AI MANAGEMENT DASHBOARD

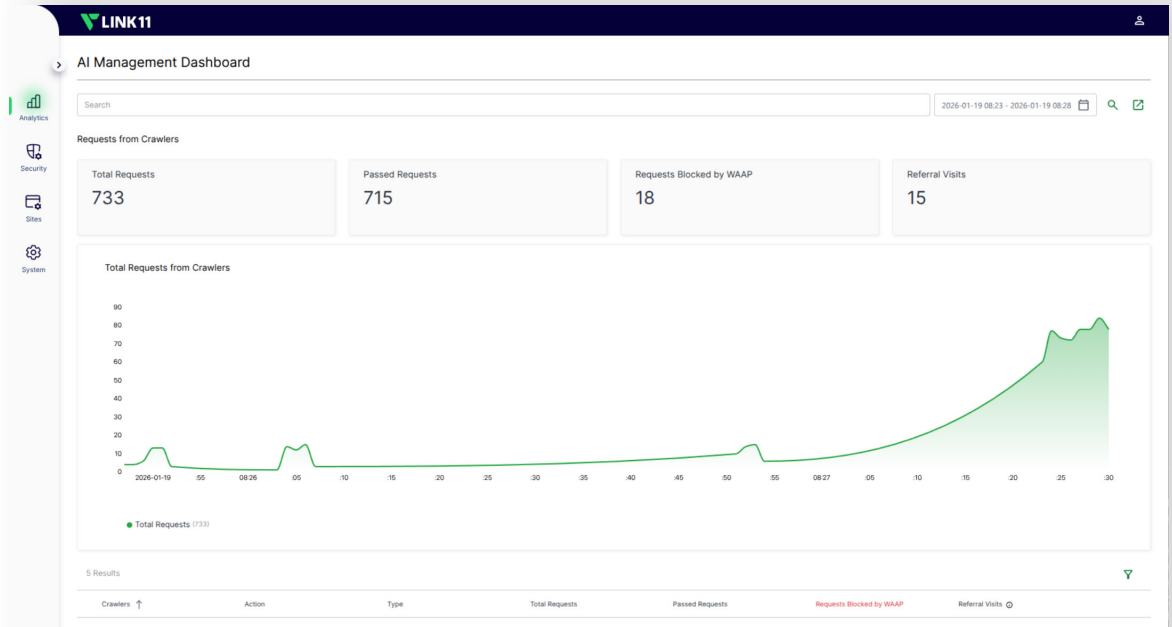
Sicherheit, Steuerung und Analyse von KI-Datenverkehr mit forensischen Erkenntnissen

KI-Crawler skalieren rasant, werden schwerer zu identifizieren und sind zunehmend in der Lage, sensible Inhalte in bemerkenswerter Geschwindigkeit zu extrahieren. Die wachsende Unsicherheit darüber, wer auf Daten zugreift und wie diese genutzt werden, darf kein ernsthaftes operatives Risiko und keine Gefahr für geistiges Eigentum werden. Sicherheitsteams benötigen deshalb eine spezielle Lösung, um KI-Aktivitäten zu sehen, zu steuern und zu kontrollieren.

Das AI Management Dashboard ermöglicht Sicherheits- und Web-Teams, KI-Crawler-Aktivitäten über alle geschützten Anwendungen hinweg vollständig zu verstehen und zu steuern. Mit klarer Transparenz, referral-basierten Einblicken und präziser Richtlinienkontrolle.

Mit dem AI Management Dashboard können Sie:

- Sofort erkennen, welcher Crawler (z. B. ChatGPT, Gemini, Claude oder Perplexity) auf Ihre Website zugreift.
- Einfach unterscheiden zwischen Suchbots, LLM-Trainingsbots und KI-Assistenten.
- Trends frühzeitig erkennen, indem Sie Fragen beantworten wie: „Skaliert ein bestimmter Crawler seine Anfragen plötzlich hoch?“



Die wichtigsten Vorteile

Verbesserte Transparenz über KI-Aktivitäten

Gewinnen Sie detaillierte Einblicke in den KI-Datenverkehr mit klarer Kategorisierung nach KI-Tool und Crawler-Typ. KI-Aktivitäten werden sauber vom allgemeinen Bot-Rauschen getrennt und als eigenständige Kategorie dargestellt, anstatt in das traditionelle Bot-Management integriert zu werden. So verstehen Sie relevante Informationen schneller und können entsprechend handeln.

Granulare Kontrolle für verbesserte Sicherheitslage

Verwalten Sie den KI-Zugriff mit Crawler-genauer Präzision durch Monitor-, Zulassen- oder Blockieren-Aktionen auf bestimmte Crawler-Kategorien. Dank detaillierter Steuerungsmöglichkeiten können Richtlinien direkt auf einzelne Crawler angewendet werden. Dadurch wird die Verantwortlichkeit gewährleistet, und pauschale, allgemeine Bot-Regeln werden vermieden.

Datenbasierter Einfluss auf Sicherheitsentscheidungen

Vereinfachen Sie Audits und Governance mit Belegen, die es Prüfern und Ermittlern ermöglichen, genau nachzuvollziehen, was bei jeder KI-bezogenen Aktivität vorgefallen ist. Gewinnen Sie tiefere Einblicke und unterscheiden Sie, wer Ihre Daten liest („Scraping“) und wer Nutzer auf Ihre Website leitet („Referrals“).

Über Link11

Link11 bietet Cybersicherheitslösungen für Unternehmen aller Art. Als führender Anbieter von Cybersicherheitslösungen schützen wir Kunden weltweit vor sich ständig weiterentwickelnden Bedrohungen durch sorgfältige Detailgenauigkeit und frühzeitige Integration modernster Methoden.

Wir bieten umfassende Lösungen für Netzwerksicherheit, Anwendungs- und API-Sicherheit sowie Application Performance. Unsere Plattform schützt Unternehmen branchenübergreifend – von vollständigem Netzwerk-DDoS-Schutz bis hin zu einer umfassenden WAAP-Lösung. Dazu gehören Web Application Firewall, Web-DDoS-Schutz, Bot-Management (inkl. ATO), API-Sicherheit sowie ein sicheres CDN und DNS.

PCI DSS COMPLIANT · ISO 27001 Information Security Management · Datenschutz Grundverordnung DSGVO Certified · C5 Typ II BSI C5 CLOUD SECURITY

LINK11

Link11 GmbH | +49 69 5800492677 | sales@link11.com | www.link11.com