IDC MarketScape

IDC MarketScape: Weltweite Unternehmensplattformen zum Schutz von Webanwendungen und APIs 2024 – Anbieterbewertung

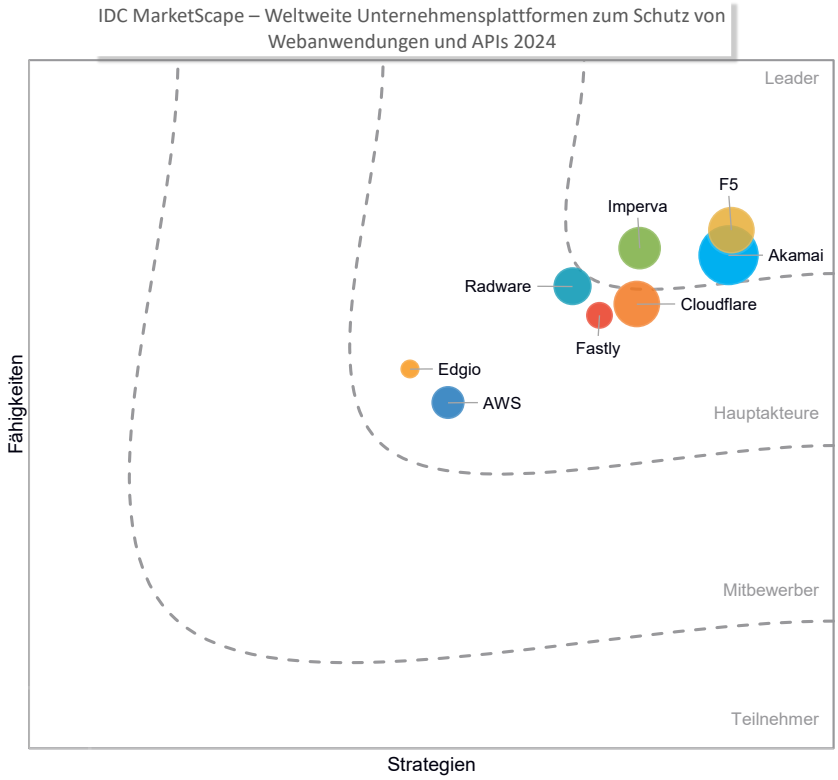
Christopher Rodriguez

THEMA DIESES IDC MARKETSCAPE-AUSZUGS: AKAMAI

IDC MARKETSCAPE-ABBILDUNG

ABBILDUNG 1

IDC MarketScape: Weltweite Unternehmensplattformen zum Schutz von Webanwendungen und APIs – Anbieterbewertung



Quelle: IDC, 2024

September 2024, IDC #US51795524e

Einzelheiten zu Methodik, Marktdefinition und Bewertungskriterien finden Sie im Anhang.

INHALT DIESES AUSZUGS

Der Inhalt dieses Auszugs ist unmittelbar folgender IDC MarketScape-Studie entnommen: Weltweite Unternehmensplattformen zum Schutz von Webanwendungen und APIs 2024 – Anbieterbewertung (Doc # US51795524). Die folgenden Abschnitte wurden ganz oder teilweise in diesen Auszug aufgenommen: IDC-Standpunkt, IDC MarketScape-Einschlusskriterien für Anbieter, Wichtige Hinweise, Kurzprofil des Anbieters, Anhang und Mehr erfahren. Zudem wurden Abbildung 1 und 2 übernommen.

IDC-STANDPUNKT

Webanwendungen sind grundlegende Komponenten des modernen digitalen Geschäftslebens und bieten die notwendige Funktionalität für die Interaktion mit Kunden und Interessenten, Partnern und Gästen sowie Mitarbeitern und Auftragnehmern. Angreifer durchsuchen diese Anwendungen und ihre Anwendungsprogrammierschnittstellen (APIs) ständig nach Möglichkeiten, Daten zu stehlen, sich unberechtigten Zugang zu verschaffen oder Unternehmen zu betrügen, um sich persönlich zu bereichern. Angriffe auf Webanwendungen und APIs haben zu schwerwiegenden Datenschutzverletzungen, kostspieligen Ausfallzeiten und realen Auswirkungen wie Diebstahl geführt. Endnutzer und Kunden tragen oft die Hauptlast der Auswirkungen durch finanzielle Verluste. Dies kann letztlich zu einem Vertrauensverlust der Kunden und zu einer geringeren Bereitschaft führen, Geschäfte online abzuwickeln.

Cyberkriminalität ist mehr als ein Ärgernis. Sie hat das Potenzial, die Geschäftsergebnisse zu verschlechtern und zu unterbrechen. Im Laufe der Jahre haben Unternehmen eine Vielzahl von Sicherheitstools eingeführt, um den sich ständig ändernden Bedrohungstaktiken und den sich ausweitenden Angriffsflächen zu begegnen. Web Application Firewalls (WAF) bieten einen grundlegenden Schutz gegen bekannte und neu auftretende Exploits auf Anwendungsebene. Unternehmen haben zahlreiche spezialisierte Lösungen wie DDoS-Abwehr, Bot-Management und seit kurzem auch API-Sicherheit eingeführt.

Der Schutz von Webanwendungen und APIs (WAAP) kombiniert diese grundlegenden Sicherheitstechnologien in einer integrierten, kohärenten Plattform, um einen zuverlässigen Schutz gegen die zahlreichen Online-Bedrohungen zu bieten.

Konsolidierte, integrierte Plattformen tragen dazu bei, Sicherheitslücken zu schließen, die Komplexität der Verwaltung zu reduzieren und Inspektionen zu optimieren. Untersuchungen von IDC zeigen, dass 77 % der Unternehmen die Integration von Sicherheitslösungen als „wichtig" oder „äußerst wichtig" einstufen. Anwendungen sind tagtäglich einer Vielzahl von Bedrohungen ausgesetzt, und Angreifer setzen gezielt verschiedene Taktiken ein, um Schwachstellen in der Verteidigung zu identifizieren. Daher sind die Sicherheitsstrategien für Anwendungen, die sich auf spezielle Sicherheitssilos konzentrieren, letztendlich zum Scheitern verurteilt. Sicherheitskonvergenz und -konsolidierung sind ein entscheidender Schritt, um die Sicherheit zu erhöhen, sei es durch eine verbesserte Erkennungsgenauigkeit, die Reduzierung von Fehlalarmen oder die zuverlässige Erkennung von fortgeschrittenen und Zero-Day-Bedrohungen.

Die Konvergenz bringt jedoch auch viele geschäftliche Vorteile mit sich, wie zum Beispiel einen geringeren Zeit- und Ressourcenaufwand für die Bereitstellung und Verwaltung, ein verbessertes Nutzererlebnis und bessere Analysen. Darüber hinaus reduziert die Ausführung aller Sicherheitsfunktionen in einem Dienst die Latenzzeit, die durch die Weiterleitung des Datenverkehrs an mehrere Sicherheitskontrollpunkte entsteht.

Gleichzeitig müssen die Unternehmen bei der schrittweisen Einführung des gesamten Spektrums an Technologien zum Schutz von Anwendungen einen maßvollen Ansatz verfolgen, je nach Bedarf und Verfügbarkeit von Zeit und Ressourcen. Für Kunden ist eine modulare, integrierte Plattform für eine einfache, schrittweise Implementierung von WAAP unerlässlich. Für die Anbieter besteht die Herausforderung darin, die genaue Mischung der integrierten Funktionen in den Kernbereichen der Sicherheit zu bestimmen, die auf den verschiedenen Produktebenen enthalten sein sollten.

Bei WAFs handelt es sich zwar um grundlegende Komponenten, aber ohne eine kohärente API-Strategie ist ein moderner Anwendungsschutz nicht möglich. APIs spielen heute eine wichtige Rolle in der modernen digitalen Geschäftswelt, da sie einen optimierten und effizienten Prozess für die Integration von Anwendungen bieten, um leistungsstarke neue Funktionen bereitzustellen. APIs verändern jedoch die Angriffsfläche auf neue Weise. APIs sind anfällig für Fehlkonfigurationen, die Offenlegung sensibler Daten und Denial-of-Service-Angriffe. Es ist wichtig zu beachten, dass APIs zwar für viele der gleichen Angriffe anfällig sind, die auf Benutzerschnittstellen abzielen, dass sie aber auch API-spezifische Bedrohungen wie BOLA (Broken Object-Level Authorization) aufweisen. APIs bieten auch eine Möglichkeit zur Kommunikation zwischen Anwendungen, die möglicherweise nicht durch eine Perimeterschutzlösung wie WAF geschützt ist. Dies kann zu einem blinden Fleck in der Sicherheit führen, den Angreifer ausnutzen können, um hinter netzwerkbasierten Abwehrmaßnahmen lateral tätig zu werden.

Die Kombination von WAF- und API-Sicherheit ist entscheidend, um eine vollständige Abdeckung von Webanwendungen über alle Schnittstellen und Angriffsflächen hinweg zu gewährleisten. Abgerundet wird das WAAP-Wertversprechen durch Technologien, die auf spezielle Bedrohungsarten wie DDoS-Attacken und unerwünschte Bot-Aktivitäten abzielen. Diese Bedrohungen unterscheiden sich stark hinsichtlich ihrer Erkennbarkeit, der Schwierigkeit ihrer Eindämmung, der Häufigkeit ihres Auftretens und der Schwere ihrer Auswirkungen. Letztendlich erfordert ein vollständiger Stack zum Schutz von Anwendungen WAF- und API-Sicherheit, DDoS-Abwehr und Bot-Management. Die spezifischen technischen Anforderungen von APIs und die besonderen Anforderungen von DDoS-Angriffen und Bot-Aktivitäten bedeuten jedoch, dass die Entwicklung hin zu WAAP ein langer und komplizierter Weg ist.

IDC MARKETSCAPE-EINSCHLUSSKRITERIEN FÜR ANBIETER

WAAP ist eine konvergente Sicherheitslösung für den aktiven Schutz von Anwendungen mit WAF als Kernkomponente. In diesem Abschnitt hat IDC wichtige Attribute identifiziert, die eine Lösung aufweisen muss, um in die IDC MarketScape-Analyse für WAAP-Unternehmensplattformen aufgenommen zu werden.

Anbieter müssen eine konvergente WAAP-Lösung anbieten, die mindestens zwei der folgenden Elemente in einer einheitlichen Sicherheitsplattform kombiniert:

- API-Sicherheit
- Bot-Verwaltung
- DDoS-Abwehr
- Web Application Firewall

Beachten Sie, dass die WAF als grundlegend angesehen wird und enthalten sein muss, um als WAAP zu gelten. Darüber hinaus werden einmalige Verkäufe von WAAP-Komponenten als eigenständige Lösungen nicht als WAAP gezählt.

Zudem umfasst diese IDC MarketScape-Analyse die folgenden Anforderungen an die Marktteilnahme und -präsenz:

- **Teilnahme am Markt:** Der Anbieter bietet ab 2023 wichtige WAAP-Funktionen als einheitliche Lösung an. Bestimmte Kern- oder erweiterte Funktionen können als Teil eines anderen Pakets oder einer anderen Plattform oder als eigenständige Lösungen angeboten werden, sofern die Funktionen nicht nur als eigenständige oder separate Produkte angeboten werden. Eine vollständige und detaillierte Beschreibung der erforderlichen und optionalen Funktionen finden Sie im Abschnitt Marktdefinition.

- **Marktpräsenz:** Der Anbieter erreicht 2023 einen festgelegten Mindestumsatzanteil auf dem wettbewerbsintensiven WAAP-Markt, wie der IDC-Tracker für Sicherheitsprodukte bestätigt.
- **Globale Präsenz:** Der Anbieter hat eine Mindestverteilung der Umsätze auf jede der großen globalen Regionen, einschließlich Nordamerika, Lateinamerika, EMEA und Asien/Pazifik, ab 2024, wie im IDC-Tracker für Sicherheitsprodukte bestätigt.

IDC weist darauf hin, dass einige Cloud- und Sicherheitsanbieter, die Komponenten eines WAAP anbieten, in der Analyse nicht berücksichtigt wurden, da sie sich auf einzelne Produkte konzentrieren und keinen integrierten WAAP-Ansatz verfolgen. Ebenso haben einige Anbieter, die WAAP anbieten, die Mindestanforderungen an die Marktpräsenz oder die weltweite Präsenz nicht erreicht.

EMPFEHLUNG FÜR TECHNOLOGIE-EINKÄUFER

Wichtige Überlegungen zu den Fähigkeiten der Anbieter

Die IDC MarketScape-Analyse für WAAP-Unternehmensplattformen berücksichtigt das von IT-Einkäufern geforderte und erwartete Sicherheitsniveau, den Integrationsgrad, die Benutzerfreundlichkeit, relevante professionelle und Managed Services sowie die Gesamtbetriebskosten. Auf Unternehmensebene muss eine WAAP hervorragenden Schutz bieten, die Auswirkungen der Sicherheit auf die Leistung reduzieren und die Endbenutzererfahrung so wenig wie möglich beeinträchtigen. Die Analyse unterstreicht auch das Hauptziel von WAAP, nämlich die Kombination mehrerer wichtiger Sicherheitstechnologien in einer einzigen integrierten und kohärenten Plattform. Erweiterbarkeit und das Angebot verschiedener Preismodelle sind ebenfalls erforderlich, um die WAAP-Implementierung so zu gestalten, dass sie dem Bedarf an konsistentem Schutz vor den zahlreichen Online-Bedrohungen und dem Bedürfnis nach geschäftlichem Mehrwert am besten gerecht wird.

Die Erwartungen der Nutzer steigen ständig. Unternehmen setzen weiterhin auf neue Technologien, um innovative und ansprechende Nutzererlebnisse zu bieten. Anwendungen hängen zunehmend von komplexen, verteilten Infrastrukturen ab. DevOps-Teams arbeiten schneller und intelligenter, um neue Funktionen auf den Markt zu bringen. Unternehmen sollten möglicherweise besonderes Augenmerk auf spezialisierte produkt- und funktionsspezifische Fähigkeiten legen, die von den Anbietern nativ, standardmäßig in die Lösung integriert oder auf andere Weise angeboten werden können, beispielsweise als Add-on-Funktionen von Erstanbietern, als separate Produkte, durch OEMs oder technische Integrationen von Drittanbietern. Weitere Überlegungen sind:

- **Client-seitige WAF:** Client-seitige WAFs werden auch als clientseitiger Schutz bezeichnet. Dabei handelt es sich um eine neue Sicherheitstechnologie, die zur Bekämpfung eines bestimmten Bedrohungsvektors entwickelt wurde – den Code von Webanwendungen, die auf Endbenutzergeräten ausgeführt werden. Dieser Code enthält Skripte, die im Browser ausgeführt werden, um verschiedene Funktionen auf dem Gerät und nicht auf dem Webserver auszuführen.
- **Prävention von Betrug/Missbrauch:** Funktionen zur Verhinderung von Online-Betrug und -Missbrauch basieren in der Regel auf Bot-Management-Funktionen, die speziell darauf ausgerichtet sind, einzigartige Muster zu erkennen, die auf bestimmte betrügerische Aktivitäten hinweisen, wie zum Beispiel Kontoübernahmen oder Betrug mit neuen Konten (auch als Fake-Account-Betrug bezeichnet). Um Betrug und andere auf einen Missbrauch ordnungsgemäß funktionierender Anwendungen und APIs hindeutenden Handlungen vollständig zu erkennen, sind Einblicke in die Identität des Nutzers, die Telemetrie auf Kunden- und Geräteebene und das Nutzerverhalten erforderlich. Daher gibt es erhebliche Unterschiede zwischen den WAAP-Lösungen hinsichtlich ihrer Fähigkeit, Betrug zu erkennen, und der Art und Weise, wie diese Fähigkeit genutzt wird.
- **Residential Proxies:** WAAP-Lösungen unterscheiden sich in ihrer Fähigkeit, Angreifer zu erkennen, die sich hinter Residential Proxys oder anderen Verschleierungsmethoden wie IP-Rotation verstecken.
- **WebSockets:** Dazu gehört die Unterstützung von Anwendungen, die WebSockets nutzen, ein Protokoll, das Echtzeitkommunikation über eine Vollduplex-Verbindung ermöglicht. Die Unterstützung von WebSockets wird immer wichtiger, da Online-Nutzer interaktive Echtzeitanwendungen erwarten.
- **WebAssembly (WASM):** Es handelt sich um eine Low-Level-Sprache, die ein portables binäres Codeformat zur Verfügung stellt. Der Hauptvorteil von WASM bestand bisher darin, dass es eine Vielzahl von Entwicklungssprachen problemlos unterstützt. Die Bedeutung der WASM-Unterstützung in WAAP nimmt mit zunehmender Verbreitung zu.
- **Selbstschutz von Runtime-Anwendungen (RASP):** RASP ist eine erweiterte Sicherheitsfunktion, die die Laufzeitumgebung der Anwendung schützt und Dateneingaben überwacht, um Angriffe zu identifizieren, zu erkennen und zu blockieren. RASP kann eine nützliche Option für eine umfassende Anwendungssicherheit sein, wenn die Erwartungen an die Komplexität der Bereitstellung und die Auswirkungen auf die Leistung richtig verstanden werden.
- **Private Access Tokens (PATs):** Apple und andere Technologieunternehmen haben ihre Aufmerksamkeit verstärkt auf den Schutz der Privatsphäre der Endnutzer gerichtet und bieten Methoden an, mit denen die Authentizität und Vertrauenswürdigkeit von Geräten, die Zugang anfordern, ohne die Offenlegung

personenbezogener Daten bestätigt werden kann. Die Unterstützung von WAAP für Apple PAT kann dazu beitragen, die Abhängigkeit von CAPTCHAs und anderen Techniken zur Bot-Erkennung zu verringern, die das Nutzererlebnis beeinträchtigen oder unsicher machen. Apple PAT ist Teil einer umfassenderen Initiative der Branche zur Förderung von Technologien zum Schutz der Privatsphäre, die die Weitergabe und Verarbeitung von Nutzerdaten an ausgewählte Parteien ermöglichen, ohne dass sensible personenbezogene Daten offengelegt werden.

- **Automatisierung:** Die automatische Implementierung von Updates verbessert die Benutzerfreundlichkeit und erhöht den Geschäftswert.
- **Simulationstests:** Diese ermöglichen das Testen von Regelaktualisierungen vor der Implementierung in die Produktion. Simulationstests sind am effektivsten, wenn sie mit tatsächlichem Datenverkehr durchgeführt werden können.
- **eBPF:** eBPF ist eine Linux-Funktionalität, die es Sandbox-Programmen ermöglicht, im Kernel des Betriebssystems ausgeführt zu werden, was insbesondere in Cloud-nativen Umgebungen einen großen Einfluss auf die Verbesserung der Sicherheitsüberwachung hat.

Strategische Überlegungen

Angesichts der raschen Entwicklung von Webanwendungs- und API-Technologien, der sich ändernden Geschäftspraktiken und der ständigen Anpassung und Innovation durch Bedrohungsakteure sollten die Käufer von Sicherheitslösungen unbedingt darauf achten, ob die Lösung ihre Anforderungen in den nächsten drei bis fünf Jahren erfüllen kann. Weitere Überlegungen sind:

- **Verschleierung der Erkennung:** Cyberkriminelle werden immer dreister in ihren Bemühungen, Daten und Produkte zu stehlen, Betrug zu begehen und Unternehmen zu belästigen oder zu erpressen. Die ausgefeilten Tools und cleveren Taktiken sind in der Regel den lukrativen Zielen vorbehalten. Wenn Sicherheitsunternehmen Angriffe erkennen und abwehren, beginnen Cyberkriminelle mit einem Anpassungsprozess. Die Anbieter von WAAP sollten erhebliche Anstrengungen unternehmen, um die Art der Entdeckungen zu verbergen und die Nachhaltigkeit ihrer Eindämmungsmaßnahmen zu gewährleisten. Außerdem verhindern die produktivsten Strategien, dass die Angreifer erkennen, wann sie entdeckt wurden, wodurch sich ihre Ressourcen erschöpfen lassen. Es wurden fortschrittliche Maßnahmen zur Bekämpfung von Botnets und Betrug festgestellt, einschließlich des Einsatzes von Täuschungstechnologien, um Angreifer daran zu hindern, den Kreislauf der Entwicklung von Cyberwaffen zu schließen.

- **Plattformisierung:** Branchen werden durch Plattformen neu gestaltet, die Komplexität reduzieren und spezialisierte Funktionen über eine einfache Benutzeroberfläche bereitstellen, die die Notwendigkeit einer ursprünglichen technischen Entwicklung abstrahiert. Shopify beispielsweise ist eine E-Commerce-Plattform, die den Prozess der Gründung eines neuen Online-Unternehmens vereinfacht. Funktionen wie Kundeninformationen, Lagerbestand und Zahlungsabwicklung werden als komplette, schlüsselfertige SaaS-Lösung angeboten. Sicherheit, einschließlich grundlegender WAF- und DDoS-Schutzmaßnahmen, ist als integrierte Funktionalität der Plattform enthalten. Dies wird die Bedürfnisse und Erwartungen der Käufer an WAAP-Lösungen verändern und strategische Anpassungen der Anbieter erfordern.
- **„Shift-Left"-Strategien:** Die Notwendigkeit, Sicherheitstests und -praktiken früher im Softwareentwicklungszyklus zu implementieren, ist nicht neu. Die Erkennung von Schwachstellen vor der Freigabe für die Produktion verhindert, dass Angreifer überhaupt die Möglichkeit haben, die Schwachstelle zu entdecken und auszunutzen. Eine frühzeitige Erkennung und Korrektur ist zudem effizienter und kostengünstiger. In den letzten Jahren hat sich jedoch das Konzept des „Shift Left" entwickelt, das diese Ideale durch die Integration traditioneller Postproduktionswerkzeuge mit Tools und Prozessen für die Entwickler erreicht. Beispielsweise können DevOps durch den Einsatz von APIs zum Aufrufen von Dynamic Application Security Tests (DAST) Bedrohungen schnell und einfach erkennen und beheben. Da DevOps-Teams schneller arbeiten und Microservices, zusammensetzbaren Code, Infrastructure as Code (IaC) und andere Mittel zur Verkürzung der Entwicklungszyklen einsetzen, gewinnt die Unterstützung von Shift-Left-Strategien an Bedeutung.
- **Wechselnde Personas:** Tendenzen zur Plattformisierung, „Shift-Left"-Strategien und eine allgemeine Zunahme einer sicherheitsbewussten Kultur (jeder ist für die Sicherheit verantwortlich) führen zu Veränderungen bei Käufern und Entscheidungsträgern. Entwickler, Cloud- und Netzwerkteams und sogar die Einkäufer der einzelnen Geschäftsbereiche sind am WAAP-Beschaffungsprozess beteiligt. WAAP-Anbieter müssen zunehmend in Vereinfachung, Automatisierung, starken und unmittelbar verfügbaren Schutz und in die Aufklärung des Marktes investieren, um ein breites Publikum von Käufern und Entscheidungsträgern besser bedienen zu können.
- **GenAI:** Die Einführung von GenAI hat Bedenken über mögliche neue Risiken aufgeworfen, die diese Technologie in Geschäftsumgebungen mit sich bringen könnte. Eine IDC-Umfrage unter Einkäufern hat ergeben, dass Unternehmen deshalb eine Erhöhung der Budgets für Anwendungssicherheit in Erwägung ziehen. Die WAAP-Anbieter unterscheiden sich stark in Bezug auf ihre

Aufmerksamkeit und Planung für potentielle GenAI-Risiken, die mehrere Faktoren betreffen, wie zum Beispiel:

- Potenzielle neue Bedrohungen die zur effektiveren Umgehung von Abwehrmechanismen GenAI nutzen
- Mögliche Anwendungen für neu entstehende Technologien (z. B. GenAI zur Eindämmung von Bot-Aktivitäten, Tarnung, Verlangsamung oder Sabotage von Bot-Operationen)
- Die mögliche Notwendigkeit, spezialisierte Funktionen oder Produkte einzusetzen oder sich auf bestehende Abwehrmaßnahmen zu verlassen, wenn Unternehmen ihre LLM-Fähigkeiten ausbauen oder LLMs von Drittanbietern in ihre Anwendungsstrategien einbeziehen
- Potenzielle Anwendungen für GenAI zur Verbesserung der Effizienz und Produktivität von Sicherheitsmaßnahmen
- Mögliche Anwendungen für KI zur Verbesserung der Sicherheitserkennung

Insgesamt hat IDC festgestellt, dass die in diesem IDC MarketScape betrachteten Lösungen trotz der enormen Bandbreite an Funktionen, die in der Definition von WAAP gefordert und impliziert werden, ein hohes Leistungsniveau aufweisen. Es wird erwartet, dass sich die Definition von WAAP mit neuen Technologien und sich verändernden Bedrohungen weiterentwickelt. In einigen Funktionsbereichen besteht noch Verbesserungsbedarf, und die Anbieter haben umfassende Roadmaps entwickelt. Während in bestimmten Anwendungsfällen oder für außergewöhnliche Anforderungen spezialisierte Einzelprodukte erforderlich sein können, haben WAAP-Anbieter große Fortschritte auf dem Weg zu vollständigen, leistungsfähigen Plattformen mit umfassender Funktionalität gemacht, die zur Gewährleistung eines starken Anwendungsschutzes und einer hohen Sicherheit erforderlich ist.

KURZPROFILE DER ANBIETER

Dieser Abschnitt erläutert kurz die wichtigsten Beobachtungen von IDC, die über die Position eines Anbieters im MarketScape-Report entscheiden. Während jeder Anbieter anhand der im Anhang aufgeführten Kriterien bewertet wird, bietet die Beschreibung hier eine Zusammenfassung der Stärken und Herausforderungen des Anbieters.

Akamai

Akamai ist ein Leader in diesem IDC MarketScape 2024 für weltweite WAAP-Unternehmensplattformen.

Akamai ist ein globaler Anbieter von Netzwerk- und Sicherheitslösungen, die über die Akamai Connected Cloud bereitgestellt werden. Diese verteilte Edge- und Cloud-

Plattform bringt die Anwendungen und Erlebnisse näher an die Nutzer und hält Bedrohungen fern. Akamai hat sich auf den Unternehmensmarkt spezialisiert und ist bei den Fortune-500-Unternehmen stark vertreten. Das Sicherheitsportfolio von Akamai umfasst eine integrierte WAAP-Lösung namens App & API Protector (AAP) sowie dedizierte Lösungen in den Kategorien API-Sicherheit, DDoS-Abwehr, Bot-Management, Account-Schutz, WAF, clientseitiger Schutz und Compliance, DNS und Markenschutz. Akamai hat mit Lösungen für ZTNA, Mikrosegmentierung, DNS-Firewall, Threat Hunting und MFA in den Bereich Unternehmenssicherheit expandiert.

Stärken

Fähigkeiten

- Die Adaptive Security Engine (ASE) bietet eine Selbstoptimierung für die zuverlässige Nutzung von Out-of-the-Box-Regeln. ASE bietet einen besseren Schutz vor Zero-Day-Angriffen, verbessert die Erkennungsrate (laut Akamai um den Faktor 2), reduziert Fehlalarme (laut Akamai um den Faktor 5) und ermöglicht automatische Updates für eine kontinuierliche Benutzerfreundlichkeit. ASE wird unterstützt durch Akamai Security Intelligence.
- ASE bietet eine Fehlalarm-Kennzeichnung zur einfacheren/schnelleren Behebung von Fehlalarmen. Akamai erreicht mehr als 50 % nach einem Tag und 75 % nach einer Woche.
- Die umfassende WAAP-Suite bietet ein One-Stop-Shopping-Erlebnis für vereinfachte und komplette Sicherheit. Eine einzige WAAP-SKU ist verfügbar, mit Add-ons für erweiterte oder spezialisierte Funktionen.
- Umfangreiche Add-ons und spezialisierte Lösungen ermöglichen die Anpassung an fallspezifische Anforderungen wie ATO, Markenschutz und Scraper-Schutz (Hype Event).
- Akamai bietet eine sehr umfassende Edge/CDN-Infrastruktur. Der Schutz in der Nähe des Anwenders sichert die Leistungsfähigkeit.
- Die Unterstützung von DevOps-Workflows unterstützt die Shift-Left-Strategien von Unternehmenskunden. Die Unterstützung von Verwaltung und Bereitstellung durch APIs, CLI und Terraform verbessert die Sicherheit, ohne die Entwickler zu behindern.
- Bestehende Integrationen mit verwandten Sicherheitstools erleichtern die Integration in eine umfassendere Sicherheitsarchitektur für bessere Sicherheitsergebnisse. Die Lösung umfasst vorgefertigte Konnektoren für Splunk, Qradar und ArcSight.
- Es wird ein multimodaler Ansatz für die API-Sicherheit angeboten. Der Ansatz bietet unmittelbaren Schutz für bekannten API-Verkehr auf der Plattform und, falls erforderlich, vollständigen API-Schutz zu einem späteren Zeitpunkt.

- Der Umfang der zusätzlichen verwandten Fähigkeiten, die zusammen mit WAAP angeboten werden, stellt sicher, dass die Sicherheit die Leistung nicht beeinträchtigt. Das Portfolio umfasst Lösungen wie SiteShield, mPulse Lite, EdgeWorkers, Image & Video Manager und API Acceleration.
- Akamai hat kürzlich neue Funktionen für die DDoS-Abwehr auf Anwendungsebene eingeführt, darunter die Erkennung kurzer Spitzen und eine anpassbare Ratenbegrenzung auf der Grundlage detaillierter kontextbezogener Hinweise. Diese decken das gesamte Spektrum von DDoS-Angriffen ab, einschließlich der speziellen Anforderungen von Angriffen auf Anwendungsebene.
- Eine einheitliche Ansicht der Sicherheitstelemetrie ist enthalten, die eine umfassende Sicherheitsanalyse und Transparenz mit Drilldown-Funktionen bietet. Web Security Analytics ist in allen Produkten zur Anwendungssicherheit enthalten.
- Der Evaluierungsmodus bietet die Möglichkeit, die Auswirkungen von Regeländerungen anhand von Live-Datenverkehr zu überprüfen, bevor die Änderungen umgesetzt werden. Diese Funktion ermöglicht die Implementierung neuer Regeln ohne das Risiko unbekannter Auswirkungen auf den Produktionsverkehr.

Strategie

- Akamai hat Pläne zur Integration von WAAP mit verwandten Sicherheitstools wie Mikrosegmentierung angekündigt. Dies ergänzt die Sicherheitstools und bietet einen umfassenden Schutz.
- Akamai entwickelt Strategien zum Schutz der zunehmenden Nutzung von LLM. Die Verwendung vorhandener Tools für neue Sicherheitsverfahren erhöht den Kundennutzen. GenAI-spezifische Schutzmaßnahmen können jedoch noch spezialisierter sein.
- Das Unternehmen hat ambitionierte Expansionspläne im Bereich Edge Computing. Optionen zur Sicherung von Transaktionen am Edge können dazu beitragen, dass Bedrohungen die Ursprungsserver nicht erreichen.
- Es wurden Belege für die Umsetzung der Strategie festgestellt, insbesondere im Bereich der API-Sicherheit. Die API-Sicherheitsstrategie steht nach den Übernahmen von Noname Security und Neosec kurz vor dem Abschluss.
- Das Unternehmen kann auf eine lange Erfolgsgeschichte strategischer Akquisitionen zurückblicken und hat mit bahnbrechenden Produkten wie Cyberfend, Neosec, Noname Security und Prolexic eine kohärente Plattform geschaffen. Investitionen sind ein Zeichen des Engagements für die Sicherheit der Kunden.

- Akamai setzt Telemetrie ein, um strategische Fortschritte wie die Nutzung und die Akzeptanz von Richtlinien, den automatischen Modus und den Status des Schutzes zu überwachen. Dadurch wird sichergestellt, dass die Entwicklungsstrategien mit der Realität der Kunden übereinstimmen.
- Das kommende WAAP-System wird weitere Sicherheitslücken des CDN schließen und den Ost-West-Verkehr, den Nicht-CDN-Verkehr und Multi-Cloud-Umgebungen absichern. Diese Funktionen stehen kurz vor der Veröffentlichung und es gibt Anzeichen für Fortschritte.
- Es werden verschiedene Wege zur Einbindung der Kunden angeboten, beispielsweise durch Kundenkonferenzen, regelmäßige Beiratssitzungen und Ad-hoc-Prozesse.

Herausforderungen

Fähigkeiten

- KI/ML-Engines können vom Kunden nicht ohne weiteres angepasst werden (d. h. die Reihenfolge der Regeln kann nicht geändert werden). Dies kann zu Verzögerungen bei der Reaktion auf Fehlalarme führen und erfordert eine Zusammenarbeit mit Akamai, um das Problem zu beheben. Vorübergehende Ausnahmen und Umgehungslösungen sind eine mögliche Option, um die Komplexität im Zusammenhang mit Regeln zu bewältigen.
- Begrenzte Formfaktoren wie Container und Serverless schränken die Unterstützung für Kunden ein, die die Sicherheitsinfrastruktur kontrollieren möchten. Derzeit liegt der Schwerpunkt von Akamai auf der Unterstützung von Terraform und API-basierten Kontrollen für die Bereitstellung und Automatisierung.
- WAAP von Akamai wird als Premium-Produkt angeboten, das für Entscheidungsträger in Unternehmen unerschwinglich sein kann. Zu den Preisoptionen von Akamai gehören jedoch der Zero Overhead Fixed Fee (ZOFF)-Schutz, eine anfragebasierte Preisgestaltung und die DDoS-Schutzgebühr, die keine zusätzlichen Kosten für Spitzen im Datenverkehr aufgrund von DDoS-Aktivitäten beinhaltet.
- gRPC wird nicht unterstützt, was in speziellen Anwendungsfällen oder bestimmten Branchen bevorzugt werden kann.

Strategie

- Spezialisierte, optionale Funktionen und Add-ons können zusätzliche Kosten verursachen, die die Gesamtbetriebskosten (TCO) erhöhen und eine vollständige Bereitstellung verhindern können. Datenverkehr, der nicht über das CDN läuft (z. B. API-Gateway-Verkehr), verursacht zusätzliche Kosten.

- Die Produktentwicklungsstrategie für WAAP beinhaltet derzeit eine nominelle Kreuzung mit der Zero-Trust-Lösung Akamai Enterprise Application Access (EAA). Webanwendungen bieten die Möglichkeit, den Arbeitsplatz neu zu gestalten, und eine verstärkte Integration zwischen Produktlinien ist der Schlüssel zur Unterstützung der gesamten Bandbreite von Anwendungsfällen für den sicheren Zugang.
- Mehrere Lösungen (z. B. Account Protector, Brand Protector und Content Protector) führen zu einer fragmentierten Strategie für den Betrugsschutz und kann die Komplexität der Nachrichtenübermittlung erhöhen.

Erwägungen zu Akamai

Akamai bietet eine Reihe von robusten Bereitstellungs-, Leistungs- und Sicherheitsfunktionen, die als ein kohärenter Service implementiert werden können. Akamai lizenziert erweiterte und spezialisierte Funktionen als optionale Add-ons. Diese Strategie ermöglicht es Unternehmen, in die maßgeschneiderte Lösung zu investieren, die ihren Sicherheits- und Lieferanforderungen am besten gerecht wird. Insgesamt erfüllt die WAAP-Lösung von Akamai die Anforderungen großer, moderner digitaler Unternehmen an Sicherheit, Verfügbarkeit, Integrität und Compliance.

ANHANG

Interpretation von IDC MarketScape-Grafiken

Für diese Analyse hat IDC potenzielle Erfolgskennzahlen in zwei Hauptkategorien aufgeteilt: Fähigkeiten und Strategien.

Auf der Y-Achse werden die derzeitigen Fähigkeiten und das Leistungsangebot sowie die Anpassung des Anbieters an die Bedürfnisse der Kunden dargestellt. Die Kategorie Fähigkeiten konzentriert sich auf das, was das Unternehmen und seine Produkte hier und heute zu bieten haben. Dabei untersuchen die Analysten von IDC, wie gut es einem Anbieter gelingt, die gewählte Strategie auf dem Markt umzusetzen.

Auf der X-Achse wird dargestellt, wie gut die Zukunftsstrategie des Anbieters auf den Kundenbedarf in 3–5 Jahren ausgerichtet ist. Im Fokus der Kategorie Strategien stehen Entscheidungen auf hoher Ebene und zugrundeliegende Annahmen über Angebote, Kundensegmente sowie Geschäfts- und Markteinführungspläne für die nächsten 3–5 Jahre.

Die Größe der einzelnen Marker im IDC MarketScape-Bericht spiegelt den Marktanteil des einzelnen Anbieters im untersuchten Marktsegment wider.

Für jedes einzelne Kriterium wurden die Anbieter auf einer Skala von eins bis fünf bewertet, wobei drei die durchschnittliche Bewertung, fünf die beste und seltenste Bewertung und eins die niedrigste und ebenfalls sehr seltene Bewertung darstellt. Die Kriterien wurden dann auf der Grundlage der Analystenperspektive und des Verständnisses der allgemeinen Markttrends gewichtet, um die Entscheidungsfindung von IT-Einkäufern bestmöglich zu unterstützen. Die Bewertungen für jedes Kriterium wurden auch zwischen einer „quantitativen“ und einer „qualitativen“ Bewertung gewichtet, je nachdem, was für das jeweilige Kriterium am besten geeignet und relevant war.

Abbildung 1 zeigt eine visuelle Darstellung mehrerer Faktoren, die in eine Position entlang jeder Achse übersetzt werden. Vorhandene produktspezifische Merkmale und Funktionen sind ein wichtiger Bestandteil der „Fähigkeiten“-Achse, aber es werden auch viele andere Faktoren berücksichtigt. Ebenso werden auf der Achse „Strategien“ die Pläne des Anbieters für künftige Produktentwicklungen stark berücksichtigt. Es werden jedoch auch andere Faktoren berücksichtigt, darunter die Stärke des Gesamtgeschäfts und die Pläne für die Markteinführung. Da diese Faktoren langfristige Auswirkungen auf die Lösung haben können, hat IDC die Gewichtung dieser Kriterien entsprechend angepasst. Insgesamt fließen mehrere Faktoren in die Bewertung der einzelnen Anbieter ein, und es wird empfohlen, Abbildung 1 im Zusammenhang mit den Anbieterprofilen zu berücksichtigen.

IDC MarketScape Methodik

Die Auswahl der IDC MarketScape-Kriterien, die Gewichtung und die Bewertung der Anbieter stellen eine gut recherchierte Einschätzung des Marktes und bestimmter Anbieter durch IDC dar. IDC-Analysten passen die Bewertungsfaktoren durch strukturierte Diskussionen, Umfragen und Interviews mit Marktführern, Teilnehmern und Endbenutzern an. Die Marktgewichtungen basieren auf Benutzerinterviews, Kundenumfragen und dem Input von IDC-Experten für die einzelnen Märkte. Die Analysten von IDC stützen sich bei der Bewertung der einzelnen Anbieter und letztlich auch bei der Positionierung der Anbieter in der IDC MarketScape auf detaillierte Befragungen und Interviews mit den Anbietern, öffentlich verfügbare Informationen und Erfahrungen von Endanwendern, um eine genaue und konsistente Bewertung der Eigenschaften, des Verhaltens und der Fähigkeiten der einzelnen Anbieter zu erhalten.

Marktdefinition

WAAP ist eine konvergente Sicherheitslösung für den aktiven Schutz von Anwendungen mit WAF als Kernkomponente. WAAP-Lösungen kombinieren mehrere Funktionen in einer einheitlichen Sicherheitsplattform, darunter WAF, Bot-Management, API-Sicherheit, DDoS-Abwehr und andere Sicherheitstechnologien. Die WAF wird jedoch als grundlegend angesehen und muss ein integraler Bestandteil sein, um als WAAP zu

gelten. Darüber hinaus werden einmalige Verkäufe von WAAP-Komponenten als eigenständige Lösungen nicht als WAAP gezählt.

Grundlegende WAAP-Komponenten

Web-Anwendungs-Firewall

WAF-Produkte überwachen, filtern oder blockieren die Kommunikation auf dem Weg zu und von einer Webanwendung. Eine WAF kann entweder netzwerk- oder cloudbasiert sein und wird häufig über einen Proxy vor einer oder mehreren Webanwendungen bereitgestellt. Die WAF ist die Kernkomponente einer WAAP-Lösung.

API-Sicherheit

API-Sicherheitslösungen sind speziell für den Schutz der API-Kommunikation vor Missbrauch und Exploits konzipiert. Diese Lösungen bieten ganz oder teilweise wesentliche Funktionen wie die Aufnahme, Validierung und Durchsetzung von API-Schemata, die dynamische und adaptive Überwachung des Datenverkehrs und die Analyse von Mustern sowie die Erkennung/Vermeidung von Bedrohungen wie Malware, Exploits, Code-Injection, Bots, DDoS-Angriffen, Betrug und Missbrauch.

Einige API-Schutzfunktionen können standardmäßig in einem WAAP-Angebot enthalten sein, z. B. die Überprüfung des API-Verkehrs, die am selben Prüfpunkt wie eine WAF durchgeführt werden kann. Für eine vollständige API-Sicherheitsbereitstellung können jedoch zusätzliche Sensoren und Komponenten erforderlich sein, um die Sichtbarkeit und den Bestand aller API-Endpunkte und letztlich den Schutz der gesamten API-Kommunikation zu gewährleisten.

Bot-Management

Bot-Management ist die Praxis, die Integrität der Online-Kommunikation sicherzustellen, indem nur authentischen menschlichen Nutzern und erwünschten Bot-Aktivitäten unter kontrollierten und genehmigten Bedingungen Zugang gewährt wird. Bot-Management-Lösungen nutzen eine Vielzahl von Signalen und Erkenntnissen über Kunden, Geräte, Browser, Benutzeridentität und -verhalten in Kombination mit fortschrittlicher Analyse, um selbst die raffiniertesten und schwer aufzuspürenden Bots zu erkennen. Diese Lösungen bieten auch eine granulare Kategorisierung und Kontrolle des gesamten Bot-Ökosystems auf der Grundlage von Risikoprofilen, Bot-Typen oder für bestimmte Bots.

Der breitere Markt für Bot-Management umfasst auch speziell entwickelte Lösungen, die auf die besonderen Sicherheitsanforderungen von unerwünschten Bots zugeschnitten sind. Es gibt verschiedene Stufen der Integration von WAAP-Lösungen. Ein Mindestmaß an Bot-Erkennung und -Kontrolle wird in der Regel als Teil einer WAAP-

Lösung angeboten, während erweiterte Funktionen als Zusatz- oder Upgrade-Abonnement erhältlich sind.

DDoS-Abwehr

Der Markt für DDoS-Abwehr umfasst Lösungen, die verteilte Denial-of-Service-Angriffe erkennen und filtern. Während DDoS-Abwehrfunktionen in Firewalls, IPS und anderen Sicherheitsprodukten vorhanden sein können, sind speziell entwickelte Lösungen zur Abwehr der größten, komplexesten und neuartigen DDoS-Angriffe ausgelegt. Solche Produkte können vor Ort, über die Cloud, oder eine Mischung aus beidem bereitgestellt werden.

Je nach Art der WAAP-Lösung oder der Bereitstellung können unterschiedliche Schutzniveaus frei in die Lösung integriert werden. Erweiterter Schutz in Form von zusätzlicher Kapazität oder Abdeckung spezieller Angriffsarten kann als Add-on oder Upgrade-Abonnement angeboten werden.

Erweiterte, fortgeschrittene und optionale Komponenten der WAAP

Client-seitige WAF

Die clientseitige WAF (CSWAF) erweitert die Sichtbarkeit und Kontrolle der Anwendungssicherheit auf die Skripte, die in den Browsern der Endbenutzer ausgeführt werden. CSWAF-Lösungen unterscheiden sich drastisch in Bezug auf den Umfang ihrer Fähigkeiten. Zu den Kernfunktionen gehören in der Regel Sichtbarkeit, Bewertung und Inventarisierung von Skripten und Kommunikation. Der Markt für fortgeschrittene Sicherheitsfunktionen wie Schwachstellenerkennung, Verschlüsselung, Codeverschleierung, Erkennung von Anomalien und Bedrohungen sowie die Durchsetzung von Richtlinien ist noch nicht ausgereift.

Online-Betrugsprävention

Betrugsprävention umfasst eine breite Palette von Lösungen, die unabhängig voneinander oder im Zusammenspiel digitale Systeme vor betrügerischen oder anderweitig unerwünschten Aktivitäten schützen. Online-Betrugsprävention kann den Einsatz von Identitätsmanagement, starker Authentifizierung, Lösungen für den Identitätsnachweis, Schutz vor Zahlungsbetrug, Erkennung von Transaktionsbetrug, Betrugsprävention in Unternehmen und spezielle Lösungen zur Verhinderung von Online-Betrug umfassen.

Bei WAAP sind die Funktionen zur Verhinderung von Online-Betrug und -Missbrauch in der Regel in Bot-Management-Funktionen verwurzelt, die speziell darauf ausgerichtet sind, einzigartige Muster zu erkennen, die auf bestimmte betrügerische Aktivitäten

hinweisen, wie zum Beispiel Kontoübernahmen oder Betrug mit neuen Konten (auch als Fake-Account-Betrug bezeichnet). Um Betrug und andere auf einen Missbrauch ordnungsgemäß funktionierender Anwendungen und APIs hindeutenden Handlungen vollständig zu erkennen, sind Einblicke in die Identität des Nutzers, die Telemetrie auf Kunden- und Geräteebene und das Nutzerverhalten erforderlich. Daher gibt es erhebliche Unterschiede zwischen den WAAP-Lösungen hinsichtlich ihrer Fähigkeit, Betrug zu erkennen, und der Art und Weise, wie diese Fähigkeit genutzt wird.

MEHR ERFAHREN

Ähnliche Forschungsbeiträge

- *Web Application and API Security Survey Presentation, 2024* (IDC #US52509324, August 2024)
- *Identifying and Measuring the Costs of Cyberattacks Targeting Web Applications and APIs* (IDC #US52025924, April 2024)
- *Market Analysis Perspective: Worldwide Active Application Security Market, 2023* (IDC #US51332023, November 2023)
- *IDC TechBrief: Client-Side WAF* (IDC #US51199423, September 2023)
- *Worldwide Application Protection and Availability Forecast, 2023–2027: Threat Escalation and New Frontiers* (IDC #US51178423, September 2023)
- *Worldwide Application Protection and Availability Market Shares, 2022: Platforms Compete with Emerging Technologies* (IDC #US51204923, September 2023)
- *Tales of the Tape: WAF and API Protection Emerge as Security Essentials* (IDC #US51187923, September 2023)

Zusammenfassung

Diese IDC-Studie bietet einen Überblick über die verfügbaren WAAP-Lösungen und berücksichtigt dabei die Vorteile eines breiteren Anbieterportfolios, strategische und technische Partnerschaften, geistiges Eigentum, Akquisitionen, Gesamtbetriebskosten, Kundenzufriedenheit und Wettbewerbsvorteile. WAAP ist ein integrierter Ansatz, der einen sicheren und leistungsfähigen Zugriff auf wichtige Webanwendungen und die zugehörigen APIs ermöglicht. Der Markt entwickelt sich rasant, so dass einzelne Produkte nicht mehr ausreichen, um Risiken ausreichend zu mindern. Daher gibt es nach wie vor eine Vielzahl von Möglichkeiten und Ansätzen, die Käufer von Sicherheitslösungen in Betracht ziehen können.

„Der WAAP-Markt befindet sich an einem kritischen Punkt, da die Anbieter darum wetteifern, sich vor der nächsten Generation von Online-Bedrohungen zu schützen und sich gleichzeitig gegen die unerbittlichen Angriffe von heute zu verteidigen“, so

Christopher Rodriguez, Forschungsleiter des IDC Security and Trust Teams. „Gleichzeitig gehen die Einkäufer in den Unternehmen ihre WAAP-Planung im Kontext der sich schnell verändernden Technologien an.“

ÜBER IDC

International Data Corporation (IDC) ist der weltweit führende Anbieter von Marktinformationen, Beratungsdienstleistungen und Veranstaltungen auf dem Gebiet der Informationstechnologie und der Telekommunikation sowie der Verbrauchertechnologiemärkte. Mit mehr als 1.300 Analysten bietet IDC globale, regionale und lokale Expertise zu Chancen und Trends in Technologie und Wirtschaft in mehr als 110 Ländern. Analysen und Erkenntnisse von IDC unterstützen IT-Profis, Geschäftsleute und Investoren bei fundierten Entscheidungen über Technologien und die Erzielung ihrer wichtigsten Geschäftsziele. IDC wurde 1964 gegründet und ist eine hundertprozentige Tochtergesellschaft der International Data Group (IDG, Inc.).

Internationaler Hauptsitz

140 Kendrick Street
Building B
Needham, MA 02494
USA
+1 508 872 8200
Twitter: @IDC
blogs.idc.com
www.idc.com

Urheberrecht und Markenhinweis

Dieses IDC-Forschungsdokument wurde als Teil der kontinuierlichen IDC-Marktforschung bereitgestellt, die schriftliche Forschungsberichte, Gespräche mit Analysten, Telebriefings und Konferenzen umfasst. Besuchen Sie www.idc.com, um mehr über IDC-Abonnements und -Beratungsleistungen zu erfahren. Eine Liste aller IDC-Niederlassungen weltweit finden Sie unter www.idc.com/about/worldwideoffices. Bitte wenden Sie sich an den IDC-Berichtvertrieb unter +1.508.988.7988 oder www.idc.com/?modal=contact_repsales, um Informationen über die Anrechnung des Preises dieses Dokuments auf den Kauf eines IDC-Dienstes oder über zusätzliche Kopien oder Webrechte zu erhalten.

Copyright 2024 IDC. Reproduktion ohne entsprechende Genehmigung ist untersagt. Alle Rechte vorbehalten.