illumio

SOLUTION BRIEF

KI-gestützte Segmentierung von Illumio

Cyberresilienz vereinfachen und Angriffe schneller eindämmen mit dem Illumio Virtual Advisor (IVA) und KI-Labeling

Die größte Cyber-Herausforderung: effizienter arbeiten

Laut Forrester werden 47 % der Zero-Trust-Projekte nie zu Ende geführt, weil die richtigen Fachkräfte fehlen. Selbst stark aufgestellte Security-Teams haben ihre Probleme beim Segmentieren mit herkömmlichen Tools – es ist einfach zu viel Aufwand.

Und es gibt noch weitere Hindernisse: Viele Teams verwenden CMDBs (Configuration Management Databases), die sich nur mühsam einrichten und aktuell halten lassen, und Cloud- und Datacenter-Umgebungen ändern sich ständig.

In hybriden oder Multi-Cloud-Setups ist es auch schwierig, auf Bedrohungen zu reagieren. Tools wie Data Lakes und SIEMs sind häufig langsam und kompliziert in der Anwendung.

Wenn Sie keinen vollen Einblick in Ihre Systeme haben, ist es fast unmöglich, schnell genug klare Informationen zu erhalten, um Angreifer zu stoppen, bevor sie sich ausbreiten.

Deshalb ist der Fachkräftemangel in der Cybersecurity ein so großes Problem. Viele Team sind unterbesetzt und haben auch gar nicht die nötigen Spezialkenntnisse, um Angriffe abzuwehren. All das stellt ein großes Risiko für Organisationen dar.

Was wäre die Lösung? Security-Teams brauchen Tools, die ihnen die Arbeit erleichtern und Echtzeitdaten liefern, damit sie ihre Organisation trotz eingeschränkter Ressourcen besser schützen können.

Mit dem richtigen Produkt lassen sich Fachkräftelücken kompensieren und Angriffe stoppen – unabhängig davon, woher sie kommen.

Wichtigste Vorteile

Schnellere Eindämmung
Aussagekräftige Informationen vereinfachen die Segmentierung und reduzieren das Risiko – keine technische Erfahrung nötig.

Einfache, konsistente Sicherheitsmaßnahmen
Security-Policies für hybride Multi-Cloud-Umgebungen lassen sich ganz leicht erstellen – mit automatisierten Aufgaben, wenig manuellem Aufwand und minimaler Fehlerwahrscheinlichkeit.

Entlastung des Betriebs
Überlastete Security-Teams brauch viel weniger Zeit, um die Segmentierung umzusetzen und zu verwalten.

Die Lösung: KI-gestützte Segmentierung

Workloads zu kennzeichnen und Security-Policies festzulegen, geht mit der KI-gestützten Segmentierung von Illumio schneller und leichter.

Durch Einsatz leistungsstarker KI für die Segmentierung hilft Illumio, die Bereitstellung zu beschleunigen, bessere Segmentierungsregeln zu erstellen und Angriffe schneller einzudämmen. So ist Ihr Team für jede Bedrohung bestens gewappnet, auch mit wenig Security-Fachwissen.

Die wichtigsten Funktionen

Illumio Virtual Advisor (IVA)

Der „virtuelle Berater“ von Illumio (IVA) liefert praktische, KI-gestützte Anleitungen selbst für komplexe Aufgaben.

Er sorgt für optimierte Workflows, weil die Teams sofort fachkundige Antworten auf ihre Fragen erhalten. Auf diesem Weg können sie schnell kritische Informationen abrufen oder sich Hilfestellung bei komplexen Tätigkeiten holen.

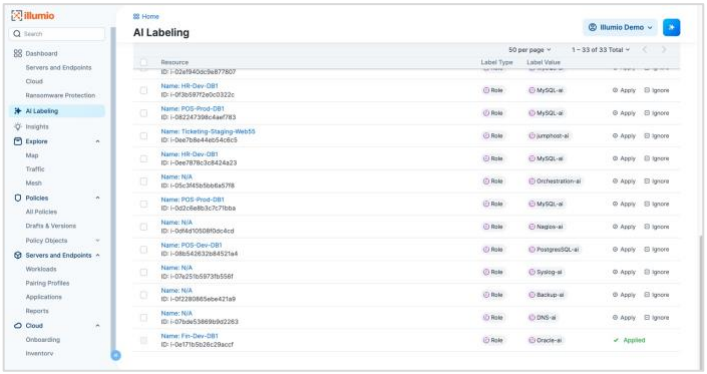
Gerade für unterbesetzte Teams mit wenig Zeit kann der IVA eine spürbare Entlastung bringen, weil er den manuellen Aufwand reduziert.

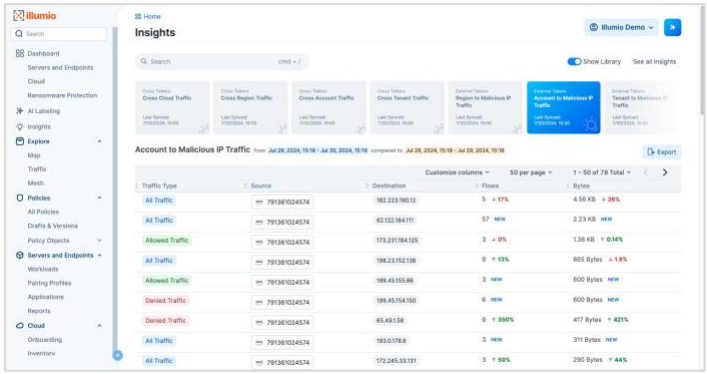
KI-Labeling

Mithilfe von maschinellem Lernen automatisiert das KI-Labeling eine komplizierte Tätigkeit: das Kennzeichnen von Workloads auf Grundlage von Metadaten und Flow Logs.

Diese Automatisierung bedeutet eine erhebliche Zeitersparnis.

Mit der Gewissheit, dass alle Labels korrekt und einheitlich sind, kann sich Ihr Team auf strategischere Aufgaben konzentrieren. So lassen sich Deployments beschleunigen und unbeständige hybride Multi-Cloud-Umgebungen leichter verwalten.





Effizienter arbeiten mit der KI-gestützten Segmentierung von Illumio

Wenden Sie sich an uns, um mehr zu erfahren: illumio.com/de/contact

Über Illumio

Illumio, die umfangreichste Zero-Trust-Lösung für Ransomware- und Breach-Containment, schützt Organisationen vor Cyberkatastrophen und Betriebsstörungen, ohne die Komplexität zu erhöhen. Die Illumio-Plattform visualisiert Datenflüsse und legt automatisch Policies für die Segmentierung fest, um unnötigen lateralen Datenverkehr in Multi-Cloud- und Hybrid-Infrastrukturen zu vermeiden – damit kritische Ressourcen geschützt werden und Cyberangreifer sich nicht ausbreiten können.