CONTRAST SECURITY

LÖSUNGSÜBERSICHT

Laufzeitschutz für kritische Finanzanwendungen

Schutz hochsensibler Daten gegen fortgeschrittene Bedrohungen

Da die Finanzdienstleistungs- und Bankenbranche durch mobile Geldbörsen, Vermögensverwaltungs-APIs, digitale Identitätsverifizierung und ähnliche Dienste immer digitaler wird, nehmen die Cybersicherheitsrisiken zu. Der Druck, schnell zu innovieren und gleichzeitig die Compliance aufrechtzuerhalten und hochsensible Daten gegen fortgeschrittene Angriffe zu verteidigen, sorgt in der Sicherheitslandschaft für Herausforderungen.

Ein Hauptproblem ist die Komplexität von Legacy-Systemen, die in moderne Anwendungen integriert werden. Diese hybride Umgebung verfügt oft über keine standardisierten Sicherheitskontrollen, was es schwierig macht, Anwendungen plattformübergreifend einheitlich zu schützen. Viele dieser Anwendungen sind anfällig für Bedrohungen wie unsichere Deserialisierung und fehlerhafte Zugriffskontrolle, insbesondere auf der Ebene der Anwendungslogik.

Herkömmliche Sicherheitstools wie SAST und DAST sind oft unzureichend, wenn es darum geht, anfälligen Code zu erkennen und zu beheben. Vor allem SAST-Tools erzeugen große Mengen an Fehlalarmen und erfordern umfangreiche manuelle Validierung. Vor allem herkömmliche DAST-Tools können nicht mit der Geschwindigkeit oder in der Tiefe arbeiten, die von Finanzinstituten benötigt wird. Darüber hinaus haben SOC-Teams oft keinen direkten Einblick in das Anwendungsverhalten, was es schwierig macht, Angriffe zu erkennen, die infrastrukturbasierte Abwehrmechanismen umgehen.

Darüber hinaus hat der Aufstieg von Fintech-Integrationen und Open-Banking-APIs neue Angriffsvektoren eingeführt, über die Angreifer unbefugten Zugang zu Konten erlangen, schädliche Datenpakete einschleusen oder Geschäftslogik missbrauchen können.

Der Aufstieg von Fintech-Anwendungen und APIs hat neue Angriffsvektoren für Angreifer eingeführt

- Über 71% der Finanzinstitute gaben an, dass Zero-Day-Angriffe das größte Problem darstellten, dem sie beim Schutz ihrer Anwendungen gegenüberstanden
- 65% Wachstum bei Anwendungsangriffen in der Finanzdienstleistungsbranche über 12 Monate
- Die durchschnittlichen Kosten einer Sicherheitsverletzung in Finanzdienstleistungen betragen 4,9 Millionen US-Dollar

Die sich entwickelnde Angriffsfläche: Sicherung von Fintech- und Open-Banking-APIs

Der digitale Fußabdruck der Finanzbranche wächst weiter. APIs, mobile Apps und Open-Banking-Integrationen erweitern die Angriffsfläche und setzen Institutionen gängigen Bedrohungen wie Injections, fehlerhafter Zugriffskontrolle und unsicherer Deserialisierung aus — Kernprobleme der OWASP Top 10.

Die sich entwickelnde Angriffsfläche: Sicherung von Fintech- und Open-Banking-APIs (Forts.)

Da sich das Online-Banking mit neuen Technologien weiterentwickelt, entsteht eine erhebliche Herausforderung durch die Art und Weise, wie diese Innovationen mit älteren Systemen, bestehenden Apps und sogar von Dritten entwickelten Anwendungen interagieren. Diese Vernetzung kann neue Sicherheitsschwächen schaffen. Beispielsweise nutzen Bankinstitute oft Hunderte verschiedener Anwendungen, von denen einige von Dritten entwickelt, aber auf den eigenen Systemen der Bank gehostet werden. In solchen Fällen können herkömmliche Sicherheitsscans wie Static Application Security Testing (SAST) nicht helfen, da sie Zugriff auf den Quellcode der Anwendung benötigen, der für diese Drittanbieter-Tools nicht verfügbar ist.

Sicherheitsoperationszentren (SOCs) sind traditionell darauf ausgelegt, Netzwerke und Endpunkte zu überwachen, nicht die Aktivitäten auf der Anwendungsschicht. Infolgedessen übersehen sie oft ausgeklügelte, logikbasierte Angriffe, die Geschäftsabläufe ausnutzen, anstatt technische Schwachstellen. Diese blinden Flecken lassen Anwendungen ungeschützt, da herkömmliche Erkennungsmechanismen Bedrohungen auf der Anwendungsschicht nicht erkennen geschweige denn blockieren können.

Die schiere Menge an Sicherheitswarnungen stellt eine weitere große Herausforderung dar. SOC-Teams fällt es schwer, echte Anwendungssicherheitsbedrohungen von Fehlalarmen oder Hintergrundrauschen zu unterscheiden, was die Reaktionszeiten bei Vorfällen erheblich verlangsamt und das Risiko übersehener Bedrohungen erhöht.

Darüber hinaus ist die Einführung von KI-unterstützten Entwicklungstools ein zweischneidiges Schwert. Während diese Tools die Code-Generierung beschleunigen, können sie auch unsicheren Code in einem Tempo einführen, das für menschliche Teams schwer zu überwachen und zu verwalten ist. Das erhöht den Druck auf bereits überlastete Anwendungssicherheitsteams.

Schließlich stehen Finanzinstitute vor einer intensiven regulatorischen Belastung. Compliance-Anforderungen wie PCI-DSS, GLBA, NYDFS 500 und neue Vorschriften wie DORA in der EU erfordern kontinuierliche Wachsamkeit und robuste Anwendungssicherheitspraktiken, was zusätzliche Belastungen für interne Teams mit sich bringt.

Ohne moderne, laufzeitbasierte Anwendungssicherheitsstrategien riskieren Banken schwerwiegende Sicherheitsverletzungen, die zu finanziellen Verlusten, regulatorischen Strafen und Reputationsschäden führen.

Fazit: Anwendungssicherheitsrisiken überlasten die Sicherheitsteams der Banken.

Sicherheitsteams benötigen Einblick in das Live-Anwendungsverhalten und die Fähigkeit, schnell zu handeln. Sie müssen Zero-Day-Schwachstellen, unsicheren KI-generierten Code und komplexe Angriffsketten, die auf APIs, Backend-Systeme und moderne Web-Stacks abzielen, alle in Echtzeit angehen. Punktuelle Tests (SAST, DAST) und isolierte Legacy-Tools reichen nicht aus.

Warum ist Anwendungssicherheit zur Laufzeit für Banken und Finanzinstitute von entscheidender Bedeutung?

Einblick in das Verhalten von Live-Angriffen

Laufzeit-Anwendungssicherheit liefert Echtzeiteinblicke in Angriffe aus der Anwendung heraus. Teams können aktive Bedrohungen verstehen, priorisieren und blockieren, ohne das Rauschen und die Verzögerungen herkömmlicher Tools.

Ein Puffer für Patch-Verzögerungen

In regulierten und komplexen Umgebungen dauert das Patchen Zeit. Laufzeitschutz kann kompensatorische Kontrollen sofort durchsetzen, noch bevor ein Patch bereit ist, und hilft dabei, compliant zu sein und den Betrieb sicher aufrechtzuerhalten.

Schutz vor zunehmendem KI-generierten Code

Bankdienstleistungen wie Kundenportale enthalten oft Code, der von KI oder von Drittanbieter-Tools generiert wurde. Laufzeitsicherheit erkennt und neutralisiert Schwachstellen im Code, bevor sie ausgenutzt werden.

Skalierbare Sicherheit über den ganzen Stack

Laufzeitlösungen skalieren, um Web-Apps, APIs, Container und Drittanbieter-Integrationen zu schützen und dabei die digitale Transformation zu unterstützen, ohne das Risiko zu erhöhen.

Der Contrast-Vorteil: Schneller innovieren ohne Kompromisse bei Sicherheit und Compliance

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 kontextuellen Informationen Code-Ebenen-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-Laufzeitsicherheitsplattform 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