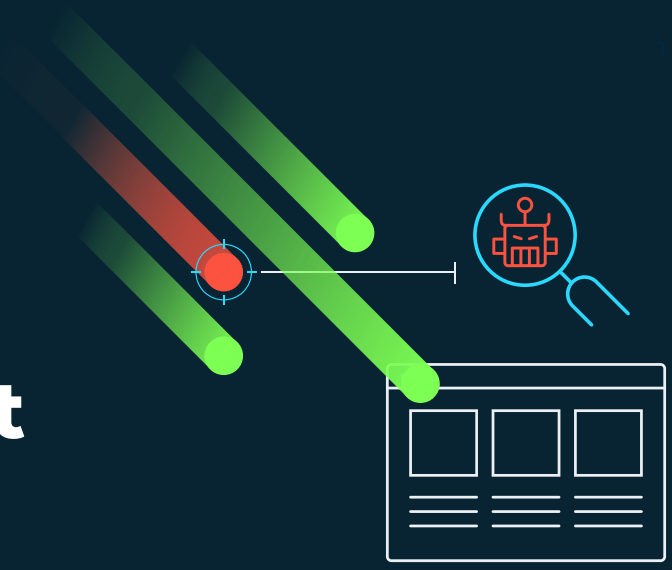
MYRA



PRODUCT SHEET

Myra Deep Bot Management

Protect your web applications from unauthorized access and malicious bots. Myra creates a unique fingerprint for all requesting bots and recognizes them quickly and reliably. This allows you to respond optimally to each request, to control automated traffic precisely, and to improve the performance of your website.

Today, autonomously operating bots represent about half of all website traffic, and about 20 percent is considered potentially dangerous. Malicious bots scan web platforms for exploitable vulnerabilities, copy content, block shopping carts, or attempt to compromise user accounts. Additionally, queries from search engines, scrapers, crawlers or other automated systems affect website performance, which can negatively impact the user experience and thus your business. Myra Deep Bot Management analyzes all incoming requests and blocks unauthorized access.

- **Passive fingerprinting**
  Myra reliably detects any deployed bot software based on a unique fingerprint - independently of IP, ASN and User Agent.
- **Automation tool detection**
  Myra reliably detects automation tools such as Selenium or PhantomJS.
- **Behavioral analytics**
  Using behavioral analysis, Myra automatically identifies unusual request patterns.
- **Alternate origin**
  If necessary, Myra redirects requests to alternative origin servers to protect the main infrastructure.
- **Fast and easy integration**
  Myra Deep Bot Management requires no additional hardware or software.

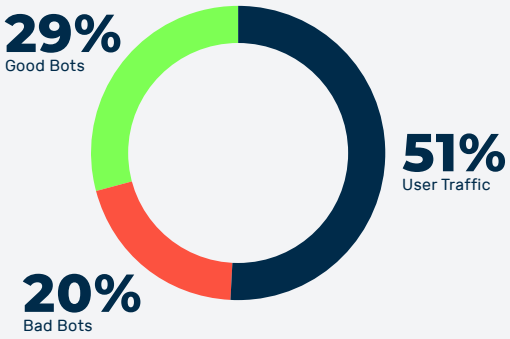
WHY MYRA SECURITY?

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).

Only half of website traffic is generated by people



This is how Myra Deep Bot Management protects your business

Myra separates, classifies and analyzes all incoming requests. Based on the result of the analysis, the appropriate response (Block, CAPTCHA, Log, Pass) is delivered for each request. Myra rejects or blocks unwanted or malicious requests even before they reach your servers. False positives are prevented by the mildest effective means, e.g. human interaction challenges. Using rate limiting, you can allow a limited number of requests per time unit to good bots such as search engines, so that the traffic load caused by them remains low and the performance of your website remains constantly high.

Fast and reliable bot detection based on unique fingerprints

Bots access websites with different IP addresses and from different networks. The automated programs pretend to be a normal browser and spoof further information such as ASN or device ID to give the appearance of regular use. Because the automated accesses are distributed, no connection between them can be seen at first glance. Myra Deep Bot Management establishes precisely this connection for you thanks to passive fingerprinting: each time a website is accessed, Myra generates a fingerprint from over 50 attributes of the access to uniquely identify the software used. As soon as the fingerprint of a bot is available, it is immediately recognized the next time it is accessed. Unwanted bot requests can thus be clearly identified, blocked or otherwise controlled or redirected.

Myra uses more than 50 attributes to identify bots, including:

These bot-based attacks threaten your business

Botnet-based denial of service attacks (DDoS)
Using botnets, attackers send a flood of automated requests to your web servers to overload it and disable the sites or services hosted on it.

Hype sales bots
Through automated bot requests, fraudsters secure desirable goods and then resell them at a high profit, negatively impacting your customer relationship.

Web scraping
Bots copy individual page contents or entire websites in a matter of seconds. Criminals use such a copy of the original page to steal login data via phishing.

Cart abandonment/inventory hoarding
Bots fill shopping carts without completing the purchase process. This is a business-damaging issue for your store because regular customers are temporarily unable to buy those items.

Click fraud
Attackers use bots to automatically click on advertisements or affiliate links contained on websites to generate revenue at the expense of the advertisers.

Account creation & takeover
Bots create masses of fake user accounts or infiltrate existing accounts, which criminals then abuse for attacks or fraud attempts.

Credential stuffing
Bots can test masses of user/password combinations in a very short time. Successfully hijacked accounts are then sold or used for further attacks.

Skewing
Using bot-based queries, attackers manipulate targeted web analytics data to mislead you into making bad strategic decisions and harm your business.

Formular spam
Bots attack your company with messages via contact forms. This phishing method often serves criminals as a starting point for further attacks.

Price grabbing
Bots copy product prices or entire pricing structures. Competitors can use this data to automatically undercut your prices.

Benefit now from Myra Deep Bot Management

Analyze incoming requests

- Protect applications and APIs from malicious bots to prevent revenue loss, data theft, and account takeover
- Better website performance for human users and good bots
- Greater customer satisfaction
- Flexible management of search engine bots with uplift of SEO scoring

Block unwanted requests

- Protection against bot-based attacks and therefore enhanced IT security
- Security against malicious requests, such as click fraud, scraping, and price grabbing.
- Reduced server costs by filtering out unwanted bot traffic
- Transparency regarding traffic and actual user behavior

Seamless integration within Myra Application Security

Deep Bot Management 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:

Hyperscale WAF
Attackers target vulnerabilities in web applications to infiltrate vulnerable systems and manipulate, steal or delete sensitive data. The Myra Hyperscale Web Application Firewall (WAF) blocks malicious requests before they reach your servers.

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.

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.

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.

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.

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.

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.

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).

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.

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