WHITEPAPER

Schutz von Workloads in Hybrid- und Multi-Cloud-Umgebungen

Schutz von Workloads in Hybrid- und Multi-Cloud-Umgebungen

Auf der Suche nach Innovation, Wettbewerbsvorteilen und gesteigerter Effizienz haben sich zahlreiche Unternehmen für ein DevOps-basiertes Cloudinfrastrukturmodell entschieden. So konnten sie die Geschwindigkeit und Agilität ihrer IT auf bisher nie dagewesene Weise steigern. Viele Unternehmen setzen weiterhin auf Public-Cloud-Infrastruktur und neue Bereitstellungsansätze wie Container und serverlose Technologien. Durch die Übernahme dieses neuen Modells beschleunigt die neueste Cloud-Computing-Technologie den Wandel drastisch. Mit diesen Ansätzen können Workloads, Anwendungen und sogar Umgebungen automatisiert, automatisch skaliert oder migriert werden – und noch vieles mehr. Die daraus resultierenden Wettbewerbsvorteile sind enorm.

Gleichzeitig bleiben einige ältere Services und Systeme, wie z. B. die herkömmliche Rechenzentrumsinfrastruktur, weiterhin in Gebrauch. Unternehmen sind zwar möglicherweise gerade dabei, sie zu entfernen oder zu modernisieren, doch die Systeme sind immer noch vorhanden, da sie geschäftskritische Anwendungen und Workflows unterstützen.

Darüber hinaus konnten herkömmliche Sicherheitstechniken nicht mit dem Tempo des Wandels Schritt halten, was die Frage aufwirft, wie Cloud-Workloads in diesen neuen Hybrid- und Multi-Cloud-Umgebungen geschützt werden können. Sicherheit durch geschlossene Netzwerke beeinträchtigt nicht nur die Geschwindigkeit, sondern ist einfach nicht mehr effektiv, wenn der Großteil des Traffics innerhalb der Cloud oder des Rechenzentrums stattfindet (East-West) und nicht mehr von außen stammt (North-South). Diese Transformation zwingt IT-Führungskräfte auch dazu, ihr Sicherheitskonzept zu überdenken.

Herkömmliche Sicherheitstechniken sind in Hybrid- und Multi-Cloud-Umgebungen nicht effektiv

Tatsächlich wurden herkömmliche Cybersicherheitsmodelle nicht mit Blick auf Infrastructure as a Service (IaaS) entwickelt. Die Public Cloud erfordert neue Strategien, die auf ihren eigenen einzigartigen Herausforderungen basieren.

Die Unternehmenssicherheit muss weiterentwickelt werden, um diese neue Geschäftsumgebung zu unterstützen. Unternehmen haben bereits drastische Änderungen vorgenommen, um Geschäftsanforderungen zu erfüllen und agile Methoden zu implementieren. Doch die Sicherheit kam trotz massiver Investitionen zu kurz.

Die Wahrheit ist: Geld für Lösungen auszugeben, die ohne Rücksicht auf die Cloud entwickelt wurden, ist ein Fehler. Denn sie tragen nicht dazu bei, aktuelle oder künftige Angriffe zu erkennen und zu verhindern. Wie können Sie also Public-Cloud-Services nutzen und die Vorteile von Geschwindigkeit und Agilität genießen, ohne den Schutz kritischer Daten zu gefährden?

Das moderne Hybrid-Cloud-Rechenzentrum

Der Aufbau moderner Rechenzentren, der zunehmende Detailgrad von Workloads und die Geschwindigkeit der Entwicklung ändern sich rasant. Ein typisches, modernes hybrides Rechenzentrum besteht aus Workloads, die sowohl On-Premises als auch in einer Public Cloud oder per IaaS ausgeführt werden. Hierbei kommen verschiedene Anbieter sowie Platform as a Service (PaaS) zum Einsatz, entweder On-Premises oder in der Cloud. Die Anzahl der Workloads, die in der Public Cloud ausgeführt werden, nimmt immer weiter zu. Gleichzeitig werden sich On-Premises-Rechenzentren in absehbarer Zeit nicht einfach in Luft auflösen. So ergab eine kürzlich unter IT-Führungskräften durchgeführte Umfrage, dass sich bei rund 59 % der Unternehmen die IT-Umgebung „zum Teil in der Cloud, aber größtenteils On-Premises“ befindet – bei 34 % ist sie „größtenteils in der Cloud und zum Teil On-Premises“. Nur bei 7 % befindet sich die Umgebung „vollständig in der Cloud“, doch diese Zahl wird voraussichtlich drastisch ansteigen.[1]

Wie wir sehen, setzen Unternehmen zunehmend DevOps-Verfahren ein und verbessern ihre Agilität. Native Cloudservices und serverlose Technologien lassen sich heute einfacher denn je implementieren. Durch den Einsatz einer Kombination aus Containern, VMs und serverlosen Workloads in der Cloud können Sie aus strategischer Sicht kostengünstiger arbeiten und Ihre Umgebung umfassender transformieren.

Doch in diesem Hybrid-Cloud-Ansatz muss auch Sicherheit ihren Platz finden. Unternehmen müssen sich in jeder Phase des DevOps-Prozesses um Sicherheit kümmern: von Planung, Entwicklung und Tests bis hin zu Überwachung, Betrieb, Bereitstellung und Freigabe neuer Funktionen. Die Umstellung auf die Cloud darf kein Hindernis für Ihren Erfolg darstellen.

Verteilte Workloads sind nicht gut geschützt, was den Einsatz neuer Cloudtechnologien einschränkt

Viele Unternehmen müssen Workloads schützen, die über On-Premises-, Colocation- und mehrere Public-Cloud-/IaaS-Plattformen verteilt sind. Mit herkömmlichen Sicherheitsmodellen für On-Premises-Netzwerke lassen sich diese Workloads nur schwer schützen.

Und wenn Sie versuchen, neue cloudbasierte Tools und Techniken zum Schutz der neuen Cloudtechnologien zu implementieren, wird die Situation sogar noch schwieriger. Die Komplexität steigt, wenn Unternehmen versuchen, verschiedene Sicherheitskontrollen in unterschiedlichen Umgebungen durchzusetzen, und es entstehen neue Risiken, wenn sie diese Kontrollen ohne ausreichende Transparenz implementieren.

Mit anderen Worten: Die Cloud – die Unternehmen eigentlich dynamischer, agiler, schneller und innovativer machen soll – gefährdet nun viele dieser Unternehmen. Und da es an relevanten cloudbasierten Sicherheitstools fehlt, sind sie nur begrenzt in der Lage, diese neue Technologie zu nutzen, ohne blinde Flecken und weitere Herausforderungen zu verursachen.

Hier kommt adaptiver Workload-Schutz ins Spiel.

Der Wechsel zu IaaS erfordert adaptiven Workload-Schutz

Die beste Möglichkeit, fein abgestufte Workloads mit kurzer Lebensdauer zu schützen, besteht darin, diesen Schutz dynamisch anzuwenden, sobald die Workload verwendet wird. In Public-Cloud-Infrastrukturen sind Workload-orientierte Lösungen bei der Durchsetzung von Sicherheitsrichtlinien weitaus einfacher als herkömmliche Netzwerksicherheitsmodelle.

Cloud Workload Protection Platforms unterstützen plattformunabhängige, workloadorientierte Sicherheitslösungen

Da eine Richtlinie der Workload folgt – unabhängig von der zugrunde liegenden Infrastruktur –, kann das Modell auf alle Workloads in der gesamten Hybrid-Cloud-Rechenzentrumsumgebung angewendet werden. Das Ergebnis ist ein einheitlicher und plattformunabhängiger Ansatz für Sicherheitskontrollen.

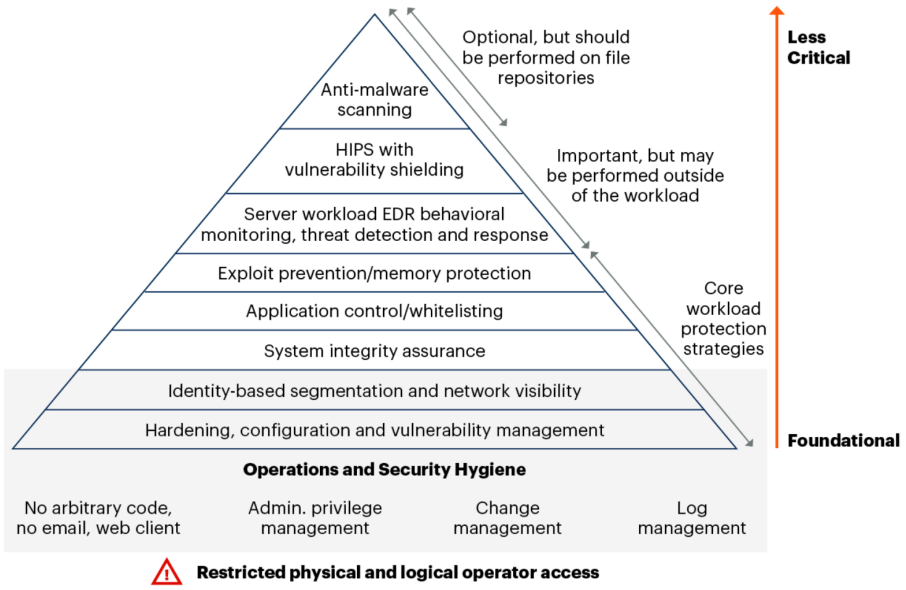
Zwar gibt es native Cloudsicherheitstools, doch adaptive Cloud Workload Protection Platforms (CWPPs, also Plattformen zum Schutz von Cloud-Workloads) bieten eine umfassendere, präzise Kontrolle auf Ebene von Prozessen, Nutzern und voll qualifizierten Domainnamen. Sie funktionieren auch über mehrere Cloudanbieter und On-Premises-Systeme hinweg und bieten einen stärkeren und umfassenderen Schutz für VMs, Container und serverlose Workloads.

So passen die Kontrollen von Akamai Guardicore Segmentation zu Gartners Kernstrategien für Cloud-Workload-Schutz

Eine der am weitesten verbreiteten Richtlinien zum Schutz von Cloud-Workloads wurde von den Branchenexperten von Gartner verfasst. Laut Gartner gibt es beim Schutz von Cloud-Workloads eine klare Hierarchie von Kontrollen:

Die Pyramide unten reicht von „grundlegend“ zu „weniger kritisch“ und zeigt die Strategien, die Gartner als Kernstrategien betrachtet, sowie die Strategien, die wichtig, aber optional sind. Im Idealfall sollten diese Schritte in jede Workload einbezogen werden, um sicherzustellen, dass jede Aktion integrierte Sicherheit erhält.

Risikobasierte Hierarchie der Workload-Schutz-Kontrollen[2]



Die Gartner-Richtlinien zum Schutz von Cloud-Workloads definieren eine klare Hierarchie der Sicherheitskontrollen für Unternehmen.

Im Folgenden finden Sie eine ausführliche Erläuterung der Kernstrategien, die unsere Lösung unterstützt. So können Sie herausfinden, wie Sie diese Strategien am besten in Ihr Sicherheitsprogramm für Hybrid- oder Multi-Cloud-Rechenzentren integrieren können:

- **Härtung, Konfiguration und Schwachstellenmanagement**
  Laut Gartner besteht die wichtigste Strategie zum Schutz von Workloads darin, Ihre Systeme und Einstellungen richtig zu konfigurieren, um Risiken zu minimieren. Tools für Schwachstellenmanagement können die manuelle Entfernung von Angriffsvektoren erheblich verbessern und diesen Prozess sogar automatisieren. Einmal eingerichtet, können sie Softwareprobleme finden und beheben, die schädliche Aktionen unterstützen könnten.

- **Identitätsbasierte Segmentierung und Netzwerktransparenz**
  Gartner nennt Netzwerksegmentierung und -transparenz als zentrale Strategien für den Cloudschutz. Die meisten Unternehmen verwenden lokale Next-Generation-Firewalls, doch viele geben sich mit einer weniger sicheren Lösung zufrieden, wenn sie in die Cloud wechseln.

  Sicherheitsteams sind sich bewusst, dass Next-Generation-Firewalls für den Cloudschutz nicht ausreichen, wissen aber nicht, wie sie in einer dynamischen, hybriden Rechenzentrumsumgebung heterogene Einblicke oder Kontrolle erreichen können. Nehmen wir uns also einen Moment Zeit, um zu besprechen, wie es richtig geht.

  Zunächst müssen Sie Transparenz gewährleisten. Schnelle Transparenz führt zu schnellerer Amortisierung, da alle Beteiligten sofort und automatisch auf dem gleichen Stand sind.

  Native Cloudtools können Snapshot-Übersichten oder Textprotokolle bereitstellen, die jedoch in der Regel unübersichtlich, unvollständig oder unzureichend sind. Eine optimale Lösung sollte automatisch alle Anwendungen, den gesamten Traffic und sämtliche Abhängigkeiten in Ihrem Netzwerk erkennen. Auf diese Weise können Sie Ihr gesamtes IT-Ökosystem auf einen Blick sehen, selbst wenn Ihr Unternehmen hybrid verteilt ist.

  Ihre Lösung sollte außerdem leistungsstarken Kontext enthalten, der einen umfassenden Einblick in die tatsächlichen Vorgänge in Ihrem Rechenzentrum bietet. Jedes Unternehmen, das Sicherheitsvorgänge und Anfragen skalierbar verwalten möchte, benötigt den nötigen Kontext für jeden Ablauf und muss in der Lage sein, einzelne Prozesse und die Kommunikation auf dem Server zu analysieren. Das ermöglicht eine datengestützte Entscheidungsfindung, die die Erstellung von Richtlinien unterstützt.

  Nachdem Sie für Transparenz und Kontext gesorgt haben, erstellen Sie Segmentierungsregeln, die den Best Practices für Ihr Unternehmen entsprechen. Sie können beispielsweise Produktions- und Entwicklungsumgebungen trennen oder Kundendaten isolieren, um die Compliance nachzuweisen. Sie können auch detailliertere Richtlinien für die Mikrosegmentierung entwickeln, um umfassende Sicherheit und Kontrolle zu erreichen – und zwar auf eine Weise, die Ihrem spezifischen Geschäftskontext entspricht.

- **Anwendungskontrolle/Zulassungslisten**
  Wenn Ihr Sicherheitsteam Richtlinien festlegen und sich stets sicher sein kann, dass sie überall durchgesetzt werden, wird der Übergang zur Cloud in jeder Phase einfacher und sicherer.

  Wenn Sie sich allein auf Ports/IPs verlassen, erhalten Sie nicht den Grad an Transparenz, den Sie für den vollständigen Schutz von Cloud-Workloads benötigen. Die strenge Kontrolle des Traffics zwischen Anwendungskomponenten ist ein Kernbestandteil einer leistungsstarken Mikrosegmentierungslösung. Die besten Technologien bieten detaillierte Transparenz und präzise Kontrolle bis hinunter zu Anwendungsprozessen, Nutzern und voll qualifizierten Domainnamen, wobei Details wie Hash-Werte, Prüfsumme, vollständiger Pfad, Lösungen und Identitätsspeicher-Authentifizierungen verwendet werden.

  Zu den weiteren Funktionen, die die Anwendungskontrolle ergänzen können, gehören:

  - Mikrosegmentierung, die laterale Netzwerkbewegung in der Cloud sogar innerhalb desselben Anwendungsclusters begrenzen kann
  - eine zentrale Verwaltungskonsole, die zu mehr Sicherheit führt
  - die Möglichkeit, Modelle zu Zulassungs- und Verweigerungslisten hinzuzufügen, um nicht autorisierte Anwendungen oder unzulässigen Traffic zu blockieren, aber gleichzeitig zu gewährleisten, dass wichtige Verbindungen ungehindert ausgeführt werden

- **Exploit-/Arbeitsspeicherschutz**
  Die letzte Kernstrategie für Serverschutz im Gartner-Leitfaden zum Schutz von Cloud-Workloads ist Exploit-Schutz. Suchen Sie nach einem Sicherheitstool für die Mikrosegmentierung, mit dem Sie Sicherheitsverstöße erkennen und darauf reagieren können. Auf diese Weise können Sie redundante Tools ersetzen und die Komplexität Ihres Rechenzentrums verringern.

  Darüber hinaus sind, wie bereits erwähnt, Transparenz und die richtige Zuordnung (Mapping) grundlegend. Sobald Sie über eine gründliche Übersicht Ihres gesamten Netzwerks verfügen, können Sie ungepatchte Schwachstellen oder schädliche Kommunikation erkennen, die außerhalb der Norm liegen. Wenn Ihr Unternehmen eine Baseline für legitimen Traffic festgelegt hat, fällt unzulässiges Verhalten sofort auf.

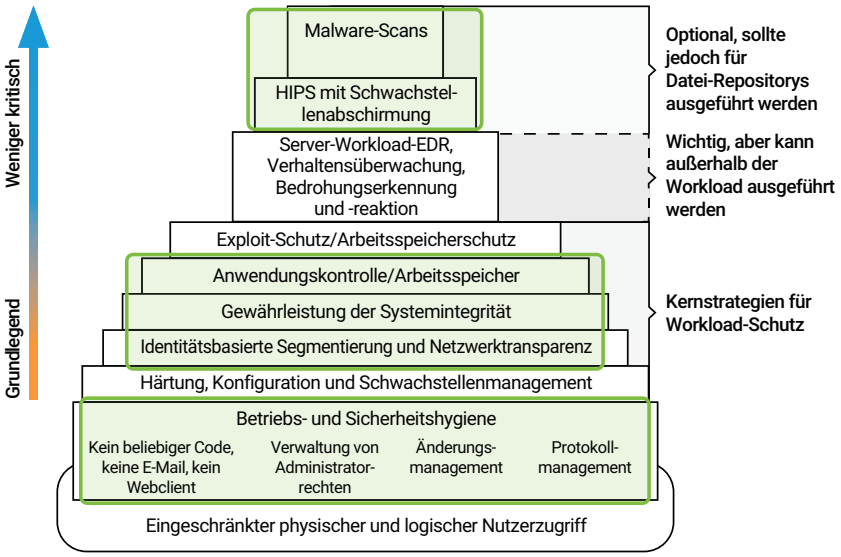
Weitere wichtige Schutzstrategien

Die oben genannten zentralen Serverstrategien bilden die Grundlage für Sicherheit in der Cloud. Doch Gartner nennt noch weitere Strategien, die Ihre Hybrid- oder Multi-Cloud-Umgebung stärken können, darunter Endpoint Detection and Response (EDR), Verhaltensüberwachung sowie Threat Detection and Response (TDR) für Server-Workloads.

EDR, Verhaltensüberwachung und TDR sind wichtige Bestandteile der Angriffserkennung und Vorfallsreaktion. Um diese Sicherheitsaspekte abzudecken, sollten Sie sich für eine Lösung entscheiden, die eine Reputationsanalyse umfasst. Auf diese Weise erhalten Sie zusätzliche Informationen über einen Angriff und können fortschrittliche Täuschungsfunktionen einsetzen, mit denen Sie Angreifer dazu bringen können, ihre Methoden preiszugeben. Auf diese Weise können Sie Ihre Richtlinien- und Sicherheitsverfahren für die Zukunft verbessern.

Möglicherweise benötigen Sie Transparenzdaten, um Informationen über vergangene Ereignisse zu erhalten. Die besten Anbieter speichern Ihre Daten monatelang, sodass Nutzer bestimmte Anwendungen, Prozesse und Zeiträume untersuchen können. Sicherheitsteams können diese Daten auch für forensische Untersuchungen und eine verbesserte Vorfallsreaktion verwenden.

Akamai Guardicore Segmentation: Schutz von Hybrid-Cloud-Workloads gemäß der Gartner-Hierarchie



Die hervorgehobenen Bereiche zeigen, wo unsere Lösung die Anforderungen für Cloud-Workload-Schutz erfüllt.

Akamai Guardicore Segmentation schließt die Lücken nativer Cloudsicherheitstools und erfüllt viele der Grundprinzipien im Gartner-Leitfaden zum Schutz von Cloud-Workloads. Darüber hinaus unterstützt die Lösung auf intelligente Weise Transparenz sowie Richtlinienerstellung und -durchsetzung in Hybrid- und Multi-Cloud-Rechenzentren.

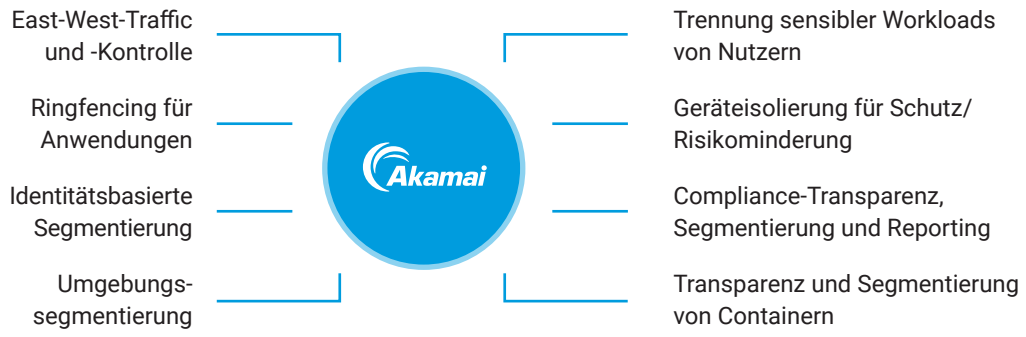
Unsere Lösung bietet umfassende Einblicke – mit einer zentralen Verwaltungskonsole, die einen Überblick über das gesamte Rechenzentrum ermöglicht. Durch die Visualisierung Ihres hybriden Rechenzentrums als Ganzes können Sie Anwendungsabhängigkeiten und die Auswirkungen jeder Richtlinie auf Ihr Netzwerk genau verstehen. Und das wirkt sich stark auf die Cloud-Migration aus: Denn so können Kunden deutlich schneller in die Cloud gelangen als mit nativen Visualisierungstools.

Diese detaillierte Transparenz ermöglicht Ihnen Folgendes:

- Erstellen einer To-do-Liste für das Cloud-Netzwerk
- schnelle Erkennung von Anwendungen über alle Infrastrukturen und Anwendungsabhängigkeiten hinweg – eine wichtige Funktion für eine erfolgreiche Migration
- Ermittlung Ihrer künftigen Infrastruktur- und Betriebskosten
- Einblicke in die beste Richtlinienerstellung zur Risikominderung bei der Migrationsplanung
- den kürzesten, einfachsten und sichersten Weg zu Ihren Geschäftszielen für die Cloud

Die umfassende und kontextbasierte Transparenz von Akamai Guardicore Segmentation ermöglicht ein schnelles und gründliches Verständnis Ihrer Umgebungen.

Unsere umfangreiche Transparenz umfasst auch Kontext für jede Kommunikation und jeden Ablauf, sodass Sie Fehler und die allgemeine Komplexität reduzieren können. Sie können die Informationen gruppieren und filtern, um alle Beteiligten beim Lesen der Übersicht zu unterstützen. So können Sie ihnen ganz einfach die genauen Informationen bereitstellen, die sie benötigen. Diese kontextbezogene Ansicht reduziert die Notwendigkeit von Drittanbietern und Richtlinienerstellern und ermöglicht so ein schnelles Verständnis Ihrer Umgebungen, damit Sie geltende Richtlinien erstellen, verfeinern oder ändern können.



Anwendungsfälle für Akamai Guardicore Segmentation

Weitere wichtige Funktionen unserer Lösung:

- Richtlinien auf Prozess- und Serviceebene, die eine einfachere und stärkere Sicherheit beim Umgang mit dynamischen Protokollen wie FTP oder Spark ermöglichen
- identitätsbasierte Mikrosegmentierungsrichtlinien, die Verbindungen basierend auf dem Nutzer erzwingen, der sie herstellt
- auf voll qualifizierten Domainnamen basierende Richtlinien, mit denen Sie Ressourcen mit dynamischen IP-Adressen automatisch skalieren können
- Verwendung bestehender Public-Cloud-Tags als Kennzeichnungen, wodurch die Visualisierung Ihres Hybrid- oder Multi-Cloud-Rechenzentrums vereinfacht wird
- automatische Erstellung von Richtlinien anhand des beobachteten Traffics, sodass Sie schnell fachkundige Anleitung erhalten, während Sie mit der Mikrosegmentierung beginnen

Unsere Lösung ist plattform- und infrastrukturunabhängig und managt Transparenz und Durchsetzung in der gesamten Infrastruktur.

Die Verringerung der Komplexität ist das ultimative Ziel beim Schutz hybrider Rechenzentren. Akamai Guardicore Segmentation ist plattform- und infrastrukturunabhängig, sodass Sie einen ganzheitlichen Überblick über die gesamte Anwendung und Richtlinie erhalten, die der Workload folgt – unabhängig von ihrem Speicherort. Jede Regel wird auf alle Workloads angewendet: von vCenter und Public Clouds (AWS, Azure, GCP) bis hin zu Bare-Metal-Servern und Containern.

Die Verringerung der Komplexität steigert nicht nur die Sicherheit, sondern verringert auch den Arbeitsaufwand für IT- und Sicherheitsteams. Bei cloudbasierten Sicherheitsgruppen benötigen Sie Cloudexperten für jeden Anbieter. Im Gegensatz dazu brauchen Sie mit einer Sicherheitslösung, die Transparenz und Durchsetzung in der gesamten Infrastruktur managt, nur zertifizierte Nutzer für eine einzige Technologie.

Eine zukunftssichere Cloud Workload Protection Platform

Einer der Eckpfeiler von Agile und DevOps ist die Fähigkeit, schnell zu scheitern, um so ganz einfach zum nächsten Erfolg zu gelangen. Leider (und ironischerweise) kann die Migration Ihrer Workloads zwischen verschiedenen Cloudanbietern viel Zeit beanspruchen. Und es kann schwierig sein, die Sicherheit beizubehalten.

Deshalb müssen Sie in der Lage sein, sich Ihre Optionen offenzuhalten. Wenn Sie auf eine Multi-Cloud-Infrastruktur umstellen oder sogar ganze Workloads zu einem neuen Cloudanbieter migrieren möchten, sollte das Ganze weder negative Auswirkungen auf die Sicherheit haben, noch sollten Sicherheitsbedenken Sie von dem Projekt abhalten.

Mit Akamai Guardicore Segmentation bleiben Sie flexibel und können mit dem Geschäftstempo Schritt halten, indem Sie Ihre Workloads mit intakten Sicherheitsrichtlinien migrieren. Sie behindert weder den DevOps-Prozess noch die Agilität und es ist auch nicht in jeder Phase eine Neukonfiguration erforderlich. Stattdessen erhalten Sie die Grundlagen einer zuverlässigen Cloud Workload Protection Platform, mit der Sie Ihr Hybrid- oder Multi-Cloud-Rechenzentrum schützen können.

Akamai Guardicore Segmentation ermöglicht die sichere Migration in die Cloud und zwischen Clouds und bietet unvergleichliche Transparenz mit umfangreichem Kontext. Mit unserer Lösung können Sie Richtlinien auf Prozess- und Nutzerebene durchsetzen und Ihren Workloads überallhin folgen.

Sie können Sicherheit zum festen Bestandteil jeder Phase des DevOps-Prozesses machen, um Flexibilität zu ermöglichen und Ihr Unternehmen zu unterstützen. So sind Sie in der Lage, die neuesten Cloudfunktionen zu nutzen und gleichzeitig die Sicherheit zu gewährleisten.

Erfahren Sie mehr über den Schutz von Cloudumgebungen mit branchenführender Mikrosegmentierung. Besuchen Sie heute noch akamai.com/guardicore.

1 2022. Cloud-Computing-Studie von Foundry (ehemals IDG).

2 Market Guide for Cloud Workload Protection Platforms (Marktleitfaden für Cloud Workload Protection Platforms), geschrieben von Gartner-Analysten Neil MacDonald und Tom Crow; veröffentlicht am 14. April 2020