Zscaler™ Cloud Protection auf einen Blick

Zscaler Cloud Protection (ZCP) – Vorteile:

Sichere Cloud Security Posture

Laufende Inventarisierung und Fehlerbehebung für alle Services in Cloud-Plattformen (Azure, AWS, GCP) und SaaS-Applikationen

Sicherer User-Zugriff auf Cloud-Workloads

Zero Trust ermöglicht User-Zugriff ohne exponierte Angriffsflächen und VPNs

Sichere App-zu-App-Kommunikation

Sichert und vereinfacht die Workload-Kommunikation mit dem Internet, mit Rechenzentren und zwischen Clouds

Keine laterale Ausbreitung von Bedrohungen

App-Identitätsverwaltung und ML-Automatisierung vereinfachen die Mikrosegmentierung und verhindern die laterale Ausbreitung von Bedrohungen

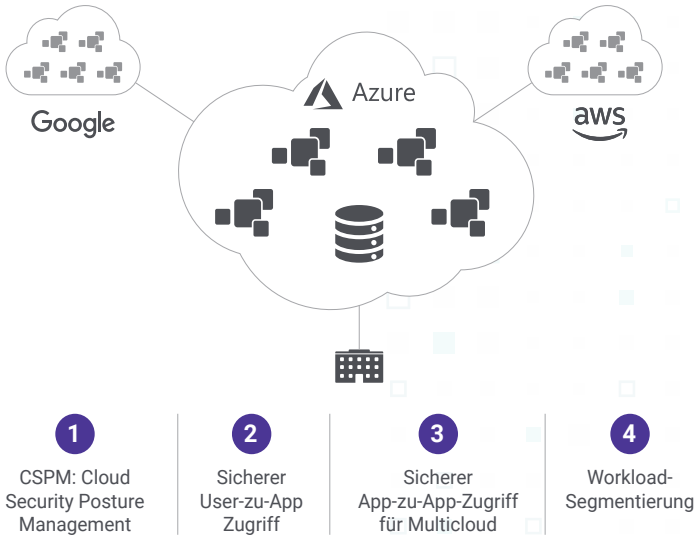
Cloud-Computing beschleunigt branchenübergreifend die digitale Transformation und erschließt völlig neue Möglichkeiten in Bezug auf Skalierung, Performance und Agilität für unternehmensfähige Cloud-Anwendungen. Leider bringen die Faktoren, die Agilität und Skalierbarkeit begünstigen, als unerwünschte Nebeneffekte Sicherheitsrisiken und Datenschutzverletzungen mit sich.

Der „Lift-and-Shift"-Ansatz, bei dem Sicherheitslösungen aus der Ära der Rechenzentren an Public-Cloud-Umgebungen angepasst werden, ist kostspielig, kompliziert und statisch. InfoSec-Teams haben so keine Chance, mit dem Tempo der DevOps bei Entwicklung und Deployment Schritt zu halten.

ZCP baut auf der Architektur des Zero Trust Exchange von Zscaler auf und mindert nicht nur das mit der Cloud-Migration verbundene Risiko, sondern auch die operative Komplexität. Die vier Kerneigenschaften von ZCP zielen auf die größten Herausforderungen in puncto Sicherheit und operative Effizienz ab, die beim sicheren Cloud-Deployment zu bewältigen sind:

- Identifizierung von Workloads in der Cloud und Gewährleistung einer starken Security Posture
- Sicherer Anwendungszugriff ausschließlich für befugte User
- Sicherer Zugriff für Workloads auf andere Clouds, Rechenzentren und das Internet
- Minderung von Angriffsrisiken durch Verhinderung lateraler Bewegungen

Die vier Kerneigenschaften von ZCP



Zscaler Cloud Protection – Kernfunktionen

Cloud Security Posture Management in der Cloud

- Inventarisierung, laufende Überprüfung und automatische Fehlerbehebung für alle Cloud-Services von IaaS und PaaS über Container bis hin zu serverlos u.v.m.
- Mehrschichtige Absicherung für AWS, Azure, GCP und SaaS mit über 3.000 vorgefertigten Policy-Vorlagen und Zuordnung zu 16 wichtigen Compliance-Frameworks

Sicherer User-zu-App-Zugriff

- Zugriffssteuerung nach dem „Zero Trust"-Prinzip gewährt Zugriff auf einzelne Anwendungen statt auf das gesamte Netzwerk, sodass sich potenzielle externe Bedrohungen ohne die Komplexitäten, negativen User Experience und exponierten Angriffsflächen herkömmlicher VPNs abwehren lassen

Sichere Cloud-übergreifende App-zu-App-Kommunikation

- Bereitstellung von Konfiguration von Cloud-zu-Cloud- und Cloud-zu-DC-Konnektivität ohne aufwendige und kostspielige Verwaltung von Transit-Gateways, Transit-Hubs, virtuellen Firewalls, VPNs, Router, Netzwerk-Policies und Peering
- Sicherer, kontrollierter Cloud-zu-Internet-Zugriff ohne exponierte Angriffsflächen mit der praxisbewährten Skalierbarkeit, Performance und Zuverlässigkeit des Zero Trust Exchange

Identitätsbasierte Mikrosegmentierung

- Geringere Angriffsfläche und Verhinderung der Ausbreitung von Malware durch identitätsbasierte Mikrosegmentierung von Cloud- und DC-Workloads
- Reduziert den Policy-Umfang um 90 Prozent oder mehr

„Fast alle erfolgreichen Angriffe auf Cloud-Services resultieren aus Fehlkonfigurationen, unsachgemäßer Verwaltung und anderen Fehlern seitens des Kunden."

– Gartner

Weitere Informationen über die Vorteile von Zscaler Cloud Protection finden Sie unter **zscaler.com/ZCP** >

Zscaler, Inc.
120 Holger Way
San Jose, CA
+1 408 533 0288
www.zscaler.com