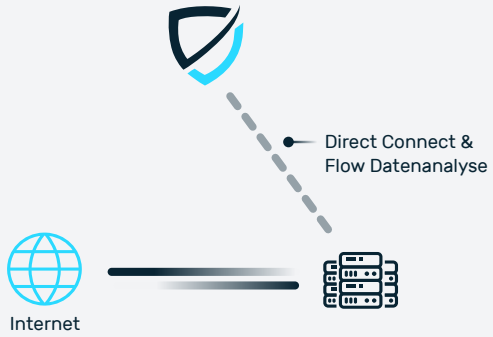
Im Angriffsfall wird sämtlicher Traffic durch ein automatisch ausgelöstes „more specific BGP announcement“ auf die Myra-Infrastruktur umgeleitet. Das Myra Scrubbing Center filtert den bösartigen Angriffs-Traffic heraus und verwirft ihn, während der valide Clean-Traffic weiterhin an den Zielserver ausgeliefert wird. Ist der Angriff vorüber, wird das BGP Announcement zurückgezogen. Die Datenpakete fließen dann wieder direkt zur Kunden-Infrastruktur und es erfolgt keine Filterung mehr durch Myra.

Angriffe zuverlässig identifizieren und abwehren – vollautomatisch oder manuell

Im On-demand-Betrieb überwacht das Myra Flow Monitoring in Echtzeit die Traffic-Ströme. Bei Überschreitung der individuell für das Kundennetz definierten Schwellenwerte kann die Mitigation binnen weniger Sekunden eingeleitet werden. Ebenso ist eine manuelle Umschaltung im Myra Dashboard (Web-GUI), per BGP Announcement oder mittels API-Call möglich. Dies erlaubt Ihnen eine proaktive Absicherung besonders schützenswerter Online-Events, Livestreams oder Traffic-intensiven Shopping-Veranstaltungen (Black Friday, Cyber Monday etc.).

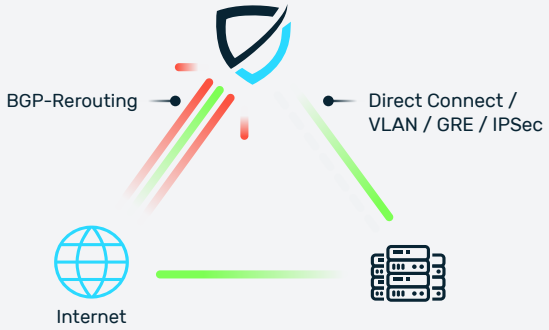
Im alternativen Always-on-Betrieb läuft jedes Datenpaket stets durch die Myra-Infrastruktur. Dieser Betriebsmodus ist von Vorteil, um augenblicklich auf Angriffe zu reagieren.

Direct Connect



Normalfall

BGP-Rerouting



Angriffsfall

Nutzen Sie jetzt die Vorteile eines maßgeschneiderten DDoS-Schutzes für Ihre Infrastruktur

DDoS-Angriffe abwehren

Sicherer Schutz für Webinfrastrukturen und Rechenzentren auf Netzwerk- und Protokoll-Ebene vor volumetrischen Angriffen:

- Schutz vor ICMP-Flood, UDP-Fragmentation, UDP-Reflection, UDP-Amplification via DNS, NTP, rpcbind, SSDP, SYN-Flood, ACK-Flood, RST-Flood und zahlreichen weiteren
- Unterstützung für IP-Subnetze ab /24 für IPv4 und /48 für IPv6
- Flexible Konnektivität via Direct Connect, GRE-Tunnel, VLAN oder IPsec

On demand oder always on

Flexibler On-demand-Schutz oder permanent aktiver Always-on-Betrieb: Mit Myra haben Sie die Wahl und profitieren von attraktiven Kostenmodellen bei niedrigem Konfigurationsaufwand.

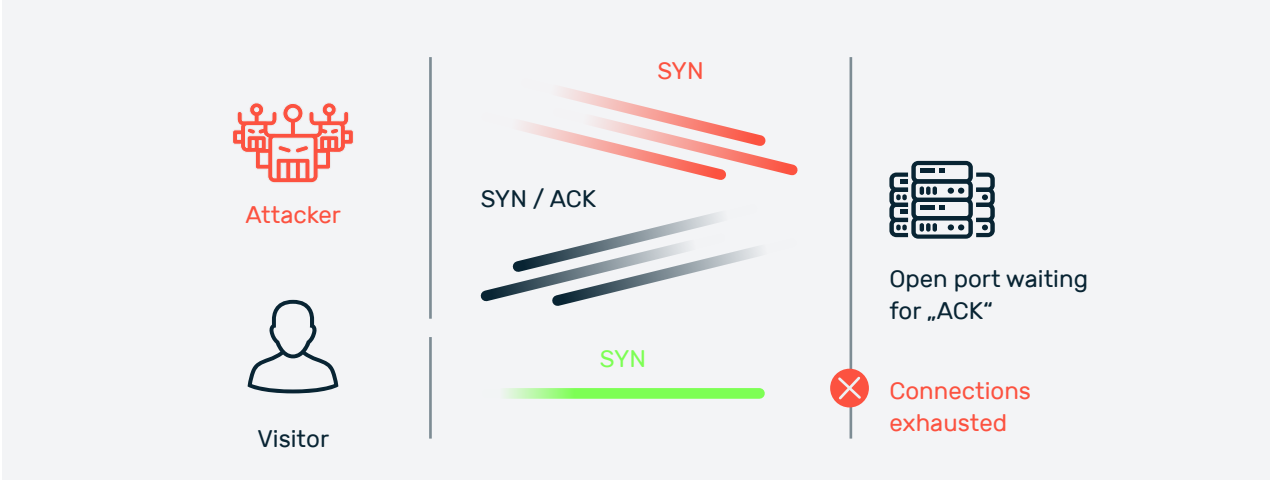
- Kein Konfigurationsaufwand im Angriffsfall durch API-Switch
- Echtzeit-Traffic-Analysen per Flow-Monitoring mit individuell definierbaren Schwellenwerten

Diese Attacken bedrohen Ihr Business auf Layer 3/4

Alle Angriffe auf Layer 3/4 belasten das Ziel entweder mit sehr hohen Bandbreiten oder immensen Paketraten. Legitime Zugriffe finden so keinen Datenkanal mehr, um eine Kommunikation zu etablieren.

Beispiel: SYN/ACK-Attacke

Bei einer SYN/ACK-Attacke (oder SYN- und ACK-Floods) bombardiert etwa ein von Angreifern ferngesteuertes Botnetz einen Server mit SYN-Paketen. Diese sind normalerweise Teil des sogenannten Three-Way-Handshake (Drei-Wege-Handschlag), der beim Aufbau einer TCP-Verbindung zwischen Client und Server erfolgt. Eine SYN/ACK-Attacke provoziert massenhaft halboffene Verbindungen, indem sie viele SYN-, aber keine zum vollständigen Verbindungsaufbau benötigten ACK-Pakete sendet. Die Folge: Es können keine neuen Verbindungen mehr hergestellt werden, und die Website ist nicht mehr erreichbar.



Das Myra Cloud Scrubbing erkennt SYN/ACK-Attacken sowie weitere DDoS-Angriffsarten automatisch und filtert den schädlichen Traffic umgehend. Auf Ihren Origin-Servern entsteht dadurch selbst im akuten Angriffsfall keine zusätzliche Last.

Transparente Einblicke in die DDoS-Abwehr

Im Angriffsfall informiert Sie das Myra SOC via Ticketcenter oder telefonisch über die Umschaltung. Außerdem erhalten Sie werktags innerhalb von 48 Stunden einen Angriffsbericht (deutsch und englisch), der Ihnen über das Ticketcenter bereitgestellt wird.

Diese Informationen erhalten Sie:

- angegriffene Domain(s)
- IP(s)
- Zeitraum
- Origin-Impact
- Angriffstyp
- Peak-Bandbreite
- Peak-Paketrate
- Angreiferdetails wie attackierende IPs / AS-Netze / Länder / Softwarestacks
- angewandte Behandlungsmethoden
- Handlungsempfehlungen

Die wichtigsten Benefits und Features auf einen Blick

+ **KRITIS-qualifizierte Sicherheit**
Schutz vor DDoS-, DRDoS- und Amplification-Angriffen

+ **On-demand-Betrieb**
Vollautomatische Mitigation mit Umschaltzeiten von wenigen Sekunden im Angriffsfall

+ **Providerunabhängigkeit**
Unabhängig von bestehender Infrastruktur und Provider in kurzer Zeit implementierbar

+ **IPv6 und IPv4**
Schutz für IP-Subnetze ab /24 für IPv4 und /48 für IPv6

+ **GRE**
Universell einsetzbare Traffic-Weiterleitung per GRE-Tunnel

+ **API**
Wahlweise automatisierte oder manuelle Umschaltung von Subnetzen per API-Call

+ **VLAN**
Hochperformante und flexibel konfigurierbare Verbindung zur Übermittlung des Clean-Traffics

+ **Direct Connect**
Die direkte Verbindung zwischen Ihrer Infrastruktur und Myra macht Sie unabhängig von Störungen im öffentlichen Netz.

+ **Umfangreiche Peering-Optionen**
Anbindung Ihrer Infrastruktur an den wichtigsten Rechenzentren und Internetknoten

+ **IPsec (optional)**
Verschlüsselte Weiterleitung des Clean-Traffics für erhöhte Sicherheitsanforderungen

+ **Flow-Monitoring**
Echtzeit-Traffic-Analysen im eigenen Rechenzentrum für individuelle Mitigations-konfiguration mit flexibel anpassbaren Schwellenwerten

+ **Myra Dashboard (Web-GUI)**
Schnelle und unkomplizierte Umschaltung für Subnetze über eine grafische Nutzeroberfläche

+ **Reporting**
Incident-Report aus dem Myra-SOC (Security Operations Center) mit detaillierten Informationen über Vorfälle

Branchenführende Sicherheit, Performance und Compliance

- **BSI-KRITIS-qualifiziert:** Myra erfüllt als einer der führenden Anbieter alle 37 Kriterien des BSI für qualifizierte KRITIS-Sicherheitsdienstleister
- **Hochzertifizierte Qualität:** ISO 27001 auf Basis von IT-Grundschutz, BSI-KRITIS-qualifiziert, BSI-C5-Testat Typ 2, DIN-EN-50600-zertifizierte Rechenzentren, PCI-DSS-zertifiziert, IDW PS 951 Typ 2 (ISAE 3402) geprüft, Trusted Cloud
- **KRITIS-Cluster:** DSGVO- und IT-SiG-konforme, mehrfach georedundante Server-Infrastruktur in Deutschland
- **Made in Germany:** volle technische Kontrolle, permanente Weiterentwicklung, 24/7-Full-Service-Betreuung durch unser IT-Expertenteam im Security Operations Center

BSI-zertifizierte IT-Sicherheit

Die Myra-Technologie ist vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach dem Standard ISO 27001 auf Basis von IT-Grundschutz zertifiziert. Zudem erfüllen wir als einer der führenden Anbieter alle 37 Kriterien des BSI für qualifizierte KRITIS-Sicherheitsdienstleister. Damit setzen wir den Maßstab in der IT-Sicherheit.

Zertifiziert vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach ISO 27001 auf Basis von IT-Grundschutz | Zertifiziert nach Payment Card Industry Data Security Standard | KRITIS-qualifiziert nach §3 BSI-Gesetz| Konform mit der (EU) 2016/679 Datenschutz-Grundverordnung | BSI-C5-Testat Typ 2 | Geprüfter Trusted Cloud Service | IDW PS 951 Typ 2 (ISAE 3402) geprüfter Dienstleister | Zertifizierung von Rechenzentren nach DIN EN 50600

Myra Security ist der neue Maßstab für globale IT-Sicherheit

Myra überwacht, analysiert und filtert schädlichen Internet-Traffic bevor virtuelle Angriffe einen realen Schaden anrichten. Unsere zertifizierte Security-as-a-Service-Plattform schützt Ihre digitalen Geschäftsprozesse vor vielfältigen Risiken wie DDoS-Attacken, Bot-Netzwerken und Angriffen auf Datenbanken.

Made in Germany

Myra Security ist der neue Maßstab für globale IT-Sicherheit.

Myra bietet als deutscher Technologiehersteller eine sichere, zertifizierte Security-as-a-Service-Plattform zum Schutz digitaler Geschäftsprozesse.
Die smarte Myra-Technologie überwacht, analysiert und filtert schädlichen Internet-Traffic, noch bevor virtuelle Angriffe einen realen Schaden anrichten.

Jetzt individuelle Sicherheitsanalyse anfordern

Myra Security GmbH

+49 89 414141 - 345
www.myrasecurity.com
info@myrasecurity.com