SOLUTION BRIEF

Post-quantum crypto readiness with Contrast Security

Find and fix quantum-unsafe encryption before it becomes tomorrow's compliance and security crisis

The coming shift to quantum-safe cryptography

Quantum computing will fundamentally change how organizations protect their data. Algorithms that have safeguarded communications for decades—AES, RSA, ECC, Diffie-Hellman—will soon be vulnerable to quantum decryption techniques. While the exact timeline is uncertain, it's clear that the transition to quantum-safe cryptography will be one of the most complex, large-scale migrations in the history of cybersecurity.

The challenge isn't limited to new systems. Many organizations rely on thousands of applications and APIs built on legacy frameworks and third-party components where encryption decisions were made long ago and never revisited. Unsafe algorithms are often buried deep within libraries, configuration files or binary modules, places traditional scanners can't reach.

Contrast Security helps organizations gain a clear, actionable view of where quantum-unsafe encryption is used and what to do about it. By detecting unsafe algorithms at runtime and providing full execution context, Contrast equips security and development teams to make informed, future-proof decisions about their cryptographic posture.

Quantum transition brings hidden risks, complex migrations and new threats

Crypto is hidden everywhere

Quantum-unsafe encryption lives deep within application stacks and custom code, embedded in frameworks, third-party libraries and configuration files that are invisible to traditional scanners. These hidden dependencies make it difficult to understand true exposure.

Crypto is dynamic

Downgrade attacks, weak cipher negotiation and misconfigurations can silently reintroduce unsafe crypto, even after migration. Traditional scanners cannot detect these issues because they occur only during runtime.

Crypto is complex to analyze

Crypto is often used for security purposes, but it also has many non-security related uses. To understand if it needs replacement requires context, including the exact algorithm, the stack trace and the use case. Without execution context, teams struggle to gauge impact or decide which issues to fix.

Unsafe crypto is challenging to remediate

Finding unsafe crypto is when the hard work begins. Remediation involves identifying the right replacement algorithm and crypto library implementation, writing scripts to decrypt and re-encrypt data with the new quantum safe algorithm, and testing for quality and performance.

Standards evolve

As new algorithms are approved and threat models shift, maintaining alignment with the latest recommendations requires constant vigilance and expertise. Rapid evolution in NIST, ETSI and CNSA 2.0 guidance forces constant updates to maintain compliance and readiness.

Visibility, context, and control for a quantum-safe future

The transition to post-quantum cryptography is a strategic initiative that affects compliance, cost and trust. Contrast Security empowers organizations to move confidently by turning uncertainty into actionable insight.

Comprehensive visibility

Discover quantum-unsafe algorithms across all applications and APIs at runtime to understand the true scope of risk. See all crypto risks in a consolidated view across diverse languages and frameworks that deliver enterprise-wide resilience and audit readiness.

Context-driven remediation

Capture execution context including route information and full stack traces, revealing not only the algorithms that are in use, but also implementation details such as padding and feedback modes. This data reveals exactly where and how unsafe algorithms are used, enabling efficient remediation planning and prioritization.

Continuous compliance

Stay aligned with emerging standards and quantum threat intelligence without constant manual updates or labor-intensive research.

Continuous insight, actionable context and broad coverage to drive crypto agility

Post-quantum crypto readiness combines runtime analysis, contextual intelligence and continuously updated quantum threat models to deliver practical, ongoing protection across modern and legacy applications.

Runtime crypto-readiness assessment

Analyzes applications and APIs during runtime to detect the actual cryptographic algorithms in use, eliminating false positives from scanning unused libraries and ensuring nothing critical is overlooked.

Continuously updated threat models

Incorporates the latest developments in quantum cryptography, ensuring detection logic and recommendations reflect the most current global standards.

Full execution context

Provides detailed insights into where unsafe cryptography resides in code execution paths, empowering teams to fix issues with precision and confidence.

Broad language and framework support

Supports modern and legacy application stacks, including Java, .NET, Go and others, ensuring comprehensive coverage across enterprise technology stacks.

Build confidence in a quantum-safe future

Contrast Security helps organizations achieve post-quantum crypto readiness, moving from uncertainty to control. By identifying hidden crypto risks, validating real-world encryption use and aligning with evolving standards, it gives security leaders a clear path to quantum-resilient operations.

Try Contrast

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