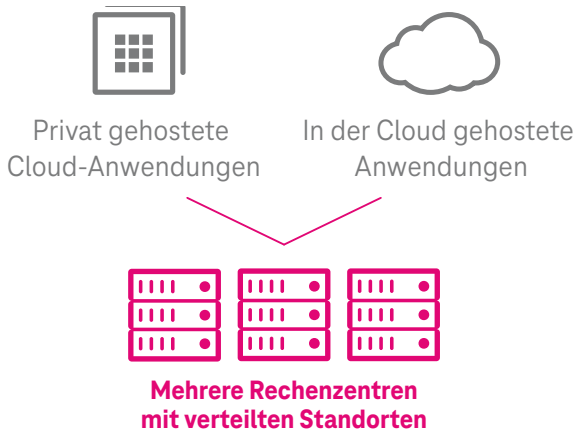
Akamai Edge Services
Führende Plattform für Enterprise Cloud Security Services

Cloud Security Services für Hybrid- & Multi-Cloud-Servicearchitekturen

Den verteidigungsfähigen Rand eines Netzwerkes gibt es nicht mehr, zumindest nicht in einer erkennbaren Form. Ein Sicherheits- und Zugriffsansatz, der vor zwanzig Jahren sinnvoll war, ist heutzutage bestenfalls falsch gewählt, schlimmstenfalls gefährlich. Wahllose wie gezielte Cyberangriffe nehmen zu. Umso wichtiger ist es, dass Unternehmen ihre Daten auch vor internen Bedrohungen – seien sie böswillig oder versehentlich – schützen. Webbasierte Geschäftsprozesse fördern Effizienz und Agilität, bieten aber auch neue Angriffsflächen, da mit jeder neue Internetverbindung neue Netz-Ports freigegeben werden. T-Systems & Akamai sind im Bereich Cloud-Sicherheit führend. Akamai bedient bis zu 30 % des weltweiten Internetverkehrs und verfügt über einen umfassenden Einblick in die Bedürfnisse des Marktes. T-Systems begleitet seit 25 Jahren Unternehmen auf ihrem Weg in die Digitalisierung und bietet hierzu die passenden Lösungen und Schutzmaßnahmen an.



Warum sollten Sie uns für Ihre Cloud Security Services wählen?

Die Sicherheitsservices werden alle durch die globale Edge-Services-Plattform von Akamai bereitgestellt, die mehr als 25 % des gesamten Internetverkehrs abwickelt. Mit dieser Infrastruktur für Threat-Intelligence-Lösungen wird Sicherheit einfacher und effektiver:

- Da die Plattform vielen Clients vorgeschaltet ist, sind die neuesten DDoS-Angriffsvektoren sofort sichtbar und werden von Akamai untersucht. Um die Gefahren zu entschärfen, implementiert Akamai sofort neue Sicherheitsmaßnahmen. Die Plattform deckt beispielsweise Angriffe auf Web-anwendungen auf und führt automatisierte Regeln ein, die auch gegen neue Schwachstellen wirken.
- Bots werden in ihrer Entwicklung und Interaktion mit der Client-Website kategorisiert und beobachtet, sodass jeder Bot individuell gesteuert werden kann.
- Reputationsdienste nutzen den Überblick über frühere bösartige Aktionen für fundiertere Sicherheitsentscheidungen.
- Die Informationen, die in der Kontroll- und Steuerungsinstanz eingehen, helfen bei der Erkennung von unberechtigten Zugriffsversuchen auf Webseiten aus dem Netzwerk heraus. Dadurch erfolgt noch schneller eine Reaktion.

Herausforderungen für Mitarbeiter

- Sicherer Zugriff auf Anwendungen
- Durchsetzung der Acceptable Use Policy (Vorschrift zur zulässigen Nutzung)

Anwendungsschutz

- Denial of Service
- Web Application Firewall
- Bot-Management
- DNS-Services

Infrastruktur-Services

- Denial of Service
- Schutz vor Malware
- Mikrosegmentierung

Die Lösungen auf einen Blick

Prolexic – DDoS-Lösung schützt Infrastruktur-Services vor Volumen-Angriffen

Über 20 netzbetreiberunabhängige Scrubbing-Center sind weltweit im Einsatz. Die gemäß SLA bereitgestellte, größtmögliche Bandbreite basiert auf Always-On-DDoS-Sicherheitsservices.

Application & API Protector – WAF-Services in Höchstform

Marktführende Position dank vollständigem Feature- und Funktionsumfang (laut Gartner). Die integrierte Lernfähigkeit ermöglicht ein automatisiertes Update-Management, das den operativen Aufwand minimiert und die Sicherheitsrichtlinien auf dem aktuellen Stand hält.

Edge DNS – DNS-Services mit 100 % Verfügbarkeit

Die separate DNS-Serviceplattform als cloudbasierte Lösung erhöht die Verfügbarkeit, Performance und Widerstandsfähigkeit der DNS-Lösung. Sie verbessert die Benutzerfreundlichkeit für Webservices, wird in privaten Rechenzentren oder öffentlichen Clouds eingesetzt und ergänzt bestehende Webinfrastrukturen.

Bot-Management – Zugriffe von Bots auf Infrastruktur verfolgen

Das Bot-Management identifiziert, kategorisiert und steuert den Bot-Verkehr und macht diesen insgesamt sichtbar. Es hilft, diesen zu protokollieren, um den Einfluss von Bots auf die IT und das Unternehmen besser zu steuern. Dabei fängt es auch ausgefeilte Bots für Internetbetrug ab, die beispielsweise auf den Missbrauch von Zugangsdaten oder Gutscheinbetrug spezialisiert sind.

Enterprise Application Access – Zugang auf Zero-Trust-Basis

Der hochleistungsfähige, KI- und cloudbasierte Service mit Identitätserkennung bietet den Nutzern jederzeit und überall einen sicheren Anwendungszugang. Er vermeidet Netzwerkkonnektivität und ist für alle Webservices verfügbar, inklusive clientbasierte und clientlose Services.

Enterprise Threat Management – Schützen Sie Ihre eigenen Infrastruktur-Services

Eine bewährte, global verteilte DNS-Plattform, die Cloud-Sicherheitsinformationen in Echtzeit nutzt. Sie identifiziert und bekämpft proaktiv und regelbasiert gezielte Bedrohungen wie Malware, Ransomware, DNS-Datenexfiltration und Phishing. Zentral gesteuert, setzt sie einheitliche Sicherheitsstandard und die Acceptable Use Policy für alle Mitarbeiter in wenigen Minuten durch.

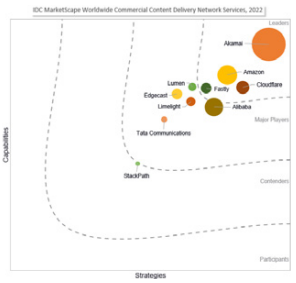
Micro-Segmentation Services – Schutz vor Ransomware (Guardicore)

Verbesserung der Sicherheit ohne Ausfallzeiten, indem sie das Netzwerk in spezifische softwarebasierte Segmente aufteilt und den Schutz erhöhen. Die Policy-Engine ermöglicht den vollständigen Einblick in die IT-Umgebung und das Selbstverteidigungssystem. Auf dieser Basis können genau abgestimmte Sicherheitsrichtlinien erstellt werden.

Gartner Magic Quadrant für Web Application & API Protection 09/2022

Forrester WaveWeb Application Firewall, Q1 2020

Forrester Wave Bot-Management, Q1 2020



IDC Worldwide Commercial CDN 08/2019

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