Cloud-Applikationsschutzservices von Radware

WAF-, Bot-, ATO-, API-, DDoS- und clientseitiger Schutz in der Cloud

Herausforderungen bei der Absicherung moderner Applikationen

Applikationen sind das Herzstück Ihres Unternehmens – von modernen E-Commerce-Plattformen über cloudbasierte Produktivitätslösungen bis hin zu persönlichen Apps auf dem Smartphone. Diese Applikationen tragen nicht nur wesentlich zu Umsatz, Wachstum und Kundenbindung bei, sondern bilden auch Ihre wichtigste Plattform für Kundeninteraktion.

Das Umfeld der Applikationen wird ständig erweitert und lässt sich immer schwieriger definieren. Ganz gleich, ob vor Ort oder in der Cloud: Applikationen sind heute über verschiedene Plattformen und Frameworks verstreut. Sie sind auf JavaScript-Dienste von Drittanbietern und die Verfügbarkeit von Informationen aus anderen Drittanbieterdiensten angewiesen, mit denen sie über APIs interagieren. Infolgedessen wächst die Angriffsfläche dieser Applikationen und ihre Gefährdung nimmt zu. Applikationen werden ständig geändert und aktualisiert, und Sicherheitsrichtlinien müssen entsprechend angepasst werden, um die Applikationen und ihre Daten zu schützen und gleichzeitig die Richtlinien zur Informationssicherheit einzuhalten. Darüber hinaus hat die allgemeine Verfügbarkeit generativer KI-Tools für Hacker zu einer neuen Generation von Zero-Day-Angriffen geführt, die hartnäckig, raffiniert und aggressiv sind. Es wird immer schwieriger, sich gegen eine wachsende Vielfalt von Angriffsmethoden zu schützen, die Richtlinien zur Abwehr automatisierter Angriffe in Echtzeit anzupassen und ein hohes Sicherheitsniveau mit wenig Fehlalarmen aufrechtzuerhalten, damit kein legitimer Datenverkehr blockiert wird. Dies erfordert oft manuelle Abläufe, Betriebskosten und Fachwissen, mit denen viele Unternehmen überfordert sind.

Adaptiver, reibungsloser Applikationsschutz von Radware

Die branchenführende WAAP-Suite für Webapplikations- und API-Schutz von Radware ist eine Komplettlösung für Ihre Applikationssicherheit. Sie bietet hochmoderne WAF, API-Sicherheit, Bot-Verwaltung, DDoS-Abwehr auf Layer 7 (L7), ATO- und clientseitigen Schutz, ohne die Flexibilität und das Wachstum Ihres Unternehmens zu beeinträchtigen.

Umfassend

Umfangreicher Schutz, der alle wichtigen OWASP-Vektoren (Open Web Application Security Project) für Sicherheitsbedrohungen und Schwachstellen von Webapplikationen abdeckt

KI-gestützt und automatisiert

Automatisierung ressourcenintensiver Prozesse für höhere Sicherheit, minimale Fehlalarme und geringere Gemeinkosten: Optimierung der Sicherheitsrichtlinien, Ereignisanalyse, API-Erkennung und Schemadatei-Generierung, Business-Logic-Schutz, KI-gesteuerte Korrelation über mehrere Engines, KI-gesteuerte Verwaltung von Vorfällen

Nahtlos und adaptiv

In den Entwicklungszyklus integriert, mit schneller und einfacher Anpassung an alle Änderungen an Ihren Applikationen und der zugrunde liegenden Bereitstellungsplattform – ohne Beeinträchtigung Ihrer Geschäftsabläufe

Konsistent

Einheitliche, hochmoderne Sicherheit für alle Applikationen an jedem Ort, um unabhängig vom Hosting der Applikationen (in privaten oder öffentlichen Clouds) dasselbe Niveau an ganzheitlichem Schutz zu gewährleisten

Entlastung

Geringere Betriebskosten und besserer Schutz durch den voll gemanagten 24x7-Service des Emergency Response Teams (ERT) von Radware, sodass weniger Ressourcen für die Konfiguration von Sicherheitsrichtlinien, die Abwehr von Angriffen und die Reduzierung von Fehlalarmen benötigt werden

Vollständige Transparenz und Kontrolle

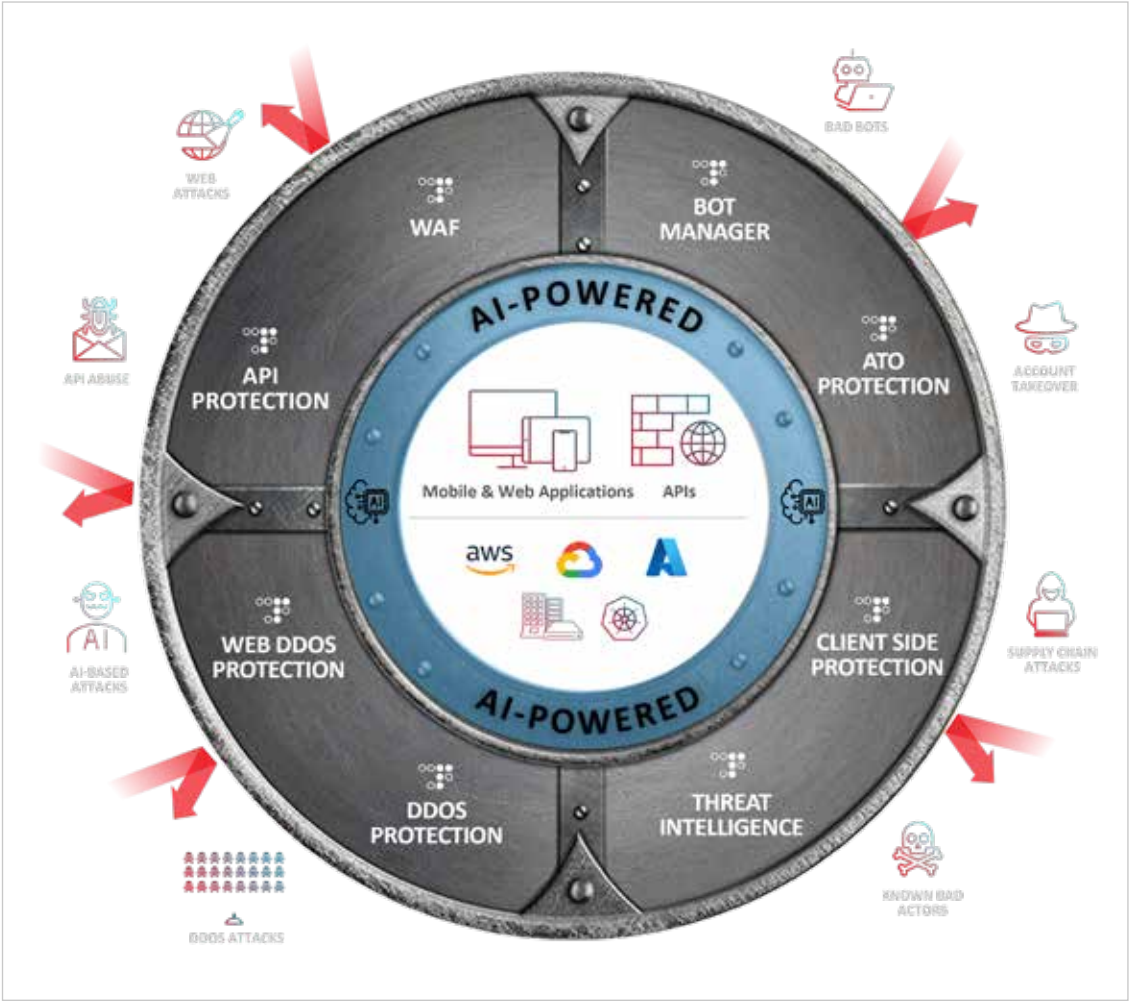
Sicherheits- und Entwicklungs-Dashboards mit aussagekräftigen Analysen, Automatisierung und benutzerdefinierten Kontrollen, die dazu beitragen, dass Sie jederzeit über Bedrohungen für Ihre Applikationen informiert sind und fundierte Entscheidungen für die Applikationsentwicklung treffen können

Umfassender Applikationsschutz: clientseitig, serverseitig und alles dazwischen

Wenn Sie Ihre Geschäfte ausbauen, Ihre Applikationsarchitektur weiterentwickeln oder Ihre Cloud-Umgebungen und -Dienste ausbauen, lässt sich Ihre Applikationssicherheit ganz einfach verwalten und nahtlos skalieren. Mit der Komplettlösung, die alle Schutzservices von Radware beinhaltet, bleiben Sie vor Bedrohungsvektoren geschützt, während Ihr Unternehmen wächst und Ihre Applikationen sich weiterentwickeln. Gleichzeitig wird die Einhaltung neuer und bestehender Vorschriften wie PCI DSS 4.0, NIS2, DSGVO, HIPAA, DORA usw. gewährleistet.

Abbildung 1:

Der Radware-Sicherheitsring: Schutz für Clientseite, Serverseite und alles dazwischen



Schutz von digitalen Ressourcen und Daten

Radware ist mit jeder Applikationsarchitektur kompatibel und schützt Ihre digitalen Ressourcen und Kundendaten in allen Umgebungen – vor Ort, in virtuellen Clouds, privaten Clouds, öffentlichen Clouds, hybriden Umgebungen und Kubernetes.

Erkennung, Verwaltung und Abwehr von Bots

Erkennen und unterscheiden Sie zwischen „guten“ und „schlechten“ Bots, um Websites, mobile Apps und APIs zu schützen. Sie können Ihre Bot-Management-Richtlinien im Nu optimieren und anpassen, um ein besseres Benutzererlebnis zu schaffen und mehr ROI aus Ihrem Applikations-Traffic zu erzielen.

Schutz vor OWASP-Schwachstellen

Bleiben Sie vor mehr als 150 bekannten Angriffsvektoren geschützt, darunter die OWASP Top 10 der Sicherheitsrisiken für Webapplikationen, die Top 10 der API-Sicherheitsschwachstellen, die Top 21 der automatisierten Bedrohungen für Webapplikationen und die Top 10 der clientseitigen Schwachstellen.

Schutz von Applikations-APIs

API-Angriffe stellen eine schnell wachsende Bedrohung für Geschäftsapplikationen und Kundendaten dar. Radware kombiniert Verhaltensanalyse und Richtlinien-automatisierung, um Ihre dynamische API-Matrix vor immer raffinierteren API-Angriffen und Business-Logic-Angriffen zu schützen.

Blockierung von KI-gestützten Zero-Day-Angriffen

Mit dem einzigartigen verhaltensbasierten positiven Sicherheitsmodell von Radware werden unbekannte Bedrohungen im Keim erstickt. Unsere KI-gesteuerten, mehrschichtigen Analyse-Engines untersuchen kontinuierlich den Applikations-Traffic und das Verhalten von Endbenutzern, um genaue Baselines zu erstellen und die Sicherheitsrichtlinien automatisch zu optimieren. So können die Benutzer jedes ungewöhnliche Verhalten erkennen und präzise blockieren.

Schutz der Clientseite vor Supply-Chain-Angriffen

Weil sich die Sicherheit auf der Serverseite verbessert, zielen immer mehr Hacker auf die weniger geschützte und selten überwachte Clientseite ab. Der clientseitige Schutz von Radware gewährleistet den Schutz der Daten von Endbenutzern, wenn sie mit Drittanbieterdiensten in der Applikations-Datenkette interagieren, und umfasst die nötigen Kontrollen für die Einhaltung von PCI DSS 4.

Abwehr von DDoS-Angriffen auf Applikationsebene

Die DDoS-Schutztechnologien von Radware ermöglichen die kürzeste Zeit zur Erkennung und Abwehr von HTTP-basierten DDoS-Angriffen. Dank patentierter Verhaltensanalyse, KI-basierter Engines und einem robusten, globalen Netzwerk für Cloud-Applikationsschutz kann Radware selbst raffinierteste HTTP-DDoS-Angriffe mit hohem Durchsatz stoppen – ganz gleich, ob sie web- oder API-basiert sind.

Bedrohungsinformationen für Sicherheits- und Entwicklungsteams

Holen Sie sich in Echtzeit verwertbare Erkenntnisse aus echten globalen Cyberangriffen, um den Angriffsverkehr zu analysieren, fundierte Entscheidungen zu treffen und Bedrohungen abzuwehren, bevor sie Schaden anrichten. Außerdem erhalten Sie Reputationswarnungen zu Angriffen im Web, die von Ihrem eigenen Netzwerk ausgehen.

KI-gestützter intelligenter Cloud-Applikationsschutz als Service

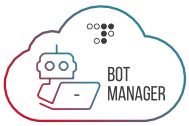
Web Application Firewall

Die adaptive und automatisierte WAF von Radware schützt vor Angriffen auf Webapplikationen, Hacking und anderen Schwachstellen. Unsere WAF-Technologie basiert auf einem KI-gestützten positiven Sicherheitsmodell, das automatisch die Verhaltensmuster legitimer Benutzeraktivitäten erlernt, die Sicherheitsrichtlinien zwecks Vermeidung von Fehlalarmen kontinuierlich optimiert und alle Aktionen, die von diesen legitimen Verhaltensmustern abweichen, präzise blockiert.

Die Kombination negativer und positiver Sicherheitsmodelle sorgt für einen umfassenden Schutz vor den OWASP-Top-10-Bedrohungen und Zero-Day-Angriffen, die WAFs mit negativen Sicherheitsmodellen nicht abwehren können, da sie auf Blockierlisten mit bekannten Angriffssignaturen beruhen.

API-Schutz

Eine spezielle, durchgängige API-Schutzlösung ist Teil der umfassenden Sicherheitsarchitektur für Webapplikationen von Radware. Diese vollautomatisierte Lösung gewährleistet die Sicherheit von Applikationen, APIs, Entwicklungsplattformen und Infrastruktur. Sie ermittelt die API-Angriffsfläche mithilfe eines automatisierten Algorithmus zur detaillierten Erkennung von API-Endpunkten und ihrer gesamten Struktur. Anschließend generiert sie maßgeschneiderte Sicherheitsrichtlinien zur Erkennung und Blockierung von gezielten API-Angriffen in Echtzeit. Durch das automatische und kontinuierliche Erlernen und Abbilden der Geschäftslogik von Applikations-APIs kann die Lösung eine Warnung ausgeben und Business-Logic-Angriffe auf APIs blockieren. Mit einer Kombination aus Zugriffssteuerung, Schutz vor Datenlecks, Bot-Management und DoS-Abwehrtools schützt sie zudem vor einer wachsenden Reihe von API-Bedrohungen, die zu den OWASP Top 10 für API-Sicherheit gehören.



Bot-Manager

Die branchenführende Radware-Lösung für Bot-Management und -Abwehr unterscheidet zielsicher zwischen menschlichem Traffic, guten Bots und schädlichen Bots und ermöglicht damit einen umfassenden Schutz von Webapplikationen, mobilen Apps und APIs vor raffinierten, KI-gestützten automatisierten Bedrohungen und Bots.

Sie bietet ein robustes und präzises Bot-Management für den Web-, Mobil- und API-Traffic, indem sie einen KI-basierten proaktiven Schutzansatz mit drei Ebenen anwendet: präventiver Schutz, verhaltensbasierte Erkennung und fortschrittliche Abwehr.

Radware Bot Manager blockiert frühzeitig unerwünschte Identitäten und nutzt dabei einzigartige Funktionen wie KI-basierte Kreuzkorrelation, JavaScript-Validierung sowie mobile Bestätigung für Android- und iOS-Geräte. Zusammen mit der eigenen Engine für sichere Identitäten werden Bot-Angriffe auf Web- und mobile Applikationen abgewehrt, bevor sie Ihre Infrastruktur schädigen können.

Die Lösung nutzt fortschrittliche KI-basierte Technologien wie Verhaltensmodellierung (granulare Intent-Analyse), verhaltensbasierte Erkennung (Aufdeckung von ausgeklügeltem Bot-Umgehungsverhalten wie rotierende IPs und Identitäten), Erkennung verteilter Angriffe, Machine-Learning-basierte Anomalie-Erkennung und Browser- und Device-Fingerprinting. Ferner können CAPTCHA-Farm-Dienste von Drittanbietern erkannt werden.

Die Lösung schützt vor allen automatisierten OWASP-Top-21-Bedrohungen, darunter Kontoübernahme, Credential Stuffing, Brute Force, Denial of Inventory, DDoS, Ad Fraud (Klickbetrug), Zahlungsbetrug und Web-Scraping, damit Unternehmen ihre Online-Aktivitäten absichern und ausbauen können.

Zudem bietet Radware Bot Manager die größte Auswahl an Abwehroptionen, einschließlich einer Blockchain-basierten kryptografischen Challenge, die die Ressourcen schädlicher Bots überlastet und gleichzeitig für eine nahtlose und CAPTCHA-freie Benutzererfahrung sorgt.

Web-DDoS-Schutz

Der branchenführende Schutz vor DDoS-Angriffen auf Applikationsebene (L7) beruht auf der einzigartigen KI-basierten Verhaltenserkennung von Radware, die zwischen legitimem und bösartigem Datenverkehr unterscheidet und automatisch granulare Signaturen in Echtzeit generiert, um vor Zero-Day-Angriffen zu schützen. Die einzigartige Lösung kann Signaturen für jede Art von Angriffsanfragen generieren, einschließlich API-DDoS-Angriffen, die mittlerweile die Mehrzahl der Angriffe ausmachen. Mit exklusiven hybriden, Always-on- und On-Demand-Cloud-DDoS-Service-Bereitstellungsmethoden sorgt der Web-DDoS-Schutzservice von Radware für erstklassige Absicherung gegen eine Vielzahl von Bedrohungen wie HTTP-Floods, HTTP-Bombs, Low-and-Slow-Angriffe, Brute-Force-Attacken und schädliche Web-DDoS-Tsunamis.

Clientseitiger Schutz

Eine fortschrittliche clientseitige Lösung gewährleistet die Einhaltung von PCI DSS 4 und schützt die Daten von Endbenutzern, wenn sie in der Datenkette der Applikation mit Drittanbieterdiensten interagieren. Blockieren Sie Anfragen an verdächtige Drittanbieterdienste in Ihrer Datenkette im Handumdrehen und halten Sie alle Datenschutzvorschriften ein. Schützen Sie sich vor clientseitigen Angriffen durch JS-Dienste von Drittanbietern (Formjacking, Skimming/Magecart), entdecken Sie automatisch und kontinuierlich alle Drittanbieterdienste in Ihrer Datenkette mit detaillierter Aktivitätsverfolgung und erhalten Sie Warnmeldungen und Bedrohungseinstufungen anhand mehrerer Indikatoren, einschließlich Skriptquelle und Zieldomäne. Beugen Sie Datenlecks vor, indem Sie unbekannte Ziele oder legitime Ziele mit unzulässigen Parametern sowie DOM-basiertes XSS blockieren. Die einzigartigen, hochpräzisen Durchsetzungsfunktionen des clientseitigen Radware-Schutzes blockieren nur heimtückische Skripte, aber keine wichtigen JS-Dienste.

ERT Active Attackers Feed

Der ERT Active Attackers Feed von Radware ist sozusagen Ihr persönlicher Netzwerkgeheimdienst. Er verstärkt den Schutz von Applikationen und Rechenzentren durch eine präventive Schutzebene über den Radware-Lösungen zur Angriffsabwehr. Der Feed versorgt Radware-Geräte und Radware-Cloud-Sicherheitsservices mit einer Liste der Angreifer, die in jüngster Zeit in Sicherheitsvorfälle verstrickt waren, z. B. DDoS-Angriffe, Angriffe auf Applikationen, Intrusions oder Scanning-Angriffe. So kann die Plattform oder der Service bekannte Angreifer frühzeitig von Ihren Ressourcen fernhalten und Angriffe im Keim ersticken.

Threat Intelligence Service

Der Radware Threat Intelligence Service verdeutlicht Ihnen, warum vor bestimmten IPs gewarnt wird, und liefert so in Echtzeit wertvolle Erkenntnisse und Zusammenhänge. Anhand dieser aussagekräftigen Informationen können Sie Bedrohungen sicher bewerten, fundierte Entscheidungen treffen und Bedrohungen proaktiv abwehren, bevor sie Schaden anrichten. Ganz gleich, ob Sie eine verdächtige IP-Adresse blockieren, Ihre Abwehrmaßnahmen optimieren oder gefährdete Systeme erkennen möchten – alles ist möglich.

Zu den wichtigsten Funktionen des Radware Threat Intelligence Service gehören:

- Verwertbare Daten aus echten Cyberangriffen
- Untersuchung jeder verdächtigen IP-Adresse mit IP Insights, offenen Proxies und Malware-Daten
- Reputationswarnungen zur Gewährleistung der Netzwerksicherheit und -integrität, indem Unternehmen proaktiv über potenzielle Cyberangriffe, die vom eigenen Netzwerk ausgehen, benachrichtig werden
- Nahtlose REST API-Integration in beliebige Umgebungen, bestehende Sicherheitsabläufe und Systeme
- Telegram Claimed Attack Reports, aus denen die Bedrohungen für Ihr Unternehmen, Ihre Branche und Ihr Land in Echtzeit hervorgehen, sodass Sie rechtzeitig gezielte Abwehrmaßnahmen ergreifen können

Modulübergreifende KI-basierte Korrelation

Die KI-gestützten Bedrohungsanalyse-Algorithmen von Radware blockieren frühzeitig und automatisch bösartige Quellen in allen Applikationen eines Accounts.

Die KI-basierte Korrelations-Engine von Radware vergleicht mithilfe von Kreuzkorrelation in Echtzeit die Sicherheitsereignisse aller aktiven Schutzmodule (WAF, API-Schutz und Bot Manager) für die ausgewählten Applikationen Ihres Accounts. Dann wird für jede Quelle ein Penalty-Score vergeben, der auf Anzahl, Typ und Schweregrad der Sicherheitsereignisse der Quell-IP basiert. Sobald ein Penalty-Score einen Schwellenwert überschreitet, wird die schädliche Quell-IP umgehend für eine bestimmte Dauer in allen aktivierten Applikationen gesperrt, unabhängig davon, ob sie eine oder mehrere Applikationen angegriffen hat. Durch diese einzigartige Methode, um das bösartige Verhalten von Quell-IPs zu analysieren und sie bei Bedarf zu blockieren, wird Ihre Sicherheitsstrategie um eine hochpräzise proaktive Schutzebene ergänzt. Sie verhindert, dass eingehender schädlicher Datenverkehr Ihren Applikationsserver überlastet, und reduziert die Gemeinkosten für die Infrastruktur und das Sicherheitsmanagement Ihrer Applikationen.

Globales Netzwerk für Cloud-Applikationsschutz

Die Cloud-Applikationsschutzservices von Radware basieren auf Radwares globalem Netzwerk verteilter Points of Presence (PoP) für Applikationssicherheit und Scrubbing Center für DDoS-Abwehr.

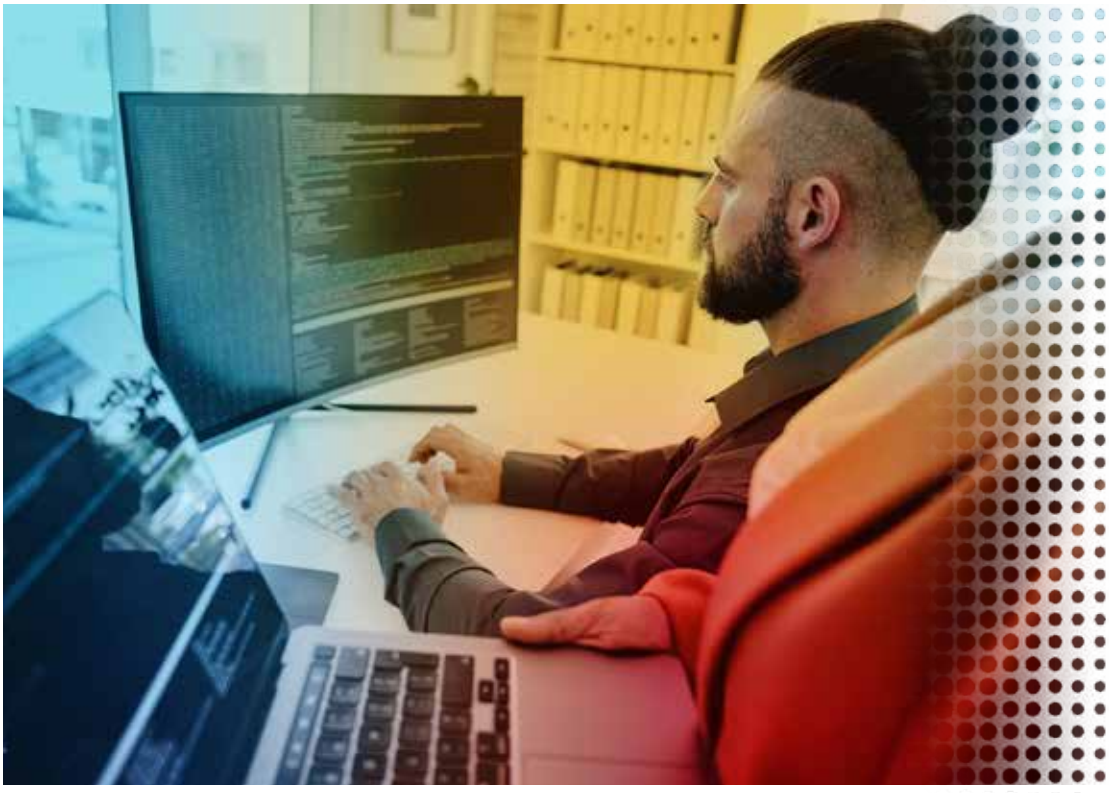
Mit Standorten an wichtigen Traffic-Hubs, die mit Tier-1-ISPs verbunden sind, und einer globalen Abwehrkapazität von 15 Tbit/s schützt Sie das Cloud-Netzwerk von Radware in der Nähe Ihres Ursprungsservers, um niedrige Latenzzeiten und minimale Leistungsbeeinträchtigungen bei Webapplikationen zu gewährleisten.

Applikationsschutz für jede Cloud mit Radware SecurePath®

Radware SecurePath® ist eine innovative, API-basierte Sicherheitsarchitektur für Cloud-Applikationen. Sie wurde für den optimalen Schutz von Applikationen entwickelt, die in beliebigen Clouds oder Rechenzentren (vor Ort, private Cloud oder öffentliche Cloud-Umgebungen) bereitgestellt werden. Gleichzeitig gewährleistet sie einen konsistenten, hochwertigen und umfassenden Schutz.

Mit Radware SecurePath® können die Radware-Applikationsschutzservices inline eingesetzt werden, wo sie als „Mittelsmänner“ oder als API-basierter Out-of-Path-Service fungieren. Letzteres ermöglicht es, dass Applikationsanfragen ohne Unterbrechung direkt vom Client zum Applikationsserver geleitet werden. Dieser innovative Ansatz eröffnet viele Vorteile, darunter:

- **Kürzere Latenzzeit** – Das gleiche Sicherheitsniveau wird ohne die Inline-Latenzzeit erreicht.
- **Keine gemeinsame Schlüsselnutzung** – Da SSL-Zertifikate nicht gemeinsam genutzt werden, erfolgt ihre Verwaltung ausschließlich am Ursprungsort, was sie privater, effizienter, schneller einsetzbar und einfacher zu pflegen macht.
- **Keine Traffic-Umleitung** – Es sind keine Änderungen am DNS- (Domain Name Server) oder BGP-Routing (Border Gateway Protocol) erforderlich, um Schutz zu erhalten. Die Anfragen gehen vom Client direkt an den Applikationsserver. Nur Kopien wichtiger Transaktionsparameter werden zur Überprüfung an die Applikationsschutz-Cloud von Radware gesendet.
- **Höhere Betriebszeit** – Da der Datenverkehr nicht inline geprüft wird, werden die Kunden nicht durch Überlastung oder Ausfälle beeinträchtigt.
- **Keine Engpässe** – Latenzschwellen können festgelegt werden, um Überlastung zu vermeiden.



Applikationsschutz und das Content Delivery Network: Das Beste aus beiden Welten

Wenn Kunden die Sicherheit ihrer Webapplikationen mit der Applikationsbereitstellung kombinieren möchten, bietet Radware ein integriertes Content Delivery Network (CDN), das direkt in den Radware-Stack für Applikationssicherheit und das Verwaltungsportal eingebunden ist. Die CDN-Lösung von Radware basiert auf dem Amazon CloudFront CDN, was für eine massive, weltweit verteilte Präsenz, bessere Leistung und DevOps-Benutzerfreundlichkeit sorgt. Das integrierte CDN von Radware ist direkt in das Portal für Radware-Cloud-Sicherheitsservices eingebunden, um die Verwaltung und Berichterstattung in einem einzigen Dashboard zusammenzuführen.

Zu den wichtigsten Merkmalen zählen:

- Massive Kapazität auf Basis des AWS-Netzwerks
- Globale Präsenz mit über 600 Points of Presence (PoP) in mehr als 100 Städten in mehr als 50 Ländern
- Einheitliche Verwaltung innerhalb des Portals für Radware-Cloud-Sicherheitsservices
- Ein einziger SSL-Schlüssel (der auch für die WAF verwendet wird)
- Erweiterte Kennzahlen und Berichte
- Kostenwirksamkeit
- Extrem schnell (schneller als die meisten CDN-Anbieter, siehe www.cdnperf.com/)
- Gemanagte Services für weniger Sorgen bei geringeren TCO

Gemanagter Applikationsschutz

Die Sicherheitsexperten des Emergency Response Teams (ERT) von Radware stehen jeden Tag rund um die Uhr für proaktive Sicherheitsservices zur Verfügung, wenn Kunden mit unterschiedlichsten Angriffen auf der Applikations- und Netzwerkebene konfrontiert sind. Mit Unterstützung des Bedrohungsanalysezentrums von Radware bekämpfen die ERT-Ingenieure täglich gängige und neuartige Angriffe und stellen den Kunden führende Branchenkenntnisse und Informationen zur Verfügung, damit sie die Applikationssicherheitslösungen von Radware auch dann nutzen können, wenn ihnen intern das Know-how über Applikationsschutz fehlt.

Load Balancer as a Service (LBaaS)

Radware Load Balancer as a Service (LBaaS) ist in die Cloud-Applikationsschutzservices von Radware integriert und auf die steigenden Bedürfnisse moderner IT-Infrastrukturen abgestimmt. Mit einer Reihe von Funktionen, die die Konfiguration vereinfachen und die Effizienz steigern sollen, werden alle Load-Balancer-Konfigurationen an einem zentralen Ort konsolidiert. So erhalten Benutzer eine nahtlose, bequeme Verwaltung mit mehr Kontrolle über ihre Load-Balancing-Anforderungen.

Radware Load Balancer as a Service ergänzt die Cloud-Applikationsschutzservices durch verbesserte SLAs und Skalierbarkeit, gewährleistet aber auch hohe Verfügbarkeit und den Schutz aller Ursprungssites. Die Lösung ermöglicht kontinuierliche automatische Health Checks des Ursprungsservers, Active/Active-Traffic, Benutzer-Load-Balancing zwischen Ursprungssites und URL-basiertes Server-Load-Balancing, um den Ressourcenzugriff und die Serverleistung zu optimieren. Außerdem stehen fortschrittliche Persistenzfunktionen bereit: IP-Persistenz, um eine gleichbleibende Netzwerkkonnektivität sicherzustellen, indem eine konstante IP-Adresse für das Gerät oder den Benutzer beibehalten wird, und Cookie-basierte Persistenz, um eine personalisierte und einheitliche Benutzererfahrung bei verschiedenen Besuchen zu gewährleisten, indem Cookies im Webbrowser des Benutzers gespeichert werden.

DNS as a Service

Radware DNSaaS (Domain Name System as a Service) ermöglicht eine umfassende DNS-Verwaltung, was für den reibungslosen Betrieb jeder Online-Applikation entscheidend ist. Durch die Nutzung von DNSaaS stellen Kunden der Cloud-Applikationsschutzservices von Radware sicher, dass ihre Applikationen geschützt, verfügbar und leistungsstark bleiben.

Die zentrale DNSaaS-Verwaltungskonsole ist vollständig in das Radware-Portal für Cloud-Applikationsschutz integriert und bietet eine benutzerfreundliche Oberfläche für die Verwaltung aller DNS-Hosts, Datensätze und Health-Check-Konfigurationen an einem einzigen Ort. Durch Steuerung der Traffic-Verteilung auf bestimmte Ressourcen oder Endpunkte sowie Echtzeitanalysen und -überwachung verbessert Radware DNSaaS die Latenzzeiten und garantiert Ihren Endbenutzern eine nahtlose Erfahrung.

Zusammenfassung

Mit den Cloud-Applikationsschutzservices von Radware können Unternehmen die Applikationssicherheit verwalten und für ihre wachsenden Geschäftstätigkeiten skalieren, Applikationsarchitekturen weiterentwickeln und ihre Cloud-Umgebungen und -Dienste ausbauen. Die Lösung bietet folgende Vorteile:

Umfassender Schutz

Ein One-Stop-Shop für Applikationsschutzlösungen: WAF, Bot-Management sowie API-, clientseitiger und Web-DDoS-Schutz.

KI-gestützte intelligente Sicherheit

Umfassender Schutz vor bekannten Bedrohungen und Zero-Day-Angriffen auf der Grundlage fortschrittlicher, patentierter Verhaltensanalysetechnologie, die auf KI und maschinellem Lernen basiert.

Geringere Gemeinkosten und kürzere MTTR

KI-gestützter adaptiver Schutz mit automatischer Analyse und Richtlinienoptimierung, gemanagten Services und 24x7-Support durch das Radware ERT.

Zentralisierte Verwaltung und Berichterstattung

Ein zentraler Ort für die Verwaltung und Überwachung der Sicherheit Ihrer Applikationen, unabhängig davon, wo diese bereitgestellt werden.

Flexible Bereitstellung und Kompatibilität

Aufrechterhaltung desselben Schutzniveaus in jeder Umgebung: vor Ort, virtuelle Clouds, private Clouds, öffentliche Clouds, Multi-Clouds, hybride Umgebungen oder Kubernetes.

Einhaltung von Datenschutz- und Sicherheitsstandards

Ganzheitliche Applikationsschutzlösung mit spezifischen Kontrollen, Transparenz und Berichten zur Einhaltung von Sicherheitsstandards wie PCI DSS 4, DSGVO, HIPAA, NIS2 und DORA.

Fundierte Entscheidungen anhand von Echtzeit-Bedrohungsdaten

Informationen zu jeder IP-Adresse, um ihre Herkunft und Legitimität zu klären und Ungewissheit in Gewissheit zu verwandeln.

Dieses Dokument wird ausschließlich zu Informationszwecken bereitgestellt. Die Fehlerfreiheit dieses Dokuments wird nicht garantiert, und das Dokument unterliegt keinerlei sonstigen Garantien oder Bedingungen, unabhängig davon, ob diese mündlich gegeben werden oder sich aus dem geltenden Recht ableiten. Radware schließt jegliche Haftung für dieses Dokument aus. Durch dieses Dokument entstehen keine direkten oder indirekten vertraglichen Verpflichtungen. Die hier beschriebenen Technologien, Funktionen, Dienste und Prozesse können ohne Vorankündigung geändert werden.

© 2025 Radware Ltd. Alle Rechte vorbehalten. In diesem Dokument genannte Produkte und Lösungen von Radware sind durch Marken, Patente und Patentanmeldungen von Radware in den USA und anderen Ländern geschützt. Weitere Informationen finden Sie unter https://www.radware.com/LegalNotice/. Alle anderen Marken und Namen sind Eigentum ihrer jeweiligen Inhaber.

RWI 153 | 06.10.2025