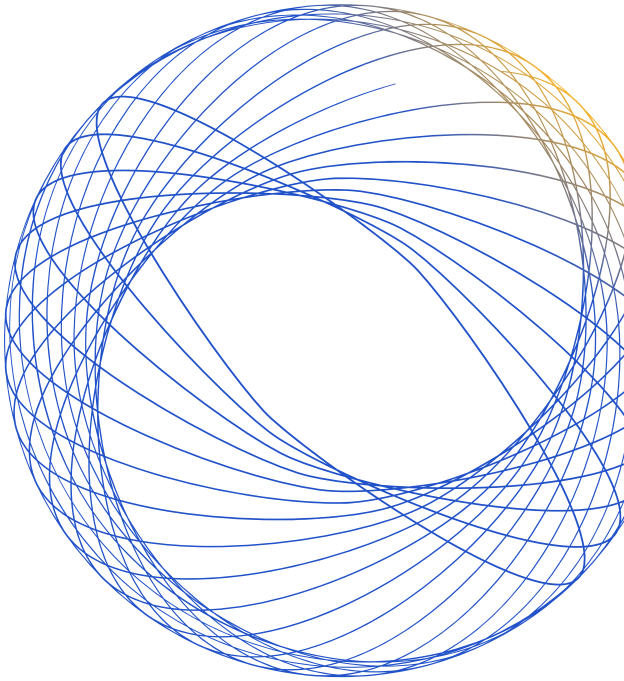
ThreatModeler®

CloudModeler Technical DATA SHEET

DATA SHEET

Overview

CloudModeler simplifies, standardizes, and accelerates threat modeling for cloud service architectures across Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). It delivers instant visibility, continuous coverage, and specific threat identification, enabling teams to increase cloud coverage while reducing effort to keep models up to date.



Key Features

AUTOMATED CLOUD MODELING

Accelerate secure design by automatically modeling cloud architectures to provide the foundation for threat analysis across AWS, Azure, and GCP.

- **Cloud Import:** Build models directly from AWS, Azure (including VNets and Resource Groups), and GCP to expedite architecture reviews.
- **IaC Import:** Import architectures from Terraform, CloudFormation, and Azure Resource Manager (ARM) templates to eliminate manual effort and maintain consistency.
- **Continuous Updates:** Automatically reflect infrastructure changes between live cloud environments, IaC, and their models, uncovering new threats and updating risk exposure.
- **Rules-Based Automation:** Automate actions based on cloud-specific triggers to reduce manual oversight and enforce consistency.
- **Application-Based Filtering for AWS Models:** Model complex cloud environments in AWS using application-based filters for a real-world representation of enterprise-scale infrastructure.

INTELLIGENT CLOUD MAPPING

Gain visibility into complex cloud environments with automated mapping that keeps models manageable and up to date.

- **Intelligent Grouping and Layout:** Automatically import, group, arrange, and link cloud components with detailed metadata to simplify risk management of complex environments.

- **Multi-Level Navigation:** Navigate large, complex models with link merging, path highlighting, and model nesting and chaining, enabling organizations to view entire architectures at scale while drilling into detailed components as needed.

CLOUD THREAT IDENTIFICATION & PRIORITIZATION

Focus on the highest-impact risks with actionable insights into cloud-specific threats.

- **Threat Libraries:** Identify risks using built-in libraries mapped to industry frameworks, including MITRE ATT&CK, OWASP Top 10, and CSA Cloud Top Threats, to provide broad coverage with cloud-specific insight.
- **Cloud-Aware Prioritization:** Prioritize remediation based on severity, impact, and affected cloud resources so teams can focus on the most critical risks.

Platform Capabilities

THREAT & RISK INSIGHTS

Strengthen analysis with curated threat libraries and continuous tracking to ensure models stay comprehensive and current.

- **STRIDE Threat Categorization:** Categorize threats by STRIDE categories, simplifying adoption and driving consistency across teams.
- **Model-Level Custom Threats and Security Requirements:** Create and add custom threats and security requirements within your model. Promote them to the global library for broader visibility and control.
- **Dynamic Tracking:** Continuously monitor threat status as mitigations are applied, ensuring risks always reflect the latest security control coverage.
- **Residual Risk Insights:** Evaluate residual risk to identify threats that remain after controls are applied, helping teams prioritize gaps and allocate resources effectively.
- **Auto-Versioning:** Automatically create new model versions when status changes occur, ensuring traceability.

COLLABORATION & REPORTING

Enable secure, cross-team collaboration with tailored access and reporting.

- **Real-Time Collaboration:** Collaborate in real time with multi-user editing and role-based permissions to enhance efficiency.
- **Operational and Compliance Reporting:** Generate targeted reports for CISOs, compliance, and technical teams to support faster decision-making.
- **Interactive Dashboards:** Monitor cloud risk posture and compliance in real time with interactive dashboards, customizable by model status, tags, and categories.

- **Saved Views:** Save and share customized filters, tags, and layouts to reduce triage time and allow each team to focus on what matters most.
- **Enterprise Access Controls:** Enforce role-based access, single sign-on (SSO), and multi-factor authentication (MFA) for secure, scalable adoption.
- **Governance Controls:** Enforce enterprise policies with scoped rules, multi-level approvals, and auto-versioning to maintain consistency and audit readiness.

ALM & CI/CD INTEGRATIONS

Connect seamlessly into enterprise workflows to keep security in sync with delivery.

- **ALM Integration:** Sync tickets with Jira, Azure Boards, and ServiceNow to centralize remediation tracking.
- **Pipeline Integration:** Seamlessly integrate with GitHub, GitLab, Bitbucket, and Azure DevOps to embed security directly into your pipelines.
- **Remediation Alignment:** Align remediation tasks with ALM and CI/CD workflows to minimize friction between security and development teams.

ATTACK PATH VISUALIZATION

Visualize how attackers could move through architectures with replayable scenarios that demonstrate real-world risks.

- **Replayable Scenarios:** Record and replay potential attack paths with annotations for threats and countermeasures to validate mitigations.
- **Stakeholder Communication:** Present attack paths in a clear, step-by-step view to improve understanding and support decision-making.

AI-POWERED ASSISTANCE

Work smarter with intelligent guidance embedded into every model.

- **Intelligent Risk Insights:** Get AI-powered summaries that translate complex threats and security requirements into clear priorities, showing what's most at risk and what to address first.
- **Diagram Suggestions:** Receive contextual diagram suggestions for grouping, trust boundaries, and protocols to expedite the design process.
- **Voice-Enabled AI Assistant:** Use voice commands to create models, ask questions, or get in-product guidance. The AI Assistant lets you describe architectures aloud and provides spoken answers to help you work faster and resolve issues hands-free.
- **Attack Path Analysis:** Use AI to analyze attacker paths and optimize placement of security controls by understanding downstream impact.
- **AI-Powered Recommendations:** Act on context-aware guidance that suggests component, connection, or configuration changes in real time.

Technical Specifications

SUPPORTED FORMATS:

- Terraform
- AWS CloudFormation
- Azure Resource Management

CLOUD PLATFORMS

- AWS
- Microsoft Azure
- Google Cloud Platform

REPOSITORY PLATFORMS:

- GitHub
- GitLab
- Bitbucket

NOTIFICATION METHODS:

- Email
- Web Notifications

AUTHENTICATION METHODS:

- AWS: IAM User, IAM Role, Organizations
- Azure: Tenant, Subscription, Client & Secret
- GCP: JSON file or keyless (Workload Identity Federation)

ALM PLATFORMS:

- Jira: Seamless ticket creation and tracking
- Azure Boards: Direct integration with Microsoft's development planning tools
- ServiceNow: Enterprise service management connection

CLOUD COMPONENT LIBRARY:

- AWS
- Google Cloud
- Microsoft Azure
- AI/ML
- Kubernetes
- SAP
- Automobile
- Medical Devices
- Critical Infrastructure
- ThreatModeler
- Other cloud-specific libraries

COMPLIANCE FRAMEWORKS:

- CIS CSC v8 (IG1, IG2, IG3)
- PCI DSS v4.0
- EMEA EU GDPR
- US HIPAA
- IEC 62443-4-2
- ISO 42001 v2023
- NIST 800-53 rev5
- NIST 800-171 rev3
- NIST AI RMF AI 100-1
- NIST CSF v2.0
- NIST Privacy Framework 1.0
- ISO/SAE 21434 v2021
- CSA CCM v4

THREAT INTELLIGENCE SOURCES

Organization	Threat Source	Security Requirement
MITRE	ATT&CK ATLAS CAPEC	ATT&CK Mitigations ATLAS Mitigations CAPEC D3FEND
OWASP	Top 10 (Web, API, Mobile, 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