

AUTONOMOUS SASE

AI ATTACKS NEED AI-RUN SECURITY.



01

WAS GERADE
PASSIERT

Angriffe laufen jetzt in Maschinengeschwindigkeit.

Angrifer nutzen AI, um Schwachstellen zu finden, Phishing zu schreiben und sich in Minuten durch Netzwerke zu bewegen. Kein Team, das Alerts und Tickets abarbeitet, hält dieses Tempo.

SO SCHNELL SIND ANGRIFFE HEUTE

27 s

schnellster je beobachteter Breakout

29 min

durchschnittlicher Breakout, 65 %
schneller als im Vorjahr

+89 %

mehr Angriffe durch AI-
gestützte Angreifer

Breakout: vom ersten Zugriff bis zur Ausbreitung im Netzwerk. Quelle: CrowdStrike 2026 Global Threat Report.

02

WARUM OPEN
SYSTEMS

DAS ARSENAL IST NICHT DAS PROBLEM.

Jedes Unternehmen hat Firewalls, ZTNA, Secure Web Gateways. Die meisten haben mehr Tools als je zuvor. Und jedes davon wartet noch immer darauf, dass ein Mensch den Alert liest, das Ticket öffnet, die Änderung freigibt. AI-Angriffe warten nicht. **Ein Security-Stack im Menschentempo ist ein Stack, der verliert.**

35

JAHRE
OPERATIVE
ERFAHRUNG

Open Systems stellt als erster Anbieter eine AI-Belegschaft an die Spitze des gesamten SASE-Arsenals - trainiert mit genau dieser Erfahrung, abgesichert durch Engineers, die jede kritische Entscheidung verantworten.



Wir liefern keine AI-Features. Wir stellen eine Belegschaft ein.

Die AI Matrix: spezialisierte Agenten mit je einer Aufgabe. Sie erkennen, entscheiden und handeln in Maschinengeschwindigkeit - innerhalb der Grenzen, die Sie freigeben.



Die Erfahrung, die niemand kaufen kann.

35 Jahre operative Entscheidungen aus Hunderten Unternehmensnetzwerken. Ein Modell kann jeder lizenzieren. Diese Erfahrung nicht.



Kein L1. Kein L2. Keine Warteschlange.

Level-3-Engineers setzen die Guardrails und verantworten jede kritische Entscheidung. Wenn es zählt, entscheidet ein Mensch.



Eine Plattform. Von der Leitung bis zur Policy.

ZTNA · SWG · CASB · Firewall · Threat Protection · E-Mail-Security · NDR · SD-WAN über ein privates globales Backbone.

**Alle anderen verkaufen Ihnen das Arsenal.
Wir betreiben es in AI-Geschwindigkeit.**

03 Nicht ein AI-Agent. Eine ganze AI Matrix - das Herzstück unserer AI-Security.

Ein AI-gesteuerter Angriff, eingedämmt in Minuten.

BEISPIELSZENARIO

T+0	T+30 s	T+90 s	T+2 min	T+3 min
Ar Argus² Erkennt eine AI-Phishing-Welle in 400 Postfächern und isoliert jede Kopie.	He Hermes² Findet den Laptop, der geklickt hat und nun eine unbekannte Domain kontaktiert.	Le Lex² Entwirft eine Policy gegen Domain und Gerät, geprüft gegen alle Regeln.	Lu L3 Lucy¹ + Level-3 Lucy legt Nachweise und Lösung vor. Ein Engineer gibt mit einem Klick frei.	SASE-Plattform An jedem Standort durchgesetzt via ZTNA, SWG und Firewall. Calli ³ dokumentiert.

Nur mit Menschen: Alert-Queue, Triage, Ticket, Eskalation, Change Board. Stunden - während der Angreifer weiterzieht.

AI Matrix + SASE-Plattform: erkannt, eingedämmt und dokumentiert in Minuten. Mit Ihrer Freigabe.

He Hermes²
Traffic & Pfade
Hält jede Applikation auf dem schnellsten, stabilsten Pfad.

Ar Argus²
Web- & E-Mail-Gateway
Fängt Phishing und Web-Bedrohungen ab, bevor sie Ihre Nutzer erreichen.

Le Lex²
Policies & Regeln
Hält Policies sauber und konfliktfrei und erklärt jede Änderung, bevor sie live geht.

Ne Nemesis¹
AI-Red-Team
Findet ausnutzbare Angriffspfade, bevor Angreifer es tun.

At Atlas³
Rollout & Provisionierung
Bringt neue Standorte und Nutzer schneller live, mit weniger manuellen Schritten.

Pr Prometheus³
Vorausschau
Erkennt Ausfälle früh und hält Ihr Netzwerk am Laufen.

Ca Calli³
Reporting & Evidenz
Liefert audit-fähige Reports und Nachweise, automatisch.

Kr Kratos³
AI-Deception
Macht Angreiferaktivität mit intelligenten Ködern zu verlässlichen Alerts.

04 Betriebsmodelle: Ihr Mass an Kontrolle.

Jedes Unternehmen hat eigene Teams, Skills und Compliance-Vorgaben. Sie entscheiden, was Sie selbst betreiben und was AI Matrix und Engineers übernehmen - jederzeit anpassbar, auf derselben Plattform.

Self-serve Platform LIVE
Selbst betreiben.
Vollständiges SASE und SSE, API-first.
Kein Console-Lock-in.

AIOps IM ROLLOUT
Mit unserer AI betreiben.
AI-Agenten übernehmen operative Arbeit innerhalb freigegebener Grenzen.

Mission Control LIVE
Wir betreiben für Sie.
Plattform, AI und Level-3-Engineers, rund um die Uhr. Kein L1. Kein L2. Keine Warteschlange.

05 Vertrauen von Unternehmen, die bleiben.

4,9/5 Gartner Peer Insights
69 Net Promoter Score
98% Jährliche Kundenbindung im Enterprise-Geschäft
Leader The Forrester Wave™: SASE Services, Q3 2026

Realistisch bräuchten wir eher 14 Mitarbeitende im Schichtbetrieb, um die Qualität und Verfügbarkeit zu erreichen, die Open Systems mit seinem globalen 24x7-Support liefert.

Thomas Muth, Vice President Group IT, Kelvion (übersetzt)

06 Über Open Systems

Open Systems ist ein AI-gestützter SASE-Plattformanbieter für sichere Zugriffe und Vernetzung in komplexen Hybrid- und Multi-Cloud-Umgebungen. Die proprietäre Plattform vereint SSE-Funktionen wie ZTNA, SWG, CASB und FWaaS mit SD-WAN, End-to-End-Konnektivität, einheitlichem Policy Management und erweiterten Analysefunktionen in einer integrierten Architektur.

Was würde ein AI-Angreifer in Ihrem Netzwerk finden?

Finden Sie es zuerst heraus, mit dem Nemesis AI Security Check¹:

open-systems.com/security-check →