

Threat Modeling and Regulatory Compliance

A Critical Security **PRACTICE**



Contents

03

Introduction

04

Understanding Regulatory Compliance: Laws vs. Frameworks

05

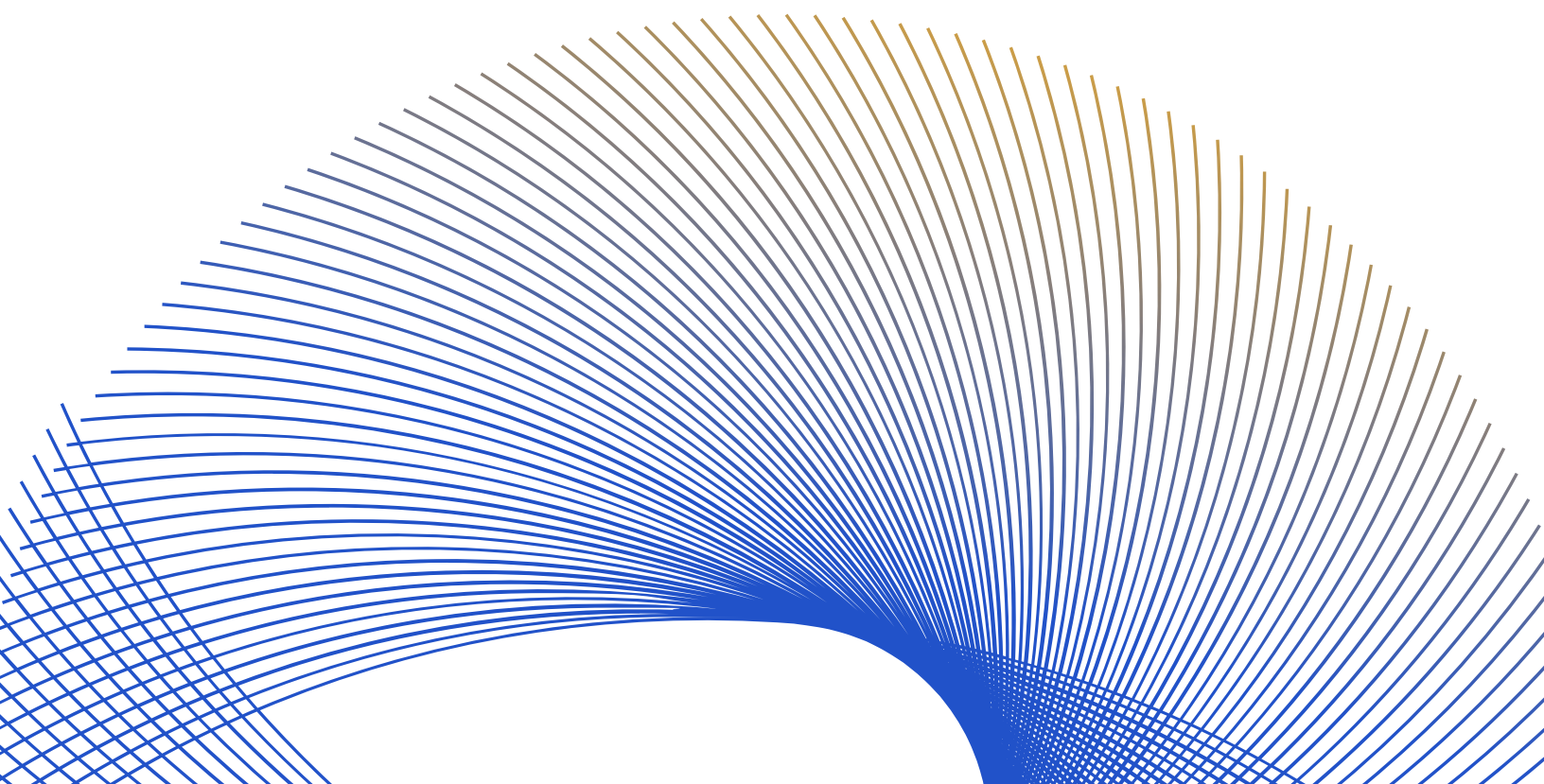
The Role of Threat Modeling in Compliance

06

ThreatModeler: Automating Threat Modeling for Compliance

08

Conclusion



Introduction

In an era of escalating cyber threats, regulatory compliance has become a fundamental requirement for organizations seeking to protect sensitive data and avoid costly penalties. Ensuring applications, cloud services, and infrastructure are secure by design is no longer optional—it's a necessity. This is where **threat modeling** plays a pivotal role, helping organizations proactively identify and mitigate security risks before they are exploited.

This whitepaper explores the significance of threat modeling in meeting regulatory and compliance obligations. It distinguishes between regulations (laws) and frameworks (guidelines) and details how **ThreatModeler** enables organizations to integrate security into their software development lifecycle (SDLC) and generate compliance reports effortlessly.



Understanding Regulatory Compliance

Laws vs. Frameworks

Compliance in cybersecurity is categorized into three primary areas:

1



Laws

Legal requirements established by governments, such as the EU's **Data Protection Directive** and **CCPA** (California Consumer Privacy Act). Laws are further clarified through regulations to provide details on how to comply. Non-compliance can lead to fines and legal consequences.

2



Regulations

A detailed rule or directive issued by an administrative agency (like the **FTC** (Federal Trade Commission), or **EU Commission**), that implements and enforces the laws passed by legislative bodies. Some well known examples are **HIPAA** (Health Insurance Portability and Accountability Act) for healthcare, **DORA** (Digital Operational Resilience Act) and **PCI DSS** (Payment Card Industry Data Security Standard) for financial services, and **GDPR** (General Data Protection Regulation).

3



Standards & Frameworks

Best-practice guidelines that organizations voluntarily adopt, such as **NIST 800-53** and **ISO 27001**. While adherence is not always mandated, it enhances security posture and simplifies compliance for regulations like GDPR, PCI DDS, HIPAA, etc.

Laws and supporting regulations are often intertwined, with significant penalties for non-compliance. Complying with and recording compliance for a broad reaching regulation like GDPR is made significantly easier by following standards. And with a solid threat modeling strategy, you can streamline adoption of standards and with the right platform, easily track compliance.

The Role of Threat Modeling in Compliance

Threat modeling is a structured approach to identifying security threats, assessing their impact, and defining mitigation strategies. It is essential for compliance as it ensures that organizations integrate security controls early in the SDLC, reducing vulnerabilities before they reach production.

Key Benefits of Threat Modeling for Compliance



Proactive Risk Mitigation

Identifies and addresses security flaws before attackers exploit them.



Automated Compliance

Aligns security measures with regulations and frameworks to streamline audits.



Continuous Security Integration

Embeds security into DevOps and CI/CD pipelines.



Cost Savings

Reduces costly rework by addressing security early in development.

Threat Modeling in Major Regulations and Frameworks

	TYPE	HOW THREAT MODELING SUPPORTS COMPLIANCE
GDPR	Regulation	Ensures data protection by identifying risks to personal data and implementing security controls.
PCI DSS	Regulation	Validates security controls in payment processing applications.
HIPAA	Regulation	Assesses threats to protected health information (PHI) and ensures compliance with security safeguards.
NIST 800-53w	Framework	Maps security threats to recommended controls.
ISO 27001	Framework	Helps organizations identify risks in their information security management system (ISMS). Used as proof of compliance for many regulatory requirements including GDPR, HIPAA, SOX, DORA.
UNR155/TARA	Regulation	Ensures compliance with cybersecurity risk assessment in automotive systems, enforced as part of UNECE vehicle regulations adoption.
DORA	Regulation	Helps financial institutions manage risks and improve operational resilience.
FDA 524B	Regulation	Supports cybersecurity compliance in medical device manufacturing and is enforceable through the FD&C Act.





ThreatModeler

Automating Threat Modeling for Compliance

ThreatModeler simplifies and automates the threat modeling process, ensuring compliance by integrating security into every phase of development.



How ThreatModeler Works

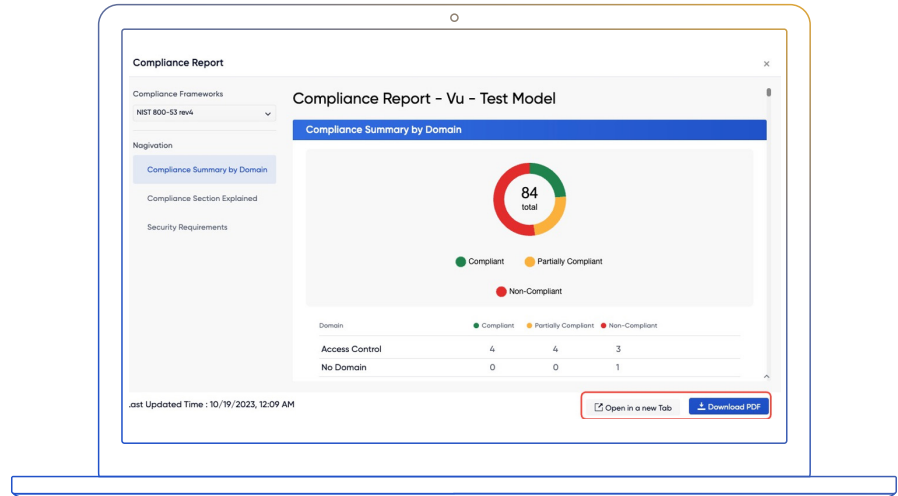
- 1**  **Build a Threat Model**
Users can generate a model using various inputs, including architecture diagrams, IaC (Infrastructure as Code), and cloud environments.
- 2**  **Identify Threats**
ThreatModeler leverages an extensive threat library to highlight potential risks.
- 3**  **Apply Security Controls**
The platform recommends security measures to mitigate identified threats.
- 4**  **Generate Compliance Reports**
Automatically maps threats to regulatory requirements and produces compliance reports.

Generating Compliance Reports with ThreatModeler

ThreatModeler offers **Compliance Reports** that assess security measures against **100+ compliance frameworks**, including **PCI DSS, NIST, GDPR, and ISO 27001**.

These reports provide:

- **A compliance summary by domain**
- **A gap analysis of security posture**
- **Recommendations for remediation**
- **Audit-ready documentation**



Example Compliance Workflow:

1. Select all frameworks that are relevant to your organization.
2. Generate a compliance report with identified security gaps.
3. Implement recommended mitigations.
4. Validate improvements and maintain continuous compliance.

Secure Development with ThreatModeler

Role	How ThreatModeler Supports Security
Developers	Identify threats and mitigate risks before deployment.
Security Architects	Automate security design reviews and integrate controls.
Compliance Officers	Generate compliance reports and ensure audit readiness.
DevSecOps Teams	Embed security into CI/CD workflows for continuous monitoring.

Conclusion

Threat modeling is **not just a security best practice—it's a compliance enabler**. By integrating **ThreatModeler**, organizations can:



Proactively **secure applications** and infrastructure.



Automatically **generate compliance reports** for major regulations.



Reduce security costs by addressing vulnerabilities early.



Maintain **continuous security assurance** in fast-paced development cycles.

With ThreatModeler, achieving regulatory compliance is **seamless, automated, and scalable**. Embrace a **secure-by-design** approach and stay ahead of evolving cyber threats while ensuring compliance with global regulations.

For more information, support, or inquiries, please contact us at:

 support@threatmodeler.com

 +1 201 266-0510

 threatmodeler.com