Autonome Cyberabwehr in der AI-Ära

Warum klassische Security-Stacks scheitern – und was jetzt zählt.

KRALOS

Carsten Klein

KI verändert die Bedrohungslandschaft grundlegend

Angreifer nutzen Künstliche Intelligenz, um Angriffe zu automatisieren, zu beschleunigen und präziser zu steuern. Was früher Tage dauerte, geschieht heute in Sekunden und passt sich dynamisch an Abwehrmaßnahmen an.

- **Schneller**
  Angriffe in Echtzeit, ohne menschliche Verzögerung.
- **Präziser**
  Maßgeschneiderte Exploits durch KI-gestützte Analyse
- **Adaptiver**
  Dynamische Umgehung statischer Schutzmechanismen

Die Grenzen klassischer Security-Stacks

Herkömmliche Sicherheitsarchitekturen bestehen aus isolierten Einzellösungen, starren Regelwerken und reaktiven Schutzmechanismen. In den modernen Cloud- und KI-Umgebungen reicht das nicht mehr aus.

Isolierte Tools

Keine integrierte Sichtbarkeit, blinde Flecken im Stack.

Statistische Regeln

Unfähig, sich an neue Angriffsmuster anzupassen.

Nachgelagerte Reaktionen

Schäden entstehen, bevor die Abwehr greifen kann.

KI-gestützte Angriffsmethoden im Detail

Angreifer setzen KI nicht nur zur Automatisierung ein, sie nutzen sie auch, um Schwachstellen zu entdecken, die Verteidigung zu testen und Angriffe zu optimieren.

Hyper-Realistic Phishing

Ki generiert personalisierte Phishing-Mails in Sekunden ohne erkennbare Fehler.

Autonome Bot-Attacken

KI gesteuerte Botnetze koordinieren DDoS-Angriffe adaptiv und schwer abwehrbar.

Zero-Day-Automatisierung

Machine Learning identifiziert und exploitiert Schwachstellen schneller als Patches bereitstehen.

Secure by Design: Das neue Paradigma

Statt Sicherheit nachträglich aufzusetzen, wird sie von Beginn an in die Infrastruktur und Anwendungen integriert. Sicherheit ist kein Add-on, sie ist das Fundament.

Identität

Zero-Trust-Prinzipt als Basis

Infrastruktur

Sicherheit in der Architektur verankert

Anwendung

Secure Coding & automatisierte Tests

Betrieb

Kontinuierliche Überwachung & Response

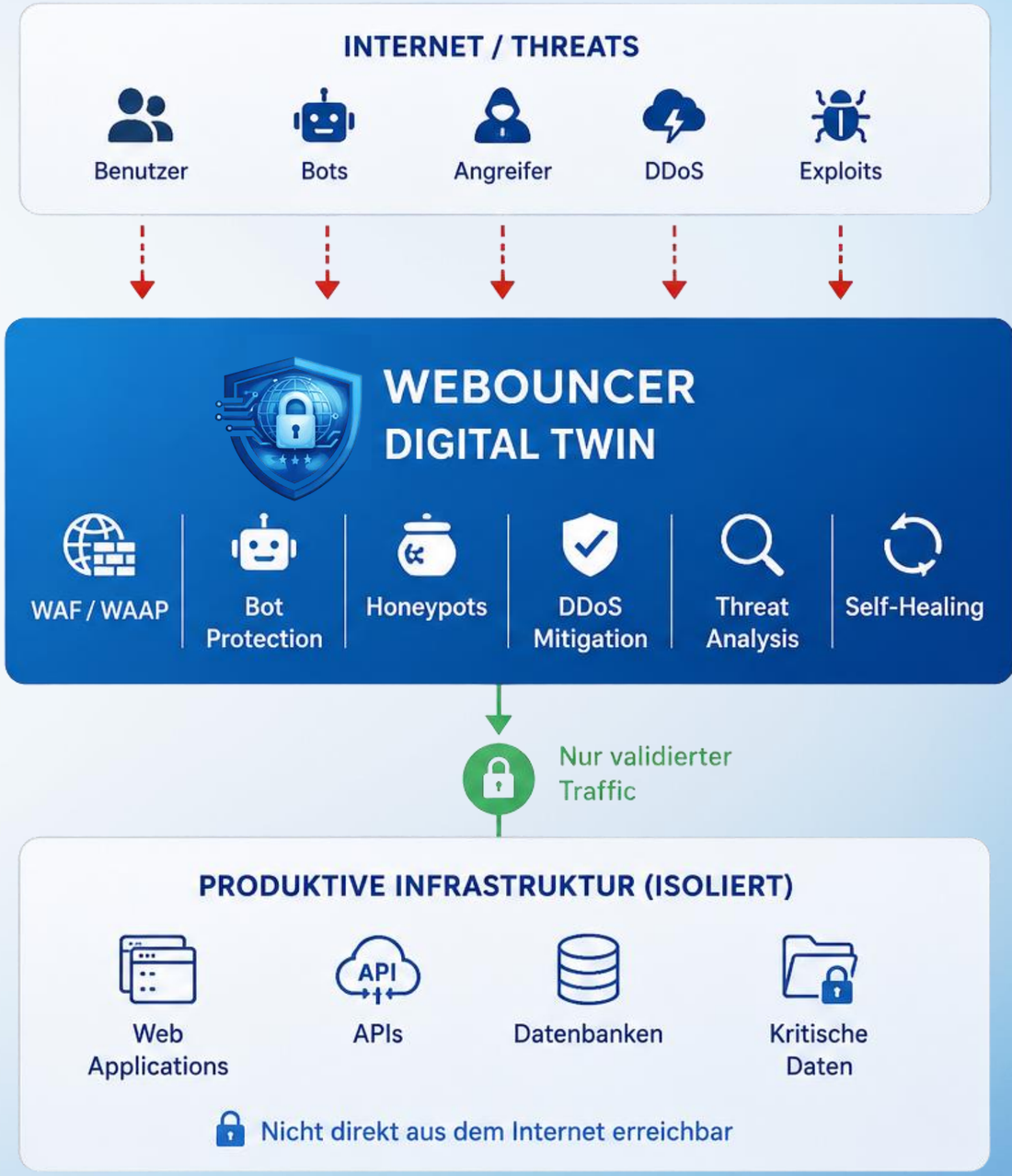
Intelligente Segmentierung & adaptive Schutzmechanismen

Digital Twin Isolation

Anstatt produktive Anwendungen direkt dem Internet auszusetzen, präsentiert WEBOUNCER ausschließlich einen intelligenten Digital Twin. Die eigentliche Infrastruktur bleibt vollständig isoliert und für Angreifer unsichtbar.

Adaptive Autonomous Protection

WEBOUNCER analysiert Angriffe in Echtzeit und aktiviert automatisch Schutzmechanismen wie Bot-Abwehr, Honeypots, Self-Healing, DDoS-Mitigation und Zero-Day-Protection – ohne manuelle Eingriffe.



Digitale Zwillinge & resiliente Systeme WEBOUNCER in Aktion

WEBOUNCER revolutioniert die Cyberabwehr durch eine patentierte Architektur, die Angreifer täuscht und Systeme schützt.

- **Secure-by-Design Schutzarchitektur**
- **Digital-Twin-Technologie**
- **Autonome Cyberabwehr**
- **Reduzierte Angriffsfläche**
- **Patentierte Innovation aus Deutschland**

Konsolidierung komplexer Security-Lanschschaft

Der Trend geht weg von punktuellen Einzellösungen hin zu integrierten Plattformen, die Sichtbarkeit, Automatisierung und Orchestrierung vereinen.

Vorher

20+ isolierte Tools, manuelle Korrelation, hohe Komplexität, viele blinde Flecke

Nachher

Integrierte Plattform, automatisierte Response, einheitliche Policy, vollständige Transparenz

70 %

Weniger Tool-Silos

Durch Plattformkonsolidierung

3 x

Schnellere Response

Durch automatisierte Orchestrierung

40 %

Kosteneinsparung

Im Security-Betrieb durch Integration

Zukunftssicherung Cloud- & Infrastruktursicherheit

WEBOUNCER bietet langfristigen Schutz durch architekturbasierte Sicherheit, nicht durch reaktive Maßnahmen

- **Widerstandsfähig gegen neue Angriffsmethoden**
- **Schutz vor AI-geschützten Angriffen**
- **Unabhängig von immer größeren Security-Stacks**
- **Anpassungsfähig an Cloud-, Hybrid- und On-Premises-Umgebungen**
- **Architektur statt Reaktion**

Bereit für den nächsten Schritt?

Carsten Klein
co-Founder / CEO

KRALOS

Hannoversche Neustadt 54, 31303 Burgdorf

www.kralos.de

+49 5136 8042985

info@kralos.de