



**BORGWARE**  
IT-SOLUTIONS & SERVICES

Christian Wagner  
Senior Sales Engineer Enterprise  
[Christian.Wagner@arcticwolf.com](mailto:Christian.Wagner@arcticwolf.com)

[illegible]

The figure displays a grid of 20 cybersecurity company logos, organized into 10 categories. Each category is represented by a blue-bordered box containing logos of leading companies in that space.

- AI Security:** AI Governance (Arista, Palo Alto, Cisco, etc.), AI Quality & Evaluation (Arista, Palo Alto, Cisco, etc.), AI Security-as-a-Service & Training (Arista, Palo Alto, Cisco, etc.), Application & Platform Security (Arista, Palo Alto, Cisco, etc.), Counter-AI & Threat Protection (Arista, Palo Alto, Cisco, etc.), Data Security & Protection (Arista, Palo Alto, Cisco, etc.), Discovery & Observability (Arista, Palo Alto, Cisco, etc.), Identity (Arista, Palo Alto, Cisco, etc.), Model Consumption Security (Arista, Palo Alto, Cisco, etc.), Model Security (Arista, Palo Alto, Cisco, etc.), Runtime Control & Interface Security (Arista, Palo Alto, Cisco, etc.), Security Automation & Operations (Arista, Palo Alto, Cisco, etc.).
- Risk & Compliance:** Cyber Insurance (Arista, Palo Alto, Cisco, etc.), Digital Risk Management (Arista, Palo Alto, Cisco, etc.), Governance, Risk, & Compliance (Arista, Palo Alto, Cisco, etc.), Pen Testing & Breach Simulation (Arista, Palo Alto, Cisco, etc.), Risk Assessment & Visibility (Arista, Palo Alto, Cisco, etc.), Security Awareness & Training (Arista, Palo Alto, Cisco, etc.), Risk Quantification (Arista, Palo Alto, Cisco, etc.).
- Digital Channel Security:** Blockchain (Arista, Palo Alto, Cisco, etc.), Fraud & Transaction Security (Arista, Palo Alto, Cisco, etc.), Messaging Security (Arista, Palo Alto, Cisco, etc.), Mobile Security (Arista, Palo Alto, Cisco, etc.), Web Security (Arista, Palo Alto, Cisco, etc.).
- Network Security:** Advanced Threat Protection (Arista, Palo Alto, Cisco, etc.), DDoS Protection (Arista, Palo Alto, Cisco, etc.), Deception (Arista, Palo Alto, Cisco, etc.), DNS Security (Arista, Palo Alto, Cisco, etc.), Network Access Control (Arista, Palo Alto, Cisco, etc.), Network Analysis & Forensics (Arista, Palo Alto, Cisco, etc.), Network Firewall (Arista, Palo Alto, Cisco, etc.), Secure Access Service Edge (Arista, Palo Alto, Cisco, etc.), Software-Defined Networking (Arista, Palo Alto, Cisco, etc.).
- Cloud Security:** CASB (Arista, Palo Alto, Cisco, etc.), Container (Arista, Palo Alto, Cisco, etc.), Infrastructure (Arista, Palo Alto, Cisco, etc.).
- Data Security:** Data Centric Security (Arista, Palo Alto, Cisco, etc.), Data Privacy (Arista, Palo Alto, Cisco, etc.), Data Loss Protection (Arista, Palo Alto, Cisco, etc.), Encryption (Arista, Palo Alto, Cisco, etc.).
- Identity & Access Management:** Authentication (Arista, Palo Alto, Cisco, etc.), Consumer Identity (Arista, Palo Alto, Cisco, etc.), IDaaS (Arista, Palo Alto, Cisco, etc.), Identity Governance (Arista, Palo Alto, Cisco, etc.), Privileged Management (Arista, Palo Alto, Cisco, etc.).
- Security Operations:** Security Analytics (Arista, Palo Alto, Cisco, etc.), Incident Response (Arista, Palo Alto, Cisco, etc.), Threat Intelligence (Arista, Palo Alto, Cisco, etc.).
- Endpoint Security:** Endpoint Detection & Response (Arista, Palo Alto, Cisco, etc.), Endpoint Prevention (Arista, Palo Alto, Cisco, etc.).
- Security Services:** Advanced MSS & MDR (Arista, Palo Alto, Cisco, etc.), Security Consulting (Arista, Palo Alto, Cisco, etc.), Traditional MSSP (Arista, Palo Alto, Cisco, etc.).

**2023**

**Application Security**

IBM, Burrows, CIPHERLOCK, citrix, CLOUDFLARE, fastly, FEATINET, FORTRA, NETSPI, omnisec, ORACLE, paloalto, riverbed, TEMPLARIT, safe-i, SEWORKS, SUCURI, TEMPLARIT, THREATX, TREND MICRO, VIRSEC, wallarm, waratek, Whitehat Security

**Application Security Testing**

IBM, CIPHERLOCK, DIGIVANTE, ESRScan, Fasoo, kryptowave, MICRO FOCUS, N-Stack, iPORT, PERFORMANCE, PORTSWAGER, Qualys, RAPID7, SiteLock, snyk, sonarsource, Synack, VERACODE, Whitehat Security, WhiteSource

**Mobile Security**

BlackBerry, Check Point, COMBUSTION, Cyble, ESET, INPEDIA, McAfee, NortonLifeLock, NowSecure, SOTI, TeleSign, ATESSALABS, VMware, wandra, wickr, Zimperium

**Messaging Security**

AREA 1, SAS SYSTEMS, Burrows, BlackBerry, Cisco, CYBONET, CALEEN, FIREEye, Forcepoint, FEATINET, FORTRA, QAOSECURE, GreatHorn, Mailguard, INKY, IBM, Microsoft, mimeraster, MICRO FOCUS, Microsoft, mimecast, NortonLifeLock, SonicWall, Sophos, Trellix, Trend Micro, Trustwave, Zoxide Secure, VALINGAIL, wdr, zerospam, ZIX

**Other Logos**

ARM, CISOVD, ESET, Deloitte, IBM, EV, GILL, HAKA, leidos, LogRhythm, nccgroup, SANS, McAfee, SANS, SYGN/A, VERINT, wdr

**Other Logos**

emalage, ethoca, EverCompass, feedzai, FICO, MagicCube, NICE, NICE Security, SpyCloud, TokenMetrics, TransUnion, UNIKEN, technology

**Other Logos**

CASB, ibtglass, BROADCOM, Cisco, CORONET, Lookout, Microsoft, netskope, ORACLE, proofpoint, SKYFORMATION, Skyhigh, Strategy

# Warum KI den Markt verändert

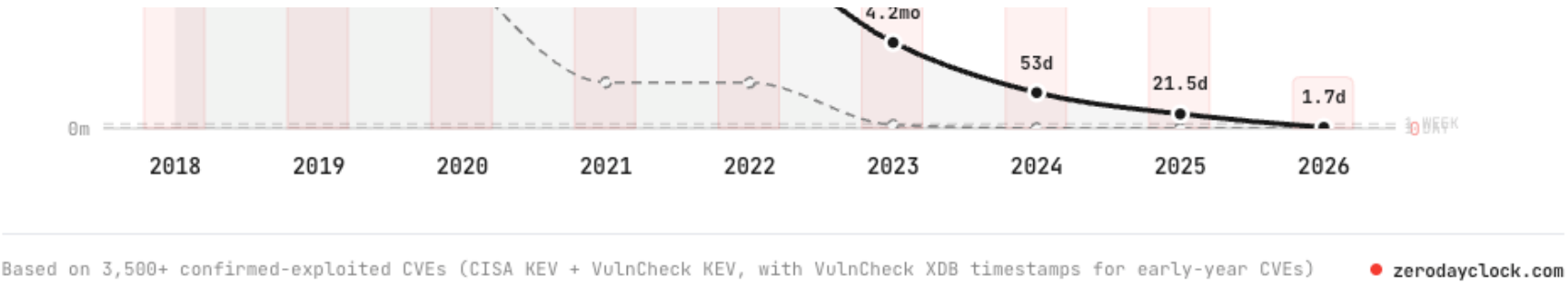
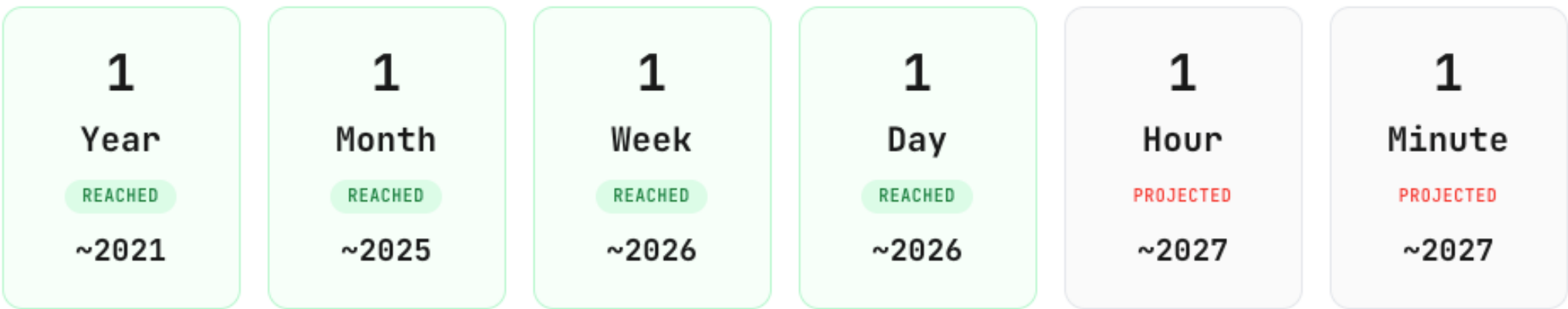
## From Vulnerability to Exploitation

TTE measures the gap between CVE public disclosure and first confirmed in-the-wild exploitation. Zero = same-day.

— Mean TTE (10% trimmed, days)    --- Median TTE (days)    ■ Weaponized Exploits (count)

### Time-to-Exploit Milestones

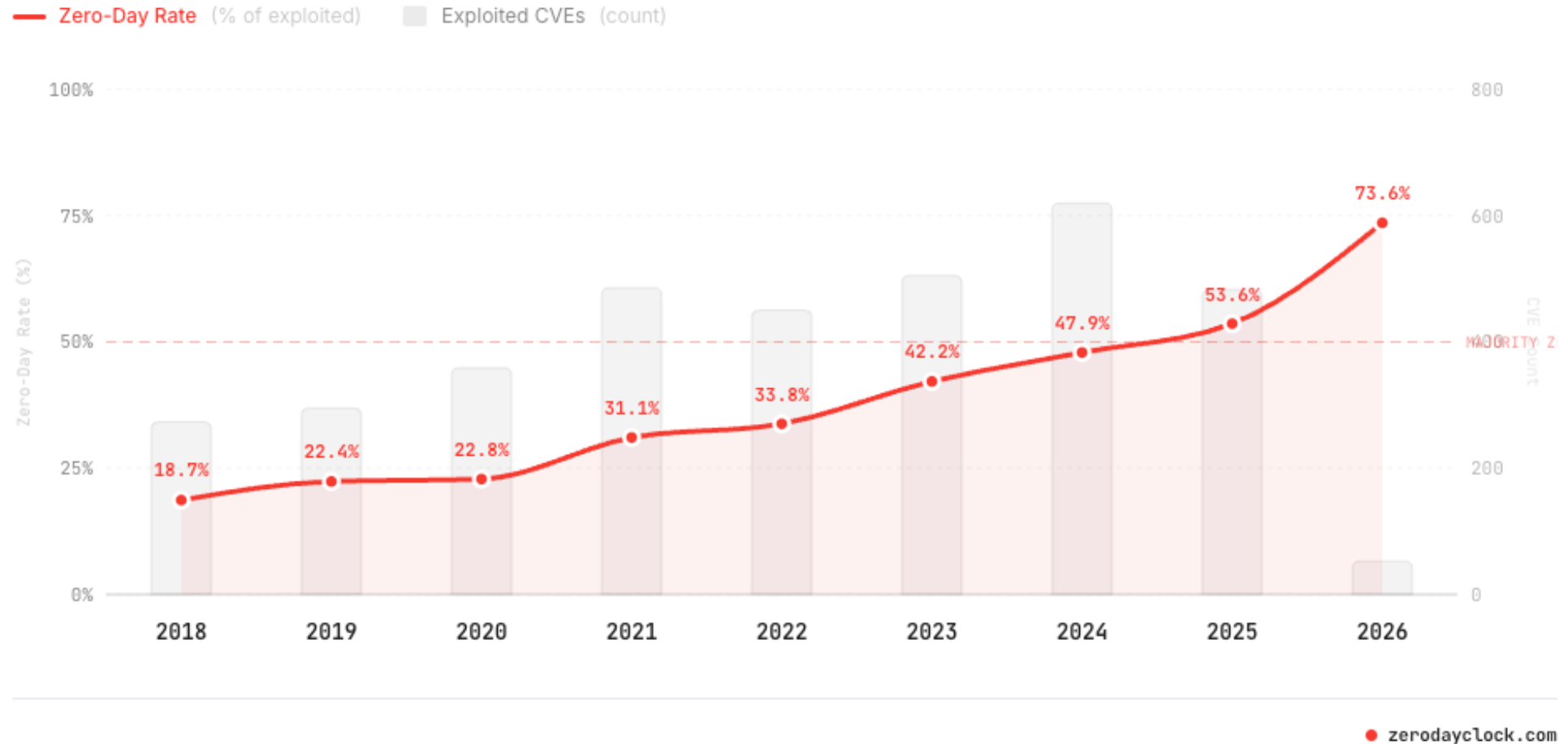
Projected year when median TTE crosses each threshold — extrapolated from observed 2018–2024 trend



# Warum KI den Markt verändert

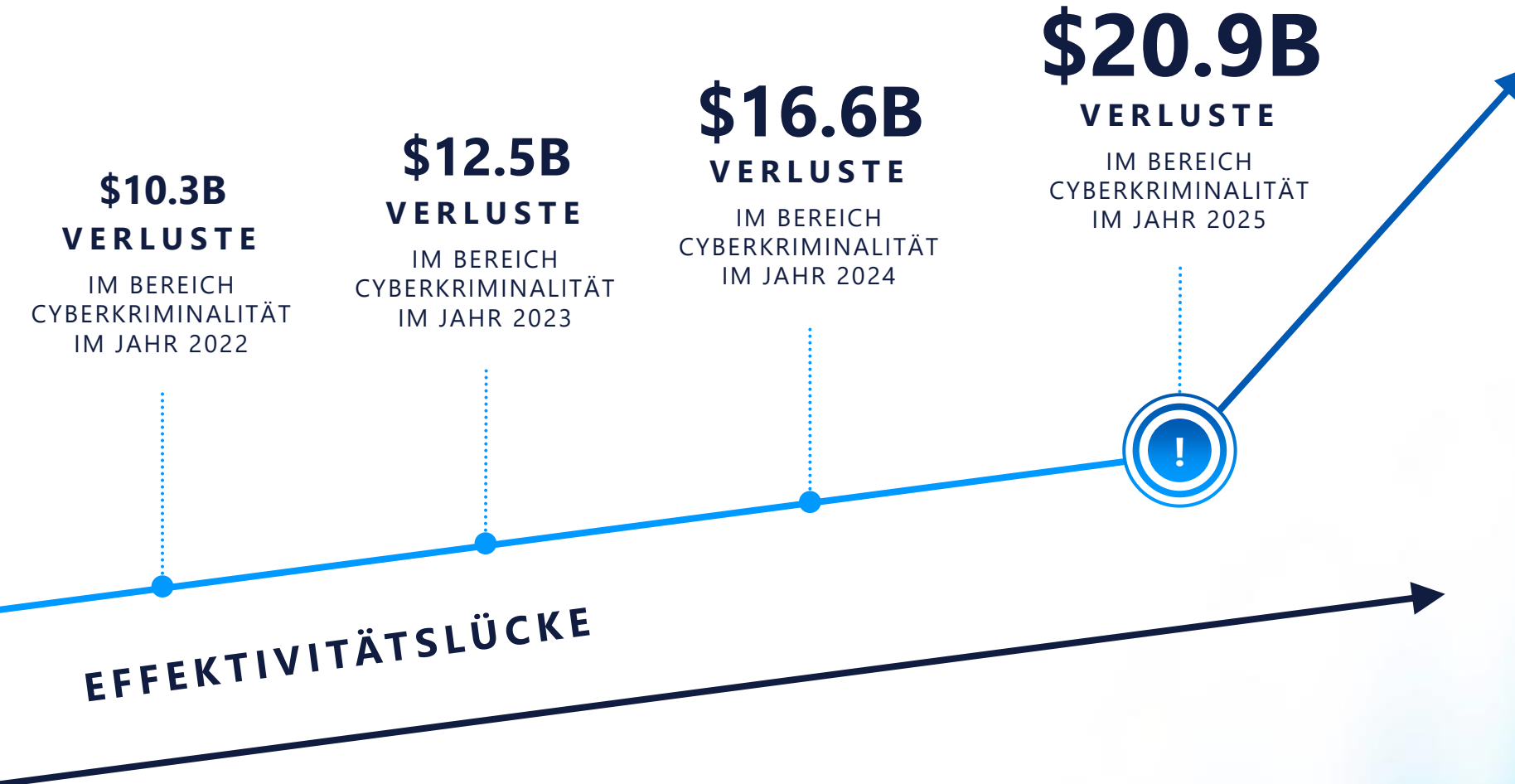
## Zero-Day Rate

Percentage of exploited CVEs where exploitation occurred before or on the day of disclosure (TTE ≤ 0)



# Cyberisiko ist Geschäftsrisiko

Jetzt durch KI beschleunigt



## KI-EINFLUSS

MACHINE SPEED  
EXPLOITATION

# 1 Stunde

time-to-exploit in 2027

AUTONOM  
AUSGEFÜHRT

# 80-90%

von einem Cyberangriff, der  
jetzt von KI automatisiert wird

HÖHERE VERLUSTE

# \$893M

bei KI-gestützten Angriffen



# IT und Security Verantwortliche versuchen, sich anzupassen

KI ist da, aber die Akzeptanz in der Cybersicherheit hinkt zurück

<5%

Organisationen haben agentische KI in Sicherheitsoperationen eingesetzt

GARTNER

95%

Generative KI-Piloten bei Unternehmen scheitern

MIT

75%

von Unternehmen werden bis 2028 KI-verstärkte Cybersicherheitsprodukte verwenden

GARTNER

## Was funktioniert nicht

### ⊗ Frontier AI Models

*"Baue es selbst von Grund auf"*

### ⊗ Bolted-On AI

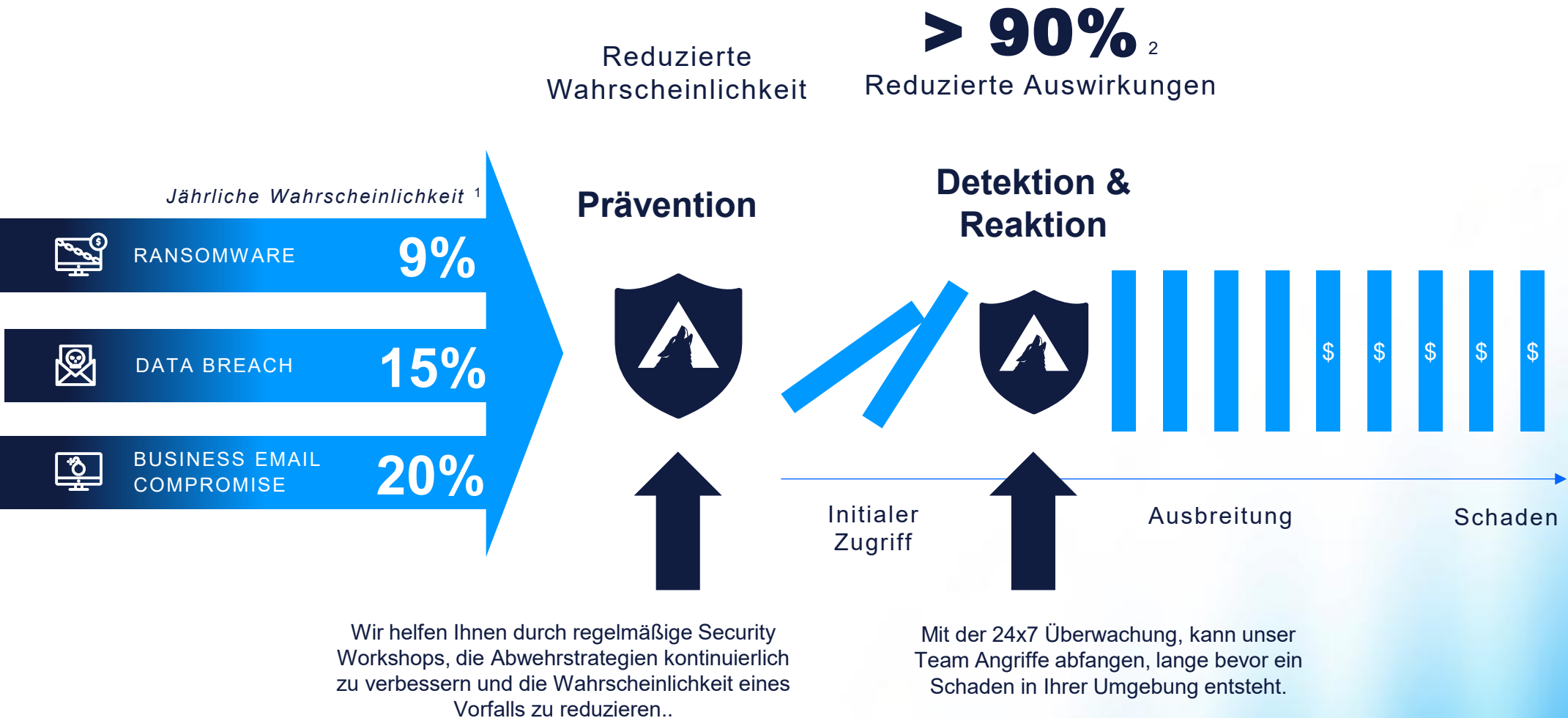
*"Hier ist eine Werkbank, viel Glück"*

### ⊗ AI Startup Agents

*"Wir machen eine Sache, so ungefähr"*



# Wir helfen, den Risiken zu begegnen



<sup>1</sup> [ACAMS, 2022](#); [IBM, 2019](#); [TechStrong Group, 2023](#)  
<sup>2</sup> [Forrester, 2023](#)



# Arctic Wolf Security Operations

## We Make Security Work

**12000+**

Kunden

**24x7**

In deutsch

**1000+**

Security Engineers

**5**

Datacenter weltweit

**5.1+**

Milliarden Logzeilen pro Tag

**3.5M+**

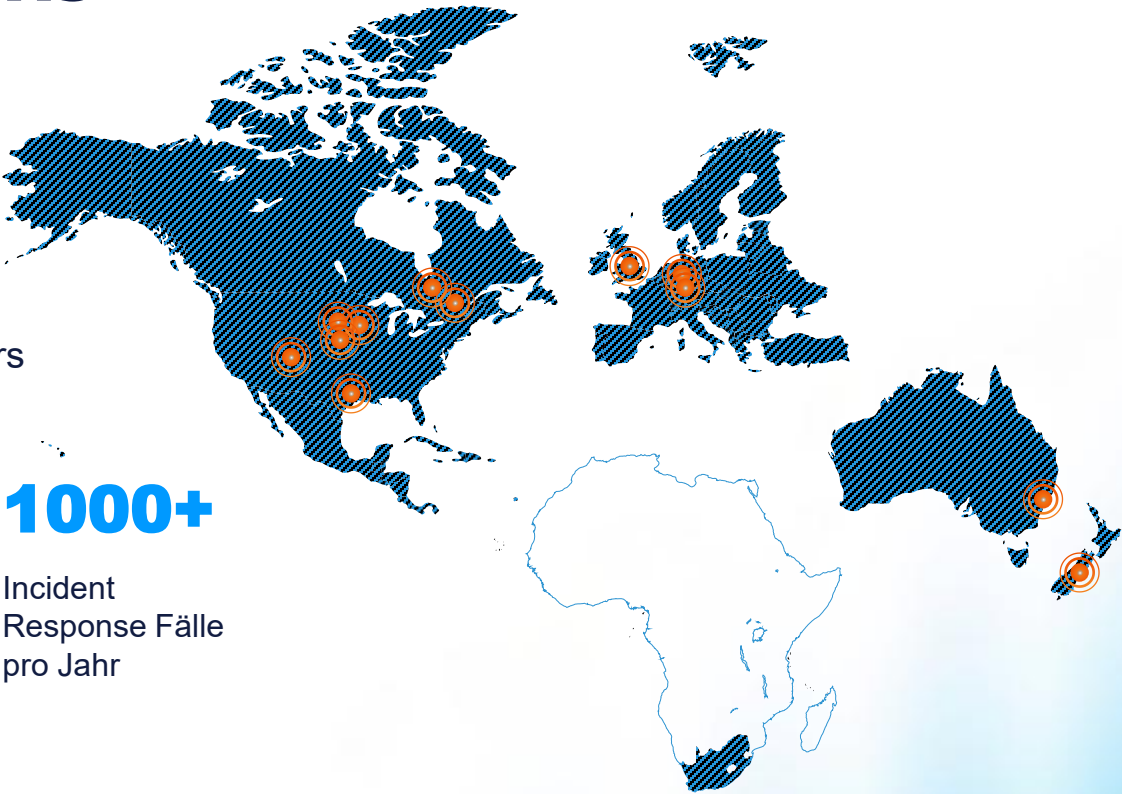
aktive Agenten and 25,000+ Sensoren

**12M+**

Schwachstellen werden pro Woche identifiziert

**1000+**

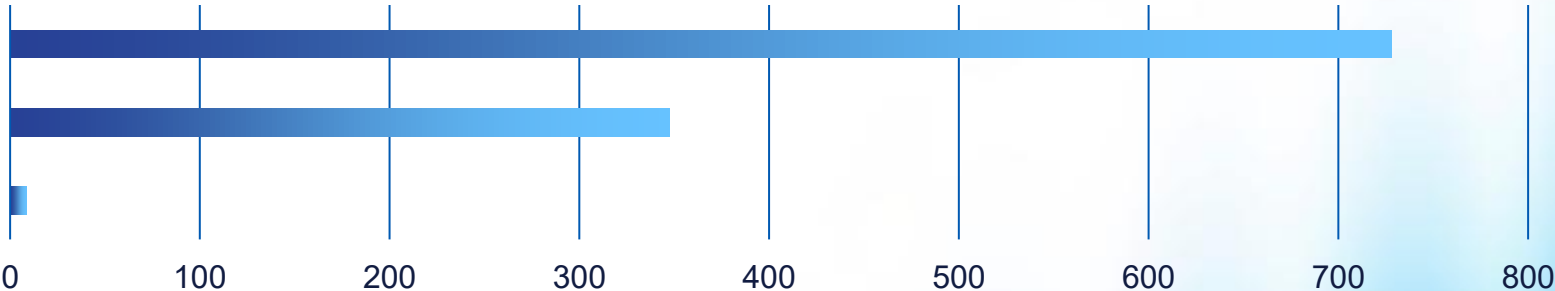
Incident Response Fälle pro Jahr



Arctic Wolf Security Observations

Global Emails Sent

Google Searches



# Arctic Wolf Security Operations

## We Make Security Work

**12000+**

Kunden

**24x7**

In deutsch

**1000+**

Security Engineers

**5**

Datacenter weltweit

**5.1+**

Milliarden Logzeilen pro Tag

**3.5M+**

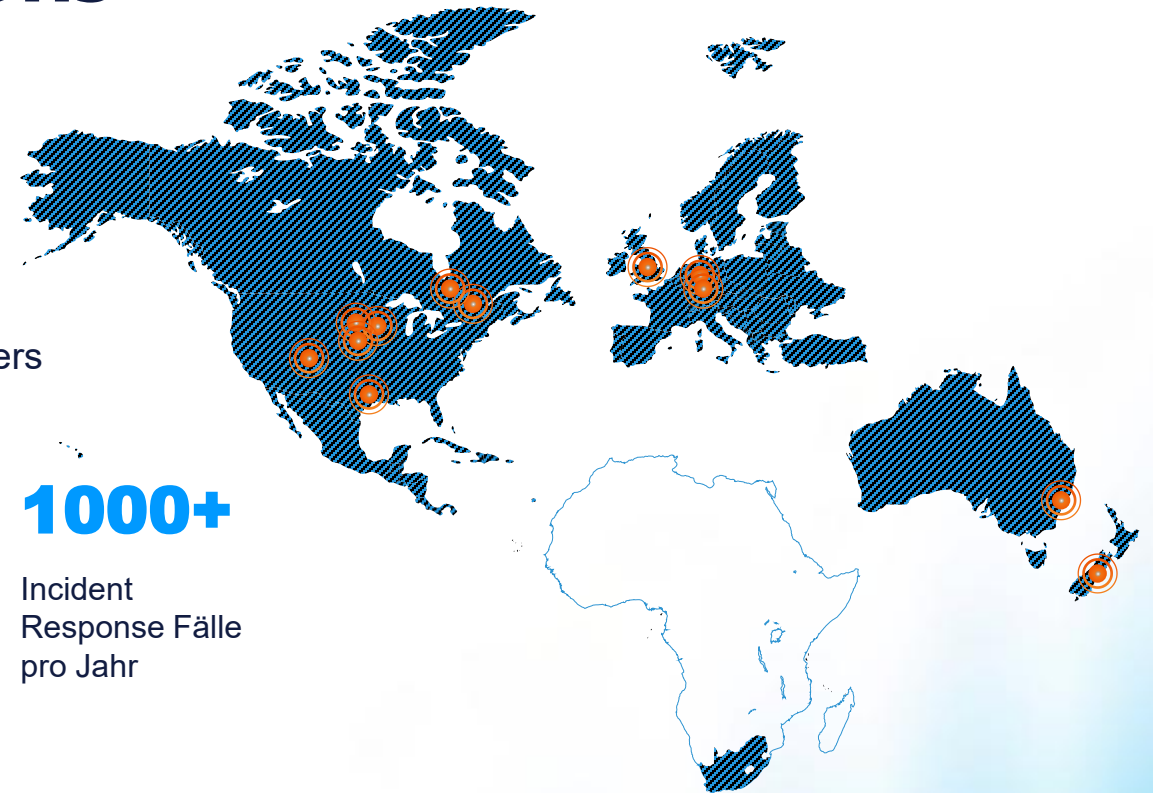
aktive Agenten and 25,000+ Sensoren

**12M+**

Schwachstellen werden pro Woche identifiziert

**1000+**

Incident Response Fälle pro Jahr



# Arctic Wolf Security Operation Teams

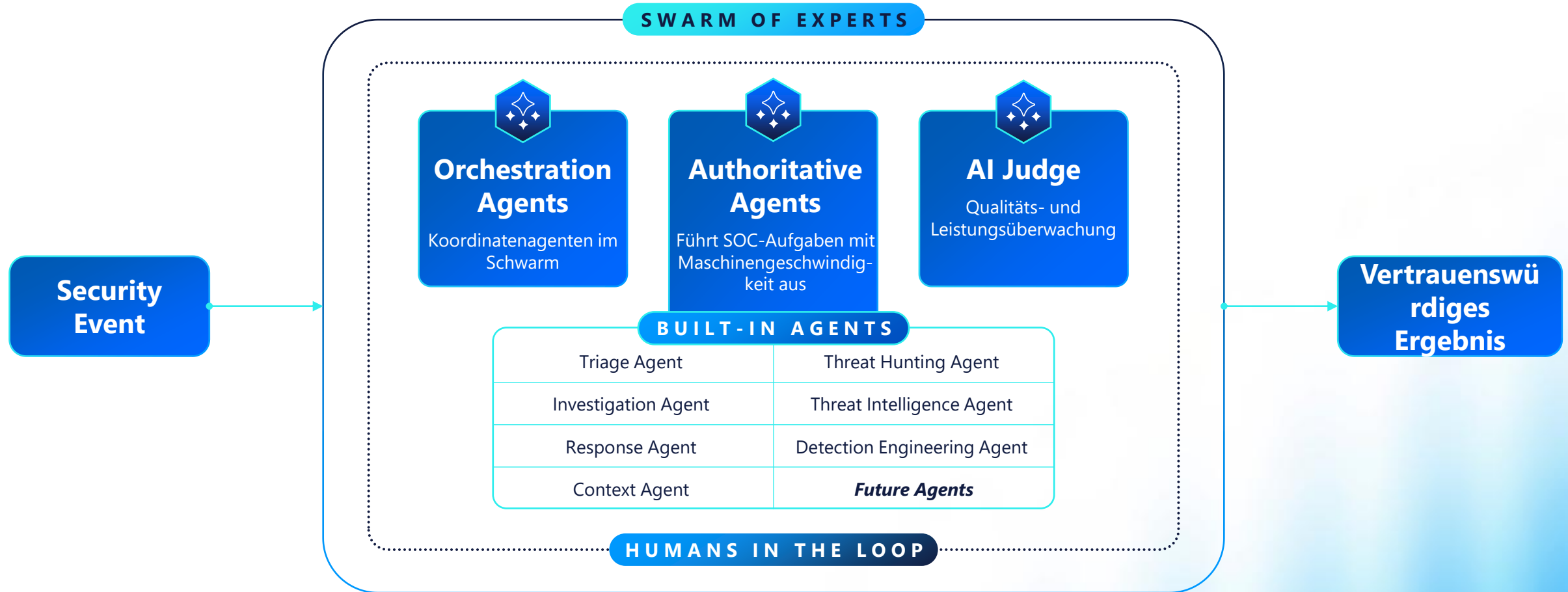
Das Triage Security Team überwacht ihre Umgebung 24x7 um Angriffe zu identifizieren und Sie bei der Behebung unterstützen



Das Concierge Security® Team entwickelt eine auf Sie angepasste Security Journey, um ihren Schutz kontinuierlich zu verbessern.



# The Agentic Future is Already Here



**15X** SCHNELLERE FALL LÖSUNG

**3X** BESSERE TICKETQUALITÄT

**12X** ROI vs. DIY AI



# Beispiel Integrationen mit Erkennungen

Mehr Integrationen verfügbar



Externe  
Risiken  
**5%**



Identität  
**20%**



SaaS  
**15%**



IaaS  
**10%**



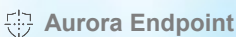
Firewall  
**5%**



Network  
**30%**



Endpoint  
**15%**



# Workshop Beispiele

## Proaktive Verbesserung ihrer Security Landschaft

- External Assessment
- FW Assessment (Basic)
- FW Assessment (Advanced)
- O365 Security Recommendations
- Identity and Lifecycle Management
- Patch and Vulnerability Management
- O365 Mail Forwarding Review
- Phishing and Employee Awareness Training
- Ransomware and Malware Hardening
- Group Policy Management Hardening
- Log Source Config Review
- Cloud Config Review
- Backup Recommendations
- PowerShell Review
- Email Gateways
- AD Attack Vectors
- Architecture and Visibility Assessment
- DNS Security Assessment
- Kerberos Assessment - Kerberoasting
- AD Audit Policy Review
- Credential Access - DCSync Attack
- MS NTLM Assessment
- Supply Chain Risk Best Practice
- Insider Threat Risk Best Practice
- Anomalous Traffic Analysis
- Cloud ID Foundation Review
- AWS CloudTrail to S3 Best Practice
- CIS Benchmarking
- Email Trust and Authentication Assessment
- Endpoint Security Review
- PsExec Utility Assessment
- Asset Classification and Criticality Review
- Vulnerability Prioritization and Asset Baseline Review
- Threat Landscape and Prioritizations Review
- Customer Incident and Pentest Report
- Pre-Pentest Prep



# Meet the Arctic Wolf SecOps Teams

Die zentrale Basis für alle unsere Kundenorientierten Security Services (S2)



## Triage Team

- 24/7 SOC Operations:
  - Investigation, Analyse, Ticketing, Kommunikation
  - Einteilung (Triaging) False/True Positive im Kundenkontext
  - Active Response
- Angeleitete Incident Behebung
- Notfallkontakt für Kunden
- Lokale Serviceerbringung, DE-Frankfurt/Main:
  - 24/7 L1-L3, 4-Schicht, no Follow-the-Sun
  - 24/7 Deutschsprachiger Support



## Concierge Team

- Dediziertes, persönliches Concierge Security Team (CST) für jeden Kunden
  - Breite & tiefgehende Security Expertise, Hersteller-unabhängig
  - 5-15 Jahre Erfahrung pro CST Teammitglied
- Guided Security Journey
  - Regelmäßige Security Posture in-Depth Reviews (SPIdR)
  - Minimierung des Kundenrisikos/-exposure
  - Ticket Root Cause Analyse
- Service Management
- Strategische Anleitungen



## AW Labs

- Global Threat Intelligence Organisation
  - IoC/IoA Maintenance
  - Detection Rule Set
  - Vulnerability / Risk Guidance
- Active Threat Hunting, Security Research
- Security Posture Engineering
- Ingestion, Detection, Response (IDR) Modelling
- AI Oversight + Data Science
- Kunden Briefing + Schulungen



**AI**

Artificial Intelligence

**+**

**HI**

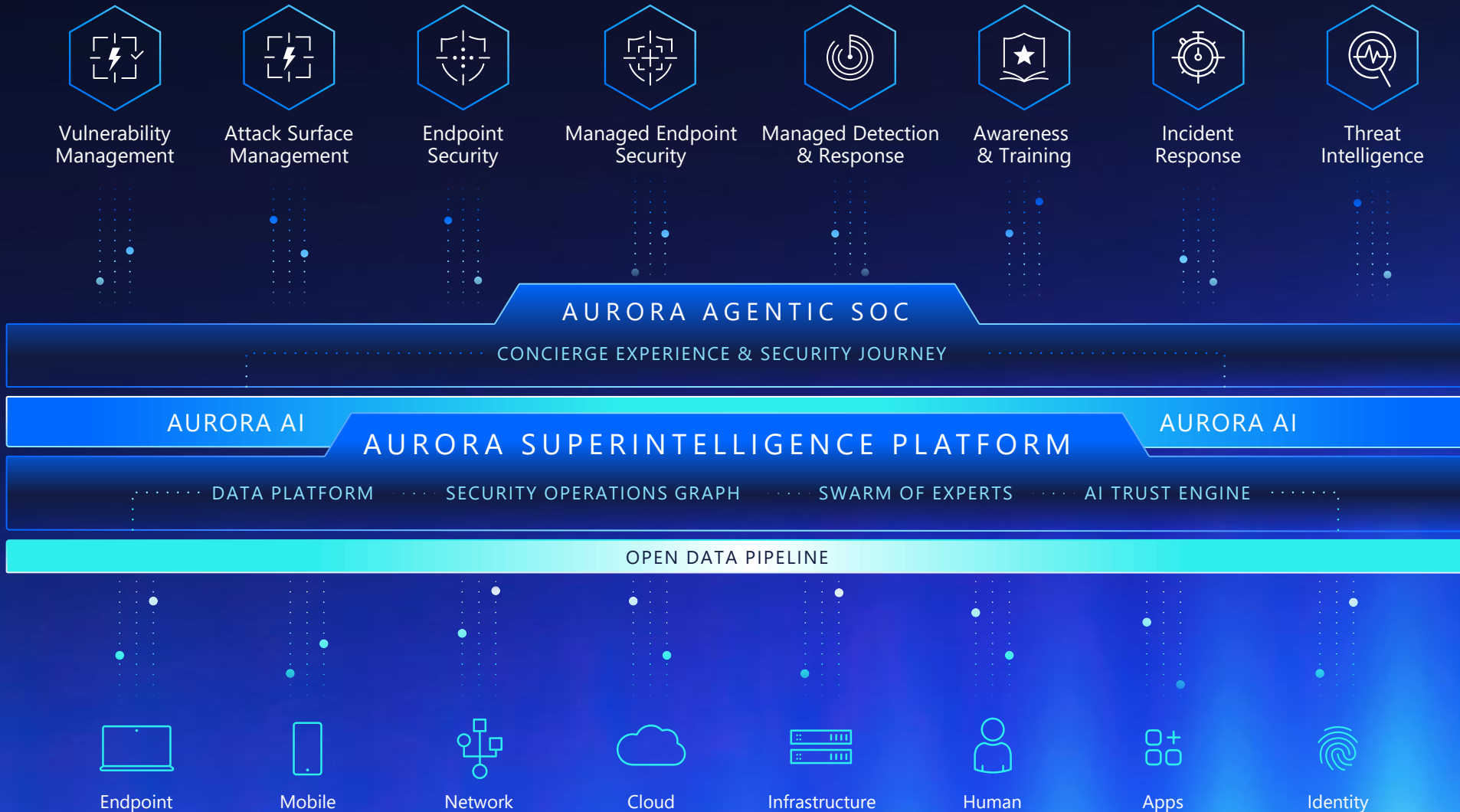
Human Intelligence

**=**

**Superintelligence**



# Die Arctic Wolf Aurora Superintelligence-Plattform



## GRUNDÜBERZEUGUNG VON ARCTIC WOLF:

# Cybersicherheit ist ein operatives Problem



### MDR Pioneer

Wir haben Managed Detection and Response vorangetrieben. Jetzt transformieren wir die Security Operations für das KI-Zeitalter.



### Security Superintelligence

Wir haben die erste Superintelligence-Plattform für Cybersecurity entwickelt, die sowohl KI- als auch nur auf Menschen basierende Ansätze übertrifft und das KI-



### Fully Agentic SOC

Wir betreiben das weltweit größte gewerbliche Agentic-SOC und liefern es unseren Kunden als schlüsselfertigen Service.

## Erprobt, Getestet & Bewiesen

1T+

Sicherheitsereignisse pro Tag



2x Leader MDR MarketScape

11K+

Globale Kunden

Gartner.

Peer Insights™

3x wiederholt empfohlen

7M+

Endpunktagenten



Einziger dreifacher Gewinner bei Cybersicherheit

20K+

Untersuchungen pro Tag



EAP Visionär im Jahr 2025

14+

Jahrelange SOC-Expertise



2025 MDR Produkt des Jahres



# END CYBER RISK

