AKAMAI-PRODUKTBESCHREIBUNG

Segmentierung für IoT und OT

Erweitern Sie Ihre Zero-Trust-Segmentierungsfunktionen auf alle verbundenen Geräte

Viele Unternehmen nutzen IoT-Geräte (Internet of Things) und Betriebstechnologie (OT, Operational Technology), um Wachstum zu fördern, die Effizienz zu steigern und Kunden effektiver zu dienen. Diese Technologien können zwar einen erheblichen geschäftlichen Nutzen bringen, stellen aber auch einen wichtigen neuen Angriffsvektor dar, den Sicherheitsteams verteidigen müssen. IoT-Geräte neigen besonders zu Hardware- und Softwareschwachstellen und viele ältere OT-Systeme können die Sicherheitsanforderungen der vernetzten Welt nicht erfüllen. Akamai Guardicore Segmentation weitet Zero-Trust-Sicherheit auf diese Geräte aus. Das reduziert das Risiko, dass Angreifer sie ausnutzen, um Zugriff auf die IT-Infrastruktur des Unternehmens zu erhalten.

Vorteile für Ihr Unternehmen

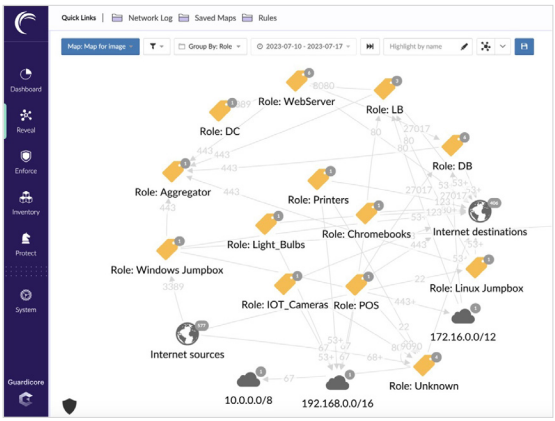
- Erkennen, Identifizieren und Klassifizieren aller angeschlossenen Geräte
- Implementieren Sie Zero-Trust-Segmentierungsrichtlinien über eine einzige Schnittstelle, einschließlich spezialisierter IoT- und OT-Systeme
- Kombinieren Sie die agentbasierte und die agentlose Richtliniendurchsetzung, um die vollständige Abdeckung zu gewährleisten

Entdecken Sie ständig neue vernetzte Geräte

Die Bereitstellung von IoT- und OT-Geräten unterscheidet sich erheblich von der Bereitstellung von Endpunkten und anderen herkömmlichen Geräten im Unternehmen. Der größte Unterschied ist, dass IoT- und OT-Geräte in viel größeren Mengen bereitgestellt werden und der Fußabdruck der Geräte sich dynamisch ändert, wenn betriebliche Anforderungen sich weiterentwickeln. Akamai Guardicore Segmentation überwacht und erkennt kontinuierlich alle verbundenen IoT- und OT-Geräte. Dadurch wird sichergestellt, dass die Kommunikation von nicht genehmigten Geräten blockiert wird und autorisierte Geräte inventarisiert und geschützt werden.

Identifizieren und kategorisieren Sie alle angeschlossenen Geräte

Akamai Guardicore Segmentation umfasst integriertes Geräte-Fingerprinting. Unser komplexer Ansatz geht weit über das problemlose Erkennen von gefälschten Gerätekennungen zur Analyse des Netzwerkverhaltens und anderer Signale hinaus, um einen vertrauenswürdigen Fingerabdruck für jedes mit dem Netzwerk verbundene Gerät zu entwickeln. Sobald Geräte identifiziert sind, werden sie in Kategorien eingruppiert, mit denen skalierbare, abstrakte Sicherheitsrichtlinien erstellt werden können.



Visualisieren Sie alle Unternehmensressourcen gemeinsam

IoT- und OT-Geräte, die über Akamai Guardicore Segmentation entdeckt und kategorisiert werden, erscheinen neben herkömmlichen Endpunkten und Anwendungs-Workloads des Unternehmens in der Reveal-Übersicht von Akamai Guardicore – einer einzigen, hochgradig interaktiven visuellen Oberfläche. So können Sicherheitsteams leicht nachvollziehen, wie alle Arten von vernetzten Geräten miteinander interagieren, und effektive Zero-Trust-Segmentierungsstrategien entwickeln, die hostbasierte und agentlose Techniken zur Umsetzung kombinieren.

Wenden Sie detaillierte Segmentierungsrichtlinien auf alle Geräte an

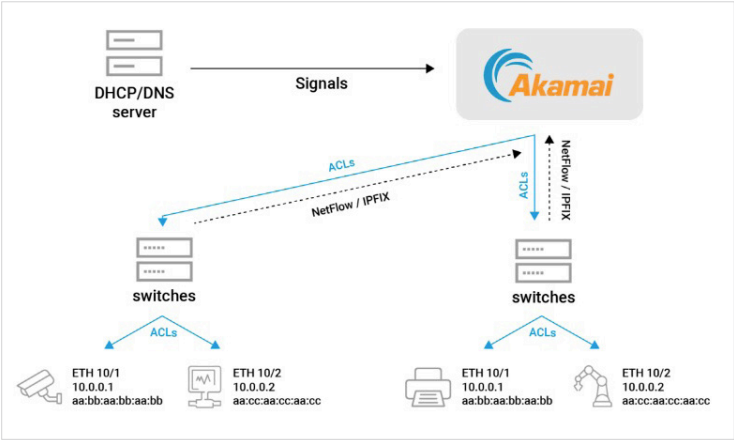
Akamai Guardicore Segmentation erweitert nahtlos seine Durchsetzung von Zero-Trust-Richtlinien um eine netzwerkbasierte Segmentierung, die speziell für IoT-Geräte und OT-Systeme entwickelt wurde, die keine hostbasierte Sicherheitssoftware ausführen können. Auf diese Weise können Sie die Kommunikation zwischen OT- und IoT-Geräten sowie anderen Netzwerkressourcen steuern und einschränken. Es ermöglicht Ihnen, sichere Grenzen festzulegen und gleichzeitig notwendige Verbindungen zu IT-Managementsystemen, dedizierten Update-Servern und Protokollierungsservern zuzulassen.

Erhalten Sie Transparenz und Kontrolle, während Geräte zu neuen Netzwerkstandorten wechseln

Die Architektur von Akamai Guardicore Segmentation sorgt auch dann für Risikobewusstsein und Transparenz, wenn Geräte zu neuen Netzwerkstandorten wechseln. So stellt sie sicher, dass die entsprechenden Zero-Trust-Segmentierungsrichtlinien – einschließlich erforderlicher standortbasierter Anpassungen – immer vorhanden sind.

So funktioniert es

Von Ihren Netzwerkgeräten erzeugter Traffic liefert Signale (z. B. DHCP, DNS, Netflow, TCP, usw.), die Akamai Guardicore Segmentation zur Identifizierung und Klassifizierung aller Geräte verwendet. Über eine einheitliche Schnittstelle können dann Segmentierungsrichtlinien erstellt werden. Für IoT- und OT-Geräte sowie andere Geräte, die keine hostbasierten Agents ausführen können, werden Segmentierungsrichtlinien durch die automatisierte Implementierung von Zugriffskontrollregeln auf Netzwerkebene durchgesetzt.



Besuchen Sie unsere Website, um mehr über die Erweiterung von Zero Trust auf IoT und OT zu erfahren