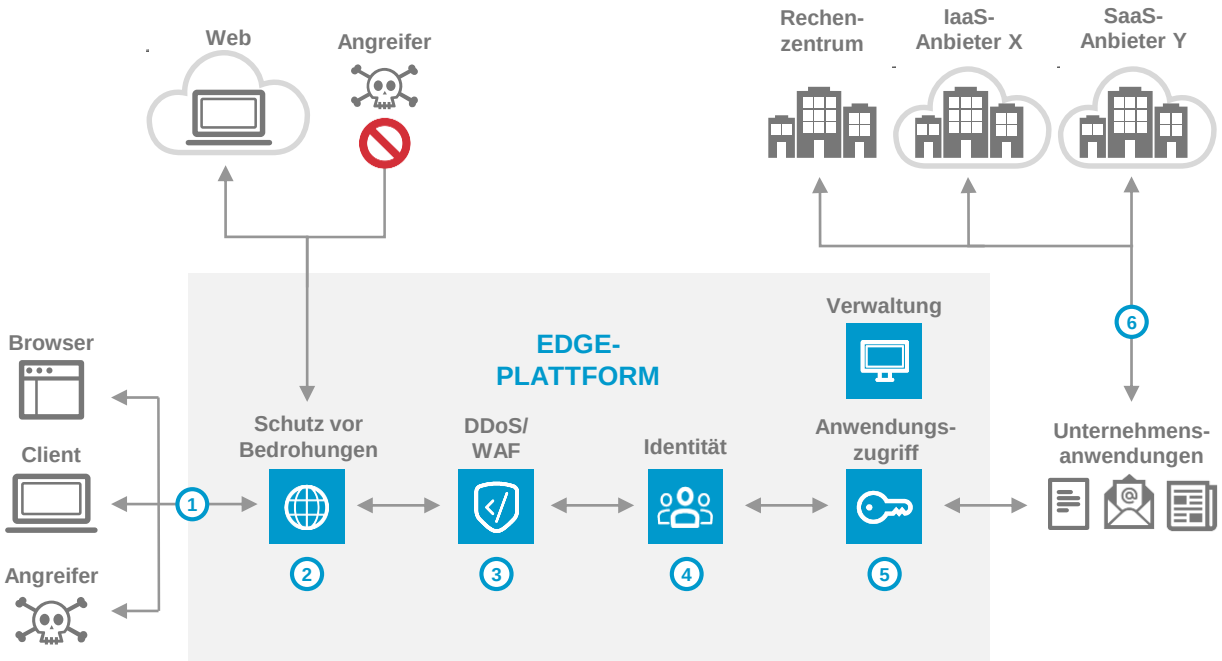
ZERO-TRUST-SICHERHEIT

Referenzarchitektur



ÜBERBLICK

Eine Zero-Trust-Sicherheitsarchitektur minimiert das Risiko, dass Cyberkriminelle in Ihr Netzwerk eindringen, sich dort frei bewegen und Daten stehlen können. Auf der Grundlage der minimalen Berechtigungsvergabe und dem standardmäßigen Default-Deny-Ansatz sorgt Zero Trust für den Schutz von Nutzern und den Zugriff über zentrale Sicherheits- und Zugriffskontrollen. Dabei können Sie sogar begrenzte Ressourcen entsprechend den Anforderungen des Unternehmens skalieren.

1. Nutzer greifen über die Akamai Intelligent Edge Plattform auf Unternehmensanwendungen und das Internet zu.
2. Nutzer werden vor Bedrohungen durch Malware, Phishing und schädliche Webinhalte geschützt bei gleichzeitiger Transparenz für das Unternehmen.
3. Bei Unternehmensanwendungen verhindern Edge-Server automatisch DDoS-Angriffe auf Netzwerkebene und prüfen Webanfragen, um bösartige Bedrohungen wie SQL Injection, XSS und RFI abzuwehren.
4. Die Identität des Nutzers wird mithilfe von lokalen, cloudbasierten oder Akamai-Identitätsspeichern ermittelt.
5. Basierend auf der Identität des Nutzers und anderen Sicherheitsmerkmalen wird der Zugriff nur für die erforderlichen Anwendungen und nicht für das gesamte Unternehmensnetzwerk ermöglicht.
6. Die Akamai Intelligent Edge Platform leitet autorisierte und authentifizierte Nutzer an die relevanten Unternehmensanwendungen weiter.

HAUPTPRODUKTE

Schutz vor Bedrohungen ► Enterprise Threat Protector
DDoS/WAF ► Kona Site Defender oder Web Application Protector
Identität und Anwendungszugriff ► Enterprise Application Access

Akamai