CONTRAST SECURITY

SOLUTION BRIEF

Runtime security for the modern insurance carrier

Protecting policyholder trust and sensitive data

The insurance industry serves as a financial safety net for individuals and businesses, mitigating risk across diverse areas such as life, health, auto, property and commerce. They increasingly service their clients and customers through digital channels, including online portals, mobile apps, underwriting APIs and automated claims processing. While these digital tools improve customer experiences and operational efficiency, they also expose insurers to elevated cyber risk, regulatory scrutiny and brand reputation threats.

Traditional application and API security fails to protect modern insurance platforms

- Up to 50% of breaches at insurance firms stemmed from third-party software
- Cross-industry software vulnerabilities caused 37% of breaches
- The average cost of a breach in the insurance industry is over $6 million
- Attackers can exploit known vulnerabilities in under a week

The problem: When every application is a gateway to policyholder trust

Insurers are evolving into digital-first enterprises. From instant quote calculators and self-service policy portals to AI-driven risk assessments and third-party fintech integrations, the industry is increasingly reliant on SaaS applications and APIs to operate. These applications are where sensitive customer data such as Personally Identifiable Information (PII), financial records and health insurance medical history is created, processed and stored.

Yet most application security programs struggle to keep pace.

AppSec teams in the insurance sector face several challenges. Legacy infrastructure still dominates. Insurance applications might run on outdated or hybrid systems that are difficult to secure and monitor using modern security tools. Security Operations Center (SOC) teams often lack visibility into application-layer events. Traditional network and endpoint monitoring tools such as WAF and EDR fall short in detecting application logic attacks or misuse. EDR monitors activities on devices, but it can't see inside the application's runtime to understand how code is behaving or if legitimate functions are being exploited maliciously. It misses the intricate dance of application logic. WAFs are perimeter defenses for blocking common, known attacks at the edge, like SQL injection or cross-site scripting. However, WAFs struggle with complex, evolving attacks that target unique application business logic, custom code vulnerabilities or subtle abuse of legitimate application features. They can't understand the intent behind a series of seemingly benign requests that, in aggregate, constitute an attack.

Additionally, the rise of AI-generated code, while enhancing productivity, is introducing new and unforeseen vulnerabilities at a scale and speed never seen before.

APIs and mobile platforms expand the insurer's digital footprint but also increase the attack surface. As these systems are gradually containerized or exposed via APIs, the attack surface expands, making them prime targets for OWASP Top 10 threats such as injection attacks, broken authentication, and insecure deserialization.

Regulatory pressure is also intense. Insurance companies must comply with regulations such as the EU's General Data Protection Regulation (GDPR) , US Gramm-Leach-Bliley Act (GLBA), and state-specific privacy laws like the California Consumer Privacy Act (CCPA). This adds complexity to securing personal and financial data, especially at the application level, where sensitive inputs and outputs are most vulnerable.

Without runtime application security solutions, organizations risk exposing critical systems to exploitation. To stay secure, security practices must evolve alongside development methodologies and emerging technologies like AI, accounting for these primary challenges. Given the industry's exposure to data breaches, delays in detection and remediation can occur, as a result of:

- Difficulty in pinpointing application exploits due to lack of context, which can overwhelm security teams.
- AI-generated insecure applications containing code trained on potentially vulnerable human code proliferation.
- Inadequate runtime protection, which leaves applications exposed to zero days and known vulnerabilities.

Bottom line: Insurance security teams are overwhelmed chasing down application vulnerabilities and exploits.

Why runtime application security for insurance carriers and providers?

Apply immediate controls to safeguard data

When an attack happens, applying immediate controls is essential for protecting sensitive policyholder data and critical business operations. Real-time visibility allows security teams to prioritize vulnerabilities and apply these controls swiftly because security teams can not only see the attack as it unfolds but also pinpoint the exact lines of code that enabled it.

An essential safety net

Deploying patches can be a lengthy process, particularly with the intricate legacy systems. Runtime application security provides a vital safety net that automatically applies compensating controls the moment a vulnerability is exploited, even before a permanent fix is deployed.

Block attacks on AI-generated code

The increasing use of AI to assist in code generation for underwriting platforms, claims processing systems and customer portals introduces new potential for insecure code and zero-day vulnerabilities. Runtime application security provides context-aware detection, which is crucial for blocking attacks against this AI-generated code.

Scalable protection for complex infrastructures

Insurance organizations manage vast and complex IT infrastructures, from customer-facing portals to internal underwriting platforms and third-party integrations. Runtime application security can scale to protect entire application stacks, including APIs and third-party applications, ensuring comprehensive coverage.

The Contrast advantage: Building application resilience for the modern insurer

Benefit	Value
Detect and quickly block attacks	Monitors application behavior and data flow identifying suspicious patterns and anomalies and when an attack is detected, leveraging agentic AI to block the attack and alert security teams with context and actionable information.
Zero-day resilience	Instruments applications from within, rather than relying on signature-based detection, enabling the detection and response to both known and unknown threats, including zero-day exploits, through behavioral analysis within the application runtime.
Automated remediation guidance	Delivers precise, actionable security insights, accelerating response times and ensuring that vulnerabilities are fixed before they impact critical services. Dynamic risk scoring brings a smarter way to prioritize based on what's actually at risk in production.
Reduce MTTR and strengthen security posture	Provides a unified platform that eliminates the guesswork that plagues traditional tools, enabling accurate, automated prioritization and remediation allowing teams to filter out noise, enabling a focus on the most critical risks to data and application integrity.

Why Contrast is different

Together, Contrast AST and ADR create a feedback loop between development, security and operations. AppSec teams can prioritize fixes based on exploitability data from AST, while SOC teams gain high-fidelity alerts enriched with code-level context.

CONTRAST APPLICATION DETECTION AND RESPONSE (ADR)

Protect applications and APIs from exploits and zero days.

Detect attacks on applications and APIs so security operations teams can respond before exploits occur.

CONTRAST APPLICATION SECURITY TESTING (AST)

Monitor code as it runs.
Identify vulnerabilities instantly.

Prioritize and address risks with faster application and API vulnerability detection and fewer false positives.

CONTRAST ONE

Defend your applications and APIs with Contrast One.

Managed application and API security powered by the people who built it.

Ready to see the Contrast runtime security platform in action?

Learn more

Contrast Security is the world's leader in Runtime Application Security, embedding code analysis and attack prevention directly into software. Contrast's patented security instrumentation enables powerful Application Security Testing and Application Detection and Response, allowing developers, AppSec teams and SecOps teams to better protect and defend their applications against the ever-evolving threat landscape.

contrastsecurity.com

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