ORIENTIERUNGSHILFE

Akamai Guardicore Segmentation im Vergleich zu herkömmlichen Lösungen zur Mikrosegmentierung

Unerreichte Transparenz

Um zu verstehen, was in Ihrer Umgebung geschieht, ist es wichtig, die Kommunikation zwischen Workloads sichtbar zu machen. Wirklich effektive Transparenz bedeutet, dass Sie jederzeit in vollem Kontext erkennen können, was jeder Workload tut. Darüber hinaus sind Gruppierungs- und Filterfunktionen sowohl für Ressourcen als auch für Regeln wichtige Komponenten für die schnelle und effektive Erstellung von Richtlinien.

Akamai	Herkömmliche Mikrosegmentierung
Einfache Visualisierung der gesamten Umgebung Akamai Guardicore Segmentation ist eine hostbasierte Firewall, die sowohl auf modernen als auch auf älteren Betriebssystemen ausgeführt werden kann und vollständige Transparenz über den Netzwerkfluss bis hin zu individuellen Prozess- und Serviceebenen sowohl für Windows als auch für Linux bietet und auch MacOS-Endpunkte abdeckt.	**Unvollständige Transparenz für ältere Systeme** Keine Einsicht in Microsoft Windows-Systeme vor Windows 2002. Dies liegt daran, dass der Agent herkömmlicher Mikrosegmentierungslösungen auf einer Windows-Firewall basiert, die erst für Systeme ab 2002 verfügbar war. Für Linux-Systemen unterstützen die Agents nur L4-Transparenz.
Umfassende, unübertroffene Kontextualisierung Beim Thema Transparenz sind Kontext und Details von entscheidender Bedeutung. Unsere Lösung erfasst neben dem Datenfluss auch kritische Kontextinformationen wie Prozesse, Dateien, Patch-Level und mehr.	**Minimaler Kontext** Es werden nur Informationen über Datenfluss und Geräte, nicht jedoch wichtige Kontextdetails wie Prozess- und Dateiinformationen erfasst. Dadurch ist es schwieriger und langwieriger, Abhängigkeiten von Anwendungen zu erkennen.
Keine Beschränkung der Art oder Anzahl von Labels Wir beschränken die Art oder Anzahl der Labels nicht, was Flexibilität ermöglicht und zusätzliche Nutzungsszenarien unterstützt. So müssen Sie Ihre vorhandenen Labels aus Configuration Management Datenbanken (CMDBs) und anderen Datenquellen nicht übersetzen.	**Starres Labeling** Herkömmliche Lösungen zwingen Sie mit festen, vordefinierten Kennzeichnungshierarchien dazu, Ihre Anwendungen unabhängig von den Anforderungen Ihrer eigenen Umgebung oder Ihres Unternehmens mit einer bestimmen Menge an Labels zu versehen, die sie bestimmen.
KI-gesteuertes Labeling Dank Anwendungserkennung und Labeling durch KI können Sie Anwendungen identifizieren, auch wenn es keine zuverlässige CMDB gibt, und sie dem richtigen Label zuweisen.	**Keine CMDB? Pech gehabt …** Mit manueller Kennzeichnung und einer vorkonfigurierten Label-Hierarchie wird der Kennzeichnungsprozess extrem kompliziert, falls Ihr Unternehmen nicht über eine zuverlässige CMDB verfügt.

Akamai

Branchenführende Abdeckung

Eines der Kernelemente einer guten Lösung zur Mikrosegmentierung ist die Fähigkeit, wichtige Ressourcen zu schützen, egal, wo sie bereitgestellt werden oder wo auf sie zugegriffen wird – ältere oder moderne Systeme, Windows oder Linux, Container vor Ort oder virtualisierte Container und vieles mehr.

Akamai

Vollständige Unterstützung für Windows und Linux

Die Agents von Akamai Guardicore Segmentation werden auf allen neuen und älteren Windows- und Linux-Betriebssystemen unterstützt, da unsere Lösung nicht von der zugrunde liegenden Infrastruktur abhängig ist.

Umfassende Unterstützung von Containern

Vollständige Transparenz für containerisierte Umgebungen bei gleichzeitiger Nutzung von CNI-Kontrollen (Container Network Interface) zur Durchsetzung.

Herkömmliche Mikrosegmentierung

Eingeschränkte Unterstützung für Windows und Linux

Die Durchsetzung von Richtlinien hängt für Windows-Umgebungen von der Windows-Firewall und für Linux-Umgebungen von iptables ab. Dies bedeutet unweigerlich entweder eingeschränkten oder gar keinen Schutz für einige ältere Windows-Betriebssysteme und keine L7-Regeln auf Prozessebene für Linux-Umgebungen.

Begrenzte Unterstützung für Container

Die Durchsetzung ist von iptables und der dauernden Berechnungen von Richtlinien abhängig, die in einer Container-Umgebung nicht skaliert werden können und zu Latenz und Ausfallzeiten führen.

Einfache Richtlinien erstellen. Schnell.

Mit einer guten Richtlinien-Engine können Sie Ihre Absicht in möglichst wenigen Regeln ausdrücken, ohne sprachliche Einschränkungen für Richtlinien zu erzwingen. Außerdem ist die Richtlinienverwaltung durch Automatisierung und Assistenten nicht so aufwändig.

Akamai

Zulassen und ablehnen

Wir unterstützen Regeln mit Zulassungs- und Verweigerungslisten und beliebige Kombinationen dazwischen. Auf diese Weise können Sicherheits- und IT-Teams schnell auf jedes Sicherheitsszenario reagieren und müssen nicht jeden legitimen Flow erst auf eine Zulassungsliste setzen.

Richtlinienvorlagen für eine Vielzahl von Anwendungsfällen

Sofort einsetzbare Vorlagen und Workflows zur Richtlinienbildung für übliche Szenarien – Abwehr von Ransomware, Ringfencing von Anwendungen, Umgebungssegmentierung und vieles mehr. Vorlagen helfen Ihnen, Zeit zu sparen und reduzieren menschliches Versagen.

Umfassende Richtlinienkriterien

Zu den Richtlinienkriterien gehören Quelle, Ziel, Port, Protokoll, Prozess, Service (z. B. Task Scheduler, der häufig von Ransomware verwendet wird), Nutzer und vollständig qualifizierter Domänenname (FQDN).

Herkömmliche Mikrosegmentierung

Zulassen mit eingeschränkter Unterstützung für Verweigerungsregeln

Die Einhaltung eines sicheren, aber zeitaufwendigen Zulassungsmodells erlaubt es herkömmlichen Segmentierungslösungen nicht, automatisch auf bekannte Bedrohungen zu reagieren, die eine schnelle Blockierung erfordern.

Ein begrenzter Satz von Vorlagen

Segmentierungsvorlagen werden hauptsächlich in Microsoft-Umgebungen unterstützt. Vorlagen für gängige Segmentierungsfälle wie Ringfencing und die Abwehr von Ransomware und Wiederherstellung werden nicht unterstützt.

Begrenzte Kriterien

Keine L7-Richtlinien auf Prozessebene für Linux-Betriebssysteme und keine Möglichkeit, Richtlinien auf Basis von Microsoft Windows-Diensten zu erstellen.

Sicherheit geht vor

Die Bekämpfung komplexer Sicherheitsbedrohungen wie Ransomware erfordert einen umfassenden Sicherheitsansatz. Obwohl Segmentierung sowohl vom National Institute of Standards and Technology (NIST) als auch vom Weißen Haus als grundlegende Reaktion auf Cyberbedrohungen vorgeschrieben ist, wird ein integrierter Ansatz für die Sicherheit und Erkennung von Sicherheitsverstößen benötigt, um die Sicherheit Ihres Unternehmens zu gewährleisten.

Akamai	Herkömmliche Mikrosegmentierung
Prävention und Abwehr von Ransomware Akamai Guardicore Segmentation stellt sofort einsetzbare Vorlagen für alle Phasen der Killchain bereit – von der Prävention über die Eindämmung bis zur Abwehr.	**Keine Vorlagen für Ransomware** Herkömmliche Lösungen sind nur eingeschränkt in der Lage, mit sofort einsatzfertigen Vorlagen Ransomware-Angriffe zu blockieren.
Abfrage von Endpunkten für Bedrohungserkennung und Compliance Mit unserem Osquery-basierten Tool Insight können Sie Server und Endpunkte in Echtzeit abfragen, um Compliance-Vorgaben einzuhalten und Malware zu erkennen.	**Keine Erkennung in Echtzeit** Herkömmliche Lösungen können keine schädlichen Aktivitäten im Rechenzentrum in Echtzeit erkennen.
Täuschungsfunktionen Basierend auf einer patentierten Technologie leitet der Agent von Akamai Guardicore Segmentation blockierte und fehlgeschlagene Sitzungen zur weiteren Analyse und Quarantäne an eine dynamische Deception-Engine um.	**Keine Quarantäne möglich** Herkömmlichen Lösungen mangelt es an Täuschungsfunktionen sowie an der Fähigkeit, Geräte, die bekannte Indicators of Compromise (IoCs) verwenden, zu erkennen oder unter Quarantäne zu stellen.
Managed Threat Hunting-Team Akamai bietet Managed Threat Hunting-Services, die die Möglichkeiten Ihres Sicherheitsteams erweitern, damit Ihr Unternehmen den aktuellsten Bedrohungen immer einen Schritt voraus ist.	**Keine Bedrohungsbekämpfung** Herkömmliche Anbieter können keine Threat Hunting-Services bereitstellen, die auf ihrer Lösung basieren, was angesichts von steigenden Ransomware- und Malware-Angriffen ein wichtiges Alleinstellungsmerkmal sein kann.
Threat Intelligence Firewall Um bekanntermaßen schädliches Verhalten zu verhindern, blockiert Akamai Guardicore Segmentation gefährliche IPs, Dateien und Hashes mit automatischen Firewall-Regeln.	**Keine Bedrohungsfeeds** Da herkömmliche Lösungen nicht über Bedrohungsfeeds oder ähnliche Funktionen verfügen, können sie den Zugriff auf bekannte schädliche IPs und URLs nicht verhindern.

Betrieb oder Performance und Latenz

Eine geringe Latenz ist für ein erfolgreiches Segmentierungsprojekt von entscheidender Bedeutung. Das bedeutet, dass Sie in der Lage sein müssen, Ihre Richtlinien mit mehr Regeln, Labels pro Ressourcen und anderen Richtlinienobjekten zu skalieren, ohne dabei zusätzliche Latenz zu verursachen.

Akamai

Latenzoptimierte Engine

Unsere Segmentierungs-Engine wurde für große Szenarien entwickelt. Dies wird durch einen optimierten Filtermechanismus erreicht, der zu einer Latenzzeit führt, die relativ unempfindlich gegenüber der Richtliniengröße ist.

Herkömmliche Mikrosegmentierung

Mehr Regeln führen zu einer erhöhten Latenz

Mit der wachsenden Anzahl und Größe der Regeln führen die Agents zu mehr Latenz. Linux iptables wurden schlichtweg nicht zur Skalierung von umfangreichem Ost-West-Traffic von Unternehmen entwickelt. Das Ergebnis ist eine große Latenz, die sich mit der Richtliniengröße erhöht.

Weitere Informationen über Akamai Guardicore Segmentation oder eine personalisierte Produktdemo erhalten Sie unter akamai.com/guardicore.