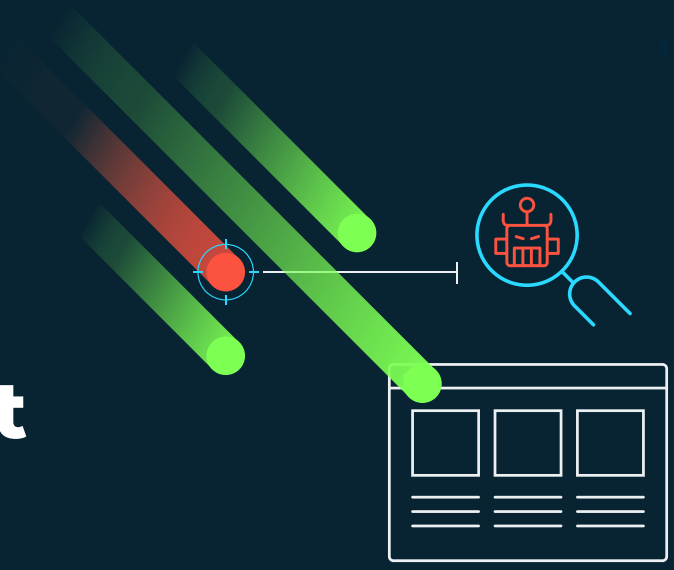
MYRA



PRODUCT SHEET

Myra Deep Bot Management

Schützen Sie Ihre Webapplikationen vor unerwünschten Zugriffen und schädlichen Bots. Myra erstellt für alle anfragenden Bots einen eindeutigen Fingerprint und erkennt sie anhand dessen schnell und zuverlässig wieder. So können Sie auf jede Anfrage optimal reagieren, automatisierte Zugriffe zielgenau steuern und die Performance Ihrer Website verbessern.

Etwa die Hälfte aller Website-Zugriffe entfällt heute auf autonom agierende Bots, rund 20 Prozent gelten als potenziell gefährlich. Bösartige Bots scannen Webplattformen nach ausnutzbaren Schwachstellen, kopieren Inhalte, blockieren Warenkörbe oder versuchen, Nutzerkonten zu kompromittieren. Zusätzlich beeinträchtigen Anfragen von Suchmaschinen, Scrapern, Crawlern oder anderen automatisierten Systemen die Website-Performance, was sich negativ auf das Nutzererlebnis und somit auf Ihr Geschäft auswirken kann. Das Myra Deep Bot Management analysiert alle eingehenden Anfragen und blockiert unerwünschte Zugriffe.

- **Passives Fingerprinting**
  Myra erkennt und klassifiziert eingesetzte Bot-Software anhand eindeutiger Fingerprints – unabhängig von IPs, ASN und User Agent.
- **Automation Tool Detection**
  Automatisierungstools wie Selenium oder PhantomJS erkennt Myra zuverlässig.
- **Behavioral Analytics**
  Mittels Verhaltensanalyse identifiziert Myra unübliche Zugriffsmuster automatisch.
- **Alternate Origin**
  Bei Bedarf leitet Myra Anfragen zum Schutz der Haupt-infrastruktur auf alternative Origin-Server weiter.
- **Schnelle und einfache Integration**
  Das Myra Deep Bot Management erfordert keine zusätzliche Hard- oder Software.

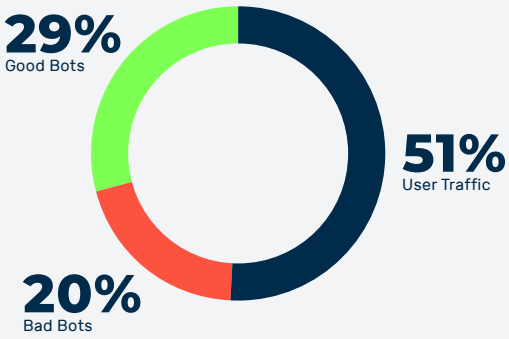
WARUM MYRA SECURITY?

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.

Nur die Hälfte des Website-Traffics wird von Menschen erzeugt



So schützt das Myra Deep Bot Management Ihr Business

Myra unterteilt, klassifiziert und analysiert alle eingehenden Anfragen. Basierend auf dem Ergebnis der Analyse wird für jeden Request die passende Reaktion (Block, CAPTCHA, Log, Pass) ausgeliefert. Unerwünschte oder schädliche Anfragen verwirft oder blockiert Myra, noch bevor sie Ihre Server erreichen. False Positives werden dabei mit dem jeweils mildesten effektiven Mittel verhindert, z.B. Human Interaction Challenges. Gutartigen Bots wie Suchmaschinen können Sie per Rate Limiting eine begrenzte Zahl an Anfragen pro Zeiteinheit erlauben, damit die davon verursachte Traffic-Last gering und die Performance Ihrer Website konstant hoch bleibt.

Schnelle und zuverlässige Bot-Erkennung anhand eindeutiger Fingerprints

Bots greifen mit unterschiedlichen IP-Adressen und aus unterschiedlichen Netzwerken auf Webseiten zu. Die automatisierten Programme geben vor, ein normaler Browser zu sein und fälschen weitere Informationen wie ASN oder Geräte-ID, um den Anschein regulärer Nutzung zu erwecken. Weil die automatisierten Zugriffe verteilt erfolgen, ist auf den ersten Blick kein Zusammenhang zwischen ihnen zu erkennen. Genau diesen Zusammenhang stellt das Myra Deep Bot Management mit Hilfe des passiven Fingerprinting für Sie her: Bei jedem Zugriff auf die Webseite erzeugt Myra aus über 50 Attributen des Zugriffs einen Fingerprint zur eindeutigen Identifikation der verwendeten Software. Sobald der Fingerprint eines Bots vorliegt, wird dieser beim nächsten Zugriff sofort wiedererkannt. Unerwünschte Bot-Anfragen können somit eindeutig identifiziert, geblockt oder anderweitig kontrolliert bzw. umgeleitet werden.

Myra nutzt mehr als 50 Attribute zur Identifikation von Bots, u. a.:

Diese Bot-basierten Attacken bedrohen Ihr Business

Botnetz-basierte Überlastungsangriffe (Denial of Service)
Per Botnetz senden Angreifer eine Flut automatisierter Anfragen an Ihre Webserver, um diesen zu überlasten und die darauf gehosteten Seiten oder Dienste lahmzulegen.

Hype Sales Bots
Durch automatisierte Bot-Anfragen sichern sich Betrüger begehrte Waren und verkaufen sie anschließend mit hohem Gewinn weiter, was sich negativ auf Ihre Kundenbeziehung auswirkt.

Web Scraping
Bots kopieren in Sekundenschnelle einzelne Seiteninhalte oder ganze Websites. Kriminelle nutzen eine solche Kopie der Originalseite, um per Phishing Anmeldedaten abzugreifen.

Cart Abandonment/Inventory Hoarding
Bots füllen Warenkörbe, ohne den Kaufprozess abzuschließen. Das ist geschäftsschädigend für Ihren Shop, weil reguläre Kund:innen die Artikel temporär nicht mehr kaufen können.

Klickbetrug
Angreifer setzen Bots dazu ein, auf Websites enthaltene Werbeanzeigen oder Affiliate-Links automatisiert anzuklicken, um auf Kosten der Werbetreibenden Einnahmen zu generieren.

Account Creation & Takeover
Bots erstellen massenhaft gefälschte Nutzerkonten oder infiltrieren bestehende Accounts, die Kriminelle anschließend für Angriffe oder Betrugsversuche missbrauchen.

Credential Stuffing
Bots können in kürzester Zeit massenhaft Nutzer/Passwort-Kombinationen testen. Treffer zu aktiven Accounts werden anschließend verkauft oder für weitere Attacken genutzt.

Skewing
Durch Bot-basierte Anfragen manipulieren Angreifer gezielt Web-Analysedaten, um Sie zu falschen strategischen Entscheidungen zu verleiten und Ihnen zu schaden.

Formular-Spam
Über Kontaktformulare bombardieren Bots Ihr Unternehmen mit Botschaften. Diese Phishing-Methode dient Kriminellen häufig als Ausgangspunkt für weiterführende Angriffe.

Content Scraping
In Sekundenschnelle kopieren Bots Produktbeschreibungen, Preise oder ganze Websites. Die ungefragt kopierten Inhalte nutzen Angreifer anschließend für eigene Websites oder zum Erstellen von Phishing-Seiten.

Nutzen Sie jetzt die Vorteile des Myra Deep Bot Management

Eingehende Anfragen analysieren

- Schutz von Applikationen und APIs vor schädlichen Bots zur Vermeidung von Umsatzeinbußen, Datendiebstahl und Kontenübernahme
- Bessere Website-Performance für menschliche User und gutartige Bots
- Höhere Kundenzufriedenheit
- Flexibles Management von Suchmaschinen-Bots mit Uplift des SEO-Scorings

Unerwünschte Anfragen blockieren

- Schutz vor Bot-basierten Angriffen und damit verstärkte IT-Security
- Sicherheit vor schädlichen Anfragen, z.B. für Klickbetrug, Scraping und Price Grabbing
- Verringerte Server-Kosten durch Herausfiltern von unerwünschtem Bot-Traffic
- Transparenz hinsichtlich des Traffics und des tatsächlichen Nutzerverhaltens

Nahtlose Integration innerhalb der Myra Application Security

Als Security-as-a-Service-Lösung erfordert der Betrieb des Myra Deep Bot Management keine zusätzliche Software oder Hardware. Die Funktionalität ist innerhalb der Myra Application Security nach Ihren individuellen Bedürfnissen erweiterbar. Alle Lösungen arbeiten nahtlos zusammen 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.

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.

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.

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.

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.

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.

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.

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.

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