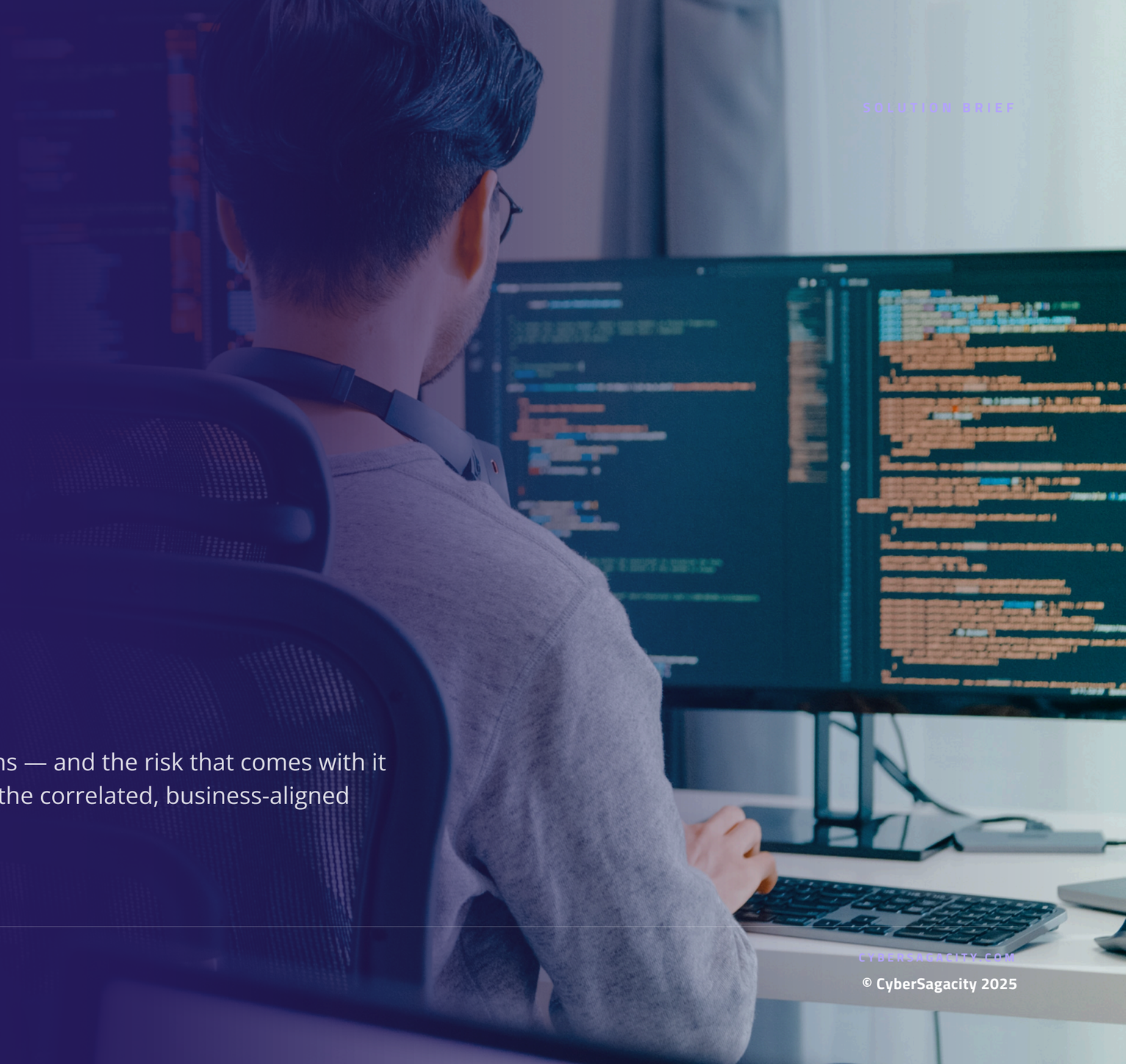
CyberSagacity

SOLUTION BRIEF



Reducing open-source software risk.

Open source now powers 80–95% of modern applications — and the risk that comes with it is systemic and under-managed. CyberSagacity delivers the correlated, business-aligned intelligence layer that traditional tools cannot.

PUBLISHED
2025

AUDIENCE
AppSec · Engineering · Security Leadership

FORMAT
Solution Brief

CYBERSAGACITY.COM

OVERVIEW

Open source is everywhere — and its risk is under-managed.

80–95% **of modern applications are open-source software.**

OSS powers cloud-native systems, AI-driven development, microservices, CI/CD, and containers. But rapid adoption has created systemic, under-managed risk:

- Unknown and unverified dependencies.
- Vulnerabilities buried in transitive chains.
- Outdated or abandoned libraries.
- Hidden supply-chain attacks.
- Licensing and regulatory exposure.
- Inconsistent, contradictory AppSec results.

> **Traditional tools detect fragments. None offer trustworthy, correlated, business-aligned risk intelligence.**

OPEN-SOURCE RISKS ARE OUTPACING TRADITIONAL APPSEC

Five reasons OSS risk stays buried in noise.

01

Exponential dependency growth

Apps contain thousands of dependencies, many auto-included via frameworks and AI-generated code — impossible to track manually.

02

SCA alone can't determine true risk

Misses behavioral exploitability, false positives from unused paths, false negatives from dynamic imports, package health and provenance, and malicious packages.

03

Tools disagree — but are treated as truth

Conflicting results waste engineering cycles, misprioritize remediation, miss critical vulnerabilities, and erode trust.

04

Business & regulatory impact is opaque

Without mapped context, no one can answer which vulnerabilities matter, what the financial exposure is, or whether you're compliant with PCI, SOX, HIPAA, GDPR, or CMMC.

05

Velocity amplifies exposure

CI/CD, containers, and microservices propagate open-source risk across environments before security teams can evaluate it.

FOUNDATIONAL APPSEC INTELLIGENCE FOR OPEN SOURCE

Correlated, accurate, business-aligned intelligence.

01

Corrected & correlated risk

Integrates signals from across the stack and produces a single authoritative view:

- SAST / DAST / IAST, SCA, PenTest
- Container & Kubernetes scanners
- Cloud posture tools
- SBOMs & CI/CD pipelines

02

Statistical accuracy modeling

Using decades of empirical data, the platform identifies:

- False positives & false negatives
- Tool strengths/weaknesses by defect type
- Real exploit likelihood

Eliminating noise and giving leaders confidence.

03

Business, financial & regulatory context

Every OSS defect is mapped to:

- Operational impact
- Expected financial loss
- License obligations
- PCI, HIPAA, SOX, GDPR, CMMC

Not just what is wrong — but why it matters.

PRIORITIZED, ACTIONABLE REMEDIATION AT VELOCITY

Developer-ready guidance — without slowing delivery.

01

Clear, unified prioritization

SATriage ranks open-source issues by:

- Actual exploitability
- Application context
- Business impact
- Compliance exposure

02

Developer-focused guidance

Action in a form developers can use:

- Specific fix instructions
- Safe upgrade paths
- License remediation guidance
- Dependency-chain risk breakdowns

03

CI/CD integration for continuous assurance

Works inside modern pipelines:

- Real-time risk scoring
- Quality gates for OSS usage
- Automated evidence collection
- Continuous governance reporting

Secure, predictable release velocity — with reliable guardrails.

WHY TECHNICAL & CYBERSECURITY LEADERS CHOOSE CYBERSAGACITY

From unknown liability to governed discipline.

- ✔ **Eliminate noise** — stop wasting capacity on false positives.
- ✔ **Focus on what's material** — real business, regulatory, financial exposure.
- ✔ **Address supply-chain risk holistically** — beyond CVEs to provenance, maintainers, license risk.
- ✔ **Reduce MTTR** — clear, correct, context-rich developer guidance.
- ✔ **Enable defensible governance** — audit-ready evidence for regulators, insurers, and boards.
- ✔ **Strengthen security–engineering trust** — validated intelligence everyone relies on.

THE OUTCOME

Use OSS at scale without unmanaged exposure; maintain posture and compliance as code volume grows; support rapid development with reliable guardrails.

Open-source risk becomes governed, predictable, and defensible.