

IaC-ASSIST

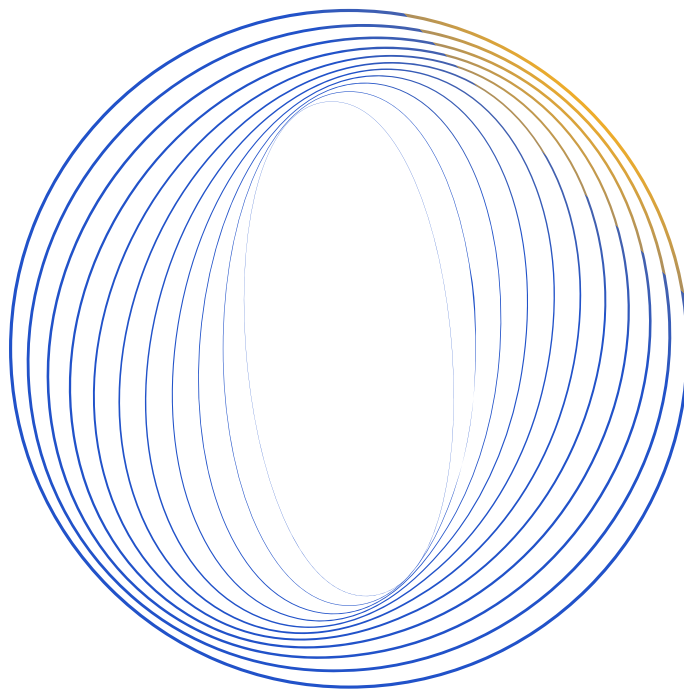
7.3 Technical Data Sheet



Overview

laC-Assist is an AI-enhanced, real-time plugin for Visual Studio Code (VSCode) that enables DevOps, DevSecOps, and security teams to secure Infrastructure as Code (IaC) early in the development process. It delivers actionable insights directly in the Integrated Development Environment (IDE), identifying misconfigurations and enforcing secure-by-design practices without interrupting agile workflows.

Seamlessly integrated with the ThreatModeler Platform, laC-Assist connects code-level decisions to system-level threat modeling, enabling continuous security from code to cloud.



Key Features

IAC MISCONFIGURATION DETECTION:

- Detects missing security attributes and weak configurations during code authoring.
- Highlights critical gaps in IaC templates using real-time scanning in VS Code.
- Prevents deployment of insecure cloud infrastructure.

AI-DRIVEN SECURITY RECOMMENDATIONS:

- Delivers intelligent, context-aware suggestions directly in the IDE.
- Offers guided remediation tailored to cloud resource definitions.
- Enables secure coding without disrupting developer velocity.

SEAMLESS THREAT MODELING INTEGRATION:

- One-click generation of threat models directly from IaC templates.
- Provides architectural visibility into risks, threats, and attack vectors.
- Integrates security architecture into developer workflows.

MULTI-CLOUD AND IAC SUPPORT:

- **Supports the following IaC templates and environments:**
 - AWS CloudFormation (YAML/JSON)
 - Terraform (for AWS, Azure, GCP)
 - Azure Resource Manager (ARM) Templates

SHIFT-LEFT SECURITY ENABLEMENT:

- Embeds security early in the Cloud Development Lifecycle (CDLC).
- Minimizes rework and reduces production vulnerabilities.
- Automates the enforcement of cloud provider and organizational best practices.

CROSS-TEAM COLLABORATION:

- Enables shared visibility between developers, security architects, and operations.
- Facilitates continuous feedback and threat validation.
- Centralizes risk ownership and standardizes secure development practices.

Benefits

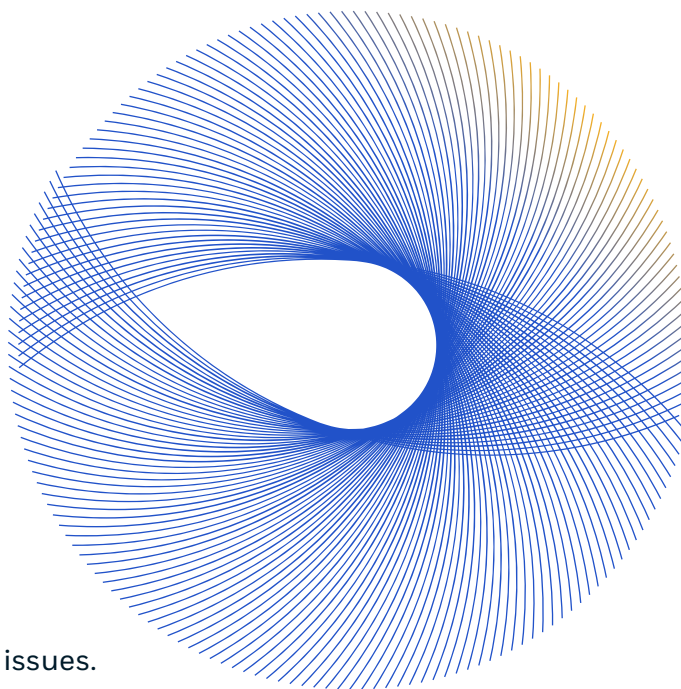
IaC-Assist delivers real-time security validation and remediation directly within developer workflows, enabling teams to detect misconfigurations, enforce secure-by-design principles, and align Infrastructure as Code (IaC) deployments with organizational security and compliance requirements.

SECURITY AND RISK MANAGEMENT:

- Flag vulnerabilities before they become production issues.
- Understand threats at both code and architecture levels.
- Implement secure-by-design policies across the SDLC.

DEVELOPER PRODUCTIVITY:

- Reduces noise and false positives with contextual insights.
- Provides in-line guidance with no context-switching required.
- Improves autonomy while aligning with security mandates.



COMPLIANCE AND GOVERNANCE:

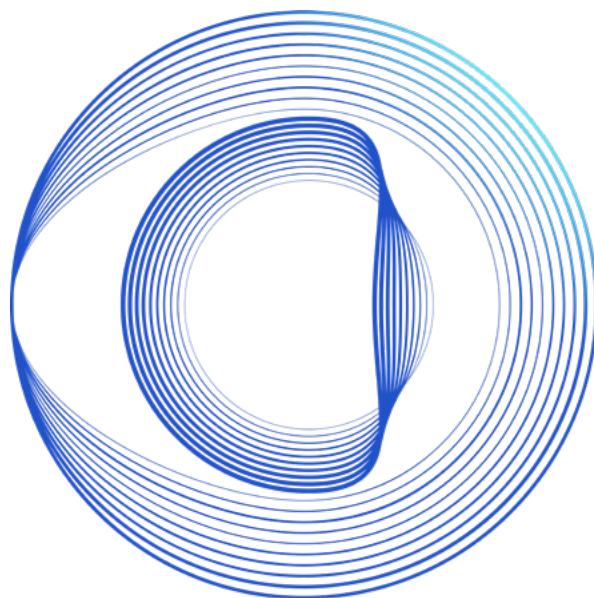
- **Enforces security policies in line with leading compliance frameworks:**
 - NIST: 800-53 (Rev. 4/5), 800-171 (Rev. 1/3), CSF v2.0, Privacy Framework, AI RMF
 - CIS Controls: Versions 7 and 8
 - PCI DSS: Versions 3.2 and 4.0
 - ISO/SAE 21434 (Automotive), IEC 62443 (Industrial)
 - GDPR: EU General Data Protection Regulation
 - CSA Cloud Controls Matrix (CCM v4)
- Streamlines audits with traceable controls and exportable threat model reports.
- Unifies risk management across IaC and cloud environments.

PLATFORM AND AI CAPABILITIES:

- **AI-Powered Guidance:** Automatically suggests fixes and best practices based on IaC context and cloud provider standards.
- **Threat Intelligence Integration:** Connects code analysis with ThreatModeler's extensive threat and security control libraries.
- **Real-time IDE Feedback:** Alerts developers as they type, eliminating the lag between coding and security checks.
- **SaaS Architecture:** Keeps security libraries up to date across all environments and teams.

Technical Specifications

- **Supported IDE:** Visual Studio Code (VS Code)
- **IaC Templates:** AWS CloudFormation (YAML/JSON), Terraform (AWS, Azure, GCP), ARM Templates
- **Security Feedback:** Real-time, contextual recommendations in IDE
- **Authentication:** Single Sign-On (SSO)
- **Platform Type:** SaaS-based, continuously updated



COMPLIANCE STANDARDS:

Category	Details
NIST	800-53 Rev. 4 & 5, 800-171 Rev. 1 & 3, CSF v2.0, Privacy Framework, AI RMF
PCI DSS	Versions 3.2 and 4.0
CIS Controls	Versions 7 and 8
ISO/ IEC Standards	ISO/SAE 21434 (Automotive) IEC 62443 (Industrial)
GDPR	EU General Data Protection Regulation
CSA CCM	Cloud Controls Matrix v4

ThreatModeler 7.3 is now available!

Contact us to get a demo.

