MyraSecurity: Deutscher Schutz für digitale Angriffe

Category: Online-Marketing
geschrieben von Tobias Hager | 6. Februar 2026

MyraSecurity: Deutscher Schutz für digitale

Angriffe – Wie ein deutsches Unternehmen zur Cyber-Wall gegen DDoS, Botnetze und Co. wird

Deutsche Ingenieurskunst trifft auf digitale Selbstverteidigung: Während halb Europa noch glaubt, mit einem simplen SSL-Zertifikat sei die Webwelt sicher, baut MyraSecurity längst an der High-End-Firewall für eine digitale Zukunft, in der Angriffe nicht die Ausnahme, sondern der Normalzustand sind. Wenn du wissen willst, warum Myra nicht nur "Made in Germany" auf die Fahne schreibt, sondern auch technisch alles plattmacht, was zwischen deinem Server und einem Botnetz steht – lies weiter.

- Was MyraSecurity eigentlich ist – und warum der deutsche Standort mehr als ein Marketing-Gimmick ist
- Wie Myras DDoS-Schutz auf Layer 3 bis 7 funktioniert – und warum das entscheidend ist
- Welche Rolle echte Rechenzentren in Deutschland für Datenschutz, DSGVO und Performance spielen
- Warum Cloud-Security „von der Stange" heute niemanden mehr schützt
- Wie Myra Bot-Traffic erkennt und eliminiert – bevor er Schaden anrichtet
- Worin sich Myra von US-Anbietern wie Cloudflare, Akamai oder Imperva unterscheidet
- Welche Tools, APIs und Schnittstellen Myra für DevOps und SecOps-Teams bereitstellt
- Wie du mit Myra deine Webanwendungen, APIs, DNS und Infrastruktur absicherst
- Warum "Zero Trust" und "Secure by Design" bei Myra nicht nur Buzzwords sind

Was ist MyraSecurity? Deutscher Anbieter für Cloud-basierte IT-Security

MyraSecurity ist ein deutscher Anbieter für Managed Security Services, spezialisiert auf Schutzmaßnahmen gegen DDoS-Angriffe, Web Application Security und sicheres DNS-Hosting. Das Unternehmen betreibt eigene Hochsicherheitsrechenzentren ausschließlich in Deutschland – und erfüllt damit nicht nur die strengen Anforderungen der DSGVO, sondern auch die

Vorgaben des BSI (Bundesamt für Sicherheit in der Informationstechnik). Klingt trocken? Ist aber ein echter Gamechanger im Security-Markt, der nach wie vor von US-Anbietern dominiert wird.

Im Gegensatz zu vielen globalen Anbietern, die ihre Infrastruktur über ein weltweites CDN verteilen, setzt Myra auf physisch getrennte, redundante Rechenzentren mit vollständiger Kontrolle über alle Datenflüsse. Kein Data-Sharing, kein Cloud-Act, keine rechtlichen Hintertüren für ausländische Behörden. Für Unternehmen aus kritischen Sektoren wie Finanzen, Gesundheit oder öffentlicher Verwaltung ist das kein nice-to-have, sondern eine regulatorische Notwendigkeit.

MyraSecurity positioniert sich als „Security-as-a-Service"-Plattform, die sich nicht auf einzelne Tools verlässt, sondern eine ganzheitliche Sicherheitsarchitektur bietet: von DDoS-Mitigation über Web Application Firewall (WAF) bis zu DNS-Security, Secure CDN und API-Schutz. Und das Ganze läuft nicht nur performant, sondern auch auditierbar – was in Zeiten von Compliance, ISO 27001 und BSI-Grundschutz kein unwichtiger Faktor ist.

Die Zielgruppe? Unternehmen, die ihre digitale Infrastruktur ernst meinen. Also nicht der Hobby-Shop mit WordPress auf Shared Hosting – sondern große Player mit komplexer Architektur, gesetzlichen Anforderungen und echtem Risikopotenzial. Myra ist kein Baukasten. Myra ist ein Sicherheitskonzept auf Enterprise-Level.

DDoS-Schutz auf Layer 3–7: Warum Myra nicht einfach nur Pakete filtert

DDoS ist nicht gleich DDoS. Während viele Anbieter sich darauf beschränken, eingehenden Traffic nach einfachen Regeln zu blockieren – Stichwort Rate Limiting oder IP-Blocking –, geht Myra deutlich weiter. Der Schutz greift auf allen relevanten Netzwerk- und Anwendungsebenen (OSI Layer 3 bis 7) und kombiniert heuristische Analysen mit Realtime-Traffic-Inspection. Das bedeutet: Es wird nicht nur geschaut, ob eine IP-Adresse verdächtig ist – sondern ob das Verhalten des Clients überhaupt mit menschlicher Nutzung übereinstimmt.

Layer-3/4-Schutz kümmert sich um volumetrische Attacken wie UDP-Floods, SYN-Floods oder ICMP-Angriffe. Diese Angriffe zielen auf die Bandbreite und Ressourcen deines Netzwerks – und werden von Myra direkt am Rande des Netzes (Edge) erkannt und eliminiert, bevor sie deinen Server überhaupt erreichen. Das funktioniert durch Anycast-Routing, Traffic-Shaping, Blackholing und Rate-Based Filtering.

Layer-7-Angriffe sind perfider. Sie sehen aus wie legitime HTTP-Requests, sind aber in Wahrheit automatisierte Angriffe, oft über Botnets orchestriert. Myra analysiert hier HTTP-Header, Request-Frequenzen, Session-Verhalten und

Payloads in Echtzeit – und nutzt Machine-Learning-Modelle zur Anomaliedetektion. Wer zu schnell klickt, zu regelmäßig anfragt oder verdächtige User-Agents nutzt, landet in der Quarantäne – oder wird direkt geblockt.

Besonders wichtig: Myra unterscheidet zwischen Bad Bots und Good Bots. Crawler wie Googlebot oder BingBot erhalten weiterhin Zugriff, während Scraper, Credential Stuffers oder Layer-7-Flooder rausfliegen. Das Ganze läuft automatisiert, skalierbar und ohne dass du dich in irgendwelche .htaccess-Dateien reinfummeln musst.

Web Application Firewall, Bot-Management & API-Security mit Myra

Die Web Application Firewall (WAF) von Myra ist kein Standard-Baukasten mit OWASP Top 10-Regeln. Sie analysiert den Traffic auf Session-Ebene, erkennt Angriffsvektoren wie SQL-Injections, Cross-Site-Scripting (XSS), Directory Traversals oder XML External Entity Attacks (XXE) – und wehrt sie in Echtzeit ab. Dabei greift sie auf Signaturdatenbanken, Verhaltensanalysen und dynamische Regeln zurück, die kontinuierlich aktualisiert werden.

Das Bot-Management von Myra geht über einfache IP-Blocklisten hinaus. Es nutzt Device Fingerprinting, Behavioral Analysis und JavaScript Challenges, um menschliche Besucher von Bots zu unterscheiden. Zusätzlich kannst du feingranulare Regeln definieren: etwa, dass bestimmte APIs nur mit gültigem Token oder aus definierten IP-Ranges aufrufbar sind. Das senkt nicht nur die Angriffsfläche, sondern schützt auch deine Serverlast.

APIs sind heute das Rückgrat moderner Webanwendungen – aber auch bevorzugtes Ziel für Angreifer. Myra bietet hier spezialisierte Schutzmechanismen: API Rate Limiting, Schema Validation, JWT-Handling, OAuth2-Integration und umfassendes Logging. Jede einzelne Anfrage kann geprüft, validiert und protokolliert werden. Ideal für Unternehmen, die RESTful APIs oder GraphQL-Schnittstellen betreiben – und endlich aufhören wollen, Sicherheitslücken mit selbstgebauten Middleware-Flickenteppichen zu kitten.

Übrigens: Alle Regeln und Metriken sind über Dashboards und APIs zugänglich – für DevOps, SOC-Teams und externe Audits gleichermaßen. Wer will, kann Alerts per Webhook, E-Mail oder SIEM-System erhalten – inklusive vollständiger Logdaten.

Rechenzentren in Deutschland:

DSGVO, BSI und digitale Souveränität

Myra betreibt alle seine Dienste in deutschen Rechenzentren – zertifiziert nach ISO 27001, BSI C5 und PCI DSS. Das bedeutet: Keine Daten verlassen das Land, keine Drittstaaten-Zugriffe, keine Cloud-Act-Schlupflöcher. Für Unternehmen, die auf DSGVO, KRITIS-Verordnung oder branchenspezifische Regulatorik achten müssen, ist das ein massives Plus.

Im Gegensatz zu Anbietern wie Cloudflare oder Google Cloud setzt Myra nicht auf globale Distribution mit regionalen POPs (Points of Presence), sondern auf kontrollierte Infrastruktur mit redundanten Standorten in Deutschland. Das mag im ersten Moment weniger „global“ wirken – ist aber in Sachen Datenschutz, Auditierbarkeit und Rechtssicherheit ein echter Vorteil. Vor allem dann, wenn du mit personenbezogenen Daten arbeitest.

Auch die Anbindung ist High-End: Myra ist direkt mit den größten Internetknotenpunkten Deutschlands verbunden (DE-CIX, ECIX) und bietet so niedrige Latenzen und hohe Bandbreiten – ohne den Umweg über ausländische Netze. Das führt nicht nur zu besserer Performance, sondern auch zu mehr Kontrolle über Routing, DDoS-Abwehr und Traffic-Inspektion.

Kurz gesagt: Wer Wert auf digitale Souveränität legt, bekommt hier eine Lösung, die wirklich “Made in Germany” ist – nicht nur im Marketing, sondern in Code, Hardware und Betrieb.

Worin sich Myra von Cloudflare, Akamai und Co. unterscheidet

Cloudflare, Akamai, Fastly – die üblichen Verdächtigen im Bereich Cloud-Security sind technisch stark, aber nicht zwangsläufig datenschutzkonform. Viele von ihnen unterliegen dem US Cloud Act, was bedeutet, dass US-Behörden unter bestimmten Umständen Zugriff auf deine Daten erhalten können – auch wenn sie in Europa gespeichert sind. Für Banken, Versicherungen oder öffentliche Einrichtungen ist das ein KO-Kriterium.

Myra hat sich bewusst gegen diese globale Struktur entschieden – und bietet stattdessen eine kontrollierte, hochsichere Infrastruktur innerhalb Deutschlands an. Gleichzeitig liefert Myra viele der gleichen Features – und in manchen Fällen sogar mehr: granularere WAF-Regeln, bessere Audit-Optionen, vollständige API-Kontrolle, individuelles Incident-Response-Management und 24/7-Support durch echte Menschen statt KI-Chatbots mit Copy-Paste-Antworten.

Ein weiterer Unterschied: Myra bietet keine Freemium-Modelle oder „gratis

CDN“ an, wie es bei Cloudflare der Fall ist. Das klingt im ersten Moment nach Nachteil – ist aber in Wahrheit ein Feature. Denn kostenlose Dienste finanzieren sich durch Datenverwertung, Upselling oder eingeschränkte Funktionalität für Nicht-Zahler. Bei Myra gibt es klare Verträge, fest definierte SLAs und keine versteckten Datenflüsse.

Kurz gesagt: Wer maximale Performance, volle Datenschutzkonformität und echte technische Tiefe will, findet bei Myra eine Lösung, die kompromisslos auf Sicherheit, Transparenz und Kontrolle setzt – made in Germany, ohne Kompromisse.

Fazit: MyraSecurity ist mehr als ein deutsches Cloud-Security-Tool

MyraSecurity ist keine Light-Version eines US-Konzerns. Es ist ein eigenständiger, hochspezialisierter Anbieter für Cloud-basierte IT-Sicherheit – mit Fokus auf DDoS-Mitigation, Web Application Security und digitale Souveränität. Wer heute noch glaubt, ein bisschen HTTPS und Firewall auf dem Server reichen aus, um Web-Anwendungen zu schützen, lebt im digitalen Mittelalter. Angriffe sind Dauerzustand. Schutz muss Standard sein.

Mit Myra bekommst du kein Security-Gadget, sondern ein skalierbares Sicherheitskonzept, das sowohl technisch als auch regulatorisch auf dem neuesten Stand ist – und dabei deutsche Standards in Sachen Datenschutz, Infrastruktur und Support setzt. Für Unternehmen, die ihre digitale Infrastruktur nicht nur irgendwie sichern, sondern strategisch absichern wollen, ist Myra der Partner, den du brauchst. Schluss mit Security-Theater. Zeit für echte Verteidigung.