illumio

PRODUKTBESCHREIBUNG

Illumio CloudSecure

Segmentierung für Anwendungen und Workloads in der öffentlichen Cloud

Cloud-Sicherheit ist besonders

Das Volumen und die Geschwindigkeit der Anwendungen und Workloads, die in die Cloud verlagert werden, wächst kontinuierlich – ebenso wie die damit verbundenen Sicherheitsherausforderungen. So bestätigen in der Tat 94 Prozent der IT-Sicherheitsverantwortlichen, dass die Konnektivität zwischen ihren Cloud-Diensten und anderen Umgebungen die Wahrscheinlichkeit eines Sicherheitsvorfalls erhöht.
In sich schnell verändernden Cloud-Umgebungen sehen sich Sicherheitsteams mit verschiedenen Schwierigkeiten konfrontiert:

- **Trotz Vorbeugung bleiben Sicherheitsvorfälle weiterhin unerkannt:**
  Wenn es Angreifern gelingt, die präventiven Maßnahmen zu unterlaufen und sanktionierte Anwendungen und Systeme zu kompromittieren, können sie sich problemlos und unauffällig durch weitere Kanäle seitwärts bewegen, die ihnen offen stehen.
- **In der Cloud ist es schwieriger, das Eindämmen von Sicherheitsverstößen zu priorisieren:** In sich ständig verändernden Cloud-Umgebungen können Anwendungen, die möglicherweise nur für den Einsatz weniger Stunden hoch- und wieder heruntergefahren werden, aus dem Fokus der Sicherheit geraten.
- **Lateral Movement ist in der Cloud einfacher:** Hybride und Multi-Cloud-Umgebungen, die dezentralisierte Bereitstellung von Anwendungen und die Streuung von Workloads können den Angreifern das Bewegen im Netzwerk erleichtern.

Eindämmung von Sicherheitsvorfällen in der Cloud

Illumio CloudSecure erweitert die Zero-Trust-Segmentierung (ZTS) auf Ihre Cloud-Anwendungen und -Workloads.

Forrester Research hat festgestellt, dass Illumio ZTS die Auswirkungen bzw. den Detonationsradius eines Sicherheitsvorfalls um 66 Prozent reduziert. Damit kann es unautorisierte Bewegungen innerhalb einer Cloud-Infrastruktur verhindern, ohne die SecOps-Teams zusätzlich zu belasten, und den operativen Aufwand um 90 Prozent verringern.

Wichtigste Vorteile durch das Isolieren von Angriffen in der Cloud

Visualisierung der Konnektivität von Cloud-Workloads

Zusätzliche Transparenz durch eine interaktive Karte zur Abbildung von Anwendungen, Ressourcen, Netzwerkverkehr und Metadaten.

Proaktive Segmentierung

Erstellen und implementieren Sie Ihre Segmente mithilfe von Labels und IP-Listen, um vertrauenswürdige Kommunikation zwischen Anwendungen zu etablieren.

Angriffe isolieren

Anpassen von Segmentierungs-Policies in dynamischen, sich ständig ändernden Umgebungen.

Kritische Funktionalität

Eine einheitliche Ansicht aller Cloud-Umgebungen

Illumio CloudSecure bietet eine umfassende Karte des Netzwerkverkehrs in Multi-Cloud-Umgebungen mit Visualisierung von Anwendungen, Daten und Cloud-Workloads – ganz ohne einen Agenten. Verschaffen Sie sich einen umfassenden Überblick über die Konnektivität von Anwendungen und Workloads sowie über kontextbasierte Labels und Objekt-Metadaten.

Mithilfe der Visualisierung können Ihre Sicherheitsteams überflüssige Konnektivität entdecken, die das Risiko erhöhen. Es kategorisiert darüber hinaus Test- und Produktions-Workloads und erlaubt Einblicke um wirksame Policies zu erstellen.

Mit Illumio CloudSecure wissen Sie zu jeder Zeit, ob ein Angriff droht oder bereits im Gange ist.

Schnelle, faktenbasierte Entscheidungen

Illumio CloudSecure identifiziert unnötig offene Kommunikation zwischen Anwendungen und Workloads in Multi-Cloud-Umgebungen. Detaillierte kontextbasierte Labels von Objekten helfen den Teams bei der Erstellung von Policies zwischen komplexen Anwendungen oder Microservices.

Teams können schneller und faktenbasiert darüber entscheiden, welcher Datenverkehr segmentiert werden soll. Dies ermöglicht ihnen, proaktiv einen starken Sicherheitsstatus aufrechtzuerhalten oder reaktiv eine Sicherheitsvorfall zu isolieren.

Eindämmen des Detonationsradius

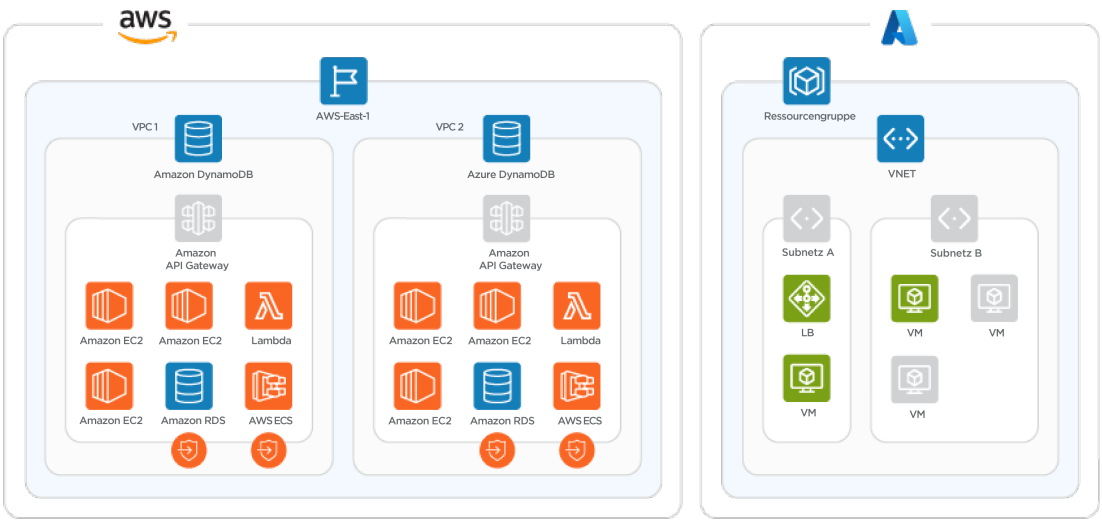
Wenn ein Sicherheitsvorfall auftritt, muss er so schnell wie möglich aufgehalten und isoliert werden. Mit Illumio CloudSecure können Sie die Zero-Trust-Segmentierung in Cloud-Umgebungen implementieren, um sich proaktiv auf Sicherheitsverstöße vorzubereiten oder sie reaktiv einzudämmen.

Im Zuge eines Sicherheitsvorfalls können Sie die Konnektivität zwischen Anwendungen und Workloads schnell und mit detaillierten Ressourcenbeschreibungen visualisieren. Machen Sie die Konnektivität zwischen Cloud-Anwendungen und -Ressourcen sichtbar, die den Angreifern freie Fahrt im Netzwerk ermöglichen. Passen Sie Ihre Policy an, um Seitwärtsbewegungen zu stoppen, Angriffe abzuwehren, Anwendungen zu schützen und das Ausmaß des Schadens zu begrenzen.

Illumio CloudSecure hilft Teams dabei, sich proaktiv gegen Sicherheitsvorfälle zu wappnen, indem es sie bei der Planung und Optimierung von Regeln unterstützt. So können sie die Angriffsoberfläche verkleinern und Programme mithilfe cloud-nativer Tools sichern.

Testen Sie Illumio CloudSecure kostenlos für 30 Tage.

Starten Sie jetzt unter illumio.com/de/clousecure-free-trial



About Illumio

Illumio, the Zero Trust Segmentation company, stops breaches and ransomware from spreading across the hybrid attack surface. The Illumio ZTS Platform visualizes all traffic flows between workloads, devices, and the internet, automatically sets granular segmentation policies to control communications, and isolates high-value assets and compromised systems proactively or in response to active attacks. Illumio protects organizations of all sizes, from Fortune 100 to small business, by stopping breaches and ransomware in minutes, saving millions of dollars in application downtime, and accelerating cloud and digital transformation projects.