SD Mikrosegmentierung – einfach implementierbare Sicherheitsservices für Unternehmen jeder Größe

Akamai Guardicore für den Schutz von Hybrid- & Multi-Cloud-Architekturen gegen Cyberangriffe

Umso komplexer die genutzten IT-Services, desto höher der Sicherheitsaufwand: Die Isolierung und Segmentierung von Anwendungen und ihren Komponenten im Netzwerk ist notwendig, um Compliance-Vorgaben einzuhalten und Unternehmensanwendungen und -daten gegen Cyberattacken zu schützen. Mit der einheitlich nutzbaren Microsegmentierungs-Lösung Guardicore Centra lassen sich neue Anwendungen schnell integrieren und das Risiko eines Cyberangriffs minimieren. Der zentral gemanagte SD Microsegmentierungs-Service bietet zahlreiche Vorteile über die Abwehrfunktion hinaus: So lassen sich etwa Abhängigkeiten von Anwendungen umfassender zuordnen und Richtlinien effektiver umsetzen.

Beziehungen zwischen Anwendungen erkennen und zuordnen

- Korrelieren Sie Aktivitäten auf Netz- und Prozessebene automatisch
- Identifizieren Sie das Anwendungsverhalten anhand des Kontexts auf Prozessebene

Richtlinien schnell entwerfen, testen und bereitstellen

- Gestalten Sie Richtlinien mithilfe automatisierter Regelvorschläge, die auf historischen Daten basieren
- Der intuitive Workflow unterstützt die kontinuierliche Präzisierung von Richtlinien und beseitigt Fehler

Starke Sicherheit in jeder Umgebung

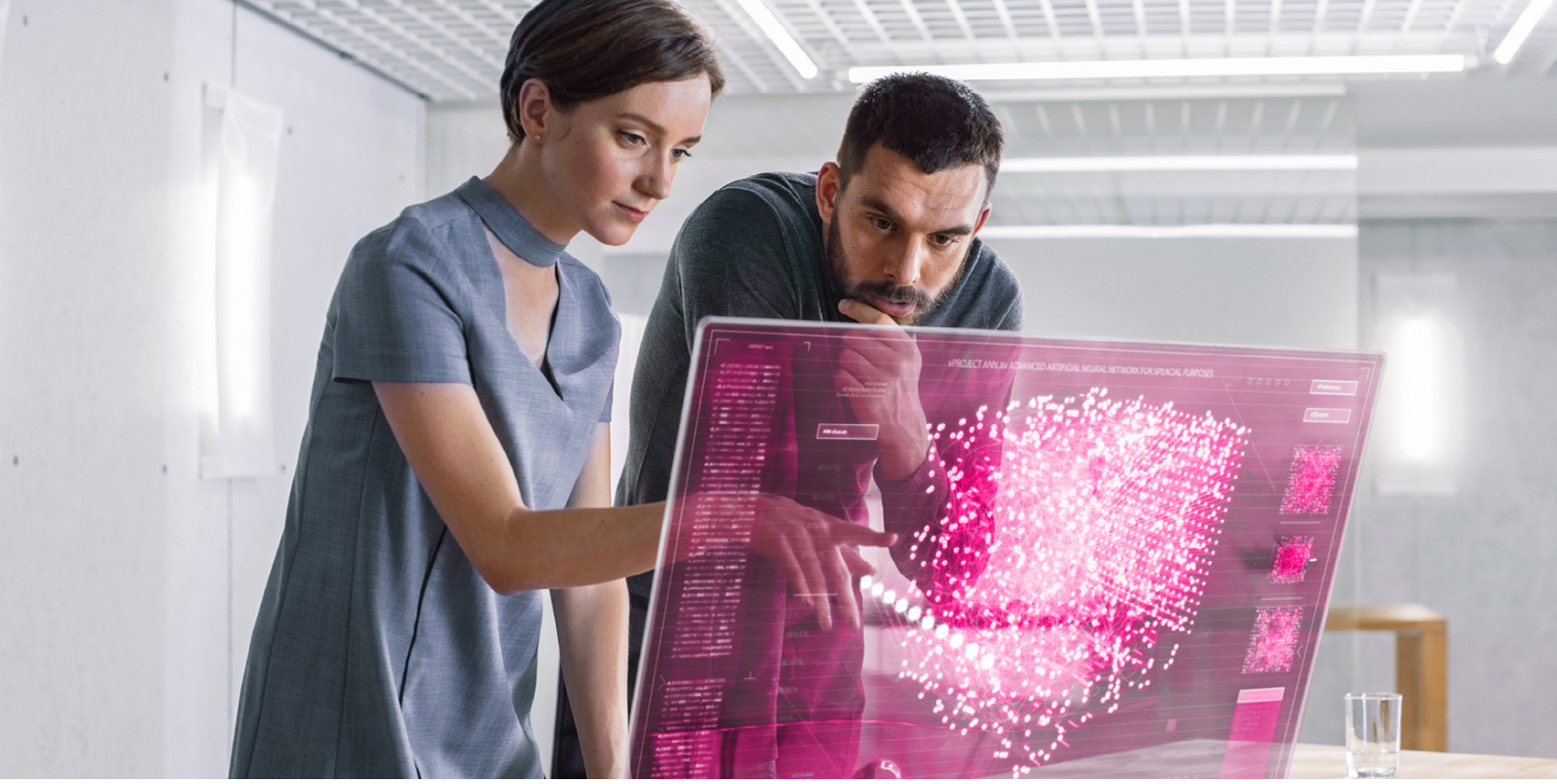
- Steuern Sie die Kommunikation sowohl auf Netz- als auch auf Prozessebene unter Windows und Linux
- Untersuchen Sie Richtlinienverstöße und erkennen Sie Verstöße schneller mit Hilfe von integrierten Daten aus mehreren Angriffsmethoden
- Sorgen Sie für Sicherheit, ungeachtet möglicher Einschränkungen durch das Betriebssystem

Die Segmentierung von Netzwerken gehört seit Jahrzehnten zum Einmaleins der IT-Sicherheit. Bei komplexen Hybrid- & Multi-Cloud-Architekturen müssen Sicherheitsmaßnahmen sowohl auf Workload- als auch auf Prozessebene umsetzbar sein. Guardicore Centra bietet einen einfachen Workflow von der Zuordnung von Anwendungsabhängigkeiten bis zum Vorschlagen und Festlegen von Regeln, sodass Auswirkungen sichtbar werden, bevor Sie auf den Datenverkehr angewendet werden.

SD Microsegmentierung steht für:

- Maximale Transparenz mittels einer visuellen Karte, die darstellt, wie Anwendungen miteinander kommunizieren.
- KI-gestützt: Priorisierung geschäftskritischer Anwendungen und Umsetzung von Segmentierungsrichtlinien mit wenigen Klicks
- Vollständige Sicht auf Sicherheitsrisiken und unmittelbare Eingriffs möglichkeit durch Anpassung der Segmentierungsregel
- Schnellere und einfache Segmentierung mittels eines flexiblen Allow -und Denylist-Modells, die zu einer zeitnah wirkenden Risikominderung mit wenigen Regeln führt
- Breite Anwendbarkeit und Schutz kritischer Ressourcen, unabhängig vom Einsatzort oder von wo aus der Zugriff erfolgt
- Umfassende Erkennung von dynamischer Täuschung und Sicherheits verstößen und -verletzungen z. B. durch Reputationsanalyse, und Threat Intelligence Firewall
- Verpflichtende Durchsetzung zentral aufgesetzter Richtlinien und eines granularen Regelwerks auf Prozessebene
- Schnellere Implementierung und Management ohne Ausfallzeiten
- Umfängliche Nutzbarkeit für viele Legacy-Systeme, z. B. auch für Windows 2003, CentOS 6, RHEL5 oder AS400

T Systems Let's power higher performance



Die Lösungen auf einen Blick

In nur drei einfachen Schritten lassen sich SD Microsegmentierungs-Services erfolgreich implementieren:

1. Transparenz: Erkennen und Zuordnen der Beziehungen zwischen Anwendungen

2. Konzeption: Entwerfen, Testen und Bereitstellen von Richtlinien in Rekordzeit

3. Umsetzung: Sicherheit in jeder Umgebung

KI-Labeling und Vorschläge für Richtlinien

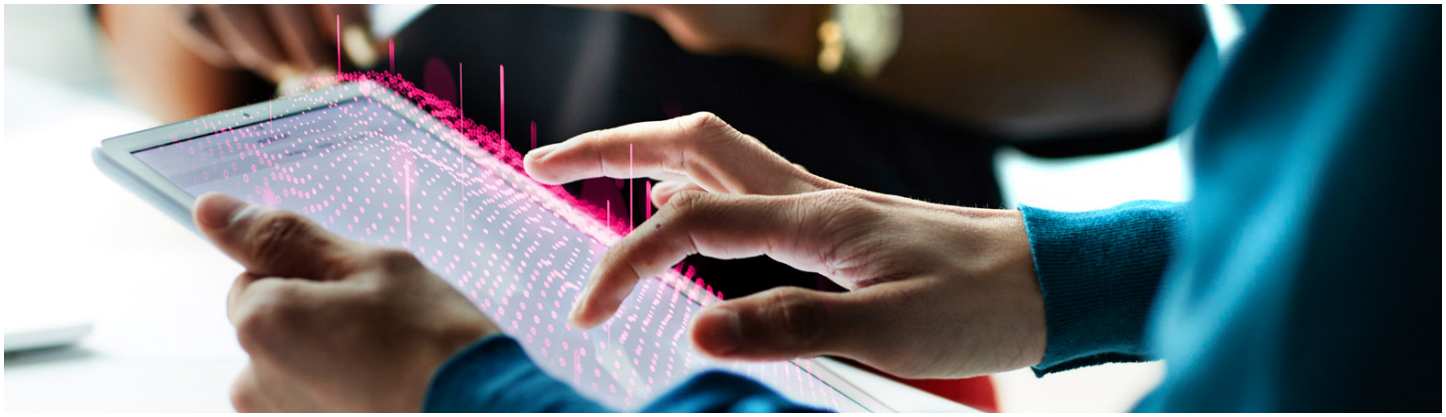
Die Zuordnung von Assets und die Durchsetzung von Richtlinien sind zwei Stufen einer effektiven Segmentierung. Mittels automatisierter Machine-Learning-Technologien lässt sich das Asset-Mapping umgehen, was zu einer noch schnelleren Implementierung führt. Hierbei werden erkannte Kommunikationsbeziehungen und als gefährlich und/oder überflüssig analysierte Datenverkehrsmuster genutzt, um daraus automatische Vorschläge für die effektivsten Richtlinien zu generieren.

SD Mikrosegmentierungs-Services in Hybrid- & Multi-Cloud-Umgebungen einführen

Das Konzept der Netzwerksegmentierung hat sich vielfach etabliert. Doch das Sicherheitsmodell stößt bei dynamischen Infrastrukturen – insbesondere in skalierbaren Cloud-Umgebungen, wenn sich Workloads zwischen Segmenten bewegen und kommunizieren – an seine Grenzen. Wenn Cloud-Services eingesetzt werden, steigt das Risiko, dass ein Angriff vor seiner Aufspürung nicht nur an einer Stelle der IT- Infrastruktur erfolgreich war. Die Bekämpfung des Angriffs muss möglichst in Echtzeit erfolgen und zwingend auf ein Segment begrenzt werden können, um Schaden von weiteren Apps und Workloads in eigenen Rechenzentren und Cloud-Services abzuwehren. Mit den SD Microsegmentierungs-Services lässt sich die auch Sicherheit von komplexen Cloud-Services steigern und diese von einem einzigen Dashboard aus für alle Anwendungen steuern.

Umfassender Schutz durch vollständige Abdeckung

SD Microsegmentierungs-Services lassen sich für alle Anwendungen in jeder Umgebung einsetzen – egal, ob es sich um einen Public-, Private- oder Hybrid-Cloud-Service oder ein On-Prem- oder Hosting-Service handelt.



Vollständige Transparenz als Basis für Segmentierungsregeln

Um die vielfältigen Kommunikationsbeziehungen bei der Anwendungsnutzung steuern zu können, müssen diese erfasst und verstanden werden. Mit dem SD-Microsegmentierungs-Service lassen sich so auch langjährig genutzte Services in ihrer Nutzung transparent machen und Zugriffsrechte erkennen, die unter Umständen längst nicht mehr erwünscht sind. Letztlich lassen sich Segmentierungsregeln erstellen, die etwa Nutzerbedarfen oder Applikationsabhängigkeiten entsprechen. Das zentrale Management erlaubt es, jederzeit eingreifen und kurzfristig aufkommende Anpassungsbedarfe ergänzen zu können.

Steuerung auf der Basis granularer Richtlinien

Mit zunehmender Komplexität der Infrastruktur müssen sich Datenflüsse immer granularer und detaillierter steuern lassen. Ziel des Ansatzes ist es, jedes Microsegment gegenüber unautorisierten Datenflüssen sicher abzuschirmen. Dies setzt voraus, dass die Zugriffs- und Nutzungsrechte zum Beispiel pro Anwendung festgelegt werden. So lassen sich Kommunikationsbeziehungen zwischen und innerhalb von Mikrosegmenten nach einheitlichen Regeln effizient steuern.

Mit dem Guardicore SD Microsegmentation Service von Akamai lassen sich Richtlinien schnell entwickeln und bereitstellen. Die Konfiguration können Nutzer*innen mittels des zentralen Dashboards unmittelbar anpassen. Dank vordefinierter Templates ist eine zeitnahe Erstimplementierung möglich, zum Beispiel im Angriffsfall. Die individuelle, bedarfsgerechte Anpassung der Konfiguration lässt sich im Anschluss – nach Abwehr des Angriffs – durchführen.

Mit dem Mikrosegmentierungs-Tool können Regeln auf „Prozessebene“ zur strikten Kontrolle der Abläufe zwischen den Anwendungskomponenten festgelegt und durchgesetzt werden. Dies führt zu einem optimalen Sicherheitsniveau.

Darum können Sie uns vertrauen!

T-Systems pflegt seit Jahren eine erfolgreiche Partnerschaft mit Akamai, dem Gesellschafter von Guardicore. Wir beraten zahlreiche namhafte Unternehmen zu Content Delivery, Web Performance und Web Security. Die Bedeutung internetbasierter Geschäftsprozesse wächst stetig, immer mehr Anwendungen werden als Cloud Services bereitgestellt. Die Edge Services von Akamai passen hervorragend zur Cloud-Strategie von T-Systems. Die Services der Delivery-Plattform bieten weltweit hochperformante Dienste, die um führende Cloud Security Services ergänzt werden und zugleich Kundeninfrastrukturen entlasten. Dadurch entsteht ein hervorragendes Erlebnis für unsere Kunden und ihre Nutzer.

HABEN SIE FRAGEN?
0800 33 09030

BESUCHEN SIE UNS:
www.t-systems.com/de/de

HERAUSGEBER
T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main
Deutschland

T Systems Let's power higher performance