AKAMAI-PRODUKTBESCHREIBUNG

# Akamai Guardicore DNS-Firewall

## Vollständige Transparenz und Kontrolle des DNS-Traffics für Workloads

Das Domain Name System (DNS) ist für Internetservices unerlässlich, kann jedoch nicht zwischen gutartigen und schädlichen Anfragen unterscheiden. Folglich implementieren Unternehmen DNS-Firewalls, um DNS-Anfragen zu überprüfen, schädliche Domains zu blockieren und sichere Domains aufzulösen. Da die DNS-Nutzung jedoch auch Workloads, Server und andere verbundene Geräte umfasst, führt der Mangel an Transparenz und Kontrolle über diesen DNS-Traffic zu weiteren Sicherheitsrisiken.

## Einheitliche Segmentierung und eine DNS-Firewall

Akamai Guardicore Segmentation bietet in Kombination mit der Akamai Guardicore DNS-Firewall einen leistungsstarken Schutz für Ihr Netzwerk. Durch das Blockieren schädlicher DNS-Anfragen und die Isolierung kritischer Netzwerksegmente reduziert diese Integration Ihre Angriffsfläche erheblich und verhindert die Ausbreitung von Bedrohungen. Dieser zweischichtige Ansatz erhöht die Sicherheit, gewährleistet Compliance und hält die betriebliche Effizienz aufrecht, was ihn zu einer unverzichtbaren Lösung für leistungsstarken Netzwerkschutz macht.

## So funktioniert die Akamai Guardicore DNS-Firewall

Die Akamai Guardicore DNS-Firewall kann innerhalb von Minuten aktiviert werden, um für Sicherheit zu sorgen und die Komplexität zu reduzieren, ohne dabei die Performance zu beeinträchtigen. Jede angefragte Domain wird anhand der Echtzeit-Bedrohungsinformationen von Akamai überprüft und Anfragen zu schädlichen Domains werden automatisch blockiert. Dank der Nutzung von DNS als erste Sicherheitsebene werden Bedrohungen frühzeitig in der Kill Chain blockiert, noch bevor eine IP-Verbindung hergestellt wird. Darüber hinaus ist das DNS über die meisten Ports und Protokolle hinweg aktiv, sodass Sie sogar vor Malware geschützt sind, die sich nicht auf standardmäßige Webports und -protokolle verlässt.

Bei Blockierung einer DNS-Anfrage wird ein Vorfall erstellt, der Sicherheits- und Threat-Hunting-Teams detaillierte Informationen über den Grund der Blockierung, die Quelle und das Ziel der Anfrage, die in einer Karte visualisiert werden können, sowie ausführliche Details zu den Indicators of Compromise (IOCs) liefert.

### Vorteile für Ihr Unternehmen

**Umfassender Schutz vor Bedrohungen**
Durch die Filterung des DNS-Traffics an der Edge und die Durchsetzung einer Mikrosegmentierung auf interner Netzwerkebene können sich Unternehmen effektiv vor Malware, Phishing, Command and Control und Datenextraktion schützen.

**Verbessertes Threat Hunting**
Vorfälle helfen Sicherheitsteams dabei, neue Bedrohungen besser zu erkennen, zu analysieren und darauf zu reagieren. So werden die Auswirkungen von Sicherheitsverstößen minimiert und Cybersicherheitsfunktionen insgesamt gestärkt.

**Verbesserte Transparenz und mehr Kontext**
Die Kombination aus DNS-Firewall und Mikrosegmentierung bietet bessere Einblicke in DNS-Trafficmuster, um potenzielle Bedrohungen und Richtlinienverstöße zu identifizieren.

**Vereinfachte Verwaltung**
Die Integration einer DNS-Firewall mit Mikrosegmentierung optimiert das Sicherheitsmanagement durch eine einheitliche Erstellung, Durchsetzung und Überwachung von Richtlinien. Dies reduziert die Komplexität und den betrieblichen Aufwand, sodass Unternehmen ihre Sicherheitsinfrastruktur effizient verwalten können.

## Akamai Cloud Security Intelligence

Die Akamai Guardicore DNS-Firewall wird durch Akamai Cloud Security Intelligence unterstützt. Dieser Service stellt Echtzeitdaten zu Bedrohungen sowie zu den Risiken bereit, die diese Bedrohungen darstellen. Die Bedrohungsinformationen von Akamai bieten Schutz vor aktuellen relevanten Gefahren, die sich auf Ihr Unternehmen auswirken könnten. Gleichzeitig minimieren sie die Anzahl von False Positives, die Ihre Sicherheitsteams untersuchen müssen. Die Informationen basieren auf den Daten, die wir rund um die Uhr über die Akamai Connected Cloud gewinnen. Hier werden täglich 30 % des globalen Webtraffics bereitgestellt und bis zu 14 Milliarden DNS-Abfragen beantwortet. Die gewonnenen Daten werden durch Hunderte externer Bedrohungsfeeds ergänzt. Die kombinierten Datensätze werden dann ausführlich analysiert und mithilfe von verschiedenen Verhaltensanalysen, künstlicher Intelligenz und eigens entwickelten Algorithmen untersucht. Werden hierbei neue Bedrohungen erkannt, werden diese umgehend zum Threat-Intelligence-Datensatz hinzugefügt – umfassendem Echtzeitschutz steht damit nichts mehr im Weg.

## Akamai Connected Cloud

Der Akamai Guardicore DNS-Firewall-Service basiert auf der Akamai Connected Cloud, der weltweit am stärksten verteilten Plattform für Cloud Computing, Sicherheit und Inhaltsbereitstellung. Die Akamai Connected Cloud erreicht eine Verfügbarkeit von 100 %, die wir auch durch unsere Service-Level Agreements (SLAs) garantieren. Damit bieten wir Unternehmen optimale Servicezuverlässigkeit im Hinblick auf die DNS-Sicherheit.

Weitere Informationen finden Sie unter Zero-Trust-Sicherheit von Akamai.


| Veröffentlicht: September 2024