



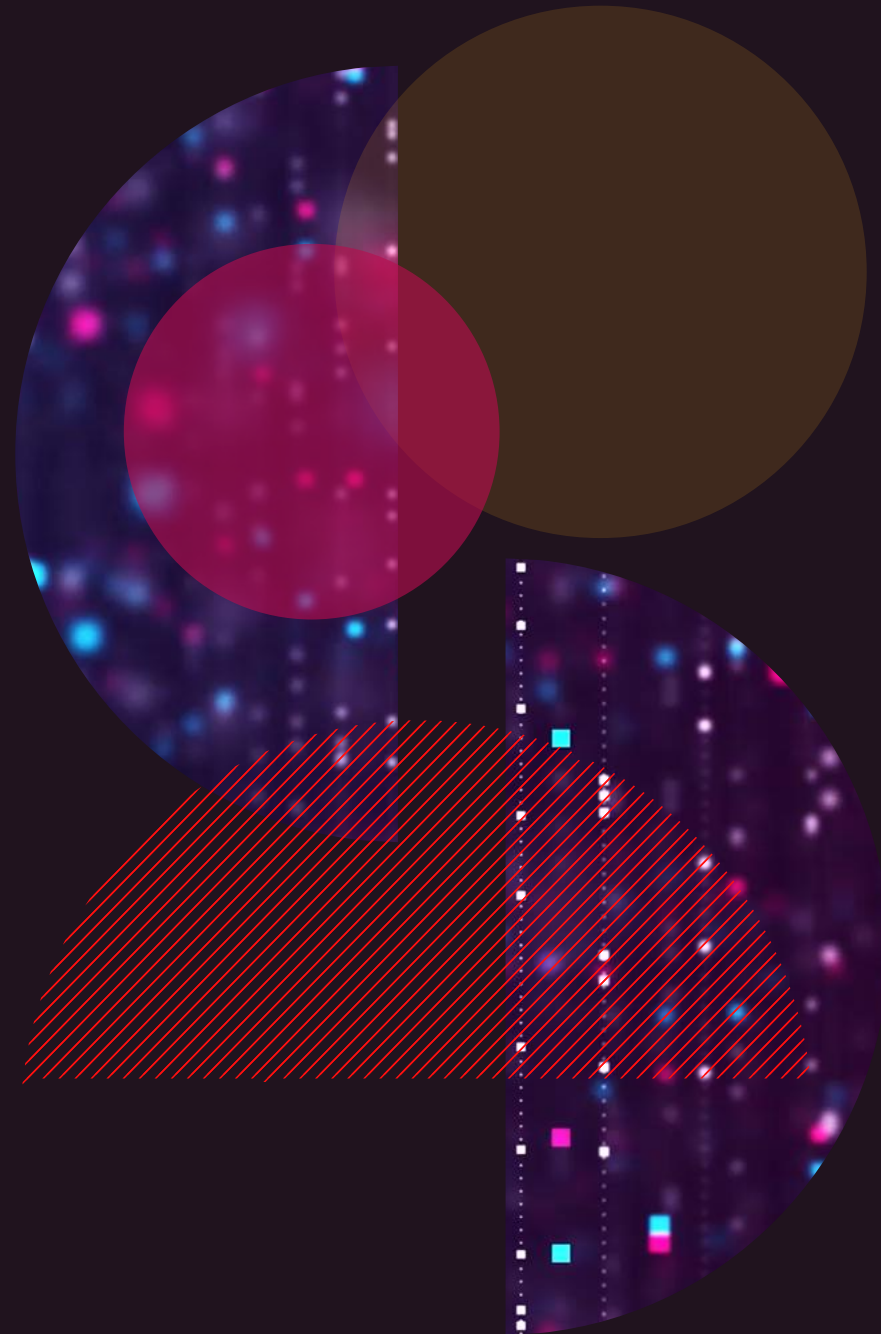
controlware

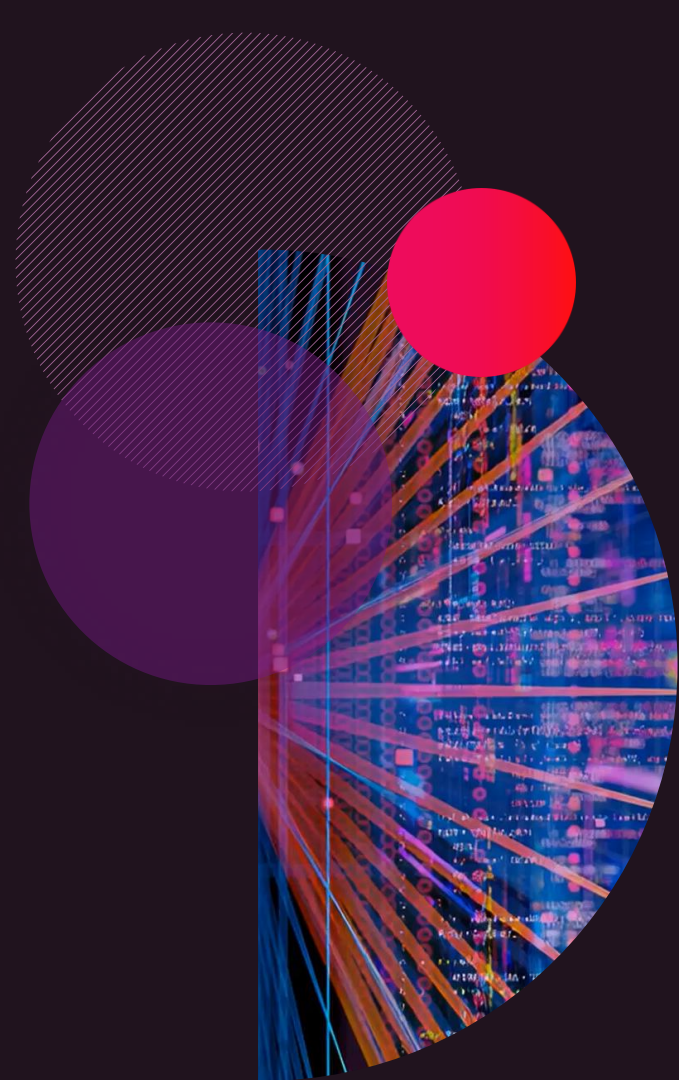
KI denkt schnell, wir denken
sicher.

Kontrolle statt Chaos!

Ulrike Scharf | Solutions Architect

März 2026





Der Schnellste Technologiewechsel In unserem Leben

KI verändert **grundlegend**
die Bedrohungslandschaft

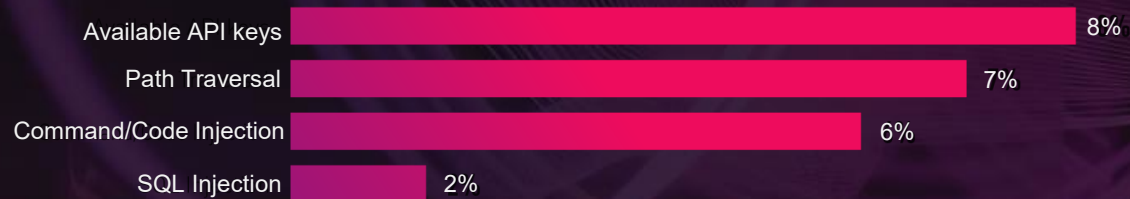


2026 Security Report



KI, von Integration zu Autonomie

- KI vollständig in Angriffe eingebettet, operativ nicht mehr von menschlicher Aktivität zu unterscheiden
- Beginn des Übergangs von der Assistenzrolle zum autonomen Operator
- KI wird zur zentralen Angriffsfläche durch Prompt-Injection, Missbrauch von Agenten und Datenlecks
- Strukturelle Schwachstellen im Model Context Protocol (MCP); Check Point Lakera Daten zeigen Sicherheitslücken in 40 % aller MCPs



Vulnerabilities in MCP Servers - CP Lakera data, Survey of >10K online servers

ANTHROPIC

Disrupting the first reported AI-orchestrated cyber espionage campaign

Full report

November 2025

anthropic.com





Verordnung (EU) 2024/1689

AI Act

Erstes umfassende Gesetz der Europäischen Union zur Regulierung von künstlicher Intelligenz (KI) in allen Mitgliedstaaten

Setzt auf einen risikobasierten Ansatz.

Sichere und transparente KI-Systeme, welche im Einklang mit den Grundrechten stehen.



ATTACKERS

KI-gesteuerte Angriffe



ORGANIZATIONS

KI-Einführung





Bestehende
Sicherheit
neu
validieren

KI-Einführung
ermöglichen

KI als
Kraft-
multiplikator
nutzen

Absicherung Ihrer KI-Transformation

01

Aktualisieren wir kontinuierlich unsere Sicherheitslösungen, um gegen das gesamte Spektrum der sich entwickelnden Bedrohungen zu schützen



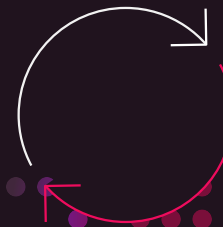
Prevention First Ansatz

02

Sichern wir die neuen KI-Angriffsflächen mit speziell entwickelten Sicherheitsfunktionen

03

Nutzung von KI zur Vereinfachung und Automatisierung von Sicherheitsmanagement und -betrieb



Sichern, was als Nächstes kommt





HYBRID MESH
NETWORK SECURITY

WORKSPACE
SECURITY

EXPOSURE
MANAGEMENT

AI
SECURITY

Check Point Services



SICHERUNG DER INFRASTRUKTUR

HYBRID MESH

NETWORK SECURITY

Die Herausforderungen von Hybrid-Mesh-Netzwerksicherheit

01

Der Perimeter
ist überall



Autonome KI

erweitert den
Explosionsradius

02

Unterschiedliche
Sicherheitswirksamkeit



KI-Verkehr

Verbirgt Risiken in normal
aussehenden Verbindungen

03

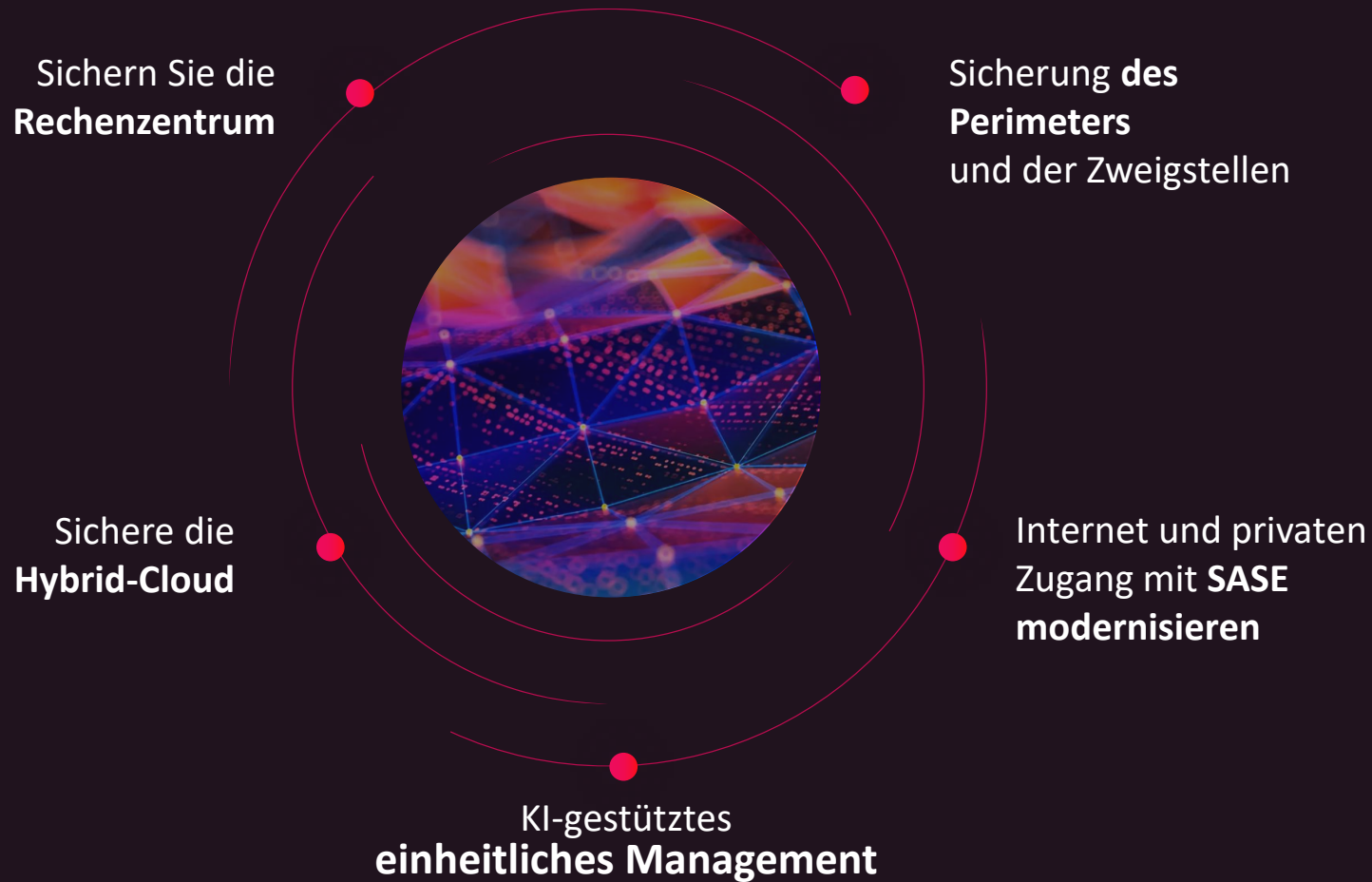
Komplexität beeinträchtigt
die Effizienz



KI-Exploits

erlaubter Netzwerkzugriff zur
Durchführung von Maßnahmen

Absicherung der Infrastruktur: Hybride Mesh-Netzwerksicherheit





ABSICHERUNG für den Menschen

WORKSPACE SECURITY

Die Herausforderungen der Arbeitsplatzsicherheit



- 01 KI-Angriffe können von überall aus gestartet werden

- 02 Schnellere, personalisierte, KI-basierte Angriffe

- 03 Getrennte Werkzeuge



EXPOSURE MANAGEMENT

Die Herausforderungen des Exposure Managements



01 Zu viele Schwachstellen, zu wenig Kontext

02 Getrennte Aufklärung und Durchsetzung

03 Verkleinerte Wartungsfenster

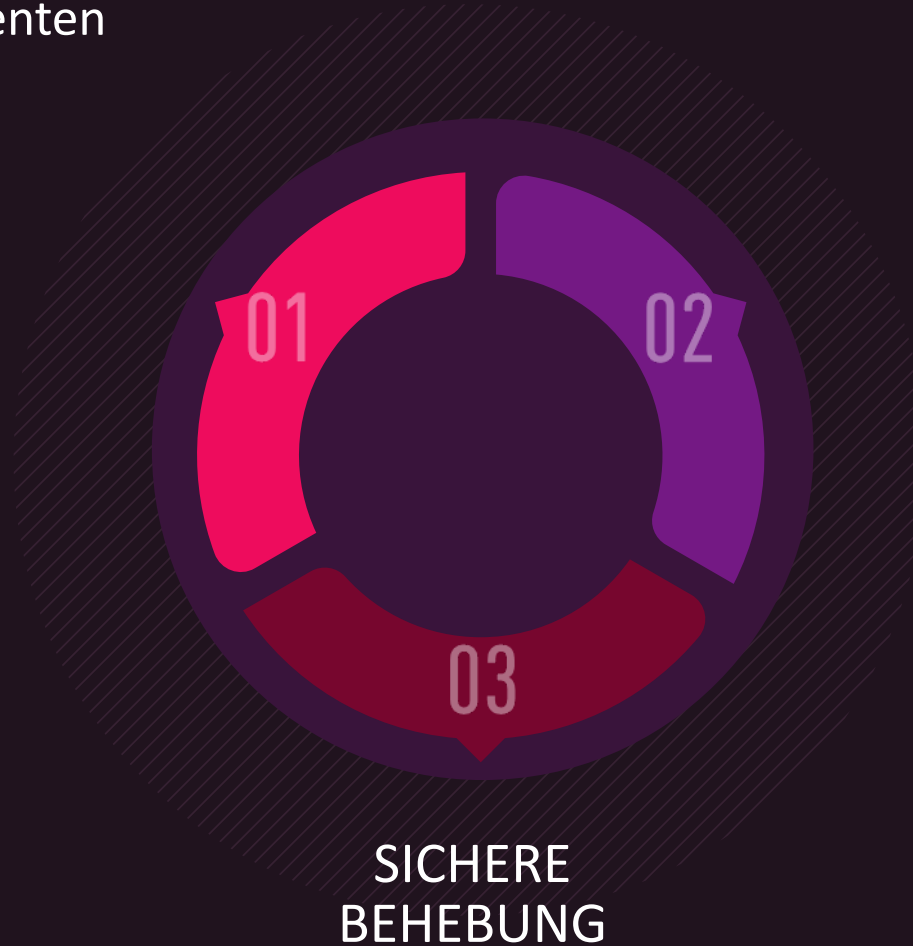
In einer KI-Ära sind wochenlange Reaktionszeiten
nicht mehr haltbar

Exposure Management:

Intelligenzgestützt, Behebungsorientiert

Eine einheitliche Fähigkeit über den gesamten CTEM-Zyklus mit 3 Hauptelementen

BEDROHUNGS-
IDENTIFIKATION



SCHWACHSTELLEN-
MANAGEMENT

SICHERE
BEHEBUNG





ABSICHERUNG VON
NICHT-MENSCHLICHEN SYSTEMEN

AI SECURITY

Die Sicherheitsherausforderungen bei der KI-Adaptierung



Datenabfluss

Über Prompts, Uploads
und Integrationen

KI-spezifische Bedrohungen

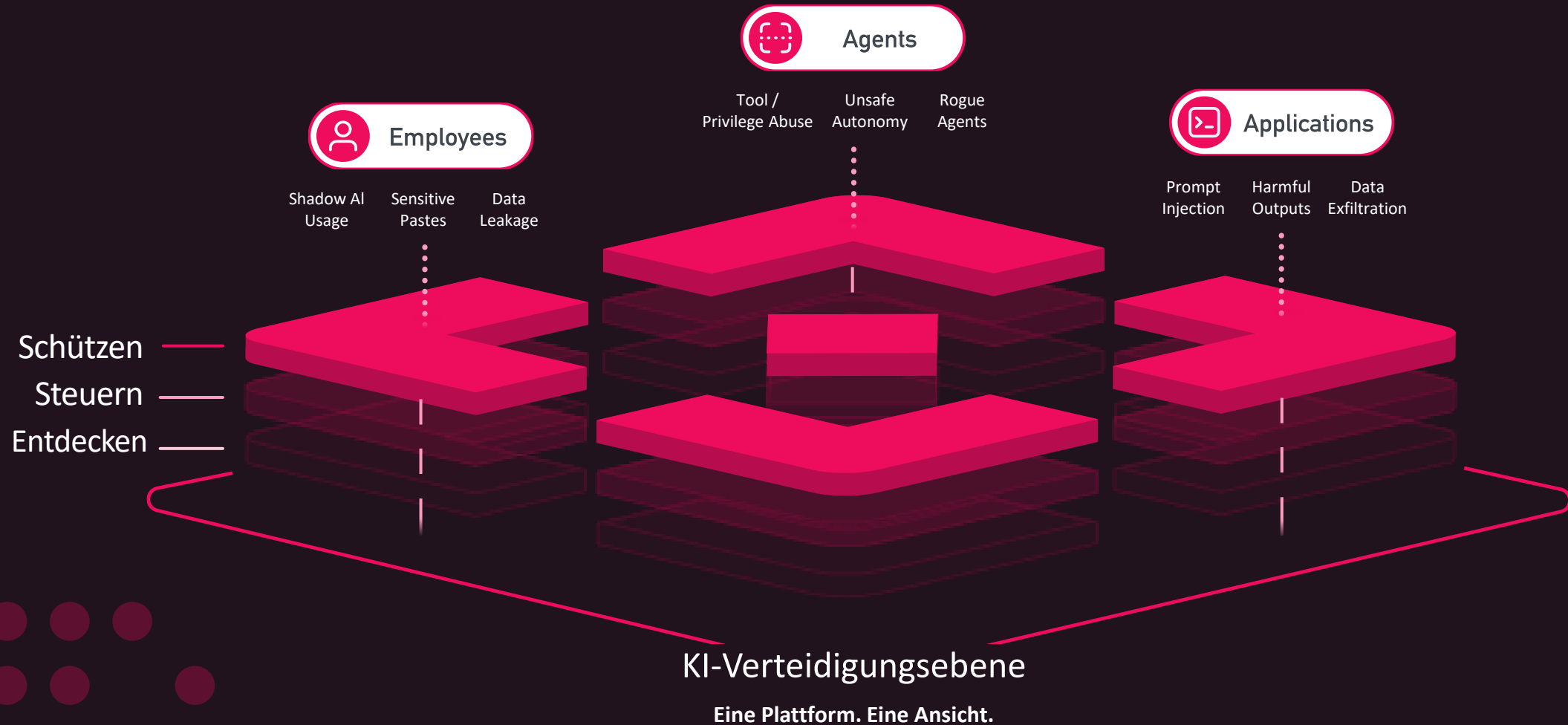
Prompt Injection, Model
Inversion, Data Poisoning
und unsichere
Output-Verarbeitung

Unkontrollierte Autonomie

Agenten, die außerhalb ihres
vorgesehenen Rahmens
handeln
—
bei unklarer
Verantwortlichkeit

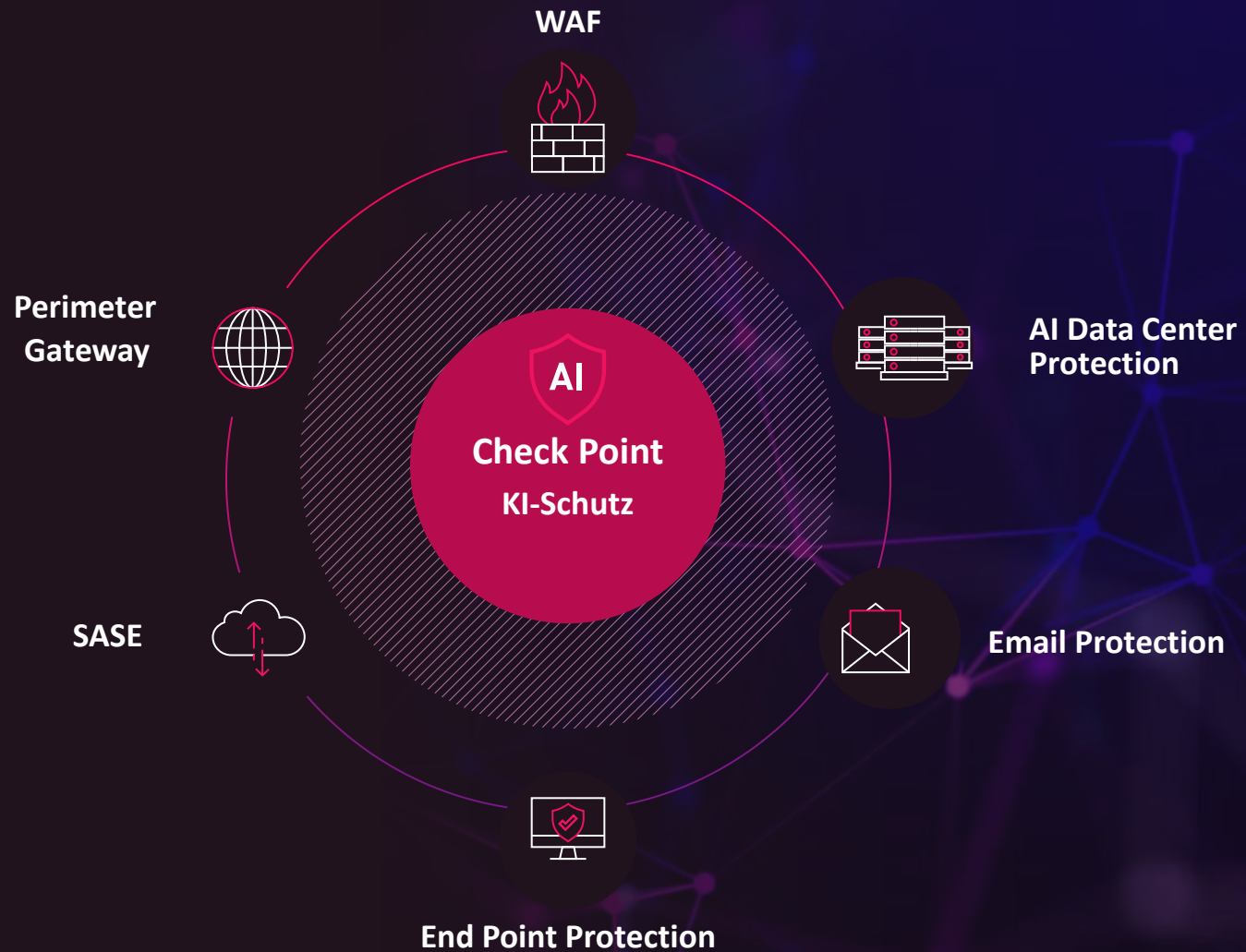
Die Check Point KI-Verteidigungsebene

Ein einheitliches Sicherheitsmodell
für Mitarbeiter, Anwendungen und Agenten

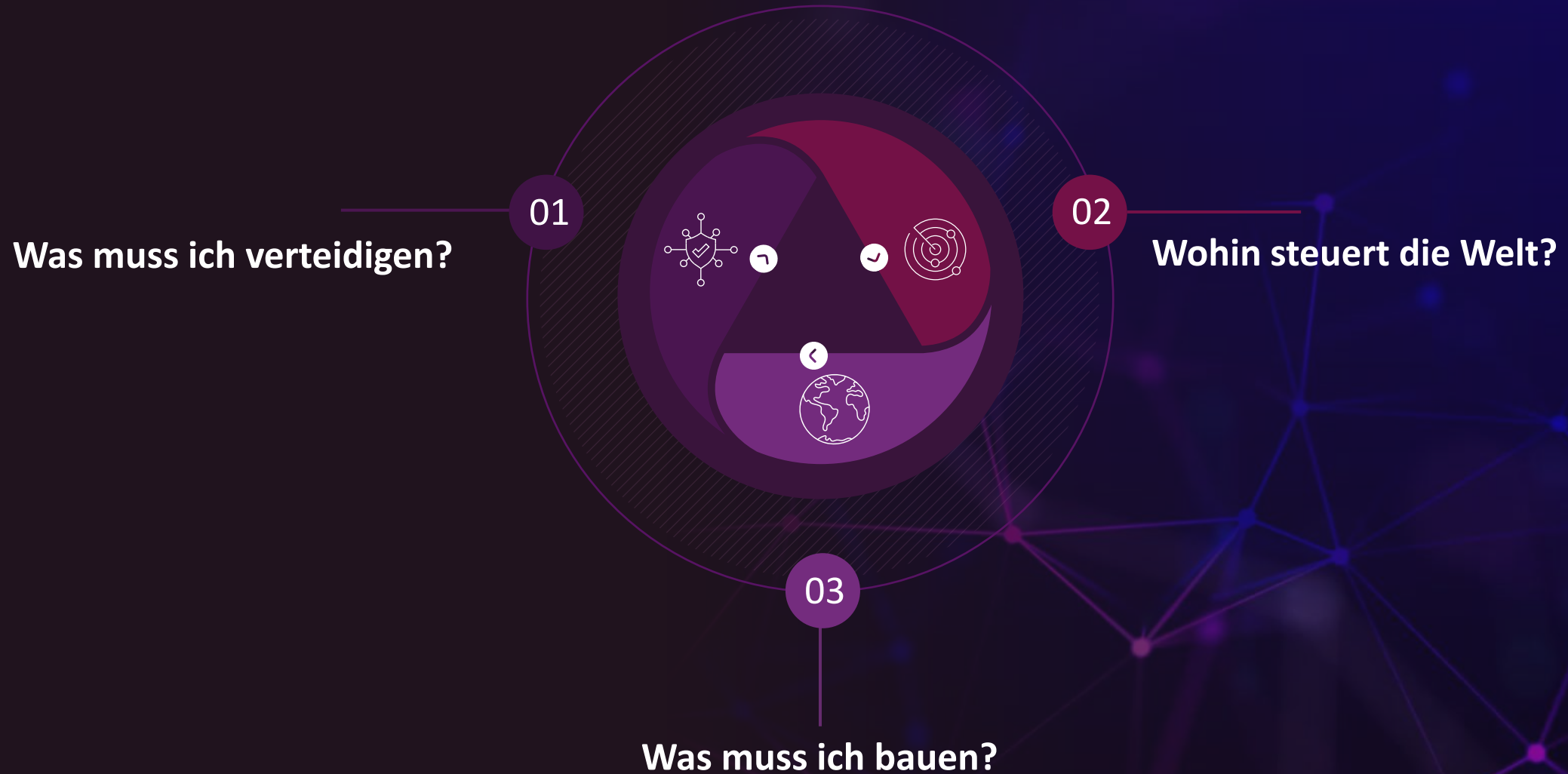


Einbettung von KI-Sicherheit

über alle Check Point Produkte hinweg



Sichere das, was als Nächstes kommt





ZUSAMMENFASSUNG

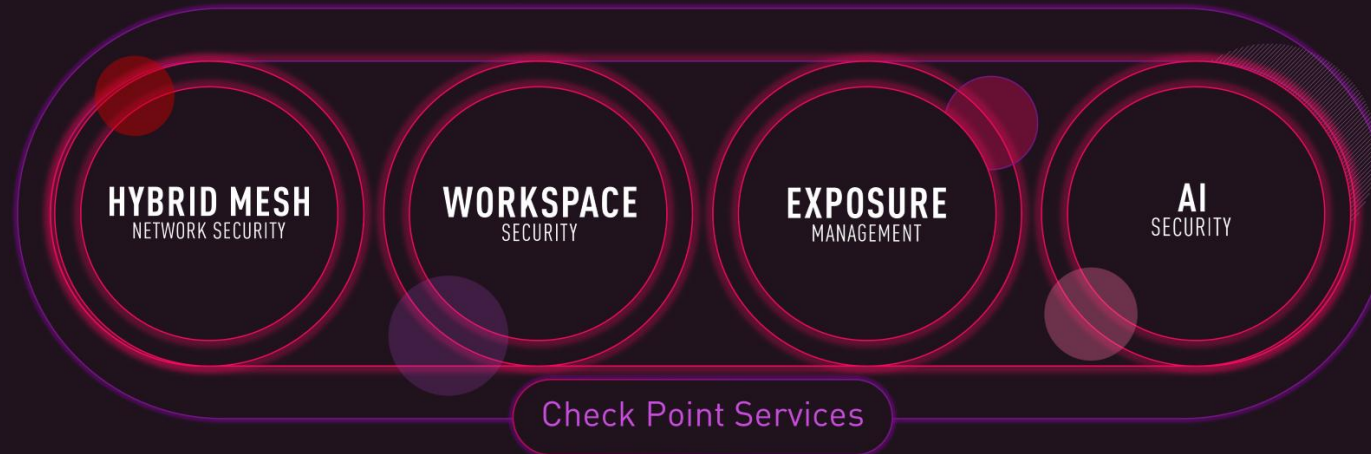
Unsere Mission:

Wir sichern Ihre KI-Transformation

Kontinuierliche
Updates der
Security

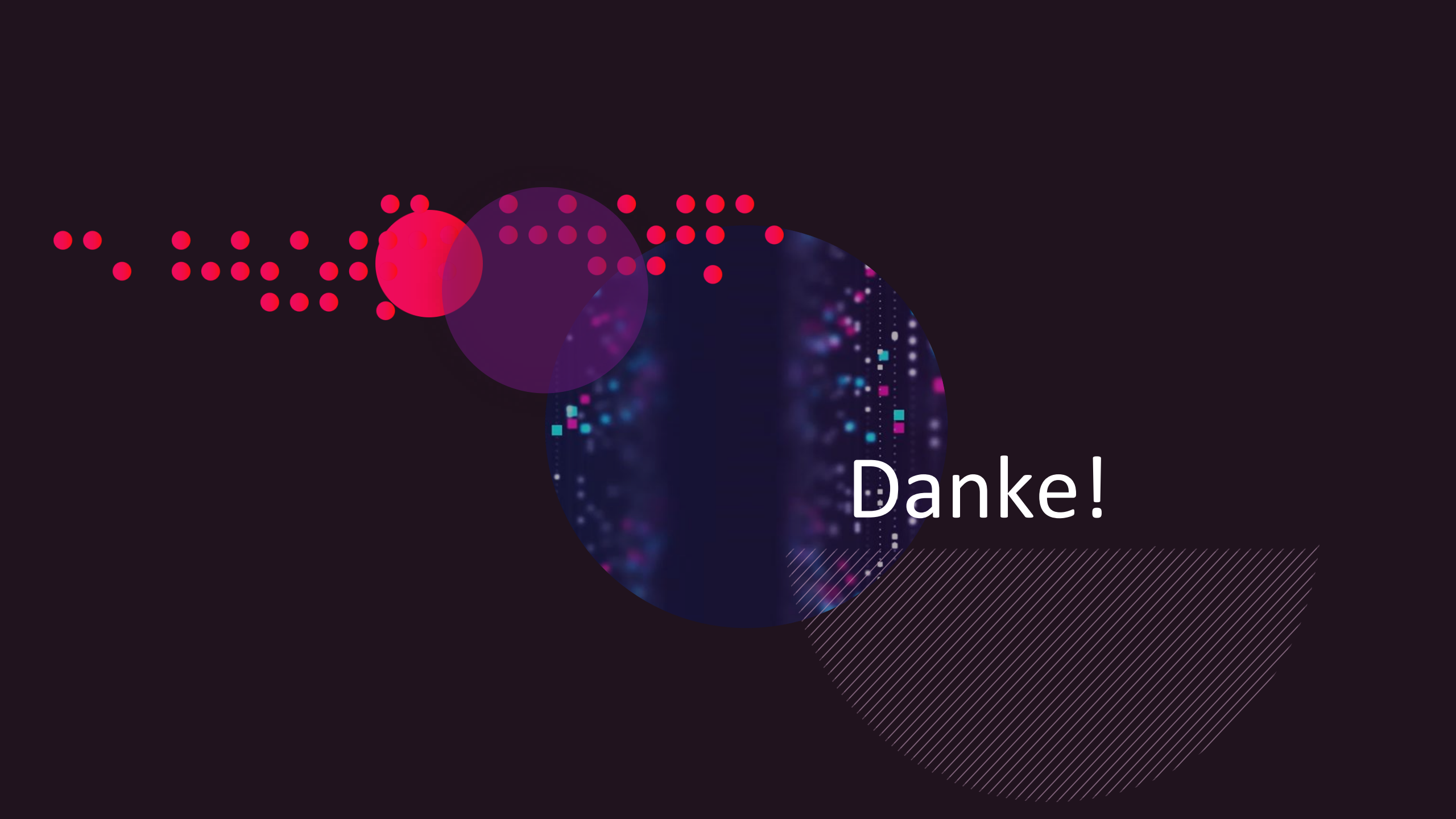
Sichern der neuen KI
Angriffsflächen

KI nutzen, um Sicherheit zu
vereinfachen und zu
automatisieren



Prevention First Ansatz

Absichern, was als Nächstes kommt

The image features a dark purple background with several overlapping circles. A bright red circle is on the left, partially overlapping a medium purple circle. This medium purple circle overlaps a large dark blue circle. The dark blue circle contains a pattern of small, colorful dots (red, blue, green, yellow) and a vertical line of white dots. Below the dark blue circle is a large, semi-circular area filled with diagonal white lines. The word "Danke!" is written in white, sans-serif font, positioned to the right of the dark blue circle and above the diagonal line area.

Danke!