Bots, Sicherheit & Performance: Neue Herausforderungen im E-Commerce-Betrieb

Wie automatisierter Traffic Umsatz, Infrastruktur & Kundenerlebnis beeinflusst

Heute ist jeder zweite Besucher kein Mensch.
Die Frage ist nicht ob du Bots hast – sondern ob du weißt, welche.

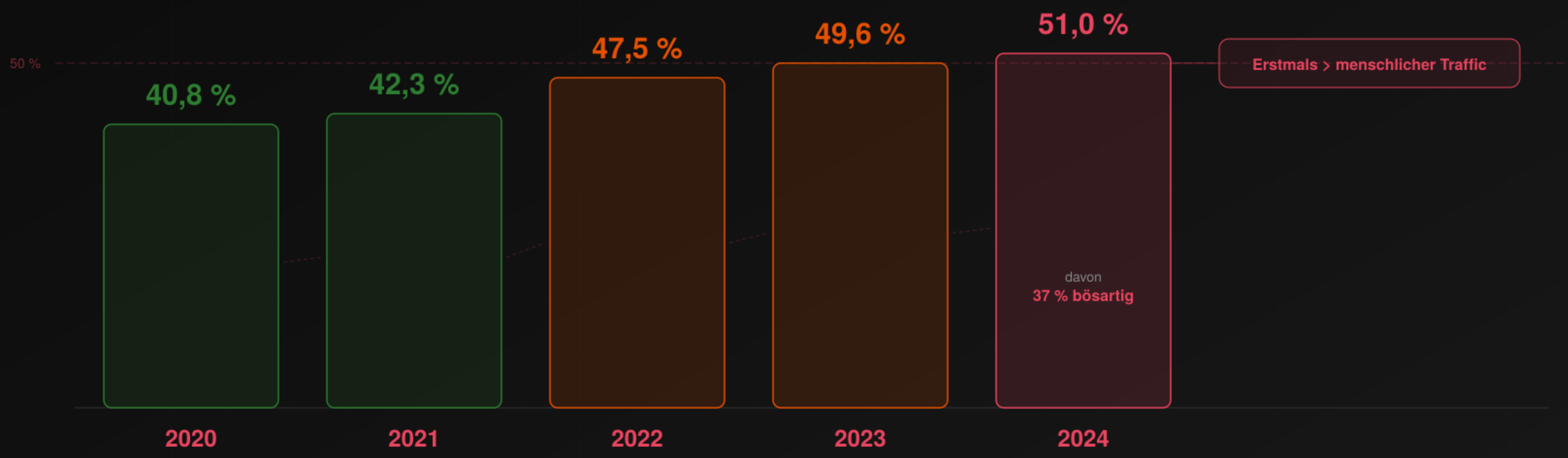
Davon sind ~37 % automated threats – der Rest sind Services, die deinen Shop am Laufen halten.

Sie gefährden Marge, Conversion Rate und Warenverfügbarkeit direkt.

Quelle: Imperva Bad Bot Report 2024

Die letzten 5-(Bot)-Jahre

Bot-Zugriffe – von Webcrawlern über Scraper bis hin zu bösartigen Bots – verzeichnen einen deutlichen Anstieg



Im E-Commerce liegt der Anteil advanced bad bots nochmal deutlich höher:
~25 % allein schwer erkennbare Bots (Imperva 2024, Retail-Segment). EMEA hat den höchsten Anteil an evasive Bots.

Quelle: Imperva Bad Bot Report 2024

Die nächsten 5 Jahre...

2025
53,5 %

Der Bot-Traffic steigt auf 53,5 % bis 60,1 %
wobei der Anteil bösartiger Bots
von etwa 40 auf 48 % zunimmt

2028
60,1 %

Der Bot-Traffic erreicht 62,0 %
50 % entfallen auf bösartige Bots

2029
62,0 %

Mehr als 6 von 10 Besuchern sind Bots.
Jeder Zweite davon bösartig.

Quelle: Eigene Projektion basierend auf Imperva-Trend 2020–2024

Sind Bots gleich Bots?

Natürlich nicht.

Im E-Commerce treffen wir auf hilfreiche Bots: Suchmaschinen, Monitoring, Payment-Integrationen und auf schädliche Bots, die Daten abgreifen, Preise scrapen oder Checkouts kapern

Der Unterschied liegt nicht im User-Agent, sondern im Verhalten.

🤖 Good Bots

Diese Bots sind nützlich. Sie unterstützen, schützen oder machen Systeme effizienter.
Sie handeln im Einklang mit deiner Plattform und deinem Business-Ziel.

Suchmaschinen-Bots

Indexieren Inhalte und machen Shops auffindbar.

Googlebot, Bingbot, Yandex

Monitoring-Bots

Prüfen Verfügbarkeit, Ladezeiten und Funktionalität.

Uptime, Synthetics, Pingdom

Security-Bots

Erkennen Schwachstellen oder blockieren Angriffe.

Vulnerability Scanner, WAF Bots

Accessibility-Bots

Helfen Nutzer:innen mit Einschränkungen beim Zugriff.

Screen Reader Bots, Assistive Tech

Customer-Bots

Beantworten Support-Anfragen oder automatisieren Workflows.

Chatbots, Ticket-Automation

Payment & Partner

Verarbeiten Zahlungs-Callbacks, Feeds und Affiliate-Tracking.

Blockierst du sie, stockt dein Umsatz.

Diese Bots arbeiten **mit** deiner Infrastruktur. Wer sie versehentlich blockt, verliert Sichtbarkeit, Umsatz oder Funktionalität.

Bad Bots

Sie sind unsichtbar bis du sie in Umsatz, Serverlast oder Conversion merkst.

Credential-Stuffing-Bots

Testen gestohlene Logins
auf deinem Shop.

Leaked DBs, Combo Lists, Brute Force

Scalper-Bots

Kaufen limitierte Produkte
in Sekunden leer.

Sneaker Drops, Limited Editions, Tickets

Preis-Scraper

Crawlen Produktdaten und
senken deine Margen.

Wettbewerber, Preisvergleicher

Fake-Traffic-Bots

Verzerren Analytics und verursachen
unnötige Serverkosten.

Click Fraud, Impression Fraud, Ad Fraud

Fraud-Bots

Lösen Gutscheine aus, fälschen
Reviews oder erzeugen Spam.

Coupon Abuse, Fake Reviews, Spam

Inventory Holding

Legen Produkte in Warenkörbe und
blockieren Verfügbarkeit.

Bes. bei Flash Sales und Limited Editions

Account Takeover (ATO)

Übernehmen Kundenkonten, lösen Guthaben ein, ändern Lieferadressen.

Einer der teuersten Angriffsvektoren im E-Commerce.

Credential Stuffing + Session Hijacking + Social Engineering

~25.000 $

Durchschnittskosten pro ATO-Incident

inkl. Chargebacks, Support und Customer Lifetime Value Loss

Wie automatisierter Traffic den E-Commerce direkt trifft

Nicht jeder Besucher ist ein potenzieller Kunde.
Ein wachsender Teil des Traffics stammt von Bots und deren Auswirkungen sind real:
Sie verzerren deine Kennzahlen, treiben Kosten nach oben und fressen Marge, bevor der Kunde überhaupt zur Kasse kommt.

Was Bots im Shop wirklich anrichten

↓ Umsatzverlust

Durch Scalping, Preisfehler oder manipulierte Warenverfügbarkeit.

Direkte P&L-Auswirkung, oft unbemerkt

Conversion Drop

Bots verfälschen Analytics, zerstören A/B-Tests und triggern unnötige Fehlermeldungen.

⚙ Infrastrukturkosten

Automatisierte Anfragen lasten CDN, Caching und Datenbanken aus.

Echte Nutzer warten länger.

☎ Support-Aufwand

Fraud-Cases, Rückbuchungen und riesige Logfiles erhöhen Kosten und senken Effizienz.

SEO-Impact / Crawl-Budget

Aggressive Bots fressen Crawl-Budget. Googlebot bekommt weniger Slots – neue Produkte werden langsamer indexiert.

Analytics-Vergiftung

Wenn 40 % deines Traffics Bots sind, sind alle deine Metriken falsch. Bounce Rate, Funnel, Heatmaps – **du optimierst für Bot-Verhalten.**

Das größte Problem: Du merkst es nicht sofort.

Bot-Schäden akkumulieren sich über Wochen und Monate – in falschen Entscheidungen, überhöhten Kosten und verlorener Marge.

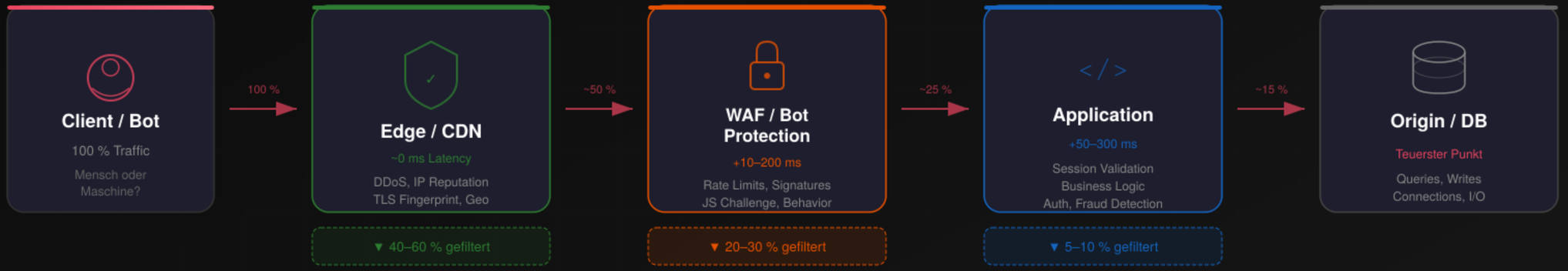
Sicherheit darf keine Bremse sein

E-Commerce-Sicherheit bedeutet nicht, immer mehr Schutzschichten aufzubauen, sondern sie so einzusetzen, dass Kund:innen nichts davon merken.

E-Commerce-Sicherheit bedeutet nicht, immer mehr Schutzschichten aufzubauen, sondern sie so einzusetzen, dass Kund:innen nichts davon merken. *Edge-basierte Bot-Mitigation reduziert Origin-Load um 30–50 %. Sicherheit wird zum Performance-Gewinn, nicht zum Trade-off.*

Wo wird geprüft?

Request-Flow: Jeder Layer weiter innen verzehnfacht die Kosten pro Bot-Request



Der teuerste Bot ist der, den du erst im Checkout erkennst.

Je früher gefiltert wird, desto niedriger die Kosten – und desto besser die Performance für echte Kund:innen.

…und wie Schutze ich meinen Shop jetzt?

Wer erst reagiert, wenn der Schaden sichtbar wird, spielt im falschen Team.

Die Antwort ist nicht ein Tool. Es sind drei Ebenen.

Der richtige Schutz

Drei Ebenen, die zusammenspielen muessen - nicht entweder-oder.

Technische Ebene

Erkennen & Blockieren

Alles, was Angriffe sichtbar und messbar macht:

- WAF / Bot-Protection
- CDN-Regeln & Rate-Limits
- Browser-Fingerprinting
- JS-Challenges & CAPTCHA
- Monitoring & Alerting

Ziel: Automatisierte Angriffe frueh stoppen, bevor sie Ressourcen kosten.

Operative Ebene

Analysieren & Reagieren

Prozesse, die sicherstellen, dass Security und Performance Hand in Hand arbeiten:

- Log-Analyse & Traffic-Auswertung
- False-Positive-Tuning
- Incident Response Playbooks
- Regelmaessige Traffic-Audits
- Bot-Score Kalibrierung

Ziel: Kontrolle behalten und flexibel reagieren - nicht erst beim Ausfall.

Strategische Ebene

Bewerten & Optimieren

Sicherheit als Teil der Business-Strategie:

- Welche Risiken sind geschaeftskritisch?
- Was kostet ein Ausfall pro Stunde?
- Wie messe ich "sicheren Umsatz"?
- ROI von Bot-Protection quantifizieren
- Security-KPIs definieren & reporten

Ziel: Datenbasiert entscheiden - nicht reaktiv, sondern vorausschauend.

Ohne Technik kein Schutz. Ohne Ops kein Ueberblick. Ohne Strategie keine Prioritaet.

...und die AI-Agents?

Diese Generation von Bots ist anders. Sie veraendern die Spielregeln.

Selbstlernend

Sie analysieren deine Seitenstrukturen automatisch. Keine fixen Selectoren oder Skripte mehr noetig.

DOM-Parsing, Layout-Erkennung, Prompt-Injection

Natuerlichsprachlich

AI-Agents verstehen Produktbeschreibungen, Filter und Bewertungen wie ein Mensch. Sie navigieren Shops semantisch.

LLM-gesteuert, kontextbewusst, multimodal

Unbegrenzte Skalierung

Millionen parallele Requests, individuell getarnt. Marginalkosten pro Request nahe Null.

API-Kosten: ~0.001 $/Request vs. deine Serverkosten

Adaptive Tarnung

Wechselnde IPs, Browser-Fingerprints und User-Flows. Sie passen sich deiner Erkennung aktiv an.

Residential Proxies, Canvas Spoofing, Human-like Timing

Automatisierte Entscheidungen

Agents bewerten Preise, Lagerbestaende oder Lieferzeiten selbststaendig und reagieren darauf - ohne menschlichen Input.

Preisvergleich, Checkout-Automation, Arbitrage

Das Problem:

Klassische Bot-Detection basiert auf Regeln. AI-Agents brechen Regeln, die es noch nicht gibt.

AI-Agents sind nicht die Zukunft - sie sind die Gegenwart. Jeder Shop mit oeffentlichen Daten ist ein Ziel.

AI-Agents: Best Practices

Klassische Regeln reichen nicht. Diese Massnahmen adressieren die neue Bedrohungslage.

Behavior-basierte Erkennung

statt IP-Blockierung

Klassische Patterns (IP, UA, Rate) reichen nicht mehr. Maus-Bewegungen, Scroll-Verhalten, Session-Tiefe und Timing analysieren.

Fingerprint-Score + Behavior-Score = Bot-Probability

Traffic-Anomalie-Erkennung

ML-basiert

Baselines fuer Zeit, Frequenz und Interaktionsmuster definieren. Abweichungen automatisch flaggen.

Request-Clustering, Session-Anomalien, Geo-Shifts

WAF/Bot-Systeme trainieren

regelmaessig

Neue Modelle, neue Signaturen. Anbieter wie Cloudflare oder BunnyCDN aktualisieren ihre Modelle laufend.

Managed Rules, ML-Modell-Updates, Custom Rules Review

API-Access & AI-Indexing pruefen

Wer darf was sehen?

robots.txt und ai.txt definieren, welche AI-Crawler deine Daten indexieren duerfen. API-Endpunkte gezielt absichern.

robots.txt, ai.txt, API Rate Limits, Auth-only Endpoints

Security als Teil der Architektur

nicht als nachtraeglicher Patch

Bot-Schutz gehoert in die Infrastruktur-Planung - nicht als Reaktion auf den ersten Vorfall.

Edge-first, Defense-in-Depth, Shift-Left Security

Kernprinzip:

Nicht einzelne Bots blockieren, sondern das System resilient machen.

Adaptive Verteidigung statt statische Regeln.

AI-Agents entwickeln sich schneller als statische Regelwerke. Dein Schutz muss genauso adaptiv sein.

Komm auf den Punkt: Was muss ich machen?

Nicht jeder braucht sofort eine teure Bot-Protection.

Aber jeder sollte verstehen, was im eigenen Traffic wirklich passiert.

Sicherheit ist kein Plugin! Sie beginnt mit Bewusstsein, Daten und klaren Entscheidungen.

Drei Prioritäten – sortiert nach Impact

Verstehen was passiert

Drei Schritte, die jeder Shop-Betreiber sofort umsetzen kann.

1 Analysiere deinen Traffic

Wie viel davon ist wirklich menschlich?

- [x] Logfiles & Access Patterns auswerten
- [x] Time-on-Page & Scroll-Depth pruefen
- [x] Conversion-Verhalten segmentieren
- [x] Bot-Anteil im Analytics identifizieren
- [x] CrUX vs. RUM-Daten vergleichen

Erkenntnis:
30-50 % der Requests sind oft keine echten Nutzer.

Server Logs, GA4 Bot-Filter, CrUX Dashboard

2 Schwachstellen schliessen

Klare technische Basis schaffen:

- [x] CDN-Regeln & Rate-Limits konfigurieren
- [x] Bot-Schutz aktivieren (Smoxy, CrowdSec, BunnyCDN, Cloudflare)
- [x] API-Endpunkte & Formular-Routen absichern
- [x] Security-Header & Logging konfigurieren
- [x] Caching-Strategie ueberpruefen

Prinzip:
Je frueher du filterst, desto guenstiger. Edge > WAF > App.

nginx, Cloudflare Rules, CrowdSec Bouncers, CSP Headers

3 Prozess etablieren

Sicherheit ist kein Projekt, sondern ein Prozess.

- [x] Regelmaessige Traffic-Audits durchfuehren
- [x] Eng mit Hosting, Dev & Marketing arbeiten
- [x] Auf Anomalien reagieren, bevor sie Umsatz kosten
- [x] Bot-Protection KPIs monatlich reviewen
- [x] Incident-Response-Playbook bereithalten

Warum:
Bot-Traffic veraendert sich. Dein Schutz muss mithalten.

Quarterly Audits, Runbooks, Cross-Team Reviews

Geschwindigkeit UND Schutz - beides gehoert zur Conversion.

Perfekte Bot-Detection gibt es nicht. Aber messbar

Das Ziel ist, zu verstehen, wer dein Traffic wirklich ist und deine Systeme so zu bauen, dass sie performant und sicher bleiben. Fang mit Wissen an, dann mit Struktur, dann mit Routine.

Alles beginnt mit dem ersten Request.

Danke fürs Zuhören.

Fragen?