



#### Facts zum Produkt

- KI-basierte Echtzeit-Erkennung von Netzwerkbedrohungen
- Priorisierte Warnungen reduzieren Alarmflut um 80 %
- Erkennung von 90 % der MITRE ATT&CK-Taktiken
- Automatisierte Reaktionen mit MITRE D3FEND-Unterstützung
- Erweiterter Schutz für Netzwerk, Cloud & Identitäten

Partnered with:

**VECTRA**

# KI-gestützte Network Detection and Response

## Erkennung, Untersuchung und Abwehr von Angriffen in Ihrem gesamten Netzwerk mit Vectra NDR und Serviceware

Ihr Netzwerk bildet die Grundlage Ihrer Unternehmensinfrastruktur und erfordert eine äußerst effektive Cyber-Sicherheitsstrategie. Ohne ausreichende Netzwerktransparenz und Tools, die große Mengen an Sicherheitsdaten mit Kontext anreichern, werden externe Angreifer und böswillige Insider weiterhin einen Vorteil haben und Kosten in Millionenhöhe verursachen.

## Das Unbekannte erkennen, Kompromittierungen stoppen

Vectra Network Detection and Response (NDR) ist die branchenweit modernste KI-gestützte Lösung zur Identifizierung und Abwehr von Angreifern in Ihrem Netzwerk, die ohne Fehlalarme und Verschlüsselung auskommt. Vectra NDR bietet dank Security AI-driven Attack Signal Intelligence™ frühzeitige Transparenz mit Klarheit, Genauigkeit und Kontext, sodass unbekannte und neue Bedrohungen, Angriffe und schädliche Aktivitäten in einer vollständigen Kette von verdächtigen Ereignissen beseitigt werden können. Mit Vectra können Unternehmen auch die Bedrohungen und Angriffe erkennen und effektiv abwehren, die von anderen Lösungen übersehen werden. Die Security-Teams müssen somit weniger Zeit mit Optimierung, Threat Hunting und Untersuchungen verbringen und können stattdessen mehr zum Wachstum des Unternehmens beitragen.

## Proaktive Bedrohungserkennung mit Vectra NDR und Serviceware

Serviceware unterstützt Unternehmen ihre digitale Infrastruktur sicher, effizient und zukunftsweisend auszurichten. Mit langjähriger Erfahrung, tiefgreifendem technologischen Knowhow und starken Technologiepartnerschaften mit namhaften Herstellern entwickeln wir passgenaue Strategien für IT Security, Netzwerkinfrastruktur und Cloud-Lösungen.

**Mehr erfahren**

## Die größten Herausforderungen

- **Lateral Movement**
- **Ungewöhnliche Netzwerkaktivitäten**
- **Mean Time to Repair (MTTR)**
- **Überlastung durch Analyse und Threat Hunting**
- **Kompromittierungserkennung in Echtzeit**
- **Nachvollziehbarkeit von Angriffen**

## Wichtige Funktionen

### Netzwerk-Transparenz

Sie können alle Netzwerkaktivitäten erkennen, analysieren und speichern sowie verborgenes schädliches Verhalten aufdecken, ohne vorherige Kenntnisse oder Mustererkennungen zu benötigen. Angreiferaktivitäten werden automatisch verfolgt (z. B. Missbrauch von Anmeldedaten, laterale Bewegung, Command & Control sowie Remote-Ausführung) – im gesamten Firmennetzwerk und in verteilten Host-Systemumgebungen, lokal sowie in der Cloud.

### KI-gestützte Erkennung

Vectra NDR automatisiert die Bedrohungserkennung durch hochentwickelte Analysen, Deep Learning, komplexe Verhaltensanalysen und Einblicke in Angreifermethoden. Die Lösung erkennt, wie ein erfahrener Analyst, effektiv Zwischenfälle in Milliarden von Datenpunkten. Das Security-Team kann Bedrohungen und Attributierungen rund um Angriffe und schädliche Aktionen im Netzwerk (z. B. duplizierten oder asymmetrischen Traffic sowie Datenkapselungen) genauer lokalisieren, um automatisch die Aussagekraft von schwachen Indikatoren sowie verschleierten und unbe-

## **Schützen Sie Ihr Unternehmen mit intelligenter NDR**

Vectra bietet führende Detection & Response für hybride Clouds. Vectra Attack Signal Intelligence erkennt und priorisiert Bedrohungen in Cloud-, SaaS-, Identitäts- und Netzwerkumgebungen. Durch die Analyse des Angreiferverhaltens liefert die Vectra Plattform zuverlässige Bedrohungssignale und wichtigen Kontext, sodass Security-Teams Bedrohungen schneller erkennen und stoppen können.

[vectra.ai besuchen](https://vectra.ai)

kannten Umgehungsmustern zu bestimmen. Dies ermöglicht die Erkennung von bis zu 90 % der im MITRE ATT&CK-Framework aufgeführten Angriffstaktiken und -techniken.

### **KI-gestützte Triage**

Der ML/KI-Ansatz ermöglicht automatisiert umfassende Analysen aktiver Erkennungen, ihres zugehörigen Kontexts, der Gemeinsamkeiten zwischen Ereignissen sowie der Scores, mit denen die Dringlichkeit von True-Positive-Erkennungen bewertet wird. Analyst:innen haben dadurch mehr Zeit für dringende Zwischenfälle, während gleichzeitig die Menge der zu prüfenden Erkennungen um 80 % reduziert wird.

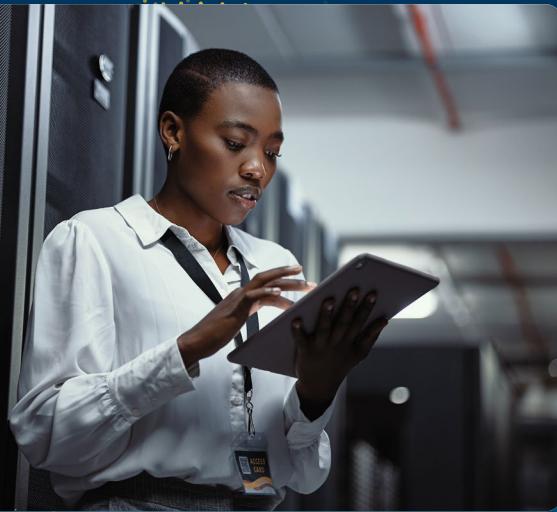
### **KI-gestützte Priorisierung**

Vectra NDR automatisiert die Priorisierung und eskaliert die dringendsten Bedrohungen durch Bewertung und Einstufung Tausender laufender Ereignisse auf dem Niveau erfahrener Security-Analyst:innen, sodass relevante Details in Millisekunden statt in Minuten oder Stunden bereitstehen.

### **Erweiterte Untersuchung**

Die Lösung sammelt kontinuierlich Erkenntnisse aus der sich stetig verändernden Netzwerkinfrastruktur und stellt die für Sie wichtigsten Informationen bereit:

- Suche nach ungewöhnlichen ausgehenden Datenströmen, selbst in verschlüsselten Kanälen
- Korrelation von Erkennungen in allen Hosts, Erlernen von Mustern und Identifizierung von Objekten, um Informationen auf verschiedene Arten zu präsentieren, sodass Beziehungen, Absichten und geschäftliche Folgen klar erkennbar sind

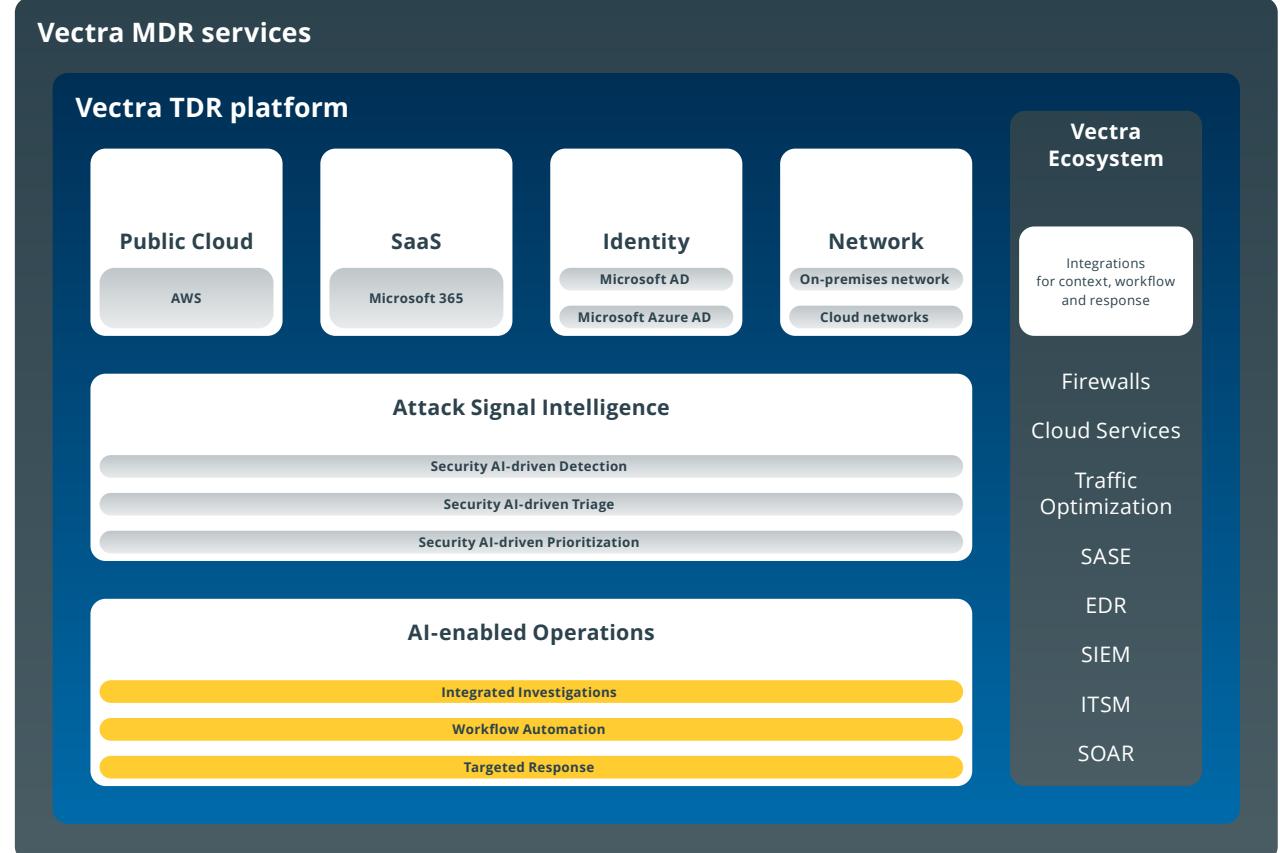


**Lassen Sie sich von unseren  
NDR Expert:innen beraten  
und profitieren Sie von den  
Vorteilen moderner Network  
Detection & Response Strategien mit Serviceware**

**Mehr erfahren**

## Integrierte Reaktionsmaßnahmen

Die Lösung verwendet patentierte MITRE D3FEND-Gegenmaßnahmen im Rahmen einer leistungsfähigen Response zur Eindämmung, Untersuchung und Behebung kompromittierter Systeme. Ihre Mitarbeitenden arbeiten konzentrierter, effizienter und effektiver, sodass es zu weniger Überlastung und Fluktuation kommt.



## Entdecken Sie die Vectra-Plattform

Die Vectra TDR-Plattform (Threat Detection and Response) bietet eine vollständige Abdeckung der Angriffsfläche für Public Cloud, SaaS, Identität und Netzwerk. Security AI-driven Attack Signal Intelligence bietet Ihnen absolut zuverlässige Bedrohungssignale und die volle Kontrolle bei der Abwehr moderner, hochentwickelter Cyber-Angreifer.

**Abdeckung:** Beseitigung unbekannter Bedrohungen für 4 von 5 Angriffsflächen – Cloud, SaaS, Identität und Netzwerk

**Hohe Signalqualität:** Nutzung von Attack Signal Intelligence zur automatischen Erkennung, Triage und Priorisierung unbekannter Bedrohungen

**Intelligente Kontrollen:** Unterstützung von Sicherheitsanalyst:innen bei der Suche, Untersuchung und Abwehr von unbekannten Bedrohungen

## Erweitern Sie Ihre Vectra NDR-Lösung mit folgenden anderen Lösungen:

**Vectra Match** ergänzt Vectra NDR mit Signaturkontext bei der Kompromittierungserkennung durch eine Kombination von Exploit-Erkennung (unterstützt durch Suricata) und KI-gestützter Erkennung, um Angreiferverhalten zu kontextualisieren.

**Vectra Recall** ermöglicht retrospektives Threat Hunting anhand angereicherter Netzwerk-Metadaten, die nach Host-Namen und IP-Adressen organisiert sind. Dank Cloud-gestützter grenzenloser Skalierung können Netzwerk-Metadaten so lange wie nötig gespeichert und durchsucht werden.

Mit **Vectra Stream** können Sie die mit Einblicken angereicherten Cloud- und Netzwerk-Metadaten direkt an SIEM-Lösungen und Data Lakes streamen, um eigene Modelle zu erstellen.

## Warum sich Unternehmen für Vectra NDR entscheiden

- Attack Signal Intelligence bietet zuverlässige Signale, mit denen Analyst:innen manuelle Aufgaben in Bezug auf Bedrohungserkennung, Triage und Priorisierung automatisieren können
- Es ist sichergestellt, dass Sie wissen, ob und wann Ihr Netzwerk kompromittiert wurde, und dass Sie für den Ernstfall bestens gewappnet sind
- Schnellere Bedrohungserkennungen durch erweiterte Abdeckung, kürzere Untersuchungszeiten und eine deutlich schnellere Mean Time to Repair (MTTR)
- Automatisierung manueller Aufgaben in Verbindung mit Tier-1- und Tier-2-Analysen, sodass die allgemeine Belastung des Security-Teams verringert wird
- Stoppen laufender Angriffe und mehr Zeit für Security-Analyst:innen, proaktives Threat Hunting sowie Recherchen durchzuführen
- Wegfall der Flut an False Positives und der dazugehörigen Aufgaben für Threat Hunting und Untersuchung, die ein höheres Risiko darstellen können
- Standortunabhängige Bereitstellung in physischen, virtuellen und Cloud-Umgebungen
- Nahtlose Integration in Cloud-Netzwerk, Firewall, XDR-Sicherheit und SIEM/SOAR

## Über Serviceware

Serviceware bietet seit mehr als 25 Jahren Software, Beratung und Managed Services zur Digitalisierung moderner Unternehmensprozesse. Von Enterprise Service Management über IT Financial Management bis Security, Data und Endpoint Management – hochautomatisiert und sicher.

### Serviceware SE

Serviceware-Kreisel 1  
65510 Idstein • Germany  
+49 6434 9450 0  
[contact@serviceware-se.com](mailto:contact@serviceware-se.com)  
[www.serviceware-se.com](http://www.serviceware-se.com)