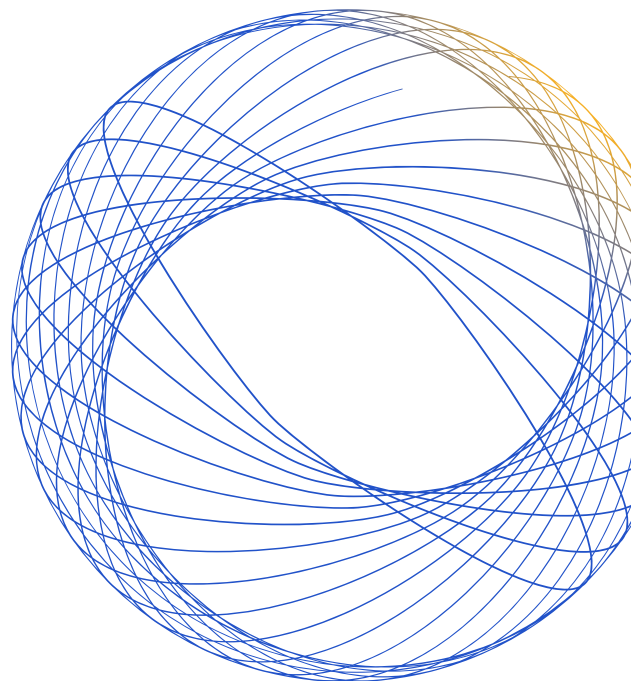


ThreatModeler Technical DATA SHEET



Model Faster. Work Smarter.

ThreatModeler streamlines every stage of the threat modeling process, helping you Visualize, Identify, Mitigate, and Document risks with greater speed, clarity, and confidence. Built to support applications, devices, and cloud infrastructure at enterprise scale, ThreatModeler enables security teams to embed secure-by-design practices across complex, hybrid environments.



Visualize

Accelerate model creation and increase visibility across attack surfaces.

ThreatModeler makes it easy to build models from scratch or reuse existing artifacts and templates, reducing time to value while increasing consistency.

CANVAS

Utilize the drag-and-drop interface with Smart Search and AI-powered component suggestions, enabling faster and more complete modeling.

AI-POWERED DIAGRAM IMPORT

Quickly turn architecture diagrams and cloud infrastructure files (Terraform, Visio, Draw.io, Miro, Microsoft TMT, JPEG, PNG) into actionable models with intelligent import.

TEMPLATES

Choose from 500+ pre-built models covering popular technologies and use cases, or build your own to standardize and accelerate adoption across teams.

NESTING

Utilize patented model chaining and nesting to embed models within other models, offering the ultimate in reuse and visibility.

CLOUD MODELING

Consistently model cloud architectures and hybrid deployments across AWS, Azure, and GCP environments.

INTELLIGENT CLOUD MAPPING¹

Automatically import, group, arrange, and link cloud components with detailed metadata, providing the advanced clarity needed to visualize risks across large-scale environments.

IAC INTEGRATION²

Use the IaC-Assist plugin in VS Code to generate threat models directly from code and track security requirements.

COLLABORATION & USABILITY

Use inline editing, group comments, custom colors, persistent filters, @mentions, and an enhanced Help & Support Center to improve alignment across security, DevOps, and compliance teams.

Identify

Prioritize the risks that matter most with clear, actionable insights.

ThreatModeler enables teams to understand attacker paths, apply trusted frameworks, and clearly identify requirements.

ATTACK PATH VISUALIZATION

Record and replay how an attacker could move through your architecture, with annotations for threats and countermeasures to demonstrate real-world attack scenarios.

STRIDE THREAT CATEGORIZATION

Categorize threats by STRIDE categories, simplifying adoption and driving consistency across teams.

THREAT LIBRARIES & FRAMEWORKS

Access continuously updated libraries and security requirements mapped to MITRE ATT&CK, OWASP Top 10, CAPEC, and D3FEND, providing you with the ultimate in flexibility and choice without the overhead.

RESIDUAL RISK INSIGHTS

Identify threats that remain after countermeasures are applied, enabling teams to prioritize gaps, allocate resources effectively, and minimize exposure.

SAVED VIEWS

Save and share customized filters, tags, and layouts to reduce triage time and allow each team to focus on what matters most.

Mitigate

Close security gaps earlier in the development lifecycle while moving at full speed.

ThreatModeler delivers intelligent recommendations, automated workflows, and integrations to help teams act quickly and consistently.

AI-POWERED RECOMMENDATIONS

Context-aware AI assistant that suggests component, connection, or configuration changes in real time.

WORKFLOW AUTOMATION

Programmable rules-based automation with triggers and context, including cloud-native metadata, workflows are applied consistently, and redundant tasks are eliminated.

GOVERNANCE CONTROLS

Enforce policies with scoped rules, multi-level approvals, and auto-versioning to support enterprise-scale consistency and audit traceability.

DEVSECOPS INTEGRATIONS

Bi-directionally sync security requirements with Jira, Azure Boards, and ServiceNow AVR. Create tickets in bulk, track progress in real time, and keep remediation flowing inside developer workflows.

ENTERPRISE SECURITY & ACCESS

Enforce enterprise-grade security with role-based permissions, SSO, and MFA to ensure scalable, compliant adoption across global teams.

Document & Report

Simplify reporting to any board or governing body.

ThreatModeler makes it easy to monitor and prove secure by design and framework compliance.

OPERATIONAL AND COMPLIANCE REPORTS

Generate built-in Audit, Developer, and Compliance reports, with automated coverage for 180+ frameworks (e.g. PCI DSS, NIST, ISO, OSFI, GDPR, HIPAA, FDA 524B) to reduce audit prep time and prove regulatory alignment. Create Custom Reports to tailor content by tag, threat, or category and deliver detailed insights to key stakeholders. (See technical specifications below.)

INTERACTIVE DASHBOARDS

Monitor risk posture and compliance in real time with built-in dashboards. Customize views by model status, tags, or categories to support team-specific workflows and streamline reviews.

CISO PROGRESS REPORT

Demonstrate security posture transformation with executive-level summaries that highlight mitigation progress, top 10 security requirements, and threat traceability.

Technical Specifications

Supported Formats and Sources

Image (JPG, PNG), Draw.io, Microsoft TMT, Visio, CloudFormation, Azure Resource Manager (including Resource Groups), MIRO, JSON, Terraform Plan (via IaC-Assist)

INTEGRATIONS

Jira, Azure Boards, Azure DevOps, ServiceNow (including AVR), Jenkins, Azure Pipelines, GitHub, GitLab, Bitbucket, BiZZdesign, ArmorCode, HashiCorp

AUTHENTICATION

- Local, SAML, Active Directory with SSO, Azure Service Principal (for ALM integrations)
- Multi-Factor Authentication (MFA) support for enhanced login security
- Keyless authentication for GCP integrations via Workload Identity Federation
- SSO login tracking and audit visibility for UI and API access

NOTIFICATION METHODS

- Email
- Web

COMPLIANCE STANDARDS

- NIST: 800-53 (rev5), 800-171 (rev3), CSF v2.0, Privacy Framework, AI RMF
- Security: CIS CSC (v8), PCI DSS (4.0), ISO/SAE 21434, IEC 62443-4-2
- Privacy: GDPR (EU), CSA CCM v4

COMPONENT LIBRARIES

AWS, Azure, GCP AI/ML, SAP, Kubernetes, Automobile, Medical Devices, Critical Infrastructure, ThreatModeler

MODELING FRAMEWORKS

STRIDE, VAST, OWASP Top 10, and custom frameworks

THREAT & SECURITY SOURCES

Organization	Threat Source	Security Requirement
MITRE	ATT&CK ATLAS CAPEC MITRE ATT&CK for Containers	ATT&CK Mitigations ATLAS Mitigations CAPEC D3FEND
OWASP	Top 10 (Web, API, vMobile, IoT, ML, LLM)	Cheat Sheet Series
Cloud Providers	–	AWS Documentation Azure Documentation GCP Documentation Kubernetes Documentation
CSA	Top 11 2024 (Azure and AWS only) Top 12 2018	–
Microsoft	Threat Matrix for Kubernetes	–
CWE	Where applicable	–
CIS	–	Yes
WP.29	Yes	Yes
Mobile	iOS Documentation Android Documentation	iOS Documentation Android Documentation

Discover how ThreatModeler can help your organization model faster, work smarter, and stay ahead of risk.

Schedule your personalized demo today.

¹Intelligent Cloud Mapping requires a CloudModeler license.

²IaC integration requires an IaC-Assist license.

