MYRA

PRODUCT SHEET

Myra Hyperscale WAF

Benefit from dynamic security for your web applications: Attackers specifically exploit vulnerabilities in web applications to manipulate, steal or delete data. Myra Hyperscale Web Application Firewall (WAF) blocks malicious requests before they reach your servers. Protect your business from malicious traffic and known vulnerability exploits. Fast. Reliable. Scalable.

Myra filters, monitors, and controls the inbound and outbound HTTP/S traffic of your web applications at the content level. In this way, the Hyperscale WAF forms an in front protective wall against a wide range of attack techniques (e.g., some OWASP Top 10 risks). With specially developed and constantly updated rules, Myra also protects against attacks on unpatched systems as well as on legacy applications that cannot be secured in any other way. This allows you to secure your web applications in the short term against attacks on zero-day vulnerabilities such as Log4j/Log4Shell or Confluence OGNL until the necessary patches have been applied.

- **Comprehensive rule sets**
  Myra-managed and continuously updated WAF rules, aligned with the OWASP Top 10, protect against the most common attack risks as well as zero-day exploits.
- **Managed WAF**
  Myra experts will analyze your web resources and assist you in creating customized rule sets.
- **Web-based rule management**
  Myra provides web-based rule management for pre- and post-origin traffic. This gives you complete control over all rule settings, which include numerous conditions and actions for the request or response phase.
- **HTTP/S request filtering**
  The filtering of HTTP/S requests is ready to use and almost infinitely scalable.

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).

These risks threaten your web applications

Web applications are exposed to a variety of security risks. The most common attacks include SQL injection, cross-site scripting and cross-site request forgery. The OWASP Top 10 lists the most acute threats. In addition, there are zero-day exploits such as Log4Shell that require quick action. With the Myra Hyperscale WAF you are protected against all these risks:

OWASP Top 10
The Open Web Application Security Project (OWASP) maintains a list of the top ten security risks for web applications. The current 2021 edition includes injection attacks, among others.

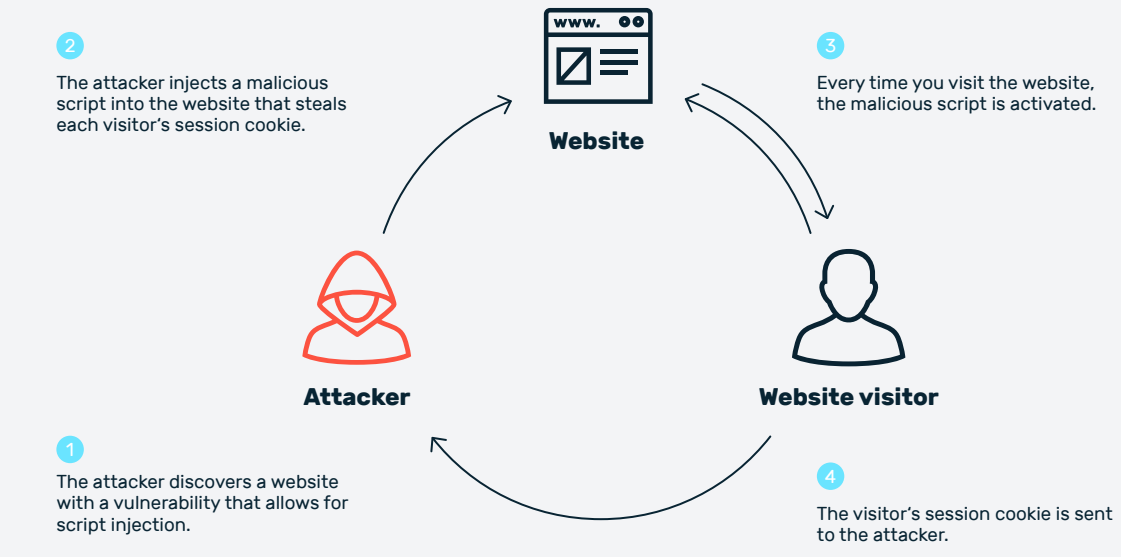
Zero-day exploits
Zero-day exploits immediately exploit newly discovered software vulnerabilities for attacks. Customized WAF rules provide protection until patches for the vulnerable software are available and applied.

SQL injection
In an SQL injection attack, cybercriminals exploit security vulnerabilities, for example, to inject manipulated commands or malicious code via input masks.

Cross-site request forgery (CSRF)
Attackers make the user's browser send HTTP requests to the attacked website or web application to trigger unwanted actions.

Cross-site scripting (XSS)
In an XSS attack, cybercriminals inject malicious code into web applications by exploiting vulnerabilities, for example, to steal sensitive information.

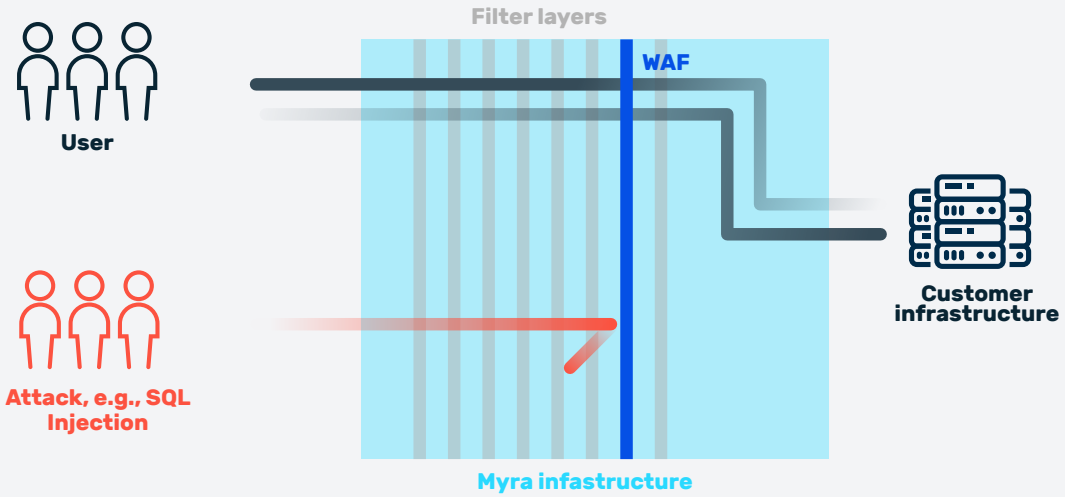
Persistent cross-site scripting



Secure your business against application-level attacks

As part of Myra's multi-layer filtering architecture, Hyperscale WAF protects your web applications from attacks over the Hypertext Transfer Protocol (HTTP/S). Unlike classic firewalls and intrusion detection systems, the WAF analyzes traffic directly at the application level. This does not require any changes to the web application to be protected.

Web applications protected by WAF



Included standard rules protect your business from the very first second

Standard rules for protection against the most common risks are already in place when the Hyperscale WAF is installed. These rules are continuously updated by the security experts in the Myra Security Operations Center (SOC) and adapted to new threat situations. You can set up and optimize your own filters and complex, application-specific WAF rules at any time via the Myra Dashboard (WebGUI).

Benefit now from Myra Hyperscale WAF

Protection against data theft, account takeover and sabotage

- Included standard rules are based on the OWASP Top 10 risks
- Easy configuration and rule management via the Myra dashboard (WebGUI)
- Protection for all web applications and APIs regardless of hosting model

Security for vulnerable systems

- The Myra experts support you in the optimal customization of your WAF rules
- Fast and easy integration into your IT infrastructure requires no additional hardware or software

Key benefits and features at a glance

HTTP/S request filtering
The filtering of HTTP/S requests is ready to use and almost infinitely scalable.

Managed WAF
Myra experts will analyze your web resources and assist you in creating customized rule sets.

Custom error pages
The Myra Hyperscale WAF supports the delivery of customized error pages that are adapted to your corporate design.

Comprehensive rule sets
Rule sets managed and constantly updated by Myra protect against the most common attack risks (OWASP Top 10) as well as zero-day exploits. Via the editor, you can define your own rule sets with hierarchies or import already existing rule sets from another WAF.

Header rewriting
Header/response rewriting without adjustments to the web application

Configuration via API
You can fully configure and control the Myra Hyperscale WAF via an API.

Alerting
Freely configurable alerting via email, API calls or SMS

Header modification
Adjustments of headers in request and response phases

Web-based rule management
Myra provides web-based rule management for pre- and post-origin traffic. This gives you complete control over all rule settings, which include numerous conditions and actions for the request or response phase.

Seamless integration within Myra Application Security

Hyperscale WAF is part of Myra Application Security and can therefore be individually extended with additional performance and security features. All solutions work seamlessly together and are conceptually aligned. These include:

DDoS Protection
Attackers use denial-of-service attacks to disrupt digital processes of companies and organizations. Myra DDoS Protection defends even highly complex attacks on your web applications and keeps them fully operational.

High Performance CDN
High speed, low latency, and flexible scalability: the demands on modern web applications are growing more and more. With Myra High Performance CDN you achieve a first-class user experience thanks to leading technologies.

Analytics Data Lake
Comprehensive monitoring and reporting are essential to optimize web resources. Myra Analytics Data Lake allows you to retrieve, search and analyze log data in near real-time.

Secure DNS
To ensure the resilience of critical web applications, name resolution protection is critical. The hardened Myra Secure DNS relies on leading technologies to protect your domains from cyber-attacks and ensure maximum performance. Entire DNS zones can be managed within the Myra secure infrastructure.

Deep Bot Management
About half of the world's web traffic is generated by bots. Myra recognizes bot requests by identifying them with a unique fingerprint. This allows you to respond optimally to each request, control automated requests precisely and improve the performance of your website.

Certificate Management
SSL/TLS ensures secure data transmission, unique authentication as well as data integrity and therefore more user trust. With Myra Certificate Management, you can automatically issue and manage SSL/TLS certificates (DV).

Video Streaming
Today's users expect to be able to access video content anytime, anywhere. Myra seamlessly optimizes your streams in real time as bandwidths, connection speeds, and network types change.

Multi Cloud Load Balancer
Low latency is critical for a first-class user experience on the Internet. Myra ensures it through ideal distribution of incoming requests, optimal load balancing across any number of backend servers, and reduced response times.

Push CDN
Move static elements of your website directly to the Myra Push CDN and benefit from geo-redundant high availability, enhanced performance and advanced resilience.

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 | 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
info@myrasecurity.com