

Posture Control: Umfassende CNAPP für AWS



Herausforderungen Sicherheitsverantwortung, Sicherheitsaufsicht

Aktuelle Abläufe in der Anwendungsentwicklung und die Einführung Cloud-nativer Architekturen haben das Innovationstempo drastisch erhöht. Unternehmen führen zeitgemäße Verfahren ein und verlagern geschäftsrelevante Daten, Anwendungen und Geschäftsprozesse zunehmend auf AWS. Dabei müssen sie sich um die Absicherung der dadurch vergrößerten Angriffsfläche, die Abwehr von Sicherheitsrisiken und Gefahrenquellen sowie die Automatisierung manueller Sicherheitsprozesse mithilfe von Echtzeitmaßnahmen und Risikominimierung kümmern. Gleichzeitig müssen sie für eine konsequente Durchsetzung der Compliance-Richtlinien und entsprechendem Reporting sowie Senkung von Kosten und Komplexität sorgen.



Posture Control von Zscaler Für sichere Cloud-native Apps.

Posture Control, eine Cloud Native Application Protection Platform (CNAPP), basiert auf den Zero-Trust-Prinzipien und vereinfacht AWS-Sicherheitsabläufe komplett agentenlos. So können Risiken der Infrastruktur- und Anwendungssicherheit in hochdynamischen AWS-Umgebungen sowie in Entwicklung und DevOps erkannt, priorisiert und behoben werden. Posture Control deckt Risiken dabei mithilfe einer erweiterten Risikokorrelation auf und optimiert Ermittlungen und Reaktionszeiten durch kontextualisierte, priorisierte und praxisnahe Analysen. Insgesamt wird auf diese Weise eine agile, sichere AWS-Infrastruktur geschaffen, die Innovationen begünstigt und zugleich Komplexität, Konfliktpotenziale und Gemeinkosten reduziert, ohne die Sicherheit zu beeinträchtigen.

Vorteile

Verschaffen Sie sich mit der integrierten Posture Control einen lückenlosen Überblick über Ihre Sicherheitslage in Sachen AWS.



Lückenlose Abdeckung

- Komplette agentenlose Verfahren mit lückenloser
- Abdeckung. Keine Transparenzlücken oder
- Zuständigkeitskonflikte.



Die wichtigsten Risiken zuerst

- Erkennen, priorisieren und beheben Sie
- gravierende Risiken mithilfe einer ausgeklügelten
- Risikokorrelation für ein noch effizienteres SOC.



Weniger Komplexität

- Kombination leistungsstarker Sicherheitstools
- für weniger Komplexität, Kosten und
- Verwaltungsaufwand



Durchgehende Sicherheit

- Binden Sie Sicherheitsbelange in DevOps-
- Abläufe ein und erkennen und beheben Sie
- Sicherheitslücken, bevor sie zum Problem werden

Zscaler für AWS

Für mehr Agilität unterstützt AWS Cloud-Architekten beim Aufbau leistungsstarker, belastbarer und effizienter Anwendungsinfrastrukturen. Der Preis dafür ist die Aufteilung der Verantwortung innerhalb der AWS-Umgebung. Die meisten Unternehmen verlassen sich dabei auf mehrere Lösungen, um Sicherheitsbedenken auszuräumen. Doch die können mit dem hohen Innovationstempo kaum Schritt halten und führen zu Sicherheitslücken, Silos und erhöhter Komplexität, was wiederum die Sicherung von AWS-Umgebungen erschwert. Gemeinsam unterstützen Zscaler und AWS Unternehmen mit einem gemeinsamen Ansatz, der die allgemeine Sicherheitslage verbessert und gleichzeitig die geschäftliche Agilität erhöht.

Funktionen

Umfassende Transparenz und Kontrolle



Posture Control steht für erhöhte Cloud-native Sicherheit. Dabei werden Tools wie CSPM, DLP, CIEM, IaC, VM und CWPP zu einer einheitlichen Plattform gebündelt. Der agentenlose Ansatz sorgt für Transparenz, ermittelt die folgenschwersten Risiken und setzt geltende Sicherheits- und Compliance-Richtlinien durch. Die erweiterte Bedrohungskorrelation geht über das herkömmliche Analysemodell hinaus, um versteckte Risiken aufzudecken und Teams in die Lage zu versetzen, kritische Risiken, die zu Kompromittierungen oder Verstößen führen könnten, sichtbar zu machen, zu analysieren und zu beheben.

Sicherheit ohne Konflikte



Das Thema Sicherheit wird bei Dev und DevOps oft als Hemmnis angesehen. Doch mit Posture Control werden Sicherheitsbelange zum Katalysator für eine sichere Entwicklung und Bereitstellung. Posture Control lässt sich nahtlos in DevOps und Sicherheitstools integrieren, um kritische Risiken mithilfe von Warnungen, Sicherheitsmechanismen und geführten Gegenmaßnahmen zu erkennen, zu priorisieren und zu bewältigen. Für einheitliche Sicherheit in allen AWS-Umgebungen und skalierte Compliance. Funktionsübergreifende Teams können so unvorhergesehene Risiken reduzieren und die Entwicklungszyklen verkürzen.

Kundenbeispiel: Jefferson Health



Herausforderungen

Als eines der wachstumsstärksten Gesundheitssysteme in den USA verordnete sich Jefferson Health eine Cloud-First-Strategie, um die Patientenversorgung und die Erfüllung seiner Geschäftsziele zu gewährleisten. Dies erforderte allerdings auch die Modernisierung des Cybersicherheitskonzepts.

Lösung

Glücklicherweise sorgte Zscaler für durchgehende Transparenz in Sachen Sicherheit, Compliance und Risikoexposition. Mithilfe von Richtlinien, Ausnahmen und der Integration in andere IT- und Risikomanagementlösungen wurde so die Sicherheit cloudübergreifend auch in AWS gewährleistet.

Ergebnisse

Mit Zscaler konnte Jefferson Health sein Risiko in der stark regulierten Gesundheitsbranche senken und gleichzeitig die interne Zusammenarbeit verbessern. So wurde der Compliance-Score in den ersten vier Wochen verdoppelt und ein hoher Mehrwert durch Reporting und Monitoring erzielt. Und dafür waren nur minimale Ressourcen des Sicherheitsteams erforderlich.



Über Zscaler

Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, resilienter und sicherer arbeiten können. Zscaler Zero Trust Exchange schützt Tausende Kunden mittels sicherer Verbindungen zwischen Benutzern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlust. Die SASE-basierte Zero Trust Exchange ist in über 150 Rechenzentren auf der ganzen Welt verfügbar und die weltweit größte Inline-Cloud-Sicherheitsplattform. Informieren Sie sich auf [zscaler.de](https://www.zscaler.de) oder folgen Sie uns auf Twitter unter [@zscaler](https://twitter.com/zscaler).

©2023 Zscaler, Inc. Alle Rechte vorbehalten. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™, Zscaler Digital Experience™ und ZDX™ sind (i) eingetragene Warenzeichen bzw. Dienstleistungsmarken oder (ii) Warenzeichen bzw. Dienstleistungsmarken von Zscaler, Inc. in den Vereinigten Staaten und/oder anderen Ländern. Alle anderen Warenzeichen sind Eigentum ihrer jeweiligen Inhaber.