MYRA

PRODUCT SHEET

Myra DDoS Protection

Schützen Sie Ihre Webseiten, Webanwendungen und Schnittstellen hocheffizient vor Cyberattacken – ohne zusätzliche Aufwände für Software oder Hardware. Die Myra DDoS Protection lässt sich schnell und einfach implementieren. Einmal aufgesetzt, schützt Sie die Lösung vollautomatisch vor DDoS-Angriffen und steigert damit die Uptime Ihrer Geschäftsprozesse.

Schädliche Anfragen und Angriffe auf der Anwendungsebene (Layer 7) haben seit einigen Jahren Hochkonjunktur. Auswertungen aus dem Security Operations Center (SOC) von Myra ergaben für das Jahr 2022 einen Anstieg der Angriffsaktivität auf Layer 7 um 178 Prozent gegenüber dem Vorjahr. Die Myra DDoS Protection schützt Ihre digitalen Geschäftsprozesse automatisiert vor diesen Bedrohungen.

- **KRITIS-qualifizierte Sicherheit**
  Hocheffizienter Schutz vor DDoS-Angriffen wie HTTP/S GET Flood, HEAD Flood, POST Flood oder „Low and slow"-Attacken
- **Upstream Monitoring**
  Myra überwacht Ihren Upstream in Echtzeit und informiert Sie vollautomatisch, sobald Probleme auftreten.
- **Advanced GeoIP Blocking**
  Die Myra DDoS Protection kann verdächtige Clients auf Basis von GeoIP, Region und weiteren IP-Merkmalen blockieren.
- **Rate Limiting**
  Bestimmen Sie die Anzahl der Webanfragen, die auffällige IP-Adressen in einem von Ihnen definierten Zeitraum durchführen dürfen.

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 die Myra DDoS Protection Ihre Webressourcen

Die cloudbasierte Myra DDoS Protection verbirgt und sichert Ihre Webseiten, Portale und Schnittstellen hinter einem eigens entwickelten Filtersystem. Für Angreifer sind damit die Server, auf denen Ihre Anwendungen betrieben werden, nicht zu erkennen. Schädliche Traffic-Ströme werden durch die mehrstufigen Filterschichten abgewehrt. Valide Anfragen erreichen Ihre Infrastruktur weiterhin wie gewohnt über einen redundanten HTTP/S-Reverse-Proxy.

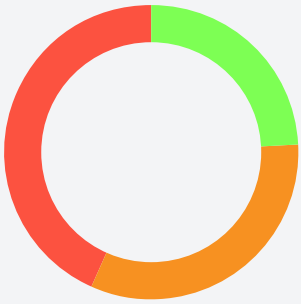
Hocheffizienter DDoS-Schutz ohne Implementierungshürden

Als Security-as-a-Service-Lösung erfordert der Betrieb der Myra DDoS Protection keine zusätzliche Software oder Hardware. Die technische Aufschaltung ist über zweierlei Wege möglich: Entweder erfolgt eine Anpassung des DNS-Eintrags über den CNAME-Eintrag oder der autoritative DNS-Server wird mithilfe eines Imports bestehender Zonen an Myra übertragen. Sobald nun die entsprechenden SSL/TLS-Zertifikate des Kunden per API oder Upload im Myra Dashboard (Web-GUI) zur Verfügung gestellt wurden, kann die SSL/TLS-Verbindung terminiert und eine Deep Packet Inspection durchgeführt werden.

In enger Abstimmung mit dem Kunden übernimmt das Myra SOC abschließend die Konfiguration der Filterregeln. Maßgeschneiderte Filter erlauben eine granulare Traffic-Steuerung, um schädliche oder verdächtige Anfragen effizient zu blockieren.

Warum sich Angreifer auf Layer-7-Attacken fokussieren

3 von 4 Firmen scheitern bei der Abwehr von Layer-7-Attacken



- **Erfolgreich:** Angriff mitigiert, maximale Mitigationszeit 30 Sekunden
- **Problematisch:** Angriff entweder nur teilweise oder manuell mitigiert, hoher Impact für mindestens 10 Minuten
- **Fehlgeschlagen:** keine Mitigation

zeroBS, 2023

Cyberkriminelle nehmen mit komplexen Attacken zunehmend die äußerste Netzwerkschicht ins Visier, weil dort die Abwehr noch vielen Unternehmen enorme Schwierigkeiten bereiten – wie eine Untersuchung der Pentesting-Fachleute von zeroBS ergab.

DDoS-Attacken auf Layer 7 basieren auf bereits aufgebauten Verbindungen. Insbesondere HTTP GET, POST und weitere Flood-Attacken sowie „Low and slow"-Angriffe sind bei Cyberkriminellen beliebt. Sie zielen darauf ab, die schwächste Komponente einer Infrastruktur zu penetrieren und so eine Überlastung der Webapplikation hervorzurufen.

HTTP-GET-Flood-Attacken belasten Webserver beispielsweise mit HTTP-Anfragen, die gezielt Seiten mit großem Ladevolumen aufrufen. Dadurch wird der Server überlastet und kann keine legitimen Anfragen mehr verarbeiten. Für die oftmals standardmäßig von Hostern implementierten Schutzsysteme für Layer 3 und 4 sind solche Angriffe nicht von herkömmlichen Nutzeranfragen zu unterscheiden. Erst durch eine Deep Packet Inspection auf Layer 7, wie sie die Myra DDoS Protection vornimmt, ist eine effektive Identifizierung solcher Angriffe möglich.

Die wichtigsten Benefits und Features auf einen Blick

+ **KRITIS-qualifizierte Sicherheit**
Hocheffizienter Schutz vor DDoS-Angriffen wie HTTP/S GET Flood, HEAD Flood, POST Flood oder „Low and slow"-Attacken

+ **Upstream Monitoring**
Myra überwacht Ihren Upstream in Echtzeit und informiert Sie vollautomatisch, sobald Probleme auftreten.

+ **Advanced GeoIP Blocking**
Die Myra DDoS Protection kann verdächtige Clients auf Basis von GeoIP, Region und weiteren IP-Merkmalen blockieren.

+ **Rate Limiting**
Bestimmen Sie die Anzahl der Webanfragen, die auffällige IP-Adressen in einem von Ihnen definierten Zeitraum durchführen dürfen.

+ **Detailliertes Reporting**
Nach der Mitigation eines Angriffs erhalten Sie ein individuelles Reporting über Dauer, Art und Stärke der Attacke.

+ **SSL/TLS-Cipher-Management**
Myra sorgt für eine ständig aktualisierte SSL/TLS-Konfiguration nach neuesten Sicherheitsstandards.

+ **Breiter Technologie-Support**
Myra unterstützt moderne Webtechnologien wie HTTP/2, WebP, ChaCha20, WebSocket und WebRTC.

+ **Automatische Benachrichtigung**
Im Angriffsfall informiert Sie das System automatisch, entsprechend vorher definierter Eskalations- und Benachrichtigungsstufen.

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

Nahtlose Integration innerhalb der Myra Application Security

Die Funktionalität der Myra DDoS Protection ist innerhalb der Myra Application Security nach Ihren individuellen Bedürfnissen erweiterbar. Alle Lösungen arbeiten nahtlos miteinander und sind konzeptionell aufeinander abgestimmt. Dazu gehören:

Hyperscale WAF
Angreifer nutzen gezielt Schwachstellen in Webanwendungen aus, um in anfällige Systeme einzudringen und Daten zu manipulieren, zu stehlen oder zu löschen. Die Myra Hyperscale Web Application Firewall (WAF) blockiert bösartige Zugriffe, noch bevor diese Ihre Server erreichen.

Deep Bot Management
Rund die Hälfte des weltweiten Web-Traffics wird von Bots erzeugt. Myra erkennt Botzugriffe anhand eines eindeutigen Fingerprints. So können Sie auf jede Anfrage optimal reagieren, automatisierte Zugriffe zielgenau steuern und die Performance Ihrer Website verbessern.

Secure DNS
Für die Ausfallsicherheit von kritischen Webapplikationen ist die Absicherung der Namensauflösung entscheidend. Das gehärtete Myra Secure DNS setzt auf führende Technologien, um Ihre Domains vor Cyberattacken zu schützen und maximale Performance sicherzustellen. Ganze DNS-Zonen lassen sich in der gesicherten Myra-Infrastruktur verwalten.

High Performance CDN
Hohe Geschwindigkeit, niedrige Latenz und flexible Skalierbarkeit: Die Ansprüche an moderne Webanwendungen wachsen zusehends. Mit dem Myra High Performance CDN erreichen Sie dank führender Technologien eine erstklassige Nutzererfahrung.

Push CDN
Verlagern Sie statische Elemente Ihrer Website direkt in das Myra Push CDN und profitieren Sie von georedundanter Hochverfügbarkeit, optimaler Performance und erweiterter Ausfallsicherheit.

Analytics Data Lake
Umfassendes Monitoring und Reporting sind zur Optimierung von Webressourcen unerlässlich. Myra Analytics Data Lake ermöglicht Ihnen, Logdaten nahezu in Echtzeit abzurufen, zu durchsuchen und auszuwerten.

Video Streaming
Nutzer und Nutzerinnen erwarten heute, Videoinhalte immer und überall abrufen zu können. Myra passt Ihre Streams in Echtzeit an sich ändernde Bandbreiten, Verbindungsgeschwindigkeiten und Netzwerktypen an.

Certificate Management
SSL/TLS sorgt für eine sichere Datenübertragung, eindeutige Authentifizierung sowie Dateninteg rität und damit für mehr Vertrauen auf Nutzerseite. Mit dem Myra Certificate Management können Sie SSL/TLS-Zertifikate (DV) automatisch ausstellen lassen und verwalten.

Multi Cloud Load Balancer
Geringe Latenz ist für eine erstklassige Nutzererfahrung im Web entscheidend. Myra stellt sie durch eine ideale Verteilung eingehender Anfragen, optimale Lastverteilung über beliebig viele Backend-Server und verringerte Antwortzeiten sicher.

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