radware

Herausforderungen der Applikationssicherheit (und warum Ihre On-Premise-WAF nicht mehr ausreicht)

Inhaltsverzeichnis

Überblick

In den meisten Unternehmen bilden Applikationen das Herzstück, weil interne Abläufe sowie Geschäftsbeziehungen zu Kunden und Partnern davon abhängig sind. Diese Unternehmen müssen sich über die Bedeutung von Applikationsschutz bewusst werden, weil sich die Bedrohungslandschaft verändert und Angriffe immer häufiger, raffinierter und massiver werden. Gleichzeitig haben sich die Applikationsentwicklung und -bereitstellung so stark weiterentwickelt, dass eine herkömmliche Web Application Firewall (WAF) nicht mehr effektiv genug ist. Somit erfordert Applikationsschutz heute einen komplett anderen Ansatz.

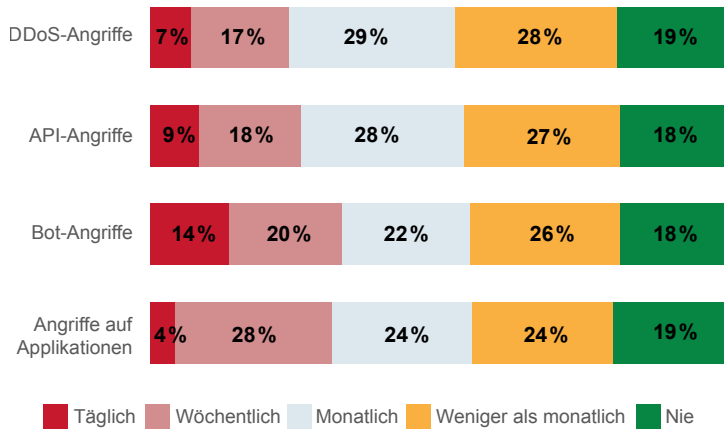
Die Bedrohungslandschaft für Applikationen

Laut einer Radware-Bedrohungsanalyse ist die Anzahl der bösartigen Vorfälle, die der Cloud-WAF-Service von Radware blockiert hat, um 392 % gestiegen (im Jahr 2022 verglichen mit 2021). Bei den Transaktionen mit schädlichen Bots wurde im selben Zeitraum eine Zunahme um 105 % festgestellt. Zudem berichteten mehr als 50 % der Unternehmen, dass sie jeden Monat oder noch häufiger von verschiedenen Angriffsvektoren betroffen waren (siehe Abbildung 1).

Abbildung 1:

Häufigkeit der Angriffe

(Quelle: Radware-Applikationsschutz in einer Multi-Cloud-Welt, 2022)



Dies führt zu dem Schluss, dass Applikationsschutz eine Kombination verschiedener Lösungen erfordert, um alle Angriffsvektoren abzudecken. Dazu gehören WAFs für Applikationsschwachstellen, API-Schutz, Bot-Management und Layer-7-DDoS-Schutz. Allerdings sind diese Lösungen nur so gut wie die Experten für Applikationsschutz, von denen sie betreut werden.

Allein im Jahr 2022 waren unterschiedlichste Unternehmen anfällig für Angriffe auf Applikationsebene, von großen Dienstleistern über bekannte E-Commerce-Marken bis hin zu renommierten Softwareanbietern. Wenn man bedenkt, dass diese Unternehmen sicherlich ultramoderne Applikationsschutzlösungen einsetzen, wird erst so richtig klar, wie ausgefeilt Angriffe mittlerweile geworden sind und wie viel Kopfzerbrechen sie den CISO-Teams bereiten.

Der Aspekt der Applikationsentwicklung und -bereitstellung

Früher waren Applikationen monolithisch und wurden nur in einem privaten Rechenzentrum bereitgestellt. Heute erfolgt diese Bereitstellung jedoch über verschiedene Umgebungen hinweg, darunter herkömmliche Rechenzentren, private Clouds und Public Clouds. Die Architektur von Applikationen hat sich ebenfalls verändert. Während die große Mehrzahl davon einst auf einem einzigen monolithischen Anwendungscode basierte, nutzen moderne Applikationen eine Micro-Services-Architektur mit vielen integrierten Drittanbieterdiensten. Sie beruhen sehr stark auf APIs für die Kommunikation zwischen Micro-Services und Drittanbieterdiensten. Darüber hinaus sind zahlreiche Applikationen auf die Ausführung von Code im clientseitigen Browser angewiesen, wodurch die Client-Geräte zu einem Teil der Applikation werden.

Aufgrund dieser Weiterentwicklung der Architektur reicht es nicht mehr aus, Applikationen mit einer herkömmlichen On-Premise-WAF zu schützen, selbst wenn sich diese in den verschiedenen Cloud-Umgebungen bereitstellen lässt.

Mangel an Sicherheitsexperten und -kompetenzen

Eine aktuelle Studie von (*ISC*)² über Cybersicherheitspersonal 2022 und eine Umfrage von Gaper ISSA/ESG ergaben, dass 70 % aller Unternehmen unter Kompetenzmangel in der Cybersicherheitsabteilung leiden und dass die starke Arbeitsbelastung zu einer hohen Burnout-Rate führt. Laut derselben Umfrage sind in der Cybersicherheit weltweit mehr als 3 Millionen offene Stellen zu besetzen, 400.000 davon in den USA.

Probleme und Anforderungen beim Management von Applikationsschutz

Angesichts dieser Schwierigkeiten stellt sich die Frage, ob eine selbstverwaltete On-Premise-WAF immer noch für einen ausreichenden Applikationsschutz sorgen kann. Im Folgenden sind einige Herausforderungen aufgeführt, die sich mit einer On-Premise-WAF in der modernen Applikations- und Bedrohungslandschaft ergeben.

Verwaltungsaufwand: Da eine steigende Anzahl an Applikationen in immer mehr Umgebungen bereitgestellt werden, läuft der Verwaltungsaufwand für den Schutz dieser Applikationen schnell aus dem Ruder.

Mangel an Cyberexperten: Aufgrund zunehmender Bedrohungsvektoren und stets raffinierterer Angriffe wird deutlich mehr Fachwissen benötigt, um alles im Griff zu behalten. Leider konnten die Anzahl und Fachkompetenz der Applikationsschutzexperten mit dieser Entwicklung nicht Schritt halten. Folglich fällt es vielen Unternehmen schwer, ihre Applikationen durch hochwertige Technologien zu schützen.

Schutzqualität: Eine WAF ist nur so gut wie ihre konfigurierten Sicherheitsrichtlinien. Eine On-Premise-WAF kann nur Sicherheitsrichtlinien für die lokale Applikation generieren, die sie schützt, was eine extreme Einschränkung bedeutet. Für optimalen Schutz und zur Abdeckung von Bot- und API-Domänen sind zudem ML/KI-basierte Algorithmen erforderlich, die auf On-Premise-WAF-Geräten nicht verfügbar sind.

Schutz aller Applikationsebenen: Aufgrund der veränderten Applikationsarchitektur reicht es nicht mehr aus, nur den Applikationsserver in einer Umgebung zu schützen. Die neue Applikationsarchitektur weist viele Stellen auf, die einen Zugriff ermöglichen – und alle davon benötigen Schutz (z. B. Server, Cloud, Drittanbieter-APIs, Client). Eine herkömmliche On-Premise-WAF kann nicht alle diese Zugriffspunkte auf Applikationen abdecken.

Agilität und Skalierbarkeit: Die Einführung eines neuen Applikationsservices ist mit viel Aufwand verbunden. Noch mehr Ressourcen erfordert die Gewährleistung, dass der Service die Applikation nicht beeinträchtigt (aber trotzdem effektiv schützt). Dies wirkt sich auf die Agilität des Unternehmens aus. Die Möglichkeit zur Skalierung leidet ebenfalls unter der Tatsache, dass Applikationsschutz eine hohe Rechenleistung erfordert.

Warum Ihre On-Premise-WAF nicht mehr ausreicht

Eine traditionelle On-Premise-WAF war sinnvoll, als alle Applikationen noch im privaten Rechenzentrum bereitgestellt wurden und eine WAF als einzige Schutzmaßnahme für Applikationen genügte. Doch die Zeiten haben sich geändert. Im Folgenden wird erläutert, warum eine selbstverwaltete On-Premise-WAF nicht mehr ausreicht und warum Unternehmen bevorzugt einen verwalteten Cloud-WAF-Service nutzen sollten.

Verwaltungsaufwand

Für effektiven Applikationsschutz müssen viele Regeln und Signaturen konfiguriert und optimiert werden. Dieser mühsame Prozess führt oft zu Fehlalarmen, die der Applikationsnutzung und damit dem Unternehmen schaden.

Außerdem müssen angesichts der Bedrohungslandschaft für Applikationen mehrere Lösungen und Technologien integriert werden, um alle Angriffsvektoren abzudecken, z. B. WAF, Bot-Management, API-Schutz, Layer-7-DDoS-Schutz usw. Dadurch steigt die Komplexität der On-Premise- bzw. selbstverwalteten Lösungen – und somit auch der Verwaltungsaufwand. Gleichzeitig müssen immer mehr Applikationen geschützt werden, sodass viele Unternehmen von der Verwaltung überfordert sind.

Ein komplett verwalteter Cloud-WAF-Service hingegen wird von Experten für Applikationsschutz betreut, die präzisere Signaturen erstellen können, um sowohl die Applikation besser zu schützen als auch weniger Fehlalarme zu verursachen.

Der Cloud-WAF-Service von Radware umfasst Algorithmen zur automatisierten Richtliniengenerierung für positive Sicherheitsregeln und erlaubt nur Transaktionen, die diesen Regeln entsprechen. Der Verwaltungsaufwand steigt dadurch nicht an. Mit anderen Machine-Learning-Algorithmen ist die Radware-Cloud-WAF in der Lage, Logs zu analysieren und verbleibende Fehlalarme automatisch zu erkennen, die sich dann per Mausklick beseitigen lassen. Ferner beinhaltet der Service alle Lösungen zum Schutz vor allen Bedrohungen, einschließlich API-Schutz, Bot-Management, DDoS-Schutz, Analysen und Forensik-Tools.

Wenn Sie eine selbstverwaltete On-Premise-WAF durch eine komplett verwaltete Cloud-WAF ersetzen, vermeiden Sie den Verwaltungsaufwand für die Einrichtung und laufende Wartung von Applikationsschutzservices.

Fehlende Cyberexperten und Schutzqualität

Wie bereits erwähnt, fällt es Unternehmen schwer, freie Cybersicherheitsstellen zu besetzen. Dieses Problem in Verbindung mit dem Verwaltungsaufwand hat zwei kritische Auswirkungen, die sich Unternehmen nicht leisten können:

- Zu wenig Applikationsexperten bedeutet, dass die Einrichtung von Applikationsschutzservices mehrere Wochen dauert und die Geschäfte erheblich beeinträchtigt.
- Da der Applikationsschutz viele Bereiche umfasst, aber nur wenige Experten alle davon beherrschen, leidet häufig die Schutzqualität.

Mit einem von Experten verwalteten Cloud-WAF-Service lassen sich diese Engpässe vermeiden. Neue Applikationsschutzservices werden in wenigen Stunden anstatt mehreren Wochen eingeführt, und in puncto Schutzqualität müssen in keinem Bereich (d. h. API, BOT, DDoS, WAF) Kompromisse eingegangen werden.

Schutzqualität

Das Schutzniveau, das eine On-Premise-WAF bieten kann, ist aufgrund einiger Designmerkmale eingeschränkt:

- Die WAF kann nur aus dem Traffic der lokalen Applikationen lernen, die sie schützt. So fehlen ihr die Erkenntnisse aus den Tausenden von Applikationen, die ein Cloud-WAF-Anbieter schützt.
- Die kontinuierliche Optimierung von Sicherheitsrichtlinien und Schutzmaßnahmen erfordert KI-basierte Automatisierung (z. B. Erkennung von Fehlalarmen und entsprechende Feinabstimmung der Richtlinien). Die dafür nötige Rechenleistung steht bei On-Premise -WAF-Lösungen nicht zur Verfügung.
- Effektiver Bot- und API-Schutz (z. B. API-Erkennung) setzt außerdem rechenintensive KI-Algorithmen voraus, die auf On-Premise-Geräten nicht ausgeführt werden können, was die Schutzqualität in diesen Bereichen begrenzt.

Ein Cloud-WAF-Service, der Tausende von Applikationen überwacht, kann lernen und automatisch Signaturen zum Schutz vor Angriffen generieren, die er in einer einzelnen Applikation erkennt, um damit alle Applikationen zu schützen.

Die Computingressourcen eines Cloud-WAF-Services sind wesentlich umfangreicher als die eines On-Premise-Geräts. Damit kann der Service viele fortschrittliche KI-Algorithmen ausführen und die Sicherheitsrichtlinien von Applikationen automatisch optimieren. Die detaillierte API-Erkennung wird ebenfalls automatisiert (und ist oft genauer als selbst dokumentierte APIs), und Bot-Traffic lässt sich besser erkennen.

Das Ergebnis ist ein deutlich höherwertiger Schutz, der eine breitere Palette an Angriffsvektoren abdeckt und Sicherheitsrichtlinien automatisch an Applikations-änderungen anpasst.

Schutz aller Applikationsebenen

Eine On-Premise-WAF ist ein Inline-Gerät (oder virtuelles Gerät), das sich vor der Applikation befindet und ihre Server schützt. Allerdings werden manche Applikationskomponenten auch auf der Client-Seite ausgeführt (z. B. Skripte, die mit Drittanbietern von Daten über den Client-Browser kommunizieren). Deshalb wird auf der Client-Seite eine andere Art von Schutz benötigt – die eine gängige WAF nicht bieten kann.

Angreifer können eine Applikation mühelos mit Bibliotheken von Drittanbietern infizieren. Diese werden dann im Browser auf der Client-Seite ausgeführt und kommunizieren vertrauliche Informationen an die Server des Hackers, ohne dass die On-Premise-WAF den Datendiebstahl bemerkt oder verhindert.

Der Cloud-WAF-Service von Radware bietet auch ein Modul für clientseitigen Schutz, das in jedem Client-Browser ausgeführt wird. Es analysiert die ein- und ausgehende Kommunikation des Browsers, erkennt unbefugte Applikations-kommunikation, meldet diese und blockiert sie.

Agilität und Skalierbarkeit

Alle Schutzfunktionen für Applikationen, insbesondere WAFs, erfordern eine hohe Rechenleistung. Sollte eine bestimmte Applikation mehr Kapazität als gewöhnlich brauchen, werden die Computingressourcen, die für ihren Schutz sorgen, stark beansprucht. Häufig kommt es bei einer On-Premise-WAF zu Engpässen, die sich nur mit viel Zeitaufwand, Kosten und Personalressourcen beseitigen lassen.

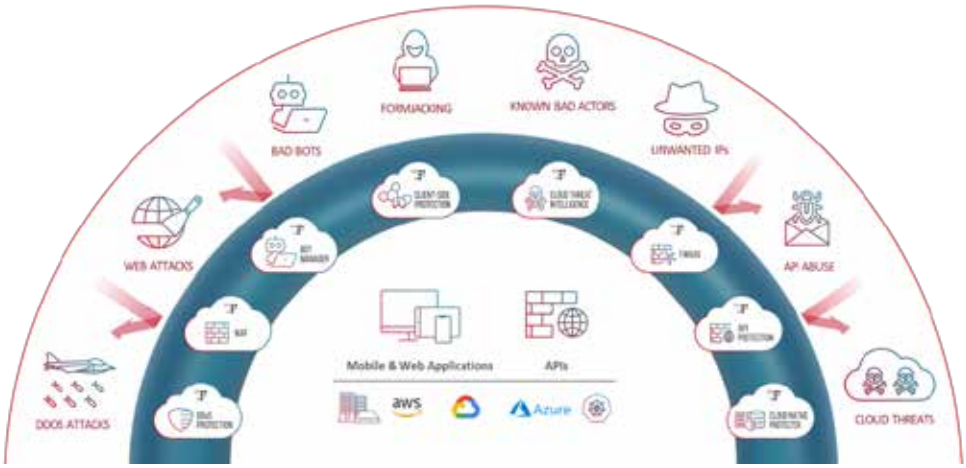
Eine On-Premise-WAF kann nur lokale Applikationen schützen. Für den Schutz von Applikationen, die in anderen privaten Clouds oder Public Clouds bereitgestellt werden, eignet sie sich nicht. Dafür benötigen die meisten Unternehmen eine andere lokalisierte WAF-Lösung (z. B. für AWS die AWS WAF), mit anderer Technologie und inkonsistenten Sicherheitsrichtlinien und -funktionen.

Mit einem Cloud-WAF-Service entfällt diese gesamte Problematik. Um die Kapazität eines Services zu erhöhen, muss einfach nur das Abonnement erweitert werden, ganz ohne physische Änderung oder Eingreifen von Experten. Funktionen wie API-Erkennung und -Schutz, Bot-Management und Layer-7-DDoS lassen sich im Handumdrehen zu einem Cloud-WAF-Service hinzufügen.

Eine Cloud-WAF kann jede Applikation abdecken, unabhängig davon, ob sie in einem privaten Rechenzentrum, einer privaten Cloud oder Public Cloud bereitgestellt wurde. Selbst für Applikationen, die keinen Traffic an die Cloud-WAF von Radware umleiten können, gibt es eine Lösung: Das Radware SecurePath-Plug-in (das sich für verschiedene Clouds und ADC-Lösungen eignet) kann den Cloud-WAF-Service von Radware im Out-of-Path-Modus bereitstellen, einschließlich Angriffserkennung und -blockierung.

Der Cloud-WAF-Service von Radware: ein umfassender und nahtloser Applikationsschutzservice

Wenn Sie Ihre Geschäfte ausbauen, Ihre Applikationsarchitektur weiterentwickeln oder Ihre Cloud-Umgebungen und -Dienste erweitern, lässt sich Ihre Applikationssicherheit ganz einfach verwalten und nahtlos skalieren. Mit dem One-Stop-Shop, der alle Schutzservices von Radware beinhaltet, bleiben Sie vor Bedrohungsvektoren geschützt, während Ihr Unternehmen wächst und Ihre Applikationen sich verändern. Dabei ersparen Sie sich den Verwaltungsaufwand und gewährleisten ultraschnellen Schutz.



Ultramoderner Applikationsschutz als Service

Web Application Firewall

Die adaptive und automatisierte WAF von Radware schützt vor Angriffen auf Webapplikationen, Hacking und anderen Schwachstellen. Die WAF-Technologie basiert auf einem positiven Sicherheitsmodell, das automatisch die Verhaltensmuster legitimer Benutzeraktivitäten erlernt, maßgeschneiderte Sicherheitsrichtlinien für diese Aktivitäten erstellt und alle Aktionen blockiert, die von diesen Mustern abweichen.

Radware kombiniert negative und positive Sicherheitsmodelle für einen umfassenden Schutz vor den OWASP-Top-10-Bedrohungen und Zero-Day-Angriffen, die WAFs mit negativen Sicherheitsmodellen nicht abwehren können.

API-Schutz

Eine spezielle, durchgängige und vollautomatisierte API-Schutzlösung 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 die Lösung maßgeschneiderte Sicherheitsrichtlinien zur Erkennung und Blockierung von gezielten API-Angriffen in Echtzeit. Mit einer Kombination aus Zugriffssteuerung, Schutz vor Datenlecks, Bot-Management und DoS-Abwehrtools schützt sie 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 automatisierten Bedrohungen und Bots.

Sie bietet präzises Bot-Management für Web-, mobilen und API-Traffic, indem Verhaltensmodellierung für detaillierte Intent-Analysen, kollektive Bot Intelligence und Fingerprinting für Browser, Geräte und Maschinen kombiniert werden. Sie 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.

DDoS-Schutz für Applikationen

Branchenführender Schutz wehrt DDoS-Angriffe auf Applikationsebene (L7) ab. Er basiert auf dem einzigartigen Verhaltensmodell von Radware, das zwischen legitimem und bösartigem Traffic unterscheidet und automatisch vor Zero-Day-Angriffen schützt. Mit exklusiven hybriden, Always-on- und On-Demand-Bereitstellungsmethoden sorgt der Cloud-DDoS-Service von Radware für erstklassigen Schutz gegen eine Vielzahl von Bedrohungen wie HTTP-Floods, HTTP-Bombs, Low-and-Slow-Angriffe und Brute-Force-Attacken.

Clientseitiger Schutz

Eine fortschrittliche clientseitige Lösung schützt die Daten von Endbenutzern, wenn sie in der Datenkette der Applikation mit Drittanbieterdiensten interagieren. Blockieren Sie Anfragen an verdächtige Drittparteidienste in Ihrer Datenkette im Handumdrehen, und halten Sie alle Datenschutzvorschriften ein. Schützen Sie sich vor clientseitigen Angriffen durch JavaScript-Dienste von Drittanbietern (Formjacking, Skimming/Magecart), und erkennen Sie dank detailliertem Aktivitäten-Tracking automatisch und kontinuierlich alle Drittparteidienste in Ihrer Datenkette. Darüber hinaus erhalten Sie Alarme und eine Bedrohungsbewertung anhand mehrerer Merkmale, darunter 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 JavaScript-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.

Vollständige Transparenz und Kontrolle

Radware stellt Dashboards für Sicherheit und Entwicklung bereit, die praxisrelevante Analysen, Automatisierung und benutzerspezifische Steuerungen enthalten. Damit sind Sie jederzeit über Bedrohungen für Ihre Applikationen informiert und können fundierte Entscheidungen für Applikationsentwicklung treffen.

Zusammenfassung

Applikationsschutz mit einer selbstverwalteten On-Premise-App reicht heutzutage nicht mehr aus. Der damit verbundene Verwaltungsaufwand sowie der Mangel an Fachleuten für Cybersicherheit führen zu inakzeptablen Engpässen und beeinträchtigen die Schutzqualität. Weil sich die Applikationsarchitektur ständig weiterentwickelt, sind On-Premise-WAFs schlichtweg nicht geeignet, um eine konsistente Lösung für alle Applikationen in allen Bereitstellungsumgebungen einzurichten.

Die Cloud-WAF von Radware hilft, diese Herausforderungen zu meistern, denn ihr führender Applikationsschutz deckt eine Vielzahl von Angriffsvektoren ab und ist in kürzester Zeit einsatzbereit. Eine zentrale Rolle spielen dabei das erfahrene Emergency Response Team (ERT) mit Experten für Applikationsschutz sowie KI-basierte Algorithmen zur Automatisierung und laufenden Optimierung von Sicherheitsrichtlinien. In Verbindung mit SecurePath werden flexible Bereitstellungsmodelle für jedes Szenario angeboten, selbst wenn keine Traffic-Umleitung oder kein Austausch von SSL-Keys möglich ist. Der Cloud-WAF-Service von Radware sorgt für einen höherwertigen Schutz, während der Verwaltungsaufwand entfällt und das Unternehmen agiler wird.

RW1167-DE