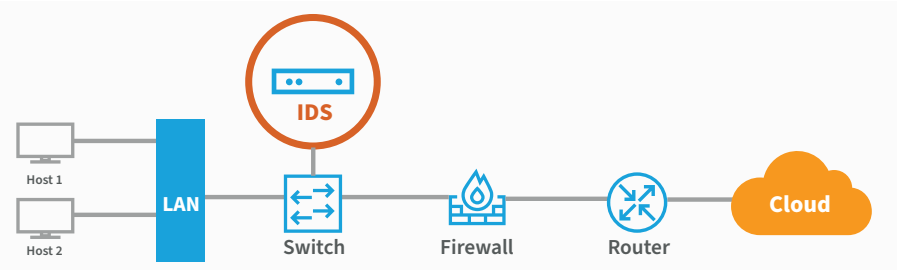
VECTRA
SECURITY THAT THINKS®

VERGLEICH MIT MITBEWERBERN

Verschleiert IPS der nächsten Generation ein altes Problem?

Bei Eindringungsschutzsystemen (Intrusion Detection System, IDS) wie Cisco Firepower (ehemals Sourcefire), Trend Micro Deep Discovery und McAfee Network Threat Behavior Analysis handelt es sich um herkömmliche Technologien, die stark auf signaturbasierte Erkennungs- und Schutzfunktionen setzen.

Diese Lösungen sind keine echte Konkurrenz für die Cognito®-Plattform für Netzwerk-Erkennung und Response von Vectra®, werden jedoch seit Kurzem als solche vermarktet. Hier erfahren Sie, warum diese IPS-Technologien hinter Cognito zurückbleiben.



Keine Verhaltenserkennung

Signaturbasierte Erkennungen und einfache Heuristiken erkennen nur bestimmte, bereits bekannte Angriffsmuster. Die meisten heutigen Angriffe – selbst die opportunistisch motivierten – wurden zumindest minimal angepasst, um den Wünschen des Angreifers so genau wie möglich zu entsprechen. Das haben wir in unserem Spotlight-Report zu Ransomware festgestellt.

Die Tage der „Spray-and-Pray"-Ansätze sind längst Geschichte. Stattdessen versuchen Angreifer mit gezielten Attacken, die Wahrscheinlichkeit des Erfolgs zu steigern. Wenn Sie sich zum Schutz Ihres Netzwerks allein auf IDS verlassen, ist das so, als ob Sie noch eine kostenlose Testversion des Kaspersky-Virenschutzes aus den frühen 2000ern nutzen und sich wundern, wenn Sie im Jahr 2020 infiziert werden.

97 %

Die Cognito NDR-Plattform unterstützt mehr als 97 % des MITRE ATT&CK-Frameworks

Für ältere Sicherheitsmodelle konzipiert

Heute setzen immer mehr Unternehmen auf ein Zero-Trust-Modell, weil veraltete IDS-Systeme sich auf die Absicherung des lokalen Außen-Perimeters konzentrieren und nur den Traffic sehen, der über die Firewall übertragen wird.

Wenn Angreifer das interne Netzwerk kompromittieren, können sie sich frei lateral bewegen, ohne dass das IDS dies feststellen kann. Genau genommen wird das IDS lediglich bemerken, dass die Firewall-Leistung nachlässt, da die übertragenen Pakete per Heuristik untersucht werden müssen.

Hinzu kommt, dass Unternehmen heute in der Cloud ebenso viel Traffic generieren wie im internen Netzwerk. Da sich IDS auf den im Netzwerk eingehenden Traffic konzentriert, bleiben Angreifer, die auf kompromittierte Cloud-Service-Konten zugreifen können, vollständig unbemerkt.

Die Cognito-Plattform kann in allen Bereichen des Netzwerks bereitgestellt werden (einschließlich Multi-Cloud-Umgebungen), sodass Security-Analysten einen vollständigen Überblick über alle Assets des Unternehmens erhalten – unabhängig von deren Standort.

Zudem unterstützt die Cognito-Plattform durch Privileged Access Analytics (PAA) auch Zero-Trust-Initiativen. Mit PAA können Sie die Kontonutzung in Ihrem Netzwerk unterbinden und interne Bedrohungsakteure identifizieren, die für ihre Angriffe kompromittierte Anmeldedaten verwenden.

Vorbereitung auf unzählige Meldungen über Anomalien

Als anomaliebasiertes Erkennungssystem ist IDS nicht in der Lage, die schwerwiegendsten Bedrohungen zu identifizieren, sodass Ihr Security-Team mit Warnmeldungen überflutet wird, die manuell und einzeln triagiert werden müssen. Das bedeutet zusätzliche Arbeit für Ihr bereits überlastetes Team.

Beim Einsatz gegen menschliche Attacken statt per Simulation ausgelöster Angriffe schneiden die Cognito-Algorithmusmodelle besser ab als einfache signatur- oder heustikbasierte Erkennungen. Fakt ist: Die Cognito-Plattform unterstützt mehr als 97 % des MITRE ATT&CK-Frameworks.

Die hervorragenden Erkennungsfunktionen zeigen bei einem Proof-of-Concept schnell ihre Vorteile.

Gleichzeitig reduziert Cognito die Belastung durch Sicherheitsprozesse um das 38-fache, indem Warnmeldungen zu Zwischenfällen automatisch triagiert, Host-Geräte mit den größten Risiken priorisiert und für Untersuchungen und Forensik aus dem gesamten Netzwerk-Traffic mit Sicherheitsdaten angereicherte Metadaten extrahiert werden.

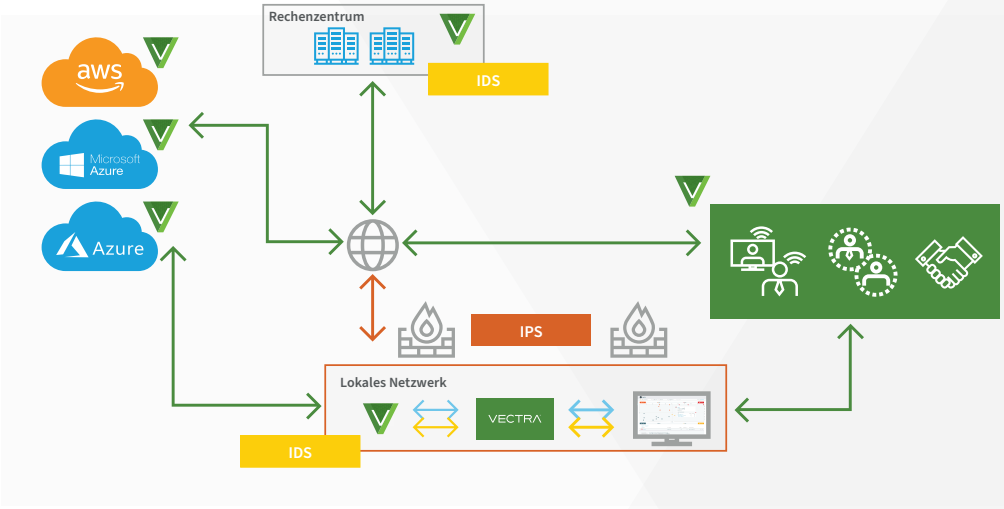
Bindung an einen Anbieter verhindert Nutzung der besten Lösung

IDS ist meist Bestandteil einer breiter aufgestellten Plattform und daher nicht eigenständig einsetzbar. Stattdessen sind zusätzliche Investitionen in Firewalls, URL-Filterung, Tools zur Anwendungsüberwachung, erweiterte Angriffserkennung uvm. erforderlich. Damit alle Bestandteile integriert werden, müssen Sie sie beim gleichen Anbieter kaufen.

Die Cognito-Plattform integriert sich hingegen problemlos per APIs mit Ihren bestehenden Sicherheitstechnologien. Unser Ökosystem aus Technologiepartnern umfasst Branchenführer für Endgeräte-Erkennung und Response, Firewalls der nächsten Generation, SIEMs, Sicherheitsorchestrierung und Netzwerkzugriffskontrolle. Die Cognito-Integrationen unterstützen erstklassige Sicherheitsstrategien und sorgen dafür, dass Ihre vorhandenen Investitionen dauerhaft Mehrwert bieten.

E-Mail: info_dach@vectra.ai vectra.ai/de

Version: **081720**



Die Zukunft von IDS

Die Cognito-Plattform von Vectra bietet im Vergleich mit IDS der nächsten Generation zahlreiche Vorteile:

- **Erkennt moderne, reale Angriffe** mithilfe überwachter und nicht überwachter Algorithmen für maschinelles Lernen.
- **Bietet vollständige Transparenz** vom Unternehmensnetzwerk bis zur Cloud, nicht nur über die Daten, die über eine Firewall übertragen werden.
- **Reduziert die Belastung Ihres Sicherheitsteams** um das 38-fache. Cognito triagiert Angriffserkennungen, um priorisierte Zwischenfälle herauszustellen und die sinnvollsten Response-Maßnahmen deutlich zu beschleunigen.
- **Echte Hochleistungsplattform**, die sich mit Ihren anderen Sicherheitstechnologien integriert.

Weitere Informationen erhalten Sie von unseren Servicemitarbeitern unter sales-inquiries@vectra.ai.