ThreatModeler
Security starts here

An Automated Platform to Design, Build and Manage Security in Your Technology Development Life Cycle

TECHNICAL DATA SHEET

Licensing Model Annual subscription; limited or unlimited threat modeling licenses

Product Tiers AppSec Edition, Cloud Edition (includes AppSec)

Deployment Options Managed single tenant instances (SaaS), On-Premises, AWS Marketplace (Shared Instance)

Single Sign On (SSO) Local Standalone Authentication, SAMLv2, LDAP/ Active Directory

Threat Modeling Approach

One easy step. ThreatModeler does the rest.

Process Flow Diagram	Easy drag-and-drop functionality to identify all architectural components, including but not limited to trust boundaries, communication protocols, data elements, threat actors, attributes, etc.
Resource Relationships	Customizable rules engine to enable any user to build complete and consistent process flow diagrams.
Nesting	Reuse existing threat models as architectural components in other threat model diagrams to avoid duplicity within the threat modeling process.
Security Controls	Identify compensating controls to mitigate threats automatically.
Templates and Patterns	Define and use pre-approved architectures to speed up the threat modeling build process.
Accelerator	Integrate with cloud service providers and automatically build threat modeling programs using your cloud configuration.

Content Libraries

Regulatory and Compliance	NIST 800-53 REV.4 CIS CSC V7 PCI DSS V.3.2	EMEA EU GDPR CSA CCM V.3.2
Threats/ Security Requirements	MITRE CAPEC OWASP (Mobile, IoT, AppSec) NVD WASC CSA Treacherous 12	AWS Security Best Practices Azure Security Best Practices GCP Security Best Practices
Component Library	All AWS Services All Azure Services All GCP Services Application-Based Components	On-Premise Infrastructure Components ICS Components IoT Components

Reports and Dashboards

Slice and Dice Output. Export as a PDF or xlsx.

Executive Report	High level overview of the threat model.
Developer Report	Details of threats as actionable outputs for developers.
Policy Compliance Report	Details and statuses of security requirements, standards.
CIS Report	Review compliance against CIS benchmarks.
Custom Report	Leverage filters to create your own report outputs.
Enterprise Dashboard	Interactive dashboard that provides a high-level overview of your entire attack surface.

Integrations

Project Management Tools	Jira Cloud & Server, Azure Boards
CI/CD Tools	Jenkins, Azure Pipelines
Cloud Integrations	AWS, AWS S3, AWS Security Hub, Azure Portal

Open Architecture

ThreatModeler also provides comprehensive, bi-directional web services APIs to integrate with your toolchain.

Import

ThreatModeler supports Visio (.vsdx), LucidChart (.vdx) and Microsoft TMT files to import diagrams.
ThreatModeler will automatically import the architectural view of your workloads on AWS or Azure.

Export

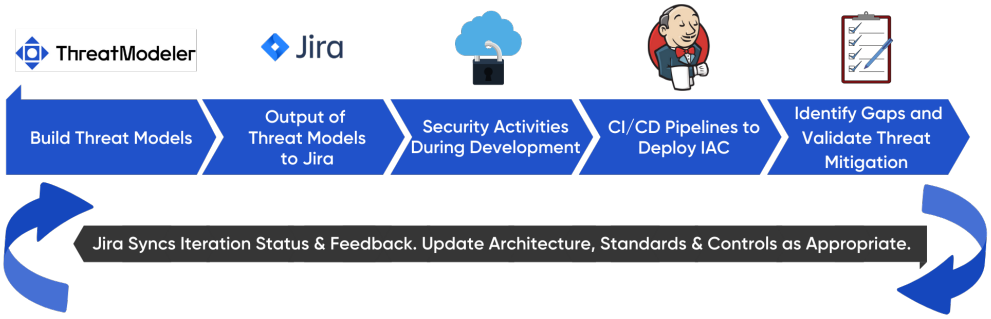
All diagrams can be exported as a JSON, PDF or .png file.

Technology Delivery Teams Can Think Like a Hacker by Instantly Understanding Their Attack Vectors

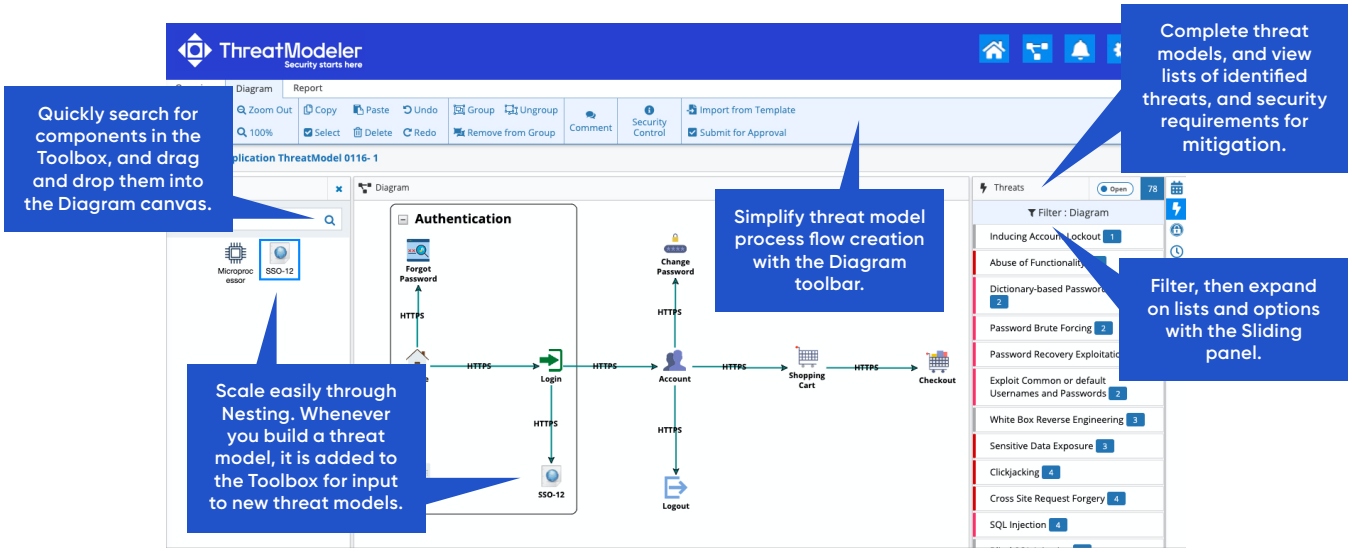
ThreatModeler enables technology development teams to prioritize threats that need to be mitigated. Even with little to no technical skills, create a threat model in less than an hour. Freed from sifting through mountains of security and compliance requirements, security teams can focus on managing product life cycles, accelerating productivity.

With autonomy, generate a threat model, assign security threats for mitigation, and establish approval touchpoints with stakeholders for security validation and sign-off. ThreatModeler eliminates the need to stitch together ad hoc processes and start from scratch each time product is deployed and/or changes are made, threat modeling becomes a sustainable part of the development process that adapts and grows with your infrastructure. Without the need to engage them, security SMEs can focus on overseeing implementations. ThreatModeler integrates with established IT issue tracking tools to ensure security requirements are pushed, synced and corrected by the mitigating party.

Streamline Security Activities Across Teams With Bidirectional Data Flow



Threat Models Are Created Visually in the Diagram Screen



ThreatModeler Automation

ThreatModeler empowers Agile teams to have security "baked in" early during the planning and design stages, instead of "latching it on" towards the end. Integrate with leading project management, CI/CD toolchain and cloud automation to implement security throughout DevSecOps life cycles. ThreatModeler features cloud automation through integrations with AWS and Azure. With its open API, any ThreatModeler feature can be automated beyond native functionality. ThreatModeler's issue tracking integration with Jira informs DevSecOps teams of whether an application is launch ready or should be blocked from deployment to production.

Ensure Compliance Policy Requirements Are Met

Provide a complete audit trail demonstrating adherence to internal and external regulatory policy in all risk management activities, demonstrating that all applications comply with security standards. Armed with a full view of the security and compliance posture, key stakeholders can make data driven business decisions more quickly, empowering them to ultimately scale the organization for growth.