AKAMAI-PRODUKTBESCHREIBUNG

Secure Internet Access Enterprise – cloudbasierte DNS-Firewall

Immer mehr Unternehmen setzen auf Direct Internet Access, SaaS-Anwendungen (Software as a Service), Cloudservices, Mobilität und Richtlinien für die ortsungebundene Arbeit und das Internet of Things (IoT). Doch durch diese Technologien vergrößern sie gleichzeitig erheblich ihre Angriffsfläche und sehen sich sehr schnell einer Vielzahl neuer Sicherheitsherausforderungen gegenüber. Denn der Schutz von Unternehmen und Nutzern vor gezielten Bedrohungen wie Malware, Ransomware, Phishing und Datenextraktion wird zusehends komplexer. Die komplizierten und zahlreichen Sicherheitskontrollpunkte und Sicherheitslücken bei veralteten lokalen Lösungen müssen mit sehr begrenzten Ressourcen bewältigt werden.

Akamai Secure Internet Access Enterprise ist eine cloudbasierte DNS-Firewall (Domain Name System), mit der Sicherheitsteams gewährleisten können, dass Nutzer und Geräte unabhängig von ihrem Standort sichere Internetverbindungen herstellen können – ohne die Komplexität und den Management-Overhead, die mit alten Sicherheitslösungen einhergehen. Secure Internet Access Enterprise basiert auf den Echtzeit-Bedrohungsinformationen, die Akamai aus seinen einzigartigen globalen Einblicken in Internet- und DNS-Traffic gewinnt.

Secure Internet Access Enterprise

Secure Internet Access Enterprise basiert auf der globalen Akamai Connected Cloud sowie unserem Carrier-Grade-Service für rekursives DNS. Es ist eine cloudbasierte DNS-Firewall mit einfacher Konfiguration und Implementierung – ohne dass hierfür Hardware installiert oder gewartet werden muss.

Secure Internet Access Enterprise nutzt Cloudsicherheitsinformationen von Akamai in Echtzeit, um gezielte Bedrohungen wie Malware, Ransomware, Phishing oder DNS-basierte Datenextraktion mit geringem Durchsatz proaktiv zu erkennen und zu blockieren.

Über das Akamai-Portal können IT-Teams zentral und in Minutenschnelle Sicherheits- und Nutzungsrichtlinien für sämtliche Nutzer erstellen, implementieren und durchsetzen – egal, von wo aus sich diese Nutzer mit dem Internet verbinden.

VORTEILE FÜR IHR UNTERNEHMEN

- Verlagern der Websicherheit in die Cloud mit einer cloudbasierten DNS-Firewall, die innerhalb weniger Minuten (ohne Unterbrechungen für Nutzer) konfiguriert und global bereitgestellt sowie schnell skaliert werden kann.
- Erhöhte Sicherheit dank proaktiver Blockierung von Anfragen für Websites, auf denen Malware und Ransomware gehostet wird, Phishing-Websites, C2-Server (Command and Control) sowie DNS-Datenextraktion geringem Durchsatz – basierend auf unseren umfassenden und topaktuellen Bedrohungsinformationen.
- Kontrollieren Sie die Verwendung von Shadow-IT und nicht genehmigten Anwendungen, indem Sie Anwendungen basierend auf der Kategorie oder Risikobewertung identifizieren und blockieren.
- Reduzierter Zeitaufwand für die Sicherheitsverwaltung durch Minimierung von False Positives, Reduzierung der Warnungen anderer Sicherheitsprodukte und blitzschnelle, ortsunabhängige Verwaltung von Sicherheitsrichtlinien und -updates – für umfassenden Schutz sämtlicher Standorte.

Akamai

So funktioniert es

Secure Internet Access Enterprise ist ein cloudbasierter Sicherheitsservice, der innerhalb von Minuten aktiviert werden kann, um für Sicherheit zu sorgen und die Komplexität zu reduzieren, ohne dabei die Performance zu beeinträchtigen. Dieser Schutz kann durch einfaches Weiterleiten von rekursivem DNS-Traffic an Secure Internet Access Enterprise mithilfe verschiedener Methoden bereitgestellt werden, z. B. IPsec-Tunnel, ein kleiner Client, der verwaltete DNS-Forwarder von Akamai oder eine Änderung Ihres vorhandenen DNS-Resolvers.

Jede angefragte Domain wird anhand der Echtzeit-Bedrohungsinformationen von Akamai überprüft und Anfragen zu identifizierten schädlichen Domains werden automatisch blockiert. Dank der Nutzung von DNS als erste Sicherheitsebene werden Bedrohungen frühzeitig in der Kill Chain und noch vor der Herstellung einer Internetverbindung blockiert. Darüber hinaus ist das DNS über alle Ports und Protokolle hinweg aktiv, sodass Sie auch vor Malware geschützt sind, die sich nicht auf standardmäßige Webports und -protokolle verlässt. Domains können auch auf ihren Inhalt hin überprüft werden, um Nutzer am Zugriff auf Inhalte zu hindern, die gemäß Nutzungsrichtlinie der Organisation ungeeignet sind.

Für zusätzlichen Schutz können riskante Domains zur URL-Prüfung an einen Cloud-Proxy weitergeleitet werden. Angeforderte HTTP/S-URLs werden mit der Echtzeitbedrohungsanalyse von Akamai verglichen und schädliche URLs werden automatisch blockiert.

Secure Internet Access Enterprise lässt sich mühelos in andere Sicherheitsprodukte und Reportingtools integrieren, einschließlich Firewalls, SIEM-Systeme (Security Information and Event Management) und externe Bedrohungsfeeds. So können Sie sämtliche Investitionen in die Sicherheit maximieren.

Darüber hinaus können sich Unternehmen durch die Bereitstellung des schlanken Secure Internet Access Enterprise-Clients auf Geräten wie Laptops oder mobilen Geräten, die außerhalb des Netzwerks verwendet werden, schnell und einfach schützen.

Akamai Cloud Security Intelligence

Secure Internet Access Enterprise 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 Bedrohungen, 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 11 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, maschinellem Lernen und eigens entwickelten Algorithmen untersucht. Werden hierbei neue Bedrohungen erkannt, werden diese umgehend zu Secure Internet Access Enterprise hinzugefügt – umfassendem Echtzeitschutz steht damit nichts mehr im Weg.

Akamai Connected Cloud

Der Secure Internet Access Enterprise-Service basiert auf der Akamai Connected Cloud, der weltweit am stärksten verteilten Plattform für Cloud Computing, Sicherheit und Content Delivery. Akamai Connected Cloud erreicht eine Verfügbarkeit von 100 %, die wir auch durch unsere Service-Level Agreements (SLA) garantieren. Damit bieten wir Unternehmen optimale Servicezuverlässigkeit im Hinblick auf die Internetsicherheit.

VORTEILE FÜR IHR UNTERNEHMEN

- Geringeres Risiko und mehr Sicherheit für Geräte außerhalb des Netzwerks – ganz ohne VPN dank des kompakten Secure Internet Access Enterprise-Clients, der Ihre Sicherheits- und Nutzungsrichtlinien durchsetzt.
- Schnelle und einheitliche Durchsetzung von Compliance-Vorgaben und Nutzungsrichtlinien, die den Zugriff auf ungeeignete oder unzulässige Domains und Inhaltskategorien blockieren.
- Erhöhen Sie die Ausfallsicherheit und Zuverlässigkeit mit der Akamai Connected Cloud und der Carrier-Grade-DNS-Plattform von Akamai.

Cloudbasiertes Managementportal

Die Konfigurations- und Verwaltungsaktivitäten zu Secure Internet Access Enterprise erfolgen über das cloudbasierte Akamai Control Center-Portal. So können Sie den Service jederzeit und von überall aus problemlos managen.

Richtlinien lassen sich schnell und einfach verwalten und Änderungen können in Minutenschnelle global verteilt werden. Damit sind Ihre Standorte und Mitarbeiter optimal geschützt. Konfigurieren Sie Echtzeit-Benachrichtigungen per E-Mail sowie geplante Berichte, um Sicherheitsteams über kritische Richtlinienereignisse zu informieren. So können diese sofort reagieren und potenzielle Bedrohungen erkennen und abwehren. Ein Echtzeit-Dashboard bietet eine Übersicht über den Traffic sowie über Bedrohungs- und Nutzungsrichtlinien-Ereignisse. Ausführliche Informationen zu sämtlichen Aktivitäten können über detaillierte Ansichten oder individuelle Dashboard-Elemente angezeigt werden. Diese detaillierten Informationen stellen wertvolle Ressourcen für die Analyse und Behebung von Sicherheitsvorfällen dar.

Sämtliche Portalfunktionen sind per API verfügbar und die Datenprotokolle können an ein SIEM-System exportiert werden. So lässt sich Secure Internet Access Enterprise einfach und effektiv in Ihre vorhandenen Sicherheitslösungen und Reportingtools integrieren.

Funktionen

Sicherheit
Blockieren von Malware, Ransomware sowie Phishing-Domains und -URLs
Blockieren von Malware CnC-Anfragen
Erkennen DNS-basierter Datenextraktion
Proxy für gefährliche Domains zur Untersuchung angeforderter HTTP- und HTTPS-URLs
Erstellen individueller Domainlisten zur HTTP- und HTTPS-URL-Untersuchung
Führen Sie rückblickende Analyse der Kunden-Trafficprotokolle zur Erkennung neu entdeckter Bedrohungen durch
Erstellen nutzerdefinierter White-/Blacklists
Einbinden zusätzlicher Feeds mit Bedrohungsinformationen
Nutzerdefinierte Fehlerseite
Abfragen der Akamai-Bedrohungsdatenbank, um Informationen zu schädlichen Domains und URLs einzuholen
Sicherheit für Geräte außerhalb des Netzwerks (Windows, macOS, iOS, Android, Chrome)
Nutzungsrichtlinie
Erstellen gruppenbasierter Nutzungsrichtlinien
Überwachen oder Blockieren von Verstößen gegen die Nutzungsrichtlinie durch Nutzer innerhalb und außerhalb des Netzwerks
Durchsetzen von SafeSearch für Google, Bing und YouTube

Cloud Access Security Broker (inline)
Identifizieren und Blockieren von Shadow-IT-Anwendungen
Blockieren von Anwendungen nach Risikobewertung oder Anwendungsgruppe
Durchsetzen von SaaS-Mandanten
Reporting, Überwachung und Verwaltung
IDP- und Active Directory-Integration
Unternehmensweite Übersicht aller Aktivitäten dank anpassbarer Dashboards
Detaillierte Analyse aller Bedrohungs- und Nutzungsrichtlinien-Ereignisse
Vollständige Protokollierung und Transparenz sämtlicher Trafficanfragen und Bedrohungs-/ Nutzungsrichtlinien-Ereignisse
Bereitstellung sämtlicher Protokolle: Protokolle werden 30 Tage lang aufbewahrt und können per API exportiert werden.
Konfiguration, nutzerdefinierte Sicherheitslisten und Ereignisse sind über eine API verfügbar
Integration in andere Sicherheitssysteme, wie z. B. SIEMs, über eine API
E-Mail-basierte Echtzeitbenachrichtigungen zu Sicherheitsereignissen
Planung täglicher oder wöchentlicher E-Mail-Berichte
Delegierte Verwaltung
Akamai Connected Cloud-Plattform
Dedizierte IPv4- und IPv6-VIPs pro Kunde für rekursives DNS
SLA für 100-prozentige Verfügbarkeit
Anycast-DNS-Routing für optimale Performance
Durchsetzung von DNSSEC, DoH und Dot für erhöhte Sicherheit
Zuordnung von Unternehmensgeräten
Inline-Zuordnung mit DNS-Forwarder
Offline-Zuordnung mit Security Connector
Clientbasierte Zuordnung für Laptops und Mobilgeräte (Windows, macOS, iOS, Android, Chrome)

Weitere Informationen zu Secure Internet Access Enterprise sowie eine kostenlose Testversion finden Sie auf akamai.com.

| Veröffentlicht: Januar 2024