AKAMAI-LÖSUNGSÜBERBLICK

Segmentierung für Nutzer-IAM (Identity and Access Management)

Eine zusätzliche kritische Kontrollebene für moderne Hybrid-Rechenzentren

Bei der Verringerung der Angriffsfläche moderner IT-Umgebungen geht es nicht nur darum, strenge Kontrollen für bestimmte Anwendungen zu erstellen und diese vor Schäden zu schützen. Das ist zwar ein großartiger erster Schritt und kann sicherlich bei einigen Anwendungsfällen wie der Eindämmung von Angriffen oder der Compliance hilfreich sein. Doch ohne eine Segmentierungslösung, die Nutzer-IAM (Identity and Access Management) unterstützt, verfügt Ihr Unternehmen über einen „toten Winkel“, der jede einzelne Person umfasst, die Ihr Netzwerk nutzt oder betritt.

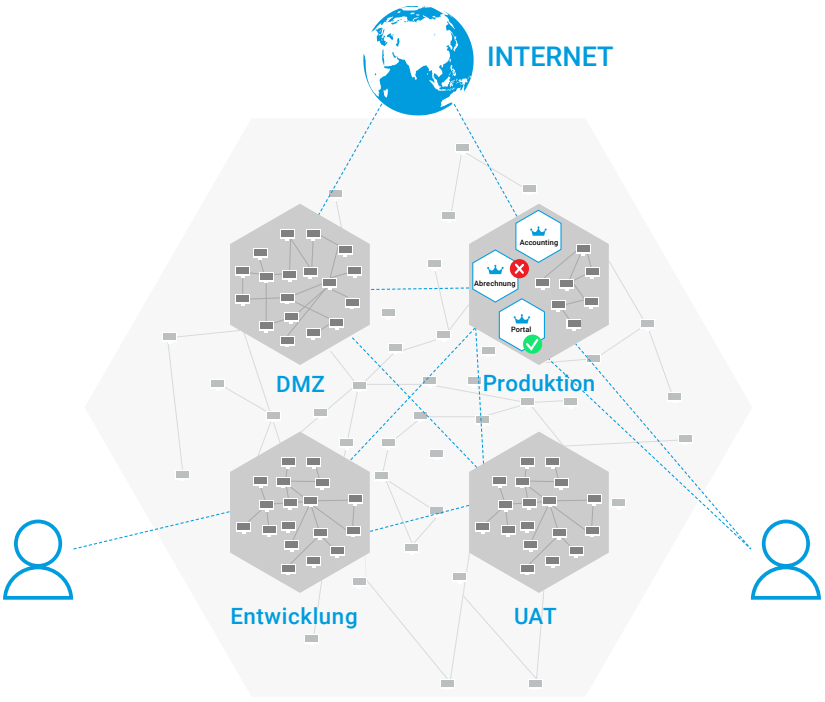
Sobald die Anwendungssegmentierung implementiert ist, besteht der nächste wichtige Schritt darin, mithilfe Ihrer Segmentierungslösung Richtlinien zu erstellen, die festlegen, wer auf diese Anwendungen zugreifen kann. So wird sichergestellt, dass diese in jeder beliebigen Netzwerkarchitektur optimal geschützt sind.

Anwendungsfälle: Segmentierung für Nutzeridentitätszugriff

Verwaltung des Nutzerzugriffs

Mithilfe einer Active-Directory-Nutzergruppe kann Akamai Guardicore Segmentation den Nutzerzugriff auf beliebige Anwendungen oder Workloads in jeder Umgebung kontrollieren. Bestimmte Nutzergruppen erhalten über bestimmte Ports oder Prozesse Zugriff auf bestimmte Server, andere wiederum nicht. Nutzergruppen verfügen über eigene Berechtigungen, während alle anderen Zugriffsrechte gesperrt werden können. Da keine zentrale Firewall erforderlich ist, können Sie eine präzise Zugriffskontrolle zwischen Workloads in bestimmten Segmenten des Netzwerks einsetzen.

Nutzerzugriffskontrolle



Warum Segmentierung für die Nutzerzugriffskontrolle?

Kontrolle des Nutzerzugriffs – überall
Richtlinien funktionieren auf Laptops, Desktops, in VDIs, auf virtuellen oder Bare-Metal-Servern sowie in der Cloud-Infrastruktur.

Softwaredefinierte Segmentierung
Keine Netzwerk- oder Architekturänderungen, keine Kabel, keine Serverausfallzeiten und kein Neustart der Systeme.

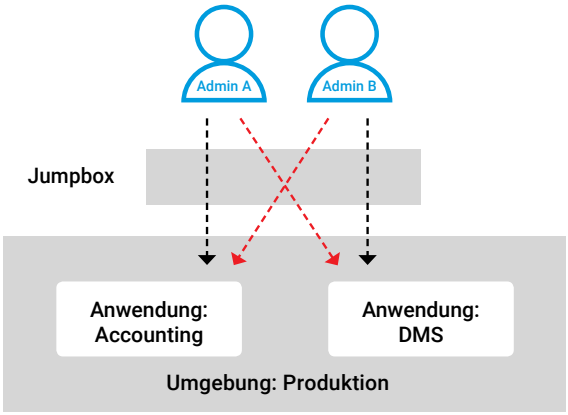
Geschwindigkeit und Performance
Richtlinien lassen sich einfach und intuitiv erstellen und werden sowohl bei neuen als auch bei aktiven Sitzungen sofort wirksam.

Kosteneffizienz
Die Kosten sind nachweislich um bis zu 60 % niedriger als bei vergleichbaren Anwendungsfällen mit einer herkömmlichen Jumpbox-Infrastruktur.

Akamai

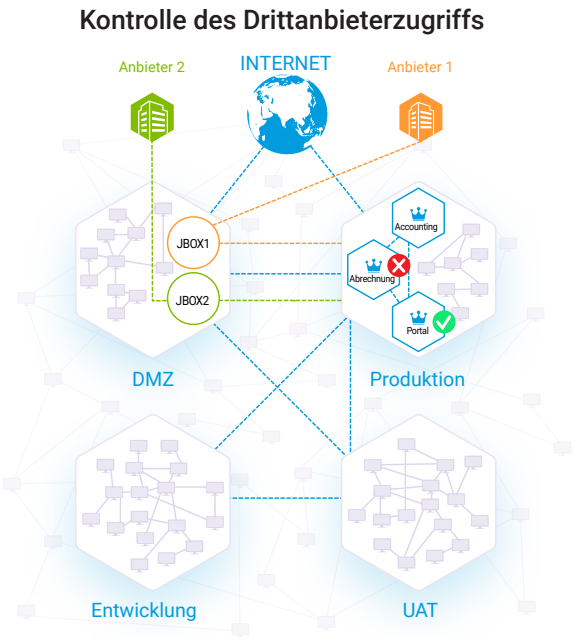
Gleichzeitigen Nutzerzugriff verarbeiten

Administratoren können über dieselbe Jumpbox oder denselben Terminalserver auf verschiedene Anwendungen zugreifen, selbst wenn sie gleichzeitig angemeldet sind. Gleichzeitig funktionieren unterschiedliche Richtlinien nahtlos zusammen, sodass Nutzer auf die Inhalte zugreifen können, für die sie berechtigt sind, während andere Inhalte gesperrt werden, ohne dass hierdurch der Service oder Zugang des Nutzers beeinträchtigt wird.



Kontrolle des Drittanbieterzugriffs

Basierend auf der Nutzeridentität kann Akamai Guardicore Segmentation die Verwaltung des Drittanbieterzugriffs kontrollieren, z. B. durch externe Lieferanten oder SaaS-Anbieter. Mithilfe von Nutzergruppen können jeder Drittanbieterverbindung eigene Zugriffsrichtlinien zugewiesen werden, die sowohl für das Rechenzentrum als auch für bestimmte Anwendungen definiert sind. So erhalten Nutzer nur die Berechtigungen, die sie für ihre Rolle brauchen – und nicht mehr.



Anwendungssegmentierung und Nutzer-IAM bieten gemeinsam den besten Schutz für moderne Rechenzentren.

Möchten Sie mehr darüber erfahren, wie sie ineinandergreifen? Dann wenden Sie sich an einen unserer Experten.