ENTERPRISE DEFENDER

Zero-Trust-Sicherheit an der Edge

Der zu verteidigende Netzwerkperimeter gehört der Vergangenheit an – zumindest in seiner ursprünglichen Form. Ein Ansatz für sicheren Zugriff, der vor 20 Jahren einmal sinnvoll war, ist für heutige Anforderungen ungeeignet und kann sogar schnell zur Gefahr werden. Und das ist nicht nur bloße Theorie. Der Beweis sind die wachsende Zahl und das steigende Ausmaß von Datenschutzvorfällen in den letzten fünf Jahren, von denen viele das Ergebnis eines ausgenutzten Vertrauensstatus innerhalb des Netzwerks waren. Es ist an der Zeit, die Zero-Trust-Sicherheit einzuführen, mit der das Vertrauen in das Unternehmensnetzwerk abgeschafft wird und Entscheidungen über Sicherheit und Zugriff dynamisch auf der Grundlage von Identität, Gerät und Nutzerkontext getroffen werden.

ENTERPRISE DEFENDER

Enterprise Defender basiert auf der Akamai Intelligent Edge Platform und vereint Malwareschutz und adaptiven Anwendungszugriff sowie Sicherheit und Beschleunigung in einer nutzerfreundlichen Sicherheitslösung an der Edge. Mit Enterprise Defender können Unternehmen ohne Hardware oder Appliances auf Zero-Trust-Sicherheit umsteigen. Abonnieren Sie Enterprise Defender, um Risiken und Komplexität zu reduzieren und gleichzeitig das Nutzererlebnis zu verbessern.

FUNKTIONSWEISE

Enterprise Defender nutzt die Intelligent Edge Platform von Akamai, um Schutz für alle Unternehmensanwendungen und -nutzer und somit größtmögliche Sicherheit zu bieten und die Komplexität zu verringern, ohne dabei die Performance zu beeinträchtigen. Mit dieser Lösung können Sie sicher auf Anwendungen zugreifen, die in Ihrer Kontrolle liegen, und gleichzeitig die Risiken verringern, die mit dem Zugriff Ihrer Nutzer auf Anwendungen verbunden sind, die sich Ihrer Kontrolle entziehen.

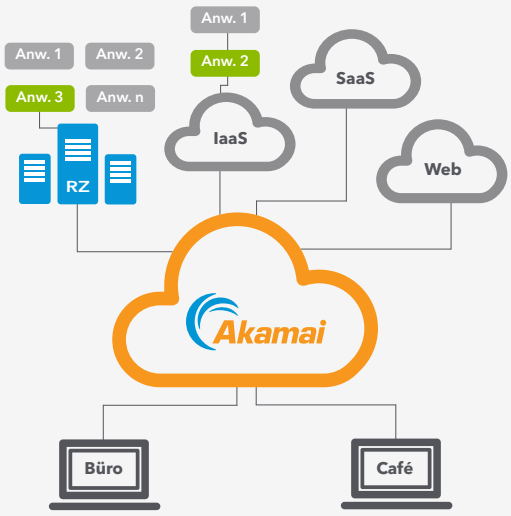
Enterprise Defender umfasst die folgenden Funktionen in einem nutzerfreundlichen Abonnementservice pro Nutzer und Monat:

Malwareschutz: Akamai erkennt und blockiert proaktiv gezielte Bedrohungen wie Malware, Ransomware, Phishing, DNS-Datenextraktion und fortschrittliche Zero-Day-Angriffe. Akamai bietet ein Secure Internet Gateway (SIG), mit dem Ihre Sicherheitsteams gewährleisten können, dass Nutzer und Geräte unabhängig von ihrem Standort sichere Internetverbindungen und den sicheren Zugriff auf Anwendungen herstellen können, die sich Ihrer Kontrolle entziehen, – ohne die Komplexität, die mit alten Lösungen einhergeht.

Sicherer Anwendungszugriff: Akamai stellt sicher, dass nur autorisierte Nutzer und Geräte Zugriff auf die von ihnen benötigten internen Anwendungen haben, und nicht auf das gesamte Unternehmensnetzwerk. Nutzer können nie direkt auf Anwendungen zugreifen, da diese vom Internet und somit der Öffentlichkeit abgeschirmt sind. Enterprise Defender vereint Datenpfadschutz, Single Sign-On, Identität, Anwendungszugriff sowie Managementtransparenz und -kontrolle in einem einzigen Service.

Web Application Firewall (WAF): Akamai bietet umfassenden Schutz für kritische Webanwendungen vor den größten und komplexesten DDoS- und Webanwendungsangriffen. Unsere WAF bietet zuverlässige Sicherheitsmechanismen für Websites, die vom branchenweit besten Threat Research Team aktualisiert werden, sodass Unternehmen stets mit den fortschreitenden Entwicklungen im Bereich Sicherheitsbedrohungen mithalten können.

Anwendungsbeschleunigung: Akamai ermöglicht Unternehmen die Bereitstellung schneller, zuverlässiger und sicherer Anwendungen – und das auch noch kostengünstig. Damit Unternehmen die Herausforderungen im Zusammenhang mit der Bereitstellung von Unternehmensanwendungen über das Internet bewältigen, werden die Funktionen zur Anwendungsbereitstellung über die Akamai Intelligent Edge Platform sehr nahe an Nutzer, Cloud und lokale Workloads gebracht – auf der ganzen Welt.



Anwendungszugriff, Beschleunigung und Sicherheitskontrollen an der Edge

Kein Zugriff für Nutzer auf das Unternehmensnetzwerk

Single Sign-on und Multi-Faktor-Authentifizierung für Unternehmensanwendungen

Blockierung des Zugriffs auf schädliche Domains, URLs und Inhalte – überall

ENTERPRISE DEFENDER

GESCHÄFTLICHE VORTEILE

- **Die Verbreitung von Malware und laterale Netzwerkbewegungen stoppen**
  In herkömmlichen perimeterbasierten Netzwerken kann Malware in der Regel aufgrund von mangelnder Segmentierung und schlechter Netzwerktransparenz tief eindringen. Enterprise Defender, die Kombination aus differenzierteren Zugriffskontrollen für bestimmte Anwendungen und proaktivem Schutz vor Bedrohungen, erschwert zum einen Angreifern den Zugriff auf andere Workloads und zum anderen die Verbreitung von Malware.

- **Die Komplexität reduzieren und Betriebsabläufe optimieren**
  Dank cloudbasierter Sicherheit wie Enterprise Defender können Teams virtuelle oder Hardware-Appliances, die eine kostspielige Verwaltung und Wartung erfordern, durch einen einfachen Sicherheitsservice an der Edge ersetzen.

- **Die Investitions- und Betriebskosten für mehr Sicherheit senken**
  Bessere Sicherheit ist oftmals mit höheren Kosten verbunden. Mit Enterprise Defender ist dies in der Regel nicht der Fall. Im Gegenteil: Durch verbesserte Sicherheit in Kombination mit cloudbasierter Einfachheit können CISOs und Sicherheitsteams mehrere, verteilte Sicherheitskontrollen konsolidieren und die Verwaltungskosten senken.

- **Die Transparenz erhöhen und die Erkennung von Angriffen beschleunigen**
  In Verbindung mit Angriffen sind oft Aussagen wie „Die Cyberkriminellen blieben *n* Monate lang unentdeckt“ oder „Nachdem die Cyberkriminellen in das Netzwerk eingedrungen waren, konnten sie sich ungehindert darin bewegen“ zu hören. Enterprise Defender, die Kombination aus detaillierterer Protokollierung von Anwendungszugriffen und DNS-basierten Sicherheitskontrollen, bietet mehr Transparenz und beschleunigt die Erkennung von Angriffen.

- **Die Extraktion von internen Daten stoppen**
  Unternehmen, deren Daten in die Hände von Cyberkriminellen gelangen, müssen mit schwerwiegenden betrieblichen Konsequenzen rechnen – etwa Geldstrafen für den unzureichenden Schutz persönlicher Daten oder Umsatzverluste aufgrund des Diebstahls geistigen Eigentums oder strategischer Pläne. Mit Enterprise Defender stoppen Sie die Extraktion interner Daten mit adaptiven Zugriffskontrollen auf Grundlage der minimalen Berechtigungsvergabe und DNS-basierter Transparenz und Sicherheit.

- **Der Transformation digitaler Unternehmen den Weg bereiten**
  Das IT- und Sicherheitsteam kann Partner bei der digitalen Transformation werden. Der Sicherheit durch geschlossene Netzwerke verdanken Teams ihren Ruf als „paranoide Aufseher“. Wenn sie zur Unterstützung eines neuen Cloudservices, Partners oder Kundenmodells Zugang zum Unternehmensperimeter gewährten, öffneten sie damit eine Tür oder Verbindung zum gesamten Unternehmensnetzwerk. Mit Enterprise Defender wird der Zugriff nur für eine begrenzte Anzahl von Anwendungen auf der Grundlage von Identität und Sicherheitskontext gewährt, und zu keinem Zeitpunkt ist der Zugriff auf das gesamte Netzwerk zulässig. Sie pflegen damit außerdem eine moderne, ortsunabhängige Unternehmenskultur, da Sie den Zugriff auf schädliche Domains, URLs und Inhalte blockieren – ganz gleich, ob Ihre Nutzer im Büro oder in einem Café sitzen.