MYRA

PRODUCT SHEET

Myra Hyperscale WAF

Profitieren Sie von dynamischer Sicherheit für Ihre Webanwendungen: Angreifer nutzen gezielt Schwachstellen in Webapplikationen aus, um Daten zu manipulieren, zu stehlen oder zu löschen. Die Myra Hyperscale Web Application Firewall (WAF) blockiert bösartige Anfragen, noch bevor diese Ihre Server erreichen. Schützen Sie sich vor schädlichen Zugriffen und bekannten Schwachstellen-Exploits. Schnell. Zuverlässig. Skalierbar.

Myra filtert, überwacht und kontrolliert den ein- und ausgehenden HTTP/S-Traffic Ihrer Webanwendungen auf Inhaltsebene. Damit bildet die Hyperscale WAF einen vorgelagerten Schutzwall gegen verschiedenste Angriffstechniken (z. B. einige OWASP-Top-10-Risiken). Mit eigens entwickelten und ständig aktualisierten Regeln schützt Myra zudem vor Angriffen auf ungepatchte Systeme sowie auf nicht anders absicherbare Legacy-Anwendungen. So können Sie Ihre Webapplikationen kurzfristig gegen Attacken auf Zero-Day-Lücken wie Log4j/Log4Shell oder Confluence OGNL absichern, bis alle notwendigen Patches eingespielt sind.

- **Umfassende Regelsätze**
  Von Myra verwaltete und ständig aktualisierte WAF-Regeln, die sich an den OWASP Top 10 orientieren, schützen vor den häufigsten Angriffsrisiken sowie vor Zero-Day-Exploits.
- **Managed WAF**
  Auf Wunsch unterstützt Sie das Myra-Expertenteam bei der Analyse Ihrer Webressourcen und der Erstellung maßgeschneiderter Regeln.
- **Webbasierte Regelverwaltung**
  Myra bietet eine webbasierte Regelverwaltung für Pre- und Post-Origin-Traffic. Damit haben Sie die vollständige Kontrolle über alle Regeleinstellungen, die zahlreiche Bedingungen und Aktionen für die Request- bzw. Response-Phase umfassen.
- **HTTP/S Request Filtering**
  Die Filterung von HTTP/S-Anfragen ist sofort einsatzbereit und nahezu beliebig skalierbar.

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.

Diese Risiken bedrohen Ihre Webapplikationen

Webanwendungen sind einer Vielzahl von Sicherheitsrisiken ausgesetzt. Zu den gängigsten Angriffen zählen SQL Injection, Cross-Site Scripting und Cross-Site Request Forgery. Die OWASP Top 10 listet die akutesten Bedrohungen auf. Hinzu kommen Zero-Day-Exploits wie Log4Shell, die schnelles Handeln erfordern. Mit der Myra Hyperscale WAF sind Sie vor all diesen Risiken geschützt:

OWASP Top 10
Das Open Web Application Security Project (OWASP) pflegt eine Liste der zehn größten Sicherheitsrisiken für Webapplikationen. In der aktuellen Ausgabe von 2021 finden sich unter anderem auch Injection-Angriffe.

Zero-Day-Exploits
Zero-Day-Exploits nutzen neu entdeckte Software-Schwachstellen umgehend für Angriffe aus. Angepasste WAF-Regeln bieten sofortigen Schutz, bis Patches für die anfällige Software verfügbar und eingespielt sind.

SQL Injection
Bei einer SQL-Injection-Attacke nutzen Cyberkriminelle gezielt Sicherheitslücken aus, um etwa über Eingabemasken manipulierte Befehle oder Schadcode einzuschleusen.

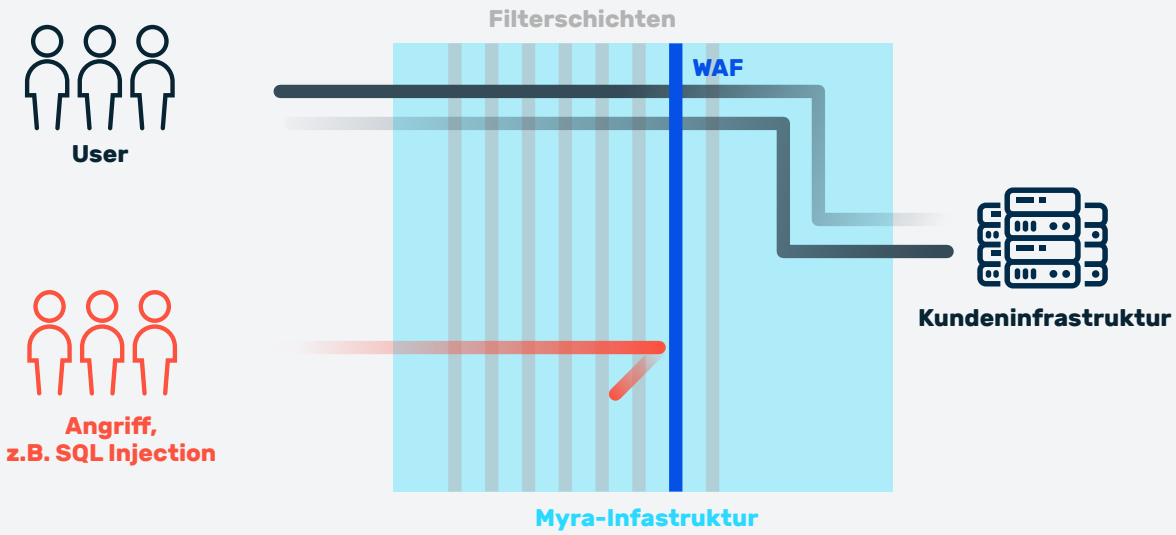
Cross-Site Request Forgery (CSRF)
Angreifer bringen den Browser des Nutzers oder der Nutzerin dazu, HTTP-Requests an die angegriffene Website oder Webapplikation zu schicken, um unerwünschte Aktionen auszulösen.

Cross-Site Scripting (XSS)
Bei einem XSS-Angriff injizieren Cyberkriminelle durch Ausnutzen von Sicherheitslücken schädlichen Code in Webanwendungen, um etwa sensible Informationen wie Login-Daten zu stehlen.

Sichern Sie sich gegen Angriffe auf Anwendungsebene ab

Als Teil der mehrschichtigen Filterarchitektur von Myra schützt die Hyperscale WAF Ihre Webanwendungen vor Angriffen über das Hypertext Transfer Protocol (HTTP/S). Anders als klassische Firewalls und Intrusion-Detection-Systeme untersucht die WAF die Kommunikation direkt auf der Anwendungsebene. Dazu sind keine Änderungen an der zu schützenden Webapplikation notwendig.

Webapplikationen durch WAF geschützt



Inkludierte Standard-Regeln schützten von der ersten Sekunde an

Bereits ab der Installation der Hyperscale WAF stehen Standard-Regeln zum Schutz vor den gängigsten Risiken bereit. Diese Regeln werden von den Sicherheitsfachleuten im Myra Security Operations Center (SOC) fortlaufend aktualisiert und an neue Bedrohungssituationen angepasst. Über das Myra Dashboard (WebGUI) können Sie jederzeit eigene Filter und komplexe, applikationsspezifische WAF-Regeln aufsetzen und optimieren.

Nutzen Sie jetzt die Vorteile der Myra Hyperscale WAF

Schutz vor Datendiebstahl, Kontenübernahme und Sabotage

- Inkludierte Standard-Regeln orientieren sich an den OWASP-Top-10-Risiken
- Einfache Konfiguration und Regelverwaltung über das Myra Dashboard (WebGUI)
- Schutz für alle Webapplikationen und APIs unabhängig vom Hosting-Modell

Sicherheit für verwundbare Systeme

- Das Myra-Expertenteam unterstützt Sie bei der optimalen Anpassung Ihrer WAF-Regeln
- Schnelle und einfache Integration in Ihre IT-Infrastruktur ohne zusätzliche Hard- oder Software

Die wichtigsten Features auf einen Blick

HTTP/S Request Filtering
Die Filterung von HTTP/S-Anfragen ist sofort einsatzbereit und nahezu beliebig skalierbar.

Managed WAF
Auf Wunsch unterstützt Sie das Myra-Expertenteam bei der Analyse Ihrer Web-ressourcen und der Erstellung maßgeschneiderter Regeln.

Custom Error-Pages
Die Myra Hyperscale WAF unterstützt die Anzeige individueller Fehlerseiten, die an Ihr Corporate Design angepasst sind.

Umfassende Regelsätze
Von Myra verwaltete und ständig aktualisierte WAF-Regeln schützen vor den häufigsten Angriffsrisiken (OWASP Top 10) sowie vor Zero-Day-Exploits. Über das Myra Dashboard (WebGUI) können Sie auch eigene Regelsätze mit Hierarchien definieren oder bereits bestehende Regeln aus einer anderen WAF importieren.

Header Rewriting
Header/Response-Rewriting ohne Anpassungen an der Webapplikation

Konfiguration via API
Sie können die Myra Hyperscale WAF vollständig über eine API konfigurieren und steuern.

Alarmierung
Frei konfigurierbare Alarmierung per E-Mail, API-Calls oder SMS

Header Modification
Anpassungen der Header in Request- und Response-Phasen

Webbasierte Regelverwaltung
Myra bietet eine webbasierte Regelverwaltung für Pre- und Post-Origin-Traffic. Damit haben Sie die vollständige Kontrolle über alle Regeleinstellungen, die zahlreiche Bedingungen und Aktionen für die Request- bzw. Response-Phase umfassen.

Nahtlose Integration innerhalb der Myra Application Security

Die Hyperscale WAF ist Teil der Myra Application Security und damit individuell um zusätzliche Performance- und Sicherheitsfunktionen erweiterbar. Alle Lösungen arbeiten nahtlos zusammen und sind konzeptionell aufeinander abgestimmt. Dazu gehören:

DDoS Protection
Angreifer zielen mit Denial-of-Service-Attacken darauf ab, die digitalen Prozesse von Unternehmen und Organisationen gezielt zu stören oder lahmzulegen. Die Myra DDoS Protection wehrt selbst hochkomplexe Angriffe auf Ihre Webanwendungen ab und hält diese hochverfügbar.

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.

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.

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.

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.

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

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.

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.

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.

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.

ISO 27001 BSI zertifiziert auf der Basis von IT-Grundschutz Zertifikat Nr.: BSI-IGZ-0479-2021 | PCI DSS Certified | BSIG KRITIS-qualifiziert | BSI C5 Testat Typ 2 | Trusted Cloud | ISAE 3402 IDW PS 951 Type 2 | DIN EN 50600 zertifiziert Betriebssicheres Rechenzentrum

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 (PCI DSS) | KRITIS-qualifiziert nach §3 BSI-Gesetz | 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.

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 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