ThreatModeler®

Whitepaper

Intelligent Threat Modeling: A New Era of Secure by Design

Executive Summary

Automated threat modeling made it possible for businesses to adopt secure-by-design practices while keeping pace with agile development methodologies.

For years, this has enabled businesses to implement threat modeling at scale, even as applications and environments have grown increasingly complex. However, with AI and cloud Technologies bringing faster development and additional threats, automated threat modeling can no longer keep pace. Complicating matters are new compliance frameworks such as PCI DSS 4.0 and DORA.

From building products to securing them, it's clear that automation alone is not enough for today's fast release cycles and low risk tolerance. **Intelligent Threat Modeling** represents the next stage in secure by design: a smarter, adaptive foundation that matches speed, scale, and security. By combining automation with contextual awareness, guided insights, and continuous visibility, Intelligent Threat Modeling removes the impossible choice of rapid delivery or risk reduction, giving businesses both.

The result is a new standard for secure by design, built on five requirements:

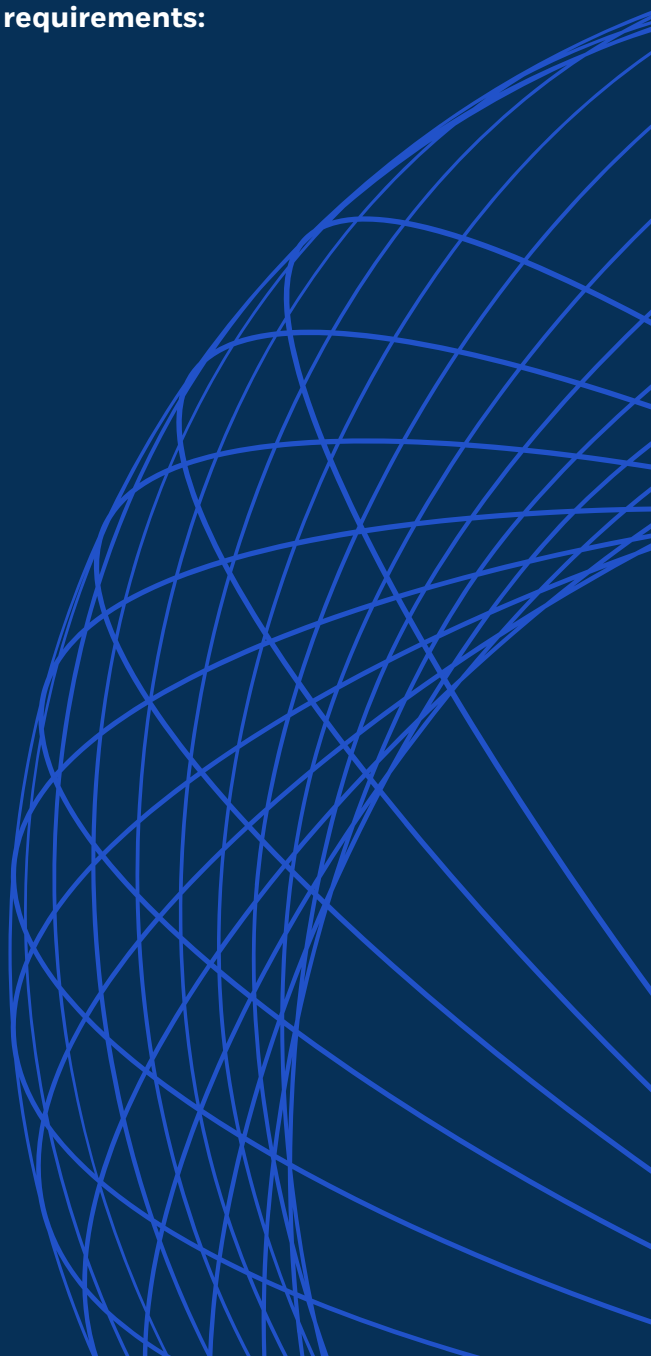
1. **Single Platform Intelligence Layer**
   Unify intelligence across applications, cloud, infrastructure, and devices.

2. **Guided Security Insights**
   Turn raw threat data into actionable recommendations that strengthen designs.

3. **Intelligent Automation**
   Transform artifacts into working models in minutes and keep them aligned as systems evolve.

4. **Continuous Risk Awareness**
   Maintain constant visibility into systems to monitor residual and emerging risks and reduce blind spots.

5. **360° Risk Visibility**
   See how risks connect across systems and clouds for enterprise-wide resilience.



Together, these five requirements represent Intelligent Threat Modeling and provide enterprises with a solution to keep pace with AI and cloud, while achieving secure by design at scale.

Cloud and AI Headwinds

As Enterprises adopt Cloud and AI to accelerate product releases, they are also facing significant challenges in securing these systems, as development velocity outpaces traditional threat modeling practices.

AI Development Velocity

Generative AI enables “vibe coding”, the rapid creation of code, prototypes, and MVPs in hours. These outputs often bypass structured design reviews, creating unmodeled and unmonitored attack surfaces.

Emerging Standards

Regulatory frameworks such as PCI DSS 4.0, OSFI B-13, MAS TRM, and DORA emphasize proactive risk management and design-time security. Meeting these requirements with outdated approaches incurs additional costs and delays.

Inverted Relationship Between Risk Tolerance and Velocity

Leaders recognize the need for speed to market, but cannot afford to ignore security and compliance. Slowing down is not an option, but neither is higher risk tolerance.

Cloud Drift Velocity

Modern architectures are in constant flux. Infrastructure-as-code (IaC) drives frequent changes, while hybrid and multi-cloud environments shift too quickly for static models to remain accurate.

Incomplete Coverage

Survey data shows 75% of enterprises lack confidence in their cloud threat modeling. Only 26% report full coverage, while 43% plan to expand cloud modeling within the next year. The top obstacles include frequent infrastructure changes (51%), integration challenges (43%), and limited time and resources (38%).

Meeting these challenges requires more than automation alone can provide, setting the stage for the next evolution of threat modeling.

From Automation to Intelligence: A New Foundation

Traditional threat modeling provided the baseline for security by design, and automation made it scalable for agile teams and more complex systems.

But the innovations in modern development practices have created a significant gap between how applications are built, and how they are threat modeled. Cloud architectures evolve daily, IaC introduces constant drift, and AI accelerates development cycles, producing code and prototypes faster than traditional design-time modeling can keep up. Compliance mandates add further pressure by requiring provable, design-time assurance, as emerging regulations worldwide continue to evolve.

Addressing these challenges calls for more than incremental improvements. It requires a new foundation—Intelligent Threat Modeling—built on five requirements that align security with the speed of modern innovation while ensuring enterprise-wide coverage and compliance.

The Five Requirements of Intelligent Threat Modeling

Meeting the challenges of AI and cloud requires looking beyond automation.

It calls for a comprehensive foundation, one that redefines how threat modeling supports speed, scale, and security.

With five fundamental requirements, we can form the blueprint for Intelligent Threat Modeling, elevating the practice from static diagrams and automated tasks to an intelligent, adaptive discipline. They provide the structure that meets even the most demanding requirements of Cloud and AI, shifting threat modeling from a blocker to a business transformation accelerator.

Single Platform Intelligence Layer

Guided Security Insights

Intelligent Automation

Continuous Risk Awareness

360° Risk Visibility

1

Single Platform Intelligence Layer

The foundation for Intelligent Threat Modeling begins with a single intelligence layer that spans every domain.

By unifying modeling across applications, cloud environments, infrastructure, and connected devices, organizations can ensure consistent analysis, shared intelligence, and enterprise-wide coverage.

This unified layer does more than centralize data. It applies AI and rules consistently across use cases, ensuring that security insights are comparable and reusable whether teams are designing a new application, mapping a multi-cloud deployment, or evaluating device architectures. The result is a common standard for modeling that reduces duplication, eliminates blind spots, and accelerates the adoption of secure-by-design practices.

Equally important, the intelligence layer connects directly with the tools teams already use, such as Jira, Azure DevOps, and ServiceNow for workflow management, as well as Terraform for IaC. Hence, threat models, risks, and security controls flow seamlessly between design and execution. By embedding into existing workflows, organizations eliminate extra handoffs and ensure intelligence stays current as projects evolve.

For enterprises, a single intelligence layer also simplifies governance. Security leaders can enforce consistent policies across teams while still enabling flexibility for different architectures or environments. Development and engineering teams gain confidence that they are working from the same intelligence source, not disconnected tools or checklists.

The ThreatModeler Approach

ThreatModeler provides a unified modeling environment that connects applications, APIs, cloud services, and devices within a single model. With built-in AI and a context-based rule engine, risks and controls are applied consistently, while integrations with Jira, Azure DevOps, ServiceNow, and IaC sources like Terraform keep intelligence synchronized across teams and environments.

Guided Security Insights

Threat modeling is only effective when it leads to action.

Yet too often, teams are left with long lists of threats or static threat lists that fail to answer the most pressing question: what should we do next?

Intelligent Threat Modeling must provide **guided security insights**—actionable, context-aware recommendations that show which security controls to apply, where to place them, and how to strengthen the design. This is about moving beyond identification to actionable insights.

With guided insights, security teams can:

- **Pinpoint** the most relevant security controls, tailored to the architecture at hand.
- **Identify** gaps that static threat lists overlook, suggesting additional components or configurations that enhance the design's security.
- **Continuously adapt** recommendations as the architecture and security frameworks change, ensuring guidance remains current.
- **Translate** raw threat data into prioritized actions that teams across security, engineering, and compliance can trust.

By embedding this level of intelligence at design time, organizations can accelerate secure decision-making without relying on specialist expertise in every conversation. Insights become a shared language across roles, enabling security to scale in tandem with development.

The ThreatModeler Approach

ThreatModeler embeds AI-driven recommendations into design workflows, highlighting the most relevant controls for the architecture in front of you and updating residual risk as designs change. Guidance adjusts with framework updates and model edits, so teams act on clear, prioritized direction inside the tools they already use, not static threat lists.

Intelligent Automation

Automation has been effective in reducing manual work, but its limits have been reached.

While you can automatically build a threat model from an image, unstructured data like a drawing requires human intervention to resolve ambiguity and fill in missing pieces.

Intelligent Automation goes further. It applies context and AI to transform artifacts, such as sketches and system diagrams, into models that are accurate from the start. It also ingests Terraform and other IaC files, automatically creating and updating models as cloud environments evolve. Together, these capabilities fill in missing information, adapt to changing architectures, and continuously align models with reality.

This shift ensures that modeling keeps pace with development. Security teams spend less time fixing gaps, developers no longer wait for models to catch up, and leaders gain confidence that what they see reflects current architecture, not a stale snapshot.

At its core, Intelligent Automation makes threat modeling not just faster, but smarter—removing bottlenecks and delivering results teams can trust.

The ThreatModeler Approach

ThreatModeler imports sketches, Miro boards, enterprise diagrams, and IaC sources (e.g., Terraform) to generate working threat models in minutes. AI-assisted context resolves ambiguities, fills in missing details, and reflects ongoing changes in cloud deployments, turning static artifacts into living, production-ready models and reducing manual rework.

4

Continuous Risk Awareness

Today's enterprises know that threat modeling can't be a one-time snapshot.

In cloud and AI-driven environments, risks shift constantly as architectures evolve, infrastructure drifts, and new components are introduced. Without continuous updates, even the most detailed models lose relevance in weeks or even days.

Continuous Risk Awareness ensures that threat modeling keeps pace with change. It provides always-on visibility into residual risk and emerging threats, so teams can act quickly and confidently.

With continuous awareness, organizations can:

- **Maintain visibility** as architectures evolve, reducing blind spots and catching risks introduced by drift or new deployments.
- **Surface unmitigated threats** directly in ALM tools, keeping risks visible where work happens.
- **Highlight top risks** so teams can focus on what matters most, rather than sifting through noise.
- **Keep relevant security controls relevant** by adapting guidance as systems and environments change.

By embedding this level of awareness into everyday workflows, Intelligent Threat Modeling ensures that risk management is not reactive but ongoing. More importantly, it begins to bridge the gap between **design-time modeling and runtime resilience**—creating a living system of security that evolves with the enterprise itself.

The ThreatModeler Approach

ThreatModeler synchronizes with Jira and Azure DevOps so unmitigated threats appear as real work items—assigned, tracked, and resolved alongside development tasks. Residual risk updates automatically as the model evolves, and new risks surface in real time, giving both security leaders and engineers a continuously current picture of what matters most.

5

360° Risk Visibility

Enterprises don't operate in silos, and neither do attackers.

A single system rarely exists in isolation—applications, cloud services, and infrastructure are deeply interconnected, and risks often emerge where these connections overlap. Traditional modeling methods that analyze systems individually can overlook the broader context, leaving organizations vulnerable to cascading or converging threats.

360° Risk Visibility creates a complete view of enterprise risk by connecting models across systems and environments. Just as important, it gives security teams the ability to **see and understand** those connections in a clear, uncomplicated way. This makes it possible to trace how threats move between applications, services, and infrastructure, to identify where defenses may be compromised, and to recognize how seemingly minor risks in one domain can escalate when combined with vulnerabilities elsewhere.

This holistic perspective is especially critical in hybrid and multi-cloud environments, where complexity multiplies and risks are more difficult to trace. By automatically organizing architectures and enriching them with context, organizations can untangle sprawling environments and reveal attack paths and points of convergence with clarity.

With 360° Risk Visibility, enterprises move from securing isolated systems to understanding their entire attack surface. It's not just about seeing risks in fragments—it's about seeing how they connect, interact, and evolve across the whole environment. That shift elevates threat modeling into a strategic capability for managing enterprise resilience.

The ThreatModeler Approach

With Intelligent Cloud Mapping, teams gain visibility into complex cloud environments via automated grouping, layout, and linking of components with their metadata. Multi-level navigation—link merging, path highlighting, and model nesting/chaining—lets you view entire architectures at scale and drill into details as needed. This clarity across hybrid and multi-cloud landscapes exposes converging risks and likely attack paths before they escalate.

Business Outcomes: Why It Matters Now

The pressure from AI and cloud is real, but it doesn't have to be overwhelming.

Intelligent Threat Modeling enables organizations to address these challenges directly, demonstrating that speed and security can improve together.

With Intelligent Threat Modeling, enterprises can:

Keep pace with AI-driven innovation by automating manual tasks so security reviews match the speed of generative code and rapid prototyping.

Adapt to cloud-scale complexity by maintaining continuous coverage as architectures evolve, reducing blind spots created by drift or multi-cloud sprawl.

Close the confidence gap by prioritizing risks in context, eliminating noise, and giving leaders clarity on where defenses matter most.

Stay ahead of compliance demands by embedding provable, design-time security into workflows aligned with frameworks such as PCI DSS 4.0, OSFI B-13, MAS TRM, and DORA.

These outcomes matter because they respond directly to today's most urgent challenges. Generative AI accelerates development cycles, cloud architectures evolve too quickly for static models to keep up, and compliance frameworks demand proof of design-time security. Intelligent Threat Modeling addresses all three, giving enterprises the foundation they need to innovate securely in the face of relentless change.

Leap Forward with Intelligent Threat Modeling

Automation brought threat modeling forward, but today's realities—AI-driven development, cloud-scale complexity, and compliance pressure—demand more.

Intelligent Threat Modeling is the next step: aligning speed and security without compromise.

See what it looks like in practice.
Explore a demo or talk with our team about how to begin.