AKAMAI-LÖSUNGSÜBERBLICK

Secure Internet Access Services für ISPs und MNOs

Akamai Secure Internet Access Services ermöglichen ISPs und MNOs, ihre Serviceangebote nicht nur schnell und zuverlässig bereitzustellen, sondern diese auch für verschiedene Sicherheitsanforderungen zu differenzieren. Anbieter können glaubhaft machen, dass sie ihre Vertragskunden unterstützen, und auf diese Weise dauerhaft Umsätze erzielen.

Die digitale Welt von heute hat zu einem rasanten Wandel beim Arbeits-, Lern- und Freizeitverhalten geführt. Sie hat jedoch auch das Risiko von Bedrohungen aus dem Internet erhöht. Mit den Akamai Secure Internet Access Services erhalten ISPs und MNOs grundlegende Sicherheitsmechanismen, die sie mühelos eingesetzt werden. Sie sorgen für den Schutz aller Geräte, über die sich Vertragskunden mit dem Internet verbinden – ganz gleich, ob sie am Arbeitsplatz, zu Hause oder unterwegs sind.

Die markenspezifischen Services von Akamai wurden speziell für gängige Marktsegmente – Verbraucher, KMU und große Unternehmen – entwickelt und helfen Anbietern, maßgeschneiderte Internetzugänge anzubieten und auf diese Weise dauerhaft Umsätze zu erzielen.

Mit den Funktionspaketen Essentials, Standard und Advanced können Anbieter ihr Umsatzpotenzial maximieren. Cloud-Optionen und Akamai-Integration vereinfachen und beschleunigen die Bereitstellung und somit die Markteinführung. Es stehen auch lizenzierte Alternativen zur Verfügung, um Compliance-Anforderungen zu erfüllen oder noch bessere Performance zu ermöglichen.

Die Cloud-Optionen für Secure Internet Access-Services nutzen die Vorteile der Akamai Intelligent Edge Platform, die Webressourcen, Anwendungen, Infrastruktur und Nutzer strategisch anreichert. Die stark verteilte Plattform verfügt über mehr als 4.200 Präsenzpunkte weltweit und bietet eine Kapazität von über 160 Terabit. Dank globaler Präsenz und Skalierbarkeit verfügt Akamai über eine beispiellose Transparenz zu den Angriffsaktivitäten und kann ständig wechselnde Bedrohungen verfolgen, sodass täglich Milliarden von Exploits abgewehrt werden.

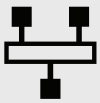
Bedrohungsinformationen und Sicherheitsforschung

Die von Secure Internet Access-Services verwendeten Bedrohungsinformationen werden von einem Team aus 20 Data Science- und Sicherheitsexperten entwickelt, die die aus weltweiten Quellen stammenden DNS-Auflösungsdaten in Echtzeit verarbeiten. Das Team konzentriert sich auf drei Kernziele:

Steigerung der Abdeckung: Wir vergleichen die von uns erkannten schädlichen Domains regelmäßig mit anderen kommerziell und frei verfügbaren Bedrohungslisten. Mehr als ein Drittel der Domain-Namen auf unseren Bedrohungslisten wird eindeutig durch unsere Erkennungsalgorithmen identifiziert.

Gewährleistung von Genauigkeit: Strenge Qualitätskontroll- und Testmethoden reduzieren False Positives auf ein Minimum. Anbieter, die eine höhere Blockierungsrate bevorzugen, haben die Möglichkeit, zwischen Domain-Klassifizierungen aus fünf Vertrauensstufen zu wählen.

Services für ISPs und MNOs



Alle Zugangsarten

Mobil, Breitband, zusammengeführt

Integrierte Sicherheit

L2–L7-Optionen, führende Bedrohungsinformationen

Funktionen für Vertragskunden

Anpassung, maßgeschneiderte Portale

Steigerung der Flexibilität: In der Regel dauert es nur wenige Sekunden, bis neue Bedrohungen in Live-Daten mithilfe von Erkennungsalgorithmen auf unserer Data Science-Plattform erkannt werden. Die Zeit bis zum Schutz – von der Erkennung bis zur Blockierung in Produktions-Resolvern in Anbieternetzwerken – beträgt weniger als 60 Sekunden.

Abdeckung

Schutz vor diversen Exploits und neuen Bedrohungen

Präzision

Minimierung des Risikos der Sperrung von zulässigem Traffic

Flexibilität

Schnelle Reaktion auf flexible Bedrohungen

Sicherheit in der Cloud

Akamai Secure Internet Access-Services verfügen zudem über ein gestaffeltes Sicherheitskonzept, mit dem sie Unternehmensressourcen schützen und die zunehmende Anzahl von Remote-Mitarbeitern unterstützen. Das cloudbasierte Secure Web Gateway bietet Sicherheit auf Anwendungsebene, erkennt ausgefeiltere Exploits und identifiziert Shadow-IT. Neben der Auswertung von DNS- und URL-Anfragen unterstützen Serviceoptionen die Überprüfung des verschlüsselten Traffics, die Payload-Analyse mit mehreren Techniken, Zero-Day-Phishing und die Vermeidung des Verlusts von integrierten Daten – und das alles bei hoher Performance und integriert in Sicherheitstechnologien für Unternehmensanwendungen. Andere nutzerfreundliche Funktionen aktivieren die Blockierung unerwünschter Inhalte und unterstützen damit Nutzungsrichtlinien, geschäftliche Compliance-Anforderungen oder den Kinderschutz.

Weitere wertschöpfende mobile Funktionen ermöglichen Datenmanagement und Netzwerk-FWaaS, sodass auch die immer stärker verbreiteten Remote-Arbeitsumgebungen mit wichtigen Kontroll- und Sicherheitsfunktionen ausgestattet werden können.

Mit einer umfassenden Palette an Funktionen, die in ihre Netzwerke integriert sind, können Anbieter die IT-Sicherheitsteams ihrer Kunden in die Lage versetzen, konsistente Richtlinien durchzusetzen, Komplexität zu reduzieren, kostspielige Backhaul-Prozesse zu minimieren und die Effizienz zu steigern.

Markenspezifisches Self-Service-Portal und APIs

Grafisch basierte Portale, die für unterschiedliche Kompetenzniveaus in verschiedenen Marktsegmenten entwickelt wurden, zeigen wichtiges Feedback und Einblicke zu Bedrohungen im Internet. Anbieter-APIs können so angepasst werden, dass sie Marke und Markenidentität vermitteln, und Funktionen und Nutzererlebnis maßgeschneidert präsentieren. Enterprise-APIs für mobile Services ermöglichen die Automatisierung und Integration mit anderen internen Systemen wie Mobile Device Management (MDM)/ Unified Endpoint Management (UEM).

Ein Self-Service-Portal für mobile Services lässt sich in MDM-Systeme integrieren, damit die Konfiguration deutlich einfacher wird. Unternehmen können innerhalb von wenigen Minuten Sicherheits- und Compliance-Richtlinien bereitstellen und Datenverwaltungsfunktionen für Tausende von SIM-basierten Geräten implementieren. Eine hierarchische Struktur ermöglicht die sichere unternehmensinterne und -übergreifende Delegierung von Konfigurationsfunktionen. Ausgereifte Business Intelligence-Funktionen auf Basis von Microsoft Power BI unterstützen detaillierte Berichte und Analysen zu Mobilgeräten, Aktivitäten und Bedrohungen. Umfangreiche APIs ermöglichen die Automatisierung und erleichtern die Integration mit anderen IT-Systemen.

Schutz von Vertragskunden

Bieten Sie grundlegende Sicherheitsmechanismen an, die sich einfach nutzen lassen und alle Geräte schützen, über die sich Vertragskunden mit dem Internet verbinden.

Erweitern Sie Ihr Portfolio an Sicherheitsservices mit Akamai

Dank der Akamai Secure Internet Access Services können Anbieter ihre Serviceangebote nicht nur schnell und zuverlässig bereitstellen, sondern diese auch für verschiedene Sicherheitsanforderungen differenzieren. Vertragskunden erhalten einen spürbaren Mehrwert durch Sicherheitslösungen der Enterprise-Klasse, die effektiv, umfassend und einfach zu nutzen sind.

Die Sicherheits- und Data Science-Experten von Akamai nutzen die unvergleichliche Transparenz der globalen Akamai Intelligent Edge Platform und anderer Echtzeit-Datenquellen bezüglich Angriffsaktivitäten und wehren täglich Milliarden von Exploits ab. Akamai verfügt über große Entwicklungsteams, die sich ausschließlich auf ISPs und MNOs konzentrieren und Produkte entwickeln, die es ermöglichen, Serviceangebote zu erweitern, Netzwerke kosteneffizienter zu betreiben und geschäftskritische und kundenorientierte Ressourcen zu schützen.

Weitere Informationen erhalten Sie unter akamai.com oder vom Vertriebsteam von Akamai.