Federal Agencies Must Transition to Instrumentation-Based Application Security

Outdated Application Security Tools Carry Multiple Risks

U.S. federal agencies depend on software development for a variety of critical operations. With the adoption of modern DevOps and Agile environments, outdated application security tools cause workflow bottlenecks that jeopardize delivery cycles while missing critical vulnerabilities that could lead to a serious breach.

Public sector developers need modern, instrumentation-based application security that spans the entire software development life cycle (SDLC). An effective solution should help improve development teams' productivity, accelerate operations, reduce risks, and streamline compliance obligations.

Read this paper to learn why federal agencies need instrumentation-based application security in order to:

Eliminate remediation roadblocks created by dependence on human security experts

Increase efficiency and productivity toward decreasing ever-expanding security debt

Keep pace with mission objectives, demanding delivery cycles, and elastic needs across different departments and agencies

Protect against unknown threats throughout the SDLC

Ensure support for all certification, compliance validation, and authority to operate (ATO) requirements