ThreatModeler®

Whitepaper

2025 Threat Modeling BUYER'S GUIDE

Questions to ask before buying or renewing a threat modeling solution.

Introduction

The Growing Security Challenge

In today's rapidly evolving digital landscape, security threats are becoming increasingly sophisticated and pervasive. Organizations face the uphill battle of safeguarding every asset while defending against every potential threat—all as application portfolios continue to grow and expand. The statistics highlight a troubling reality: 92% of businesses experienced breaches due to vulnerabilities in their own in-house applications in the past year alone[1], while over 40,000 new common vulnerabilities and exposures (CVEs) were reported in 2024[2].

The Innovation vs. Security Dilemma

Despite substantial investments in security tools and frameworks, many organizations continue to prioritize rapid innovation over security, with 90% of technologists favoring speed over security measures[3]. This downstream approach—where security becomes an afterthought addressed near production—may appear to accelerate development cycles but frequently results in costly rollbacks, extensive rework, and worse, overlooked vulnerabilities that make it into production.

Threat Modeling: Secure by Design

Threat modeling reconciles the competing demands of speed and security. By systematically incorporating security into the software development lifecycle (SDLC), it enables organizations to identify vulnerabilities and design appropriate countermeasures before writing a single line of code. This proactive approach eliminates costly late-stage fixes and security patches while building institutional security knowledge.

About This Guide

This guide is designed to help you evaluate and select a modern threat modeling solution that transforms threat modeling from a theoretical exercise into a sustainable, continuous practice that enhances security without impeding innovation. We'll explore five key evaluation criteria, essential questions to ask vendors, and explain why ThreatModeler stands as the optimal choice for organizations serious about application security.

1. Enterprise Readiness and Scalability

Security teams face an impossible challenge: securing thousands of applications with limited resources and expertise. True enterprise readiness isn't just about supporting a few models—it requires handling thousands of threat models, hundreds of users, and seamless SDLC integration.

Without this scalability, organizations make dangerous compromises, limiting threat modeling to only "crown jewel" applications while leaving the majority of their infrastructure exposed to unidentified risks. This widening coverage gap represents one of the most serious yet overlooked vulnerabilities in modern enterprises, creating an urgent need for solutions that can scale threat modeling across the entire application portfolio.

Key Questions to Ask

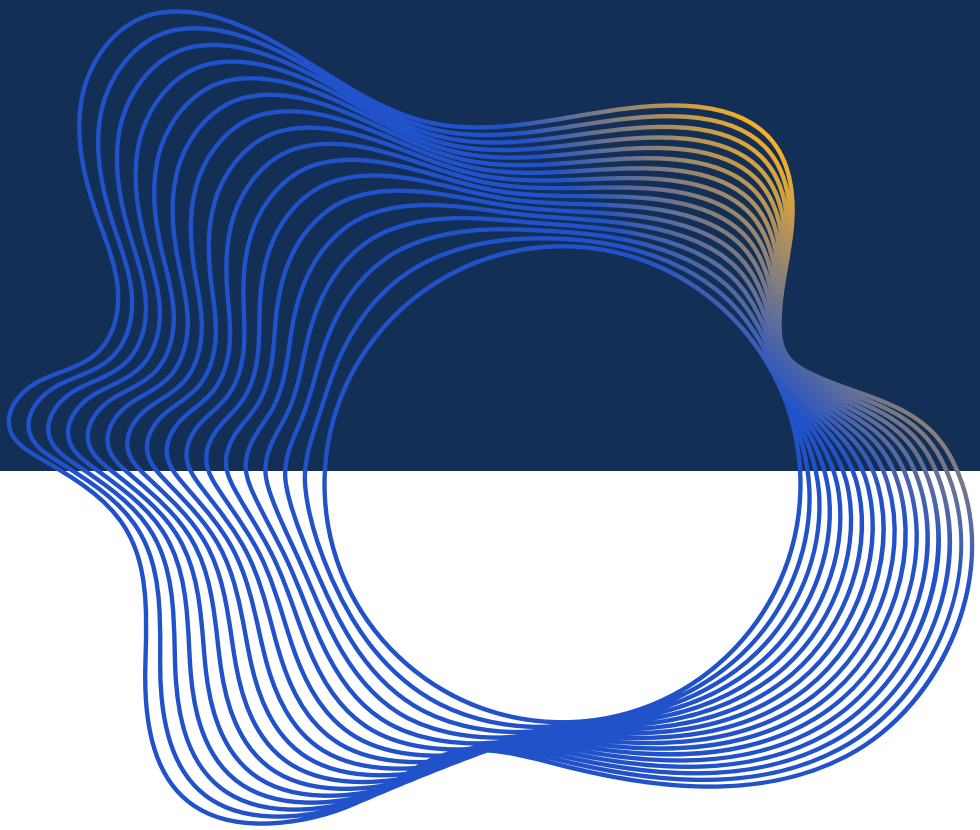
- How many concurrent users and models can the platform support?
- How does the solution handle role-based access control (RBAC) across large organizations?
- Can existing diagrams and documentation be imported without starting from scratch?
- How does the solution stay current with the latest vulnerabilities and threats?
- Can the solution scale across cloud environments, on-premises systems, and IoT applications?

How ThreatModeler Scales Security for Enterprises

ThreatModeler has been stress-tested in the most secure enterprise environments for over 14 years, serving the largest banks, automotive companies, healthcare providers, and critical infrastructure and manufacturers.

- **Continuous threat models** and concurrent users for comprehensive coverage across your entire application and infrastructure portfolio to foster widespread adoption.
- **Fine-tuned RBAC** that balances security with usability, enabling proper governance while empowering teams to work efficiently.

- **Patented import capabilities** for diagrams, whiteboard images, and more, leveraging previous work and institutional knowledge to dramatically reduce the time and resources needed to model existing systems.
- **Integration with the National Vulnerability Database** keeps your threat models current with emerging threats and vulnerabilities across 300,000+ technologies, continuously ensuring your security posture remains relevant against evolving attack vectors.
- **Governance and workflow automation** enables your organization to tailor and automate threat modeling to your specific industry challenges and compliance needs, increasing relevance, effectiveness, and efficiency.
- **Industry-specific threat intelligence** with specialized coverage for sectors including Banking, Financial Services and Insurance, Medical Devices, Healthcare, Automotive, AI/ML, and Technology.



Drawbacks of Conventional Solutions

Conventional threat modeling approaches traditionally fail to drive widespread adoption and demonstrate measurable effectiveness across enterprise application portfolios.

Upstarts offer basic enterprise software features but cannot support enterprise threat modeling programs - leading to a high failure rate and long adoption time.

Point Products are built to address individual parts of a holistic threat modeling program, create gaps and siloes.

Free and Open Source Tools are designed for single use, and lack integrations and cross-team collaborative capabilities.

2. Ease of Use and Collaboration

Security tools that create friction in the development process are often bypassed or underutilized. Complex interfaces, steep learning curves, and tools that function in isolation prevent widespread adoption across different teams and roles, creating security silos rather than a unified approach.

Key Questions to Ask

- Can multiple users collaborate on the same threat model simultaneously?
- How intuitive is the interface for both security and non-security specialists?
- Does the solution provide optimized views and outputs tailored to different stakeholders?
- How quickly can a threat model be created?

How ThreatModeler Increases Collaboration and Efficiency

- **Real-time, multi-user collaboration** enables architects, developers, and stakeholders to work on diagrams simultaneously, breaking down silos and ensuring shared understanding of risk.
- **Role-oriented products, dashboards, and outputs** deliver efficient collaboration across teams.
  - Executives get immediate insights through customized dashboards
  - GRC teams access compliance mapping across 165+ regulatory standards
  - Developers receive integrated outputs in their IDEs and ALM tools
  - Security, cloud, and enterprise architects can import existing artifacts, enforce standard templates, and leverage an intuitive drag-and-drop interface with AI recommendations.
- **AI-powered Copilot** for natural language modeling dramatically reduces the time and expertise required to create accurate threat models, increasing efficiency and scale using exsisting resources.
- **Rapid visualization** enables automatic visualization of complex environments in minutes, eliminating manual diagramming and ensuring accuracy of hybrid and cloud-native architectures to consistently meet compliance standards and policy requirements.

3. Process Automation and Integration

Security processes that exist outside the development workflow create friction and are often bypassed. Manual threat modeling becomes a bottleneck that slows down development, leading teams to skip or abbreviate security assessments to meet deadlines.

Key Questions to Ask

- How does the solution integrate with existing development tools and CI/CD pipelines?
- Can threat modeling be automated within existing workflows?
- How are security requirements delivered to development teams?
- Can the solution integrate with cloud environments for continuous threat modeling?
- Does the solution provide flexibility around how you manage and provision infrastructure, including Infrastructure as Code (IaC)?

How ThreatModeler Simplifies Your Workflows and Processes

ThreatModeler delivers comprehensive automation and integration that transforms threat modeling from a blocking task to a continuous, seamless process.

- **Patented import capabilities** convert diagrams, whiteboards, and images into threat models, preserving work and reducing context switching to make secure development effortless.
- **Trackable security requirements** integrated with issue tracking turn security findings into actionable tasks for development teams, seamlessly linking with tools like Jira for trackable remediation.
- **Continuous cloud connections** to AWS, Azure, and GCP automate current-state visualizations, providing real-time visibility, detecting configuration drift, and ensuring security during cloud migration and expansion.
- **Continuous IaC connections** with bi-directional threat model support brings cloud security insights into Visual Studio Code, identifying misconfigurations pre-deployment to shift security left and cut remediation costs.
- **Pipeline and repository integration** automates security data ingestion across development stages without manual mapping, ensuring continuous threat intelligence and centralized policy enforcement throughout the SDLC.
- **Centralized policy enforcement** ensures adherence to GRC policies including architectrual governance.

4. Innovation and Threat Intelligence

Traditional threat modeling solutions require significant manual effort to analyze threats across complex systems. This brute-force approach strains resources and often fails to address the unique challenges of modern architectures and cloud environments.

Key Questions to Ask

- How does the platform identify and prioritize threats?
- Does the solution recommend appropriate security controls and assess their efectiveness?
- Can you easily tailor the threat library and intelligence to match your business needs?
- Can the solution analyze attack vectors in addition to traditional data flows?
- Is AI bolted on, or embedded into the core platform?

How ThreatModeler Innovations Help Enterprises Manage Risk

ThreatModeler was designed to simplify creation of models, while simultaneously improving their effictiveness. With a strong patent library, and a history of industry firsts including generative AI-assisted modeling, artifact imports, and attacker path analysis, you get faster model builds with deeper insights into potential attacks and vulnerabilities while reducing noise and false positives.

- **Patented intelligent path analysis** identifies the ideal locations for security controls within your architecture, maximizing protection while minimizing redundancy and performance impacts.
- **Control efficacy analysis** evaluates how effectively security controls mitigate specific threats, enabling investment in specific controls that deliver the greatest security benefit and supporting zero-trust architecture design.
- **Extensive, customizable threat libraries** adapt to your organization's unique risk profile and technology stack, ensuring relevant threats are identified without overwhelming teams with false positives.
- **AI-powered recommendations** leverage machine learning to identify patterns and recommend appropriate mitigations based on historical usage patterns, augmenting human expertise with data-driven insights.

5. Governance and Compliance

Organizations face increasingly stringent regulatory requirements across industries, from financial services to healthcare to critical infrastructure. Manual compliance mapping is time-consuming and error-prone, while proving compliance to auditors requires comprehensive documentation.

Key Questions to Ask

- What regulatory frameworks does the solution support?
- How does the solution map threats and controls to compliance requirements?
- Can the solution generate compliance reports?
- How are compliance requirements integrated into the development process?
- Can the solution adapt to emerging regulations?

How ThreatModeler Speeds Up Compliance and Reporting

ThreatModeler brings GRC, Product Delivery, and IT Security into a unified workflow to simplify and ensure consistent compliance to security regulations and frameworks.

- **Support for 180+ regulatory standards** eliminates the need to manually map security controls to compliance requirements, saving significant time and reducing the risk of compliance gaps across frameworks including NIST, ISO 27001, GDPR, PCI, and more.
- **Built-in components and workflow automation** ensures consistent application of security requirements and policies from one model to the next, creating a standardized approach to compliance that scales across the organization.
- **One-click compliance report generation** produces audit-ready documentation that demonstrates your security measures to regulators and auditors, streamlining the compliance verification process.
- **Specialized industry regulation support** including UNR155/TARA for automotive, DORA for financial services, and FDA 524B for medical devices, ensuring coverage for your specific compliance needs.
- Continuous updates to compliance frameworks keep pace with evolving regulations, eliminating resource-intensive manual research and updates.

The ThreatModeler Advantage

Secure by Design

Today's organizations need threat modeling that provides better outcomes, faster, and scales across their entire application portfolio without creating bottlenecks or slowing innovation. ThreatModeler delivers this through enterprise-grade scalability, seamless integration into existing workflows, and an innovative approach that incorporates the attacker perspective into your modeling process for advanced threat identification.

What sets ThreatModeler apart is its ability to transform threat modeling from a theoretical exercise into a continuous practice that strengthens enterprise security. The platform's intelligent analysis reduces noise and false positives, while comprehensive policy enforcement and one-click compliance reporting across 180+ standards simplifies governance. By shifting security left, ThreatModeler helps teams identify and remediate threats, **avoiding breaches, rewrites, fines, and reputational damage.**

The results are compelling: 10x faster time-to-market, 80% cost reduction in security assessments, and 90% more efficient security reviews.

By choosing ThreatModeler, organizations can confidently embrace secure-by-design principles while maintaining the pace of innovation—building better, more secure applications from core to cloud to edge.

Experience ThreatModeler in Action

Ready to transform your organization's approach to application and infrastructure security?

Schedule your personalized demo today.

threatmodeler.com/demo

sales@threatmodeler.com

+1 201.266.0510

1.Checkmarx, "Future of Application Security Report 2024," January 2024, https://info.checkmarx.com/future-of-application-security-2024 2.CVE Details, "Browse All Vulnerabilities by Date," accessed March 2025, https://www.cvedetails.com/browse-by-date.php 3.AppDynamics, "Application Security Report," June 2023, https://www.appdynamics.com/c/dam/r/appdynamics/2023/06-resources/08-ebook/AppDynamics_Application_Security_Report-1.pdf