LÖSUNGSÜBERSICHT

Laufzeitsicherheit für den modernen Versicherungsträger

Schutz des Vertrauens der Versicherungsnehmer und sensibler Daten

Die Versicherungsbranche dient als finanzielles Sicherheitsnetz für Privatpersonen und Unternehmen und mindert Risiken in verschiedenen Bereichen wie Leben, Gesundheit, Kraftfahrzeug, Eigentum und Handel. Sie bedienen ihre Kunden zunehmend über digitale Kanäle, einschließlich Online-Portale, mobile Apps, Underwriting-APIs und automatisierte Schadensbearbeitung. Während diese digitalen Tools die Kundenerfahrungen und die operative Effizienz verbessern, setzen sie Versicherer auch erhöhten Cyberrisiken, regulatorischer Prüfung und Bedrohungen des Markenrufs aus.

Herkömmliche Anwendungs- und API-Sicherheit versagt beim Schutz moderner Versicherungsplattformen

- Bis zu 50% der Sicherheitsverletzungen bei Versicherungsunternehmen stammten von Drittanbieter-Software
- Branchenübergreifende Software-Schwachstellen verursachten 37% der Sicherheitsverletzungen
- Die durchschnittlichen Kosten einer Sicherheitsverletzung in der Versicherungsbranche betragen über 6 Millionen US-Dollar
- Angreifer können bekannte Schwachstellen in weniger als einer Woche ausnutzen

Das Problem: Mit jeder Anwendung steht das Vertrauen Ihrer Versicherungsnehmer auf dem Spiel

Self-Service-Policenportalen bis hin zu KI-gesteuerten Risikobewertungen und Fintech-Integrationen von Drittanbietern ist die Branche zunehmend auf SaaS-Anwendungen und APIs angewiesen, um zu funktionieren. Diese Anwendungen sind der Ort, wo sensible Kundendaten wie personenbezogene Daten (PII), Finanzunterlagen und auch gesundheitsrelevante Daten erstellt, verarbeitet und historisiert werden.

Dennoch haben die meisten Anwendungssicherheitsprogramme Schwierigkeiten, Schritt zu halten.

AppSec-Teams im Versicherungssektor stehen vor verschiedenen Herausforderungen. Veraltete Infrastruktur dominiert noch immer. Versicherungsanwendungen können auf veralteten oder hybriden Systemen laufen, die schwer zu sichern und mit modernen Sicherheitstools zu überwachen sind. Security Operations Center (SOC)-Teams fehlt oft der Einblick in Ereignisse auf der Anwendungsebene. Herkömmliche Netzwerk- und Endpunkt-Überwachungstools wie WAF und EDR sind unzureichend bei der Erkennung von Angriffen auf die Anwendungslogik oder deren Missbrauch. EDR überwacht Aktivitäten auf Geräten, kann aber nicht die Laufzeitumgebung der Anwendung einsehen, um zu verstehen, wie sich Code verhält oder ob legitime Funktionen böswillig ausgenutzt werden. Es verpasst den komplexen Tanz der Anwendungslogik. WAFs werden zur Perimeter-Verteidigung zum Blockieren häufiger, bekannter Angriffe, wie SQL-Injection oder Cross-Site-Scripting eingesetzt. WAFs haben jedoch Schwierigkeiten mit komplexen, sich ständig weiterentwickelnden Angriffen, die auf einzigartige Anwendungsgeschäftslogik, benutzerdefinierte Code-Schwachstellen oder subtilen Missbrauch legitimer Anwendungsfunktionen abzielen. Sie können die Absicht hinter einer Reihe von scheinbar harmlosen Anfragen nicht verstehen, die in ihrer Gesamtheit einen Angriff darstellen.

Darüber hinaus führt der Aufstieg von KI-generiertem Code, obwohl er die Produktivität steigert, zu neuen und unvorhergesehenen Schwachstellen in einem Ausmaß und einer Geschwindigkeit, die nie zuvor gesehen wurden.

Das Problem: Mit jeder Anwendung steht das Vertrauen Ihrer Versicherungsnehmer auf dem Spiel (Forts.)

APIs und mobile Plattformen erweitern die digitale Präsenz des Versicherers, vergrößern aber auch die Angriffsfläche. Da diese Systeme schrittweise containerisiert oder über APIs bereitgestellt werden, erweitert sich die Angriffsfläche, wodurch sie zu primären Zielen für OWASP Top 10-Bedrohungen wie Injection-Angriffe, fehlerhafte Authentifizierung und unsichere Deserialisierung werden.

Der regulatorische Druck ist ebenfalls intensiv. Versicherungsunternehmen müssen Vorschriften wie die Datenschutz-Grundverordnung (DSGVO) der EU, den US Gramm-Leach-Bliley Act (GLBA) und bundesstaatsspezifische Datenschutzgesetze wie den California Consumer Privacy Act (CCPA) einhalten. Dies erhöht die Komplexität bei der Sicherung persönlicher und finanzieller Daten, insbesondere auf Anwendungsebene, wo sensible Ein- und Ausgaben am verwundbarsten sind.

Ohne Laufzeit-Anwendungssicherheitslösungen riskieren Organisationen, kritische Systeme der Ausnutzung auszusetzen. Um sicher zu bleiben, müssen sich Sicherheitspraktiken parallel zu Entwicklungsmethoden und aufkommenden Technologien wie KI weiterentwickeln und dabei diese grundlegenden Herausforderungen berücksichtigen. Angesichts der Anfälligkeit der Branche für Datenschutzverletzungen können Verzögerungen bei der Erkennung und Behebung auftreten, und zwar infolge von:

- Schwierigkeiten bei der genauen Lokalisierung von Anwendungsexploits aufgrund fehlenden Kontextes, was Sicherheitsteams überlasten kann.
- KI-generierte unsichere Anwendungen, die Code enthalten, der auf potenziell anfälligem menschlichen Code trainiert wurde, breiten sich aus.
- Unzureichender Laufzeitschutz, der Anwendungen gegenüber Zero-Day-Exploits und bekannten Schwachstellen ungeschützt lässt.

Fazit: Die Sicherheitsteams von Versicherungsunternehmen sind überlastet damit, Anwendungsschwachstellen und Exploits zu verfolgen.

Warum Laufzeit-Anwendungssicherheit für Versicherungsträger und -anbieter?

Sofortige Kontrollen zum Schutz der Daten anwenden

Wenn ein Angriff stattfindet, ist die sofortige Anwendung von Kontrollmaßnahmen für den Schutz sensibler Versicherungsnehmerdaten und kritischer Geschäftsabläufe wichtig. Echtzeit-Transparenz ermöglicht es Sicherheitsteams, Schwachstellen zu priorisieren und diese Kontrollen schnell anzuwenden, da Sicherheitsteams nicht nur den Angriff während seines Ablaufs sehen können, sondern auch die |exakten Codezeilen identifizieren können, die ihn ermöglicht haben.

Ein unverzichtbares Sicherheitsnetz

Das Einspielen von Patches kann ein langwieriger Prozess sein, insbesondere bei den komplexen Legacy-Systemen. Laufzeit-Anwendungssicherheit bietet ein wichtiges Sicherheitsnetz, das automatisch kompensierende Kontrollen anwendet, sobald eine Schwachstelle ausgenutzt wird, noch bevor eine dauerhafte Lösung implementiert wird.

Blockieren Sie Angriffe auf KI-generierten Code

Der zunehmende Einsatz von KI zur Unterstützung der Codegenerierung für Underwriting-Plattformen, Schadenbearbeitungssystemen und Kundenportalen führt zu neuen Möglichkeiten für unsicheren Code und Zero-Day-Schwachstellen. Laufzeit-Anwendungssicherheit bietet kontextbewusste Erkennung, die entscheidend für die Blockierung von Angriffen gegen diesen KI-generierten Code ist.

Skalierbare Sicherheit für komplexe Infrastrukturen

Versicherungsorganisationen verwalten umfangreiche und komplexe IT-Infrastrukturen, von kundenorientierten Portalen bis hin zu internen Underwriting-Plattformen und Drittanbieter-Integrationen. Laufzeit-Anwendungssicherheit kann skaliert werden, um den ganze Anwendungs-Stack zu schützen, einschließlich APIs und Drittanbieteranwendungen, und gewährleistet so eine umfassende Abdeckung.

Der Contrast-Vorteil: Aufbau von Anwendungsresilienz für den modernen Versicherer

Vorteil	Wert
Angriffe erkennen und schnell blockieren	Überwacht das Anwendungsverhalten und den Datenfluss, identifiziert verdächtige Muster und Anomalien und blockiert bei Erkennung eines bestätigten Angriffs diesen sofort und alarmiert die Sicherheitsteams mit umfangreichen Informationen, die bei der konkreten Umsetzung von weiteren Maßnahmen helfen.
Zero-Day-Resilienz	Instrumentiert Anwendungen von innen heraus, anstatt sich auf signaturbasierte Erkennung zu verlassen, und ermöglicht die Erkennung von und Reaktion auf sowohl bekannte als auch unbekannte Bedrohungen, einschließlich Zero-Day-Exploits, durch Verhaltensanalyse innerhalb der Anwendungslaufzeit.
Automatisierte Behebungsanleitung	Liefert präzise, umsetzbare Sicherheitserkenntnisse, beschleunigt Reaktionszeiten und stellt sicher, dass Schwachstellen behoben werden, bevor sie kritische Dienste beeinträchtigen. Dynamische Risikobewertung ermöglicht eine intelligente Priorisierung basierend auf dem, was tatsächlich in der Produktion gefährdet ist.
Reduzieren Sie die MTTR und stärken Sie die Sicherheitslage	Bietet eine einheitliche Plattform, die einen holistischen Überblick über den ganzen Lebenszyklus einer Software, von der Entwicklung bis zur Bereitstellung, liefert. Ermöglicht eine genaue, automatisierte Priorisierung und Behebung, wodurch Teams Störgeräusche herausfiltern können und sich auf die kritischsten Risiken für Daten- und Anwendungsintegrität konzentrieren können.

Warum Contrast anders ist

Zusammen schaffen Contrast AST und ADR eine Rückkopplungsschleife zwischen Entwicklung, Sicherheit und Betrieb. AppSec-Teams können Korrekturen basierend auf Ausnutzbarkeitsdaten aus AST priorisieren, während SOC-Teams hochpräzise Warnmeldungen erhalten, die mit Code-Kontext angereichert sind.

CONTRAST APPLICATION DETECTION AND RESPONSE (ADR)

Schützen Sie Anwendungen und APIs vor Exploits und Zero-Day-Angriffen.

Erkennen Sie Angriffe auf Anwendungen und APIs, damit Sicherheitsteams reagieren können, bevor Exploits auftreten.

CONTRAST APPLICATION SECURITY TESTING (AST)

Überwachen Sie Code während der Ausführung. Schwachstellen sofort identifizieren.

Priorisieren und behandeln Sie Risiken mit schnellerer Erkennung von Anwendungs- und API-Schwachstellen und weniger Fehlalarmen.

CONTRAST ONE

Schützen Sie Ihre Anwendungen und APIs mit Contrast One.

Wir verwalten Ihre Anwendungs- und API-Sicherheit, zusammen mit den Menschen, die sie entwickelt haben.

Bereit, die Contrast Runtime Security Plattform in Aktion zu sehen?

Mehr erfahren

Contrast Security ist der weltweite Marktführer im Bereich Runtime Application Security und integriert Codeanalyse und Angriffsprävention direkt in Software. Contrasts patentierte Sicherheitsinstrumentierung ermöglicht leistungsstarke Anwendungssicherheitstests und Anwendungserkennung und -reaktion, wodurch Entwickler, AppSec-Teams und SecOps-Teams ihre Anwendungen besser schützen und gegen die sich ständig weiterentwickelnde Bedrohungslandschaft verteidigen können.

contrastsecurity.com

6800 Koll Center Parkway
Ste 235
Pleasanton, CA 94566
Telefon: 888.371.1333