AKAMAI-LÖSUNGSÜBERBLICK

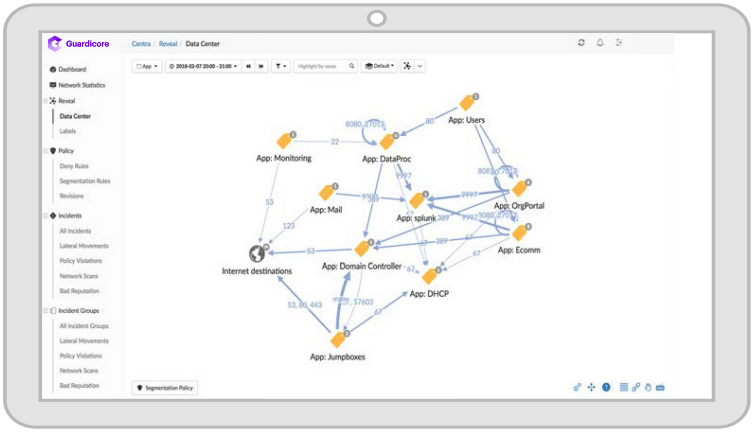
Schnelle Mikrosegmentierung in hybriden Umgebungen mit Akamai Guardicore Segmentation

Der Weg zur Implementierung von Mikrosegmentierung verläuft nicht geradlinig – es gibt viele Drehungen und Windungen, wenn Sie damit anfangen, Anwendungsabläufe in Ihrer Umgebung zu entdecken, zu verstehen und zu kontrollieren. Und ohne den richtigen Ansatz für die Navigation auf diesem Weg können Sie auf verschiedene Herausforderungen stoßen. Blinde Flecken im Netzwerk verhindern häufig eine ausreichende Erkennung und Kommunikationszuordnung von Anwendungen, Workloads und den zugrunde liegenden Prozessen. Starre Richtlinien-Engines können weitreichende Entscheidungen erfordern, die das Risiko bergen, dass Anwendungen nicht mehr richtig funktionieren. Uneinheitliche Richtlinienausdrücke in verschiedenen Betriebssystemen können zu gefährlichen Sicherheitslücken führen. Und die komplexe – und oft manuelle – Integration von Daten über Richtlinienverstöße in Angriffserkennungstools kann die Vorfallsuntersuchung und -reaktion verzögern. Akamai Guardicore Segmentation unterstützt Sie dabei, den Weg zur Mikrosegmentierung in nur drei Schritten erfolgreich zu bewältigen.

Schritt 1: Aufdecken

Automatische Erkennung von Anwendungen und Visualisierung von Abläufen

Akamai Guardicore Segmentation bietet erstklassige Transparenz, die automatisch alle Anwendungen, Workloads und Kommunikationsabläufe auf Prozessebene erkennt und visualisiert – einschließlich Kontext und unabhängig davon, wo sie sich befinden. Sie erhalten eine zentrale Ansicht für alle Assets, die sich vor Ort, in der Cloud oder in mehreren Clouds befinden. Indem Ihre Sicherheitsteams diese Visualisierung mit dem automatischen Import von Orchestrierungsmetadaten verbinden, können sie alle Assets und Anwendungen schnell und einfach kennzeichnen und gruppieren, um die Richtlinienentwicklung zu optimieren.



Schutz kritischer Anwendungen, unabhängig davon, wo sie sich befinden

Plattformunabhängig

Akamai Guardicore Segmentation kann Assets und Sicherheitsrichtlinien über Infrastrukturen hinweg visualisieren bzw. durchsetzen: vor Ort, in der Cloud und über mehrere Clouds hinweg.

Schnelle Einführung von Richtlinien

Automatisierte Regelvorschläge, eine flexible Richtlinien-Engine und eine intuitive Nutzeroberfläche sorgen für eine schnellere Erstellung und Durchsetzung von Richtlinien.

Integrierte Angriffserkennung und -reaktion

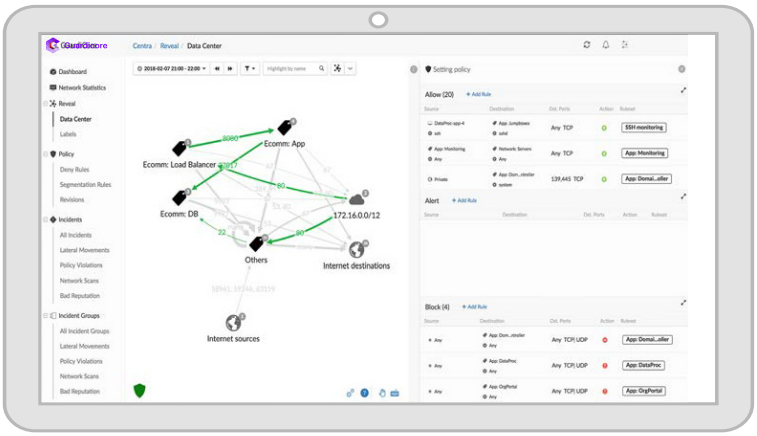
Visualisieren Sie Richtlinienverstöße und reagieren Sie schnell auf aktive Bedrohungen. So schützen Sie Ihre wichtigsten Assets, unabhängig davon, wo sie sich befinden.

Akamai

Schritt 2: Aufbauen

Schnelles Definieren, Testen und Bereitstellen von Richtlinien

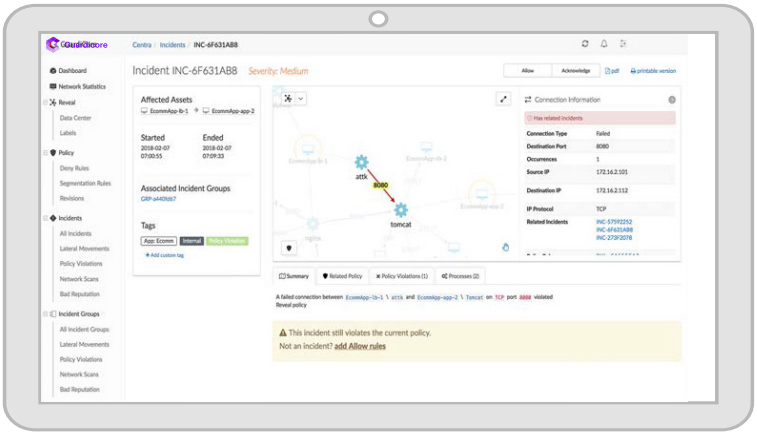
Akamai Guardicore Segmentation vereinfacht die Entwicklung und Verwaltung von Richtlinien für die Mikrosegmentierung. Durch einen einzigen Klick auf einen Kommunikationsablauf in der Übersichtskarte werden automatische Regelvorschläge auf Grundlage bisheriger Beobachtungen generiert. So können Sie schnell eine starke Richtlinie erstellen. Gleichzeitig unterstützen ein intuitiver Workflow und eine flexible Richtlinien-Engine die kontinuierliche Optimierung von Richtlinien und reduzieren kostspielige Fehler.



Schritt 3: Durchsetzen

Hohe Sicherheit in jeder Umgebung

Akamai Guardicore Segmentation kann Kommunikationsrichtlinien auf Netzwerk- und Prozessebene systemübergreifend durchsetzen und sorgt so für Sicherheit, unabhängig von Einschränkungen bei der Durchsetzung durch das Betriebssystem. Darüber hinaus können Sie mit integrierten Funktionen zur Angriffserkennung und -reaktion Richtlinienverstöße im Kontext eines aktiven Angriffs untersuchen, sodass Sie schnell die Angriffsmethode identifizieren und Abhilfe schaffen können.



Weitere Informationen finden Sie unter akamai.com/guardicore.