AKAMAI-LÖSUNGSÜBERBLICK

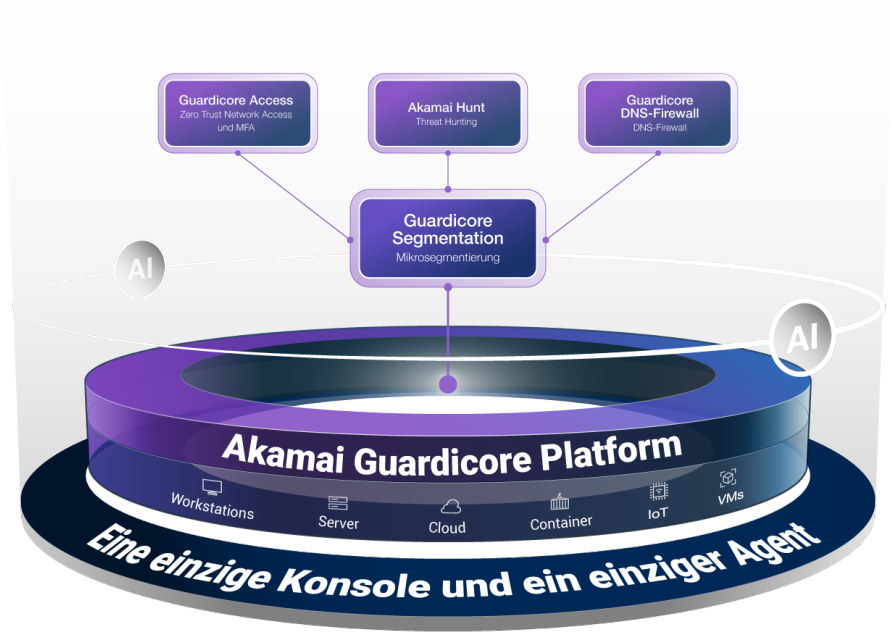
Die Akamai Guardicore Platform: Zero-Trust-Sicherheit

Die Implementierung von Zero Trust ist für die meisten Unternehmen zu komplex und zu teuer, vor allem, wenn diese Schutzmaßnahmen Assets vor Ort und in der Cloud sowie eine Belegschaft, die remote und im Büro arbeitet, abdecken müssen. Aus diesem Grund ist die Akamai Guardicore Platform so konzipiert, dass sie alle Aspekte von Zero Trust mit einer Konsole und einem einzigen Agenten effizient abdeckt.

Angesichts immer ausgefeilterer Cyberbedrohungen und immer strengerer gesetzlicher Auflagen stehen Unternehmen unter immensen Druck, ihre Netzwerke zu sichern und gleichzeitig die betriebliche Effizienz zu gewährleisten. Die Akamai Guardicore Platform bietet eine umfassende Zero-Trust-Lösung zur Bewältigung dieser Herausforderungen, mit der Unternehmen die Tools und Funktionen zur effektiven Implementierung eines leistungsstarken Zero-Trust-Sicherheitsmodells erhalten.

Die Akamai Guardicore Platform soll Zero-Trust-Projekte ermöglichen, indem sie erstklassige Mikrosegmentierung, Zero Trust Network Access, DNS-Firewall und Threat Hunting in einer Plattform vereint. Gemeinsam optimieren diese Komponenten Zero-Trust-Maßnahmen, sodass die Angriffsfläche deutlich reduziert und die Sicherheit im gesamten Unternehmen gestärkt wird.

Die Akamai Guardicore Platform



Mikrosegmentierung

Eine der Kernkomponenten der Akamai Guardicore Platform ist die Mikrosegmentierung. Üblicherweise basierte die Netzwerksicherheit auf Abwehrmechanismen am Netzwerkübergang, die sich auf die Sicherung der äußeren Netzwerkgrenzen konzentrieren. Mit der Weiterentwicklung von Cyberbedrohungen wird jedoch immer deutlicher, dass der Netzwerkschutz nicht mehr ausreicht, um sich vor ausgeklügelten Angriffen zu schützen.

Vorteile

Konsolidierte Infrastruktur
Schnelle Bereitstellung und problemlose Skalierung mit minimaler Beeinträchtigung der Performance.

Weitreichende und umfassende Transparenz
Erhalten Sie umfassende Einblicke in Netzwerkressourcen und -kommunikation.

Einheitliche Richtlinien-Engine
Vereinfachen Sie die Durchsetzung von Richtlinien in verschiedenen Umgebungen über eine einheitliche Nutzeroberfläche.

Modulare Flexibilität
Nutzen Sie modulare Komponenten, die auf Ihre Geschäftsanforderungen zugeschnitten sind.

Vollständige Abdeckung
Schützen Sie alle Ihre Assets vor Ort und in der Cloud sowie die Nutzer zu Hause und im Büro.

Branchenführende Lösungen
Kombinieren Sie branchenführende Mikrosegmentierung und Zero Trust Network Access zur Stärkung Ihrer Sicherheit.

Akamai

Bei der Mikrosegmentierung wird ein anderer Ansatz verfolgt und das Netzwerk in kleinere, besser verwaltbare Segmente unterteilt, auf die jeweils auf dem Prinzip der geringsten Berechtigungen basierende Sicherheitsrichtlinien angewendet werden. Dieser granulare Sicherheitsansatz stellt sicher, dass das übrige Netzwerk auch dann geschützt bleibt, wenn ein Segment angegriffen wird. Mit Akamai Guardicore Segmentation wird jedes Asset geschützt, einschließlich On-Premise-Rechenzentren, Cloudinstanzen, Legacy-Betriebssysteme, IoT-Geräte, Kubernetes-Cluster, und vieles mehr – ohne dass dafür Konsolen gewechselt werden müssen.

Zero Trust Network Access

Neben der Mikrosegmentierung bietet die Akamai Guardicore Platform auch Zero Trust Network Access-Funktionen. Ausgangspunkt von Zero Trust Network Access ist ein Zero-Trust-Sicherheitsmodell. Das bedeutet, dass kein Nutzer oder Gerät standardmäßig als vertrauenswürdig gilt, selbst wenn diese sich innerhalb des Unternehmensnetzwerks befinden. Stattdessen wird der Zugriff auf Ressourcen auf der Grundlage einer strengen Überprüfung der Identität, des Geräteprofils und anderer kontextbezogener Faktoren gewährt. Dieser Ansatz minimiert das Risiko unberechtigter Zugriffe und hilft Unternehmen, Datenschutzverletzungen und Bedrohungen durch interne Mitarbeiter zu verhindern.

DNS-Firewall

Eine weitere wichtige Komponente der Akamai Guardicore Platform ist die DNS-Firewall. DNS (Domain Name System) ist eine grundlegende Komponente des Internets, die menschenlesbare Domainnamen in IP-Adressen übersetzt. Es ist jedoch auch ein häufiges Ziel für Cyberangriffe, da viele Malware-Varianten DNS nutzen, um mit Command-and-Control-Servern zu kommunizieren oder Daten zu extrahieren. Durch Implementierung einer DNS-Firewall können Unternehmen schädliche DNS-Abfragen blockieren und verhindern, dass Malware mit schädlichen Domains kommuniziert, wodurch das Risiko von Datenschutzverletzungen und anderen Cyberbedrohungen verringert wird.

Threat Hunting

Schließlich umfasst die Akamai Guardicore Platform einen anpassungsfähigen Segmentierungsservice, mit dem Unternehmen Sicherheitsbedrohungen proaktiv erkennen und abwehren können, bevor daraus schwerwiegende Vorfälle werden. Das Threat Hunting umfasst die aktive Suche nach Anzeichen für eine Gefährdung im Netzwerk, wie z. B. Verhaltensanomalien oder Indicators of Compromise (IOCs). Durch die Nutzung von Threat-Hunting-Tools und -Techniken können Unternehmen Cyberangreifern einen Schritt voraus bleiben und ihre wertvollen Assets vor Schäden schützen.

Zusätzlich zu den Kernfunktionen bietet die Akamai Guardicore Platform mehrere wichtige Vorteile, mit der sie sich von anderen Sicherheitslösungen auf dem Markt abhebt. Die Plattform bietet eine reduzierte und konsolidierte Infrastruktur, die die Überladung der Agenten und eine Überlastung der Konsole minimiert, sodass Unternehmen ihre Sicherheitssysteme effizienter implementieren und verwalten können. Darüber hinaus bietet die Plattform weitreichende und umfassende Transparenz bezüglich Netzwerkressourcen und -kommunikation, sodass Sicherheitsexperten umfassende Einblicke in ihre Netzwerkumgebung erhalten und schnell und effektiv auf Bedrohungen reagieren können.

> Im Bericht Gartner®, Quick Answer: What Is Zero Trust Networking? Andrew Lerner, John Watts, 13. September 2023, empfiehlt Gartner die „Implementierung von Mikrosegmentierung und/oder Zero Trust Network Access zur Erreichung eines Zero Trust Networking-Profils“.*

* GARTNER ist eine eingetragene Marke und Dienstleistungsmarke von Gartner, Inc. bzw. seinen Vertragspartnern in den USA und weltweit und wird hierin mit Genehmigung verwendet. Alle Rechte vorbehalten.

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