DATA SHEET

datatheorem

Code SAST Secure

Find, fix, and remediate exploitable code vulnerabilities across first-party source, open source, and AI-generated code.

01 OVERVIEW

Code SAST Secure is Data Theorem's developer-side application security platform. It scans first-party source, bytecode, and compiled artifacts with SAST, verifies exploitability through DAST (SAST+), continuously inventories open source dependencies and SDKs with SCA and SBOM, and automatically generates secure patches for actively exploitable open-source and AI-generated code.

Find. Fix. Verify. Remediate.

SAST plus dynamic verification cuts dead-code noise and non-exploitable findings. SCA and SBOM cover open source and SDKs. AI code patching closes zero-day windows on AI-written and third-party dependencies.

02 CAPABILITIES

Platform capabilities

SAST across 15+ languages

Scans source, bytecode, and compiled code for SQL injection, XSS, buffer overflows, and CWE Top 25 weaknesses across the full polyglot stack.

SAST+ exploit verification

Runs DAST against SAST findings to filter out dead code, code-quality false positives, and non-exploitable bugs before they hit the developer queue.

SCA and SBOM

Continuous inventory of open source libraries and third-party SDKs. SBOM generation in CycloneDX and SPDX formats for procurement and compliance.

AI code patch for OSS

Auto-generates secure patches for actively exploitable open-source and AI-written dependencies, closing the zero-day window.

IDE and CI/CD integration

Native plugins for GitHub, GitLab, Bitbucket, Azure DevOps, and Visual Studio, with MCP support for AI-native IDEs.

Custom rules engine

Covers SQLi, XSS, buffer overflows, and OWASP Top 10, with custom rules for organization-specific security policy.

LANGUAGES COVERED	Java · JavaScript · Python · Swift · Kotlin | C, C++, C#, Objective-C · Go · Ruby · Rust · PHP · Perl · R
INTEGRATIONS	GitHub · GitLab · Bitbucket · Azure DevOps · Visual Studio · Jira · Jenkins · Slack · Teams · MCP-compatible IDEs

03 OUTCOMES

Key benefits

Catch exploitable bugs, not noise

SAST+ verifies findings with DAST, removing dead code, code-quality false positives, and non-exploitable issues before they reach the developer queue.

Fix at AI-native developer speed

Native MCP integration pushes context-aware patch suggestions into AI-enabled IDEs. Findings ship with secure code samples, not just warnings.

Collapse the open-source exposure window

Continuous SCA and automatic secure-patch generation close zero-day windows on actively exploitable open-source and AI-written dependencies.

Audit-ready SBOMs and policy

Custom rules enforce coding standards and security policy. CycloneDX and SPDX SBOMs satisfy procurement, compliance, and software supply-chain audits.

04 AI / LLM

AI security for code, woven through

AI code patch for open source

Continuously identifies actively exploitable OSS vulnerabilities and auto-generates secure patches before adversaries reach production.

Auto-remediation in AI-native IDEs

Native MCP support delivers context-aware fixes into AI-enabled IDEs and exposes APIs designed for LLM-driven remediation workflows.

Insecure LLM-generated code

Detects hallucinated dependencies and insecure patterns in AI-generated code. Findings map to OWASP Top 10, CWE Top 25, and OWASP LLM Top 10.

ABOUT DATA THEOREM

Data Theorem provides full-stack application security across mobile, API, code, and cloud, with AI/LLM coverage woven through. Continuous, automated, hacker-style discovery and dynamic runtime analysis surface what matters and route fixes to the teams that own them. Our customers cover over 2.8 billion users and include 7 of the top 10 largest banks.

GET STARTED

www.datatheorem.com
info@datatheorem.com

Schedule a Demo →