ThreatModeler

PLATFORM · TECHNICAL DATA SHEET

ThreatModeler® Nexus™

Technical Data Sheet

An agentic platform for secure design. A multi-agent system and a connected Secure Design Graph visualize, identify, mitigate, and document risk, with AI applied in deliberate, governed, and deterministic ways.

DATA SHEET

THE PLATFORM

Model Faster. Work Smarter.

The ThreatModeler Nexus platform streamlines every stage of threat modeling, helping teams visualize, identify, mitigate, and document risk with greater speed, clarity, and confidence. A multi-agent system and a connected Secure Design Graph work across all four stages, turning your architecture, code, and documentation into a living model you can query and defend. Built for applications, devices, and cloud at enterprise scale, the platform applies AI in deliberate, governed, and deterministic ways, preserving context, traceability, and reviewability as systems evolve.

01 · SEE THE ATTACK SURFACE

Visualize

Accelerate model creation and increase visibility across attack surfaces.
Build models from scratch or reuse existing artifacts and templates to increase consistency and reduce time to value. The System Mapping Agent reads your architectural artifacts, including diagrams, code, and documentation, and builds the model for you, creating missing components so you start from your real architecture instead of a blank canvas.

MODEL FROM YOUR TOOLS (MCP SERVER)

Through the MCP Server, connect AI assistants and IDEs to create threat models from source code, infrastructure-as-code, PRDs, and architecture documents, directly in the tools where teams already work.

DOCUMENT-DRIVEN MODELING

Generate threat models with AI assistance from existing design documentation containing text and images, building on prior architectural artifacts while preserving structure and reviewability.

BRING YOUR OWN AI (BYOAI)

Apply approved large language models, such as Azure OpenAI and Google Gemini, by selecting which models run for specific capabilities. AI operates within a governed, deterministic framework to produce explainable, auditable outcomes.

CANVAS

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

AI-POWERED DIAGRAM IMPORT

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

REAL-TIME PREDICTIVE INSIGHTS

Deliver continuous, context-aware insights as threat models evolve, highlighting gaps and areas requiring attention.

VOICE-ENABLED AI AGENT

Use voice commands to create models, ask questions, or get in-product guidance, with spoken answers to work faster and resolve issues hands-free.

TEMPLATES

Choose from 500+ prebuilt templates covering popular technologies and use cases, or build your own to standardize adoption across teams.

NESTING

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

CLOUD MODELING

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

INTELLIGENT CLOUD MAPPING [1]

Automatically import, group, arrange, and link cloud components with detailed metadata to visualize risk across large-scale environments.

COLLABORATION & USABILITY

Use inline editing, group comments, custom colors, persistent filters, and @mentions to improve alignment across security, DevOps, and compliance teams.

Identify

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

Understand attacker paths, apply trusted frameworks, and clearly identify requirements. The Graph Agent brings components, data flows, trust boundaries, threats, controls, and compliance into a single Secure Design Graph and keeps it current as your system changes, and you can add your own threats, requirements, and elements to tailor it to your environment.

STRIDE THREAT CATEGORIZATION

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

MODEL-LEVEL CUSTOM THREATS & REQUIREMENTS

Create custom threats and security requirements within your model, then promote them to the global library for broader visibility and control.

THREAT LIBRARIES & FRAMEWORKS

Access continuously updated libraries mapped to MITRE ATT&CK, OWASP Top 10, CAPEC, and D3FEND, for flexibility and choice without the overhead.

INTELLIGENT RISK INSIGHTS

Get AI-powered summaries that translate complex threats and requirements into clear priorities, showing what is most at risk and what to address first.

ADVANCED THREAT AND SECURITY REQUIREMENTS CONTEXT

Prioritize threats using CIA impact, ease of exploitation, Weakness/CWE-based mapping, CWE-to-threat traceability, trust ratings for trust zones and boundaries, and baseline/scope governance for security requirements.

ATTACK PATH VISUALIZATION

Record and replay how an attacker could move through your architecture, with annotations for threats and countermeasures.

RESIDUAL RISK INSIGHTS

Identify threats that remain after countermeasures are applied, so teams can prioritize gaps and minimize exposure.

CVSS 4.0 SUPPORT

Score threats using CVSS 4.0, the latest FIRST standard for vulnerability scoring, with clear version labels for comparison across models.

CUSTOM FIELDS & SAVED VIEWS

Apply user-defined metadata across components, threats, and models with grouped custom fields, conditional visibility, reusable data types, and granular access controls. Save shared filters and layouts to improve governance and reduce triage time.

Mitigate

Close security gaps earlier in the development lifecycle while moving at full speed.
Intelligent recommendations, automated workflows, and integrations help teams act quickly and consistently. Beyond security requirements, the Secure Design Graph and the System Mapping Agent produce specific, detailed mitigation guidance for each threat, with enough detail to hand to your developers, or their coding agents through the MCP Server, so fixes get implemented directly in code.

INVISIBLE SECURITY IN CI/CD (MCP SERVER)

Through the MCP Server, every pull request and architecture change is checked against the model automatically. Significant changes are analyzed, policy is enforced, and reviews are triggered without slowing developers down.

RISK-AWARE SECURITY CONTROLS

Define security controls to mitigate threats or implement requirements, then map them to the threats and requirements they protect and validate.

WORKFLOW AUTOMATION

Programmable, rules-based automation with triggers and context, including cloud-native metadata, applies workflows consistently and eliminates redundant tasks.

DEVSECOPS INTEGRATIONS

Sync security requirements bidirectionally with Jira, Azure Boards, and ServiceNow AVR. Connect multiple issue tracker profiles per integration, create tickets in bulk, and keep remediation flowing inside developer workflows.

CONTENT UPDATE PREVIEW & CONTROL

Review and approve updates to shared threat and security content before they reach existing models, preventing unintended downstream impact.

GOVERNANCE CONTROLS

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

ENTERPRISE SECURITY & ACCESS

Enforce enterprise-grade security with custom role-based, granular permissions, SSO, and MFA for scalable, compliant adoption across the global team.

CUSTOM STATUSES

Create custom statuses for threat models, threats, security requirements, and test cases to align workflows with governance processes and automate lifecycle transitions.

Document & Report

Simplify reporting to any board or governing body.

Monitor and prove secure-by-design and framework compliance. The Reporting Agent turns the Secure Design Graph into audit-ready findings, control recommendations, and compliance reports on demand, building reports that match the layouts and styles you already use.

PORTFOLIO INTELLIGENCE (MCP SERVER)

Through the MCP Server, query threat models, security requirements, and control gaps across your entire portfolio to see where controls deliver the greatest risk reduction and to guide security investment.

OPERATIONAL & COMPLIANCE REPORTS

Generate built-in Audit, Developer, and Compliance reports, with automated coverage for 180+ frameworks (PCI DSS, NIST, ISO, GDPR, HIPAA, FDA 524B) to reduce audit prep time. Create Custom Reports tailored by tag, threat, or category for stakeholders. (See technical specifications.)

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.

CISO PROGRESS REPORT

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

REPORTING AGENT

Generate stakeholder-ready reports from threat modeling data using reusable templates, natural language refinement, and multi-model reporting for consistent audit, compliance, and executive communications.

REFERENCE

Technical Specifications

SUPPORTED FORMATS & SOURCES

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

INTEGRATIONS

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

AGENTIC & AI

MCP Server for AI assistants, IDEs, and CI/CD (Claude Code, Cursor, VS Code with Copilot, Windsurf, GitHub Actions, GitLab CI, Azure DevOps); BYOAI with Azure OpenAI and Google Gemini; OAuth with role-based access

AUTHENTICATION

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

NOTIFICATION METHODS

- Email
- Web

COMPLIANCE STANDARDS

- NIST: 800-53 (rev5), 800-171 (rev3), CSF v2.0, Privacy Framework v1.0, 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, OCI Products and Platform, Automobile, Medical Devices, Critical Infrastructure, ThreatModeler

MODELING FRAMEWORKS

- STRIDE, MAESTRO, VAST, OWASP Top 10, and custom frameworks

REFERENCE

Threat & Security Sources

ORGANIZATION	THREAT SOURCE	SECURITY REQUIREMENT
MITRE	ATT&CK ATLAS CAPEC MITRE ATT&CK for Containers EMB3D	ATT&CK Mitigations ATLAS Mitigations CAPEC D3FEND
OWASP	Top 10 (Web, API, vMobile, IoT, ML, LLM) OWASP Agentic AI Threats and Mitigations (2025)	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

[1] Intelligent Cloud Mapping requires a CloudModeler license.

ThreatModeler

GET STARTED

Agentic threat modeling. Built-in confidence.

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

LEARN MORE

threatmodeler.ai/products/demo