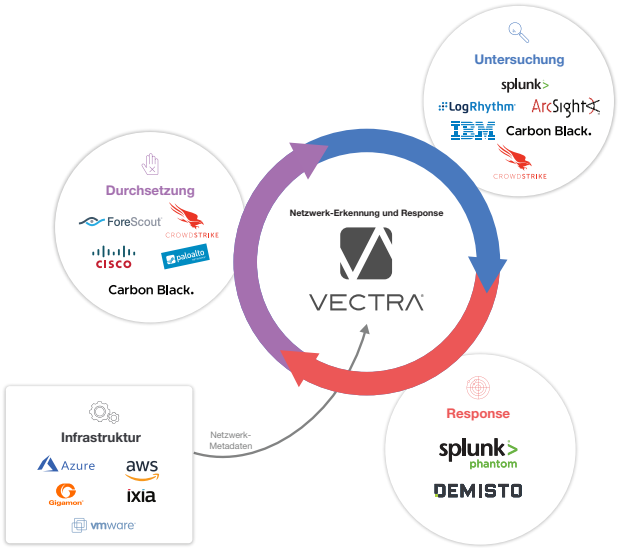
VECTRA®
Security that thinks®

Vectra ist ein weltweit führender Anbieter

bei der Nutzung künstlicher Intelligenz zur Erkennung und Reaktion auf hochentwickelte Cyber-Angriffe in Echtzeit.

Vectra® ist ein weltweit führendes Unternehmen im Bereich Netzwerk-Erkennung und Response. Die Cognito®-Plattform von Vectra revolutioniert die Netzwerksicherheit und ersetzt damit herkömmliche Technologien, die aktuellen Herausforderungen an Erkennung und Response nicht gewachsen sind. Dabei deckt die Cognito-Plattform Workloads in der Cloud und im Rechenzentrum ebenso wie Systeme für Endanwender und IoT-Geräte ab.



Die Cognito-Plattform

Die Cognito-Plattform beschleunigt die Erkennung und Untersuchung von Anwenderbedrohungen durch künstliche Intelligenz (KI), die dazu Netzwerk-Metadaten erfasst, speichert und mit relevanten Kontextdaten anreichert. So lassen sich bekannte und unbekannte Bedrohungen in Echtzeit erkennen und untersuchen.

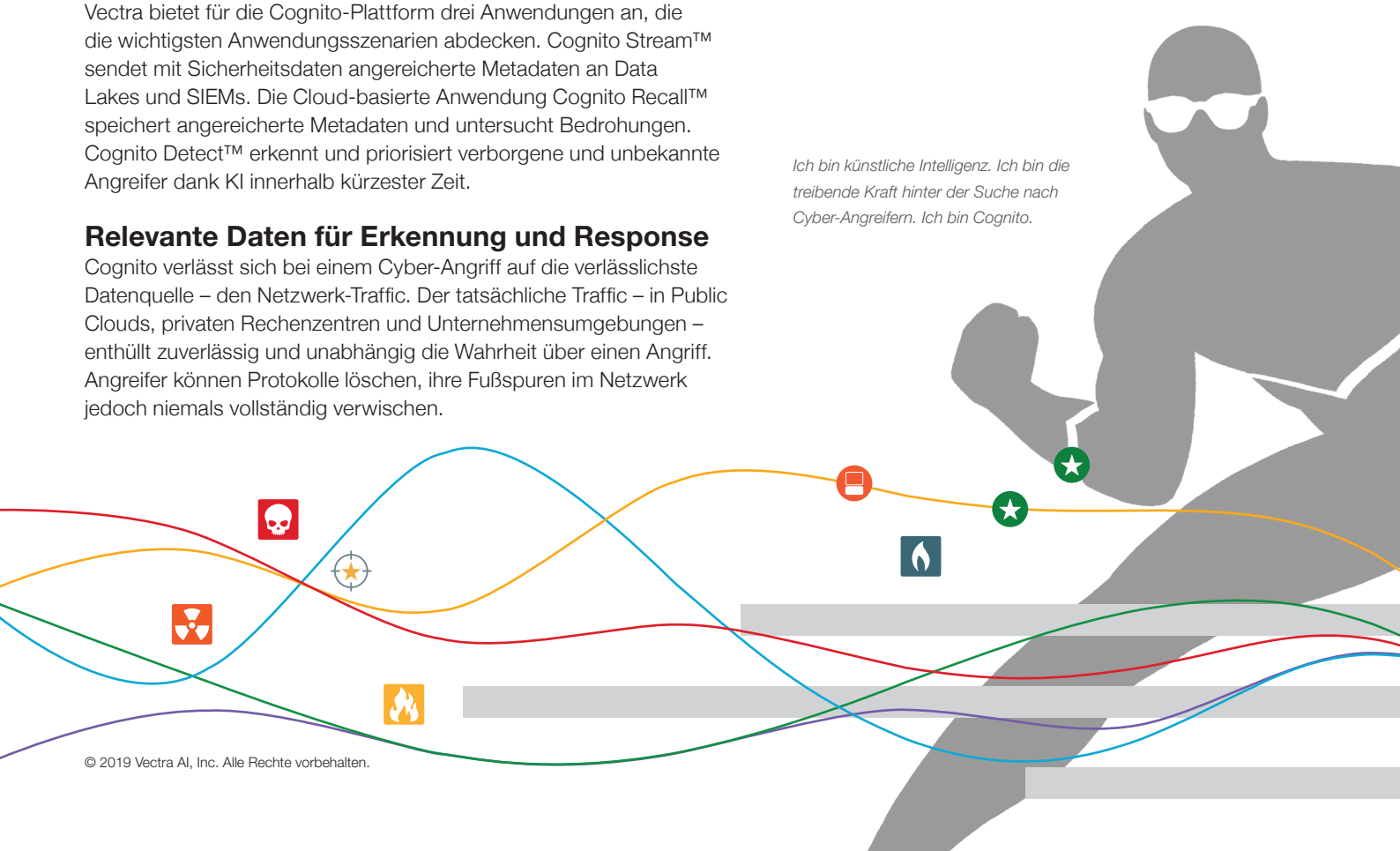
Dabei lässt sich die Cognito-Plattform auch für sehr große Unternehmensnetze mit einer verteilten Architektur effizient skalieren. Dazu unterstützt die Plattform verschiedenste Sensoren, die einen vollständigen Einblick in Cloud-, Rechenzentrum-, Anwender- und IoT-Infrastrukturen liefern.

Vectra bietet für die Cognito-Plattform drei Anwendungen an, die die wichtigsten Anwendungsszenarien abdecken. Cognito Stream™ sendet mit Sicherheitsdaten angereicherte Metadaten an Data Lakes und SIEMs. Die Cloud-basierte Anwendung Cognito Recall™ speichert angereicherte Metadaten und untersucht Bedrohungen. Cognito Detect™ erkennt und priorisiert verborgene und unbekannte Angreifer dank KI innerhalb kürzester Zeit.

Relevante Daten für Erkennung und Response

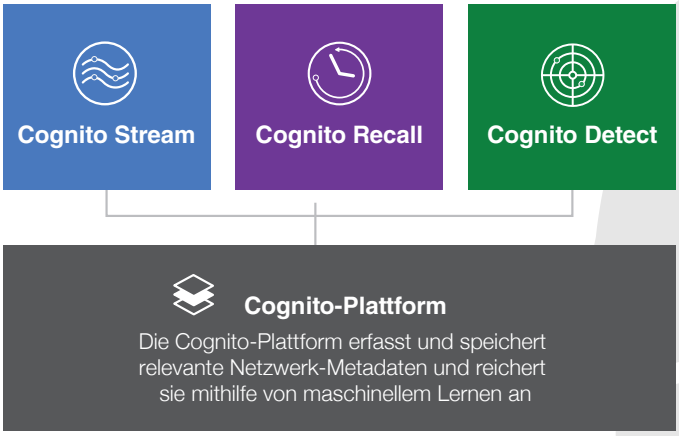
Cognito verlässt sich bei einem Cyber-Angriff auf die verlässlichste Datenquelle – den Netzwerk-Traffic. Der tatsächliche Traffic – in Public Clouds, privaten Rechenzentren und Unternehmensumgebungen – enthüllt zuverlässig und unabhängig die Wahrheit über einen Angriff. Angreifer können Protokolle löschen, ihre Fußspuren im Netzwerk jedoch niemals vollständig verwischen.

Ich bin künstliche Intelligenz. Ich bin die treibende Kraft hinter der Suche nach Cyber-Angreifern. Ich bin Cognito.



Cognito ist die ultimative Plattform für Erkennung und Response von Netzwerkbedrohungen

Ich liefere einen vollständigen Einblick in Ihre Cloud, IoT und Unternehmensnetzwerke, damit sich Angreifer nirgendwo verstecken können.



Cognito Stream: Netzwerk-Metadaten mit eigener Meinung

Sendet mit Sicherheitsdaten angereicherte Metadaten an einen Data Lake und das SIEM

Verwertbare Netzwerkdaten
Die Lösung extrahiert hunderte Metadaten-Attribute aus Netzwerk-Traffic-Rohdaten und präsentiert sie in einem kompakten, benutzerfreundlichen Zeek-Format, das vorhandene Software-Tools nutzt.

Eingebettete Sicherheitserkenntnisse
Durch maschinelles Lernen generierte Sicherheitserkenntnisse sind in die Metadaten eingebettet und können von spezialisierten Threat Huntern wie Bausteine zusammengesetzt und für schnelle Schlussfolgerungen genutzt werden.

Untersuchungen basierend auf Hosts und nicht IP-Adressen
Netzwerk-Metadaten werden automatisch mit anderen Attributen verknüpft, sodass Security-Analysten genaue Informationen zur Host-Identität erhalten und Hosts effizient untersuchen können – selbst dann, wenn sich die IP-Adresse ändert. Außerdem können auf diese Weise Beziehungen zwischen Host-Gruppen untersucht werden.

Cognito Recall: Für Untersuchungen und Threat Hunting konzipiert

Cloud-basierte Anwendung zur Speicherung und Untersuchung mit Sicherheitsdaten angereicherter Metadaten

Unterstützung für Threat Hunter
Durch die Echtzeit-Erfassung und Speicherung angereicherter Netzwerk-Metadaten, relevanter Protokolle und Cloud-Ereignisse können Threat Hunter detaillierte Erkenntnisse zu raffinierten Angriffen nutzen.

Intelligente Untersuchungen der Aktivitäten auf Geräten
Netzwerk-Metadaten werden Geräten (und nicht nur IP-Adressen) zugeordnet, sodass Sie sofort einen Überblick über die Aktivitäten auf Geräten über einen längeren Zeitraum erhalten – auch dann, wenn sich die IP-Adresse ändert.

Cloud-gestützte grenzenlose Skalierung
Threat Hunter können sich auf angereicherte Netzwerk-Metadaten verlassen, die entsprechend ihren Anforderungen gespeichert und durchsuchbar bleiben. Dabei verwaltet Vectra die Infrastruktur.

Cognito Detect: Die Vorteile der KI bei der Erkennung und Priorisierung

KI zur schnellen Aufdeckung verborgener und unbekannter Angreifer

KI-gestützte Bedrohungserkennung
Die permanent lernenden Verhaltensmodelle decken mithilfe von KI effizient verborgene und unbekannte Angreifer auf. Das ermöglicht schnelle und zielgerichtete Maßnahmen und liefert einen klaren Ausgangspunkt für Untersuchungen von Vorfällen.

Der richtige Kontext – sofort
Vermeidet endlose Suchen nach hoch entwickelten Cyber-Angriffen und ermöglicht sofortige Maßnahmen, da der relevanteste Kontext den Security-Analysten proaktiv zur Verfügung steht.

Verstärker für bestehende Sicherheitsinvestitionen
Integriert Endgeräte-Erkennung und Response, Netzwerk-zugriffskontrolle, Firewalls und andere Enforcement-Points, um neue Bedrohungsklassen zu blockieren und innerhalb von Cognito Recall, Data Lakes und SIEMs einen Ansatzpunkt für die Untersuchung von Vorfällen bereitzustellen.

Hier können Sie eine Demo anfordern: vectra.ai/demo

VECTRA®
Security that thinks®

E-Mail info_dach@vectra.ai **Tel.** +1 408 326 2020
vectra.ai