SOLUTION BRIEF

Runtime security for the applications that power patient care

Secure critical patient data and ensure compliance

The healthcare industry focuses on patient care, medical services and public health initiatives aimed at promoting and maintaining overall well-being. It spans a wide range of organizations including hospitals, clinics, pharmaceutical research, biotech and insurance. Driven by constant innovation and research, the healthcare industry integrates advanced technologies to improve outcomes, patient experiences and operational efficiency. However, it must also address complex challenges like regulatory compliance, cybersecurity and data privacy.

Stretched healthcare security teams are struggling to keep pace with the volume and complexity of modern application risks

- 92% of healthcare organizations reported experiencing a cyberattack in 2024
- Average cost of a cyber attack is $4.9 million
- Up to 30% of healthcare data breaches were caused by application layer attacks such as SQL injection and cross-site scripting
- Only 5 days for attackers to exploit vulnerabilities

The problem: Healthcare digital revolution is outpacing security

The healthcare industry is rapidly transforming through a digital revolution, driven by the widespread adoption of Electronic Health Records (EHRs), telehealth services, patient portals, connected medical devices and healthcare APIs. These systems primarily operate at the application layer, where sensitive patient information is created, accessed and exchanged.

Healthcare security teams often operate with limited resources and rely on outdated tools like network- and endpoint-focused monitoring, which struggle to detect sophisticated attacks targeting application logic.

Compounding these challenges is the prolific nature of mergers and acquisitions within hospital systems. As hospitals are exchanged between different entities, already strapped security teams face immense pressure to efficiently onboard and offload applications. This constant flux strains their ability to maintain consistent security oversight across a rapidly changing application landscape.

Given healthcare's frequent exposure to ransomware and data breaches, delays in detection or a lack of context can lead to devastating consequences, including:

- Difficulty in pinpointing application exploits due to lack of context, which can overwhelm security teams.
- Inadequate attack blocking, which allows exploits to proceed, resulting in data breach fallout.
- Proliferation of AI-generated insecure applications containing code trained on potentially vulnerable human code.
- These include unauthorized access to medical records, abuse of scheduling platforms or injection of malicious code into patient-facing systems.
- HIPAA, HITECH and other global privacy standards demand strict safeguards to protect the confidentiality, integrity and availability of patient data.

Bottom line: Application security risks are overwhelming stretched healthcare security teams.

Why runtime application security for healthcare organizations?

Visibility into actual attack behavior

Runtime application security works within the live application itself, giving real-time visibility into actual attack behavior. This means security teams can prioritize vulnerabilities more intelligently and put immediate controls in place effectively multiplying the team's impact, allowing them to better support medical professionals and the patients they all serve.

Essential safety net

When a vulnerability is identified, deploying a patch can take time, especially in complex systems with strict release schedules or regulatory constraints. Runtime application security can apply compensating controls even before a permanent fix is deployed.

Block attacks against vulnerable AI-generated code

Runtime application security provides context-aware detection, which is essential when AI might write thousands of lines of insecure code in minutes, and zero-day vulnerabilities might spread faster than manual teams can respond.

Scalable protection

Runtime application security can scale to protect entire application stacks, including APIs and third-party applications, ensuring comprehensive protection across the entire software supply chain.

The Contrast advantage: Security and compliance for the modern healthcare ecosystem

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