

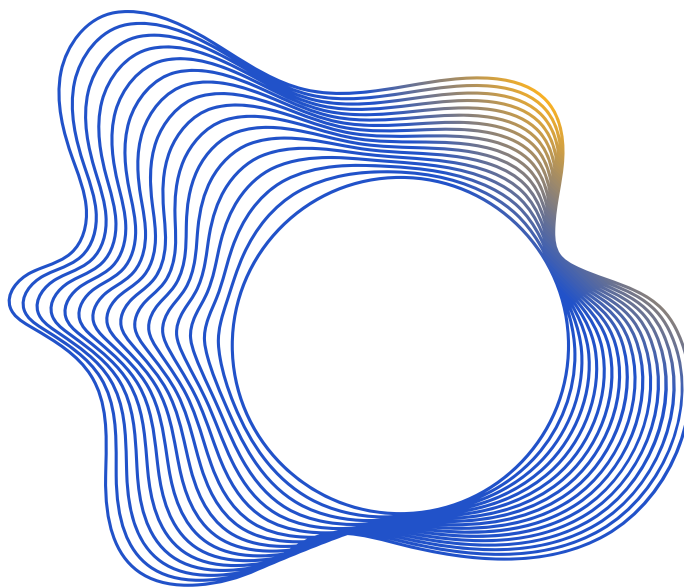


CloudModeler™

**Streamline and Automate Cloud Security
with Comprehensive Threat Modeling**

Overview

CloudModeler is specifically designed to secure and manage dynamic cloud environments that are in a constant state of evolution. We developed CloudModeler to provide continuous monitoring, enabling organizations to mitigate potential threats tailored to their specific cloud infrastructure.



Key Features

CloudModeler delivers a comprehensive suite of capabilities designed to simplify cloud security at scale. By combining instant infrastructure modeling, continuous drift detection, robust governance workflows, and actionable reporting, CloudModeler provides security teams with unparalleled visibility and control across multi-cloud environments. These features work together to enable proactive threat mitigation while adapting to the rapid pace of cloud evolution.

Import instantly and track drift continuously

KEY FEATURES:

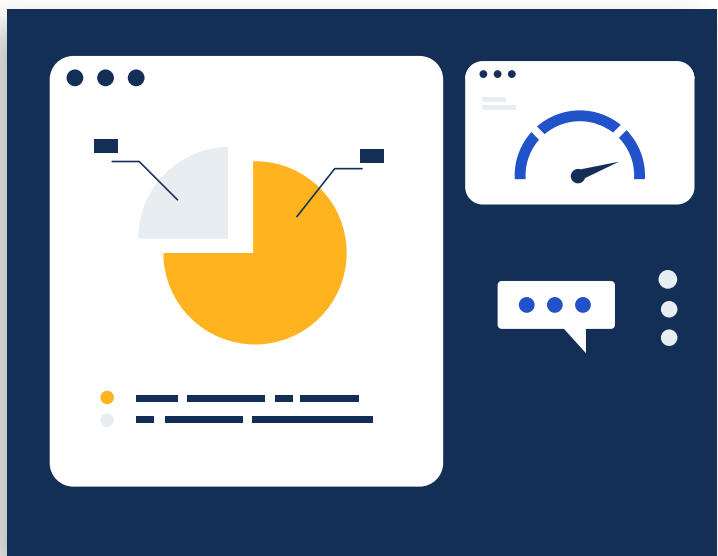
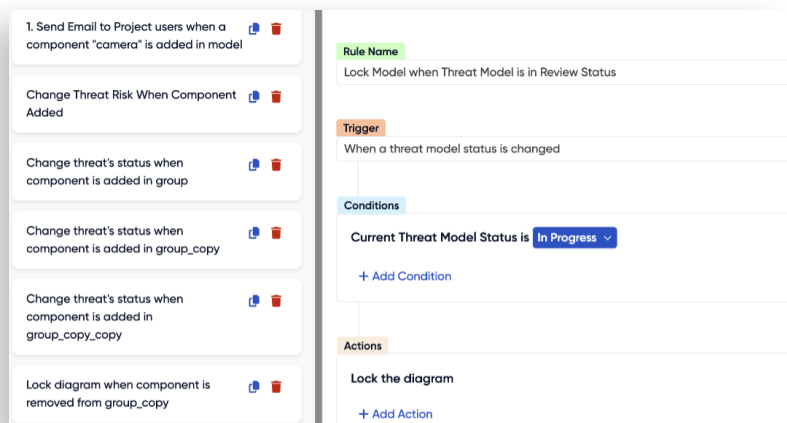
- **Visually identify and synchronize** changes between the model and the actual environment.
- **Automatically calculate risks** from infrastructure changes.
- **Connect** to Azure VNets and Resource Management Templates, AWS and Google VPCs, and Terraform Plan files.



Simplify governance and workflows

KEY FEATURES:

- **Automate governance** and compliance with a rules-based workflow automation engine.
- **Seamlessly manage** complex approval processes with support for up to five levels.
- **Simplify change management** with version control and side-by-side comparisons.



Improve Visibility

KEY FEATURES:

- **Breeze through audits** and compliance documentation with detailed reports.
- **Improve stakeholder visibility** with role-based dashboards.

Platform Benefits

CloudModeler delivers a comprehensive suite of capabilities designed to simplify cloud security at scale. By combining instant infrastructure modeling, continuous drift detection, robust governance workflows, and actionable reporting, CloudModeler provides security teams with unparalleled visibility and control across multi-cloud environments. These features work together to enable proactive threat mitigation while adapting to the rapid pace of cloud evolution.

Extensible Threat Framework

KEY BENEFITS:

- Access the latest cloud threat intelligence with a comprehensive, curated library.
- Ensure consistency with policy-based security control aligned with your organizational policies.
- Automatically change threat status to 'mitigated' when all security requirements have been fulfilled.

Flexible Authentication & Authorization

KEY BENEFITS:

- Manage logins via cloud authentication methods across AWS, Azure, and Google Cloud.
- Configure role-based access control (RBAC) with granular permissions management tied into SSO capabilities.

Enterprise Tools Integration

KEY BENEFITS:

- Integrate security throughout development with native ALM integrations to transform mitigations into trackable tickets while providing real-time compliance dashboards for stakeholders.
- Connect cloud security directly into GitHub Actions, GitLab and Bitbucket Pipelines to automatically generate threat models for your Infrastructure as Code (IaC) files as they're created.
- Instantly update security requirements in your connected threat model as IaC changes are made.

AI Assistance with ThreatModeler Copilot

KEY BENEFITS:

- Diagram Assistance provides recommendations for parent groups, and component configurations based on thousands of models and organizational patterns
- Raise and monitor service tickets directly from the ThreatModeler platform, streamlining communication between development and security teams.
- Access recommendations for optimal trust boundary settings, logical component groupings, connection protocols, and security control placements using Attacker Path Analysis.
- Speed up model creation with context-aware predictive recommendations for additional components based on analysis of your existing models.

Technical Specifications

SUPPORTED FORMATS:

- Terraform
- AWS CloudFormation
- Azure Resource Management

REPOSITORY PLATFORMS:

- GitHub
- GitLab
- Bitbucket

NOTIFICATION METHODS:

- Email
- Web Notifications

AUTHENTICATION METHODS:

- AWS - IAM User, IAM Role, Organizations
- Azure - Tenant, Subscription, Client & Secret
- Google Cloud - JSON file upload

ALM PLATFORMS:

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

CLOUD COMPONENT LIBRARY:

- AWS
- Microsoft Azure
- Critical Infrastructure
- Google Cloud
- Kubernetes
- AI/ML
- Oracle
- SAP

COMPLIANCE FRAMEWORKS:

- CIS CSC v7-8
- NIST 800-53
- ISO/SAE 21434
- PCI DSS v3.2, 4.0
- NIST 800-171
- CSA CCM v4
- EU GDPR
- NIST AI RMF AI 100-1
- IEC 62443-4-2
- NIST CSF v2.0
- NIST Privacy Framework

THREAT INTELLIGENCE SOURCES

Organization	Threat Source	Security Requirement
MITRE	ATT&CK ATLAS EMB3D CAPEC	ATT&CK Mitigations ATLAS Mitigations EMB3D Mitigations CAPEC D3FEND
OWASP	Top 10 variants for Web, API, Mobile, IoT, ML, LLM	Cheat Sheet Series
Cloud Providers	--	AWS, Azure, Google Cloud, and Kubernetes documentation
CSA	Top 11 2024 (AWS only) Top 12 2018	--
Microsoft	Threat Matrix for Kubernetes	--
CWE	Where applicable	--
CIS	--	Yes
WP.29	Yes	Yes
Mobile	iOS & Android Documentation	iOS & Android Documentation

ThreatModeler 7.3 is now available!

Contact us to get a demo.

