ThreatModeler
SECURITY STARTS HERE

Design, Build then Manage Secure Applications With Security and Compliance Automatically Built In

Why ThreatModeler?

ThreatModeler Software, Inc. 2021

Why ThreatModeler?

When choosing the perfect Threat Modeling solution, there is much to consider. In this document, ThreatModeler clearly articulates the many advantages in choosing to partner with us:

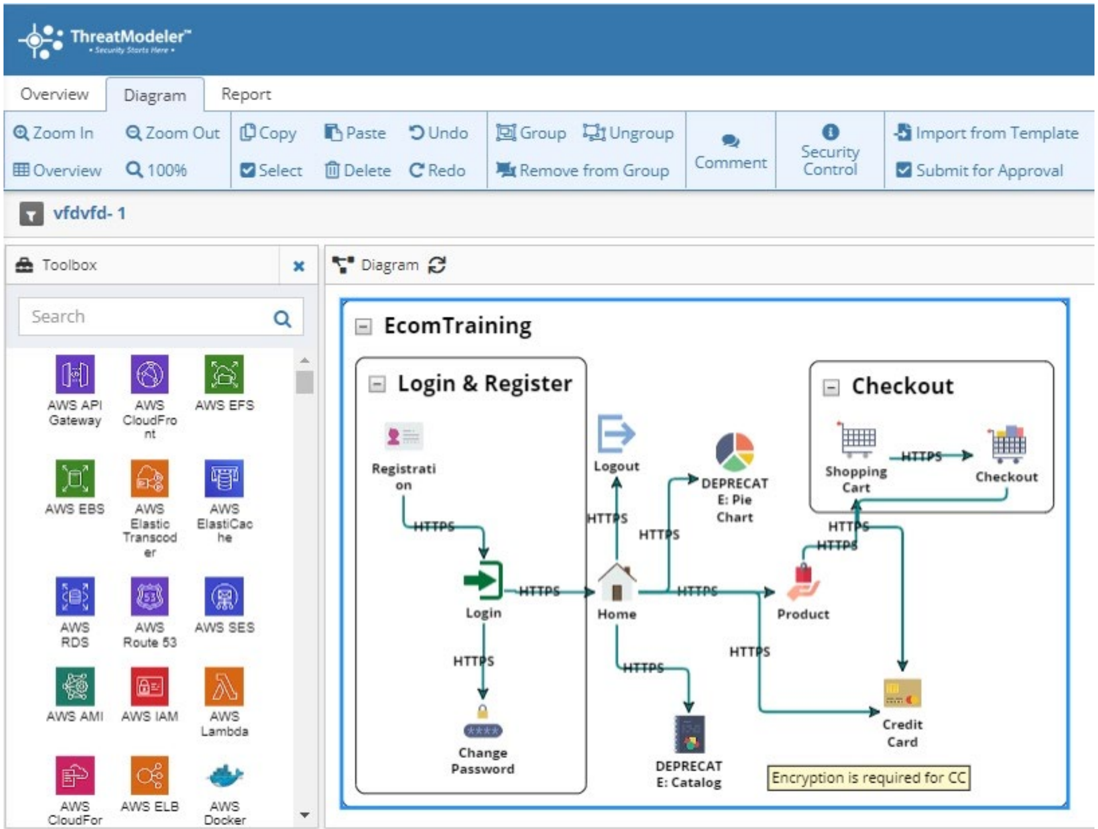
The Original and Best

ThreatModeler has been dedicated to threat modeling automation for more than a decade, far longer than our competitors. This has afforded us the opportunity to enhance the platform in close partnership with hundreds of companies of all sizes and verticals.

It's easy to claim to be innovators, but the proof is in the patents. ThreatModeler has lots of them with some pending. Of those we can mention:

- Automatically build threat model from code with Accelerator feature (Patent Pending)
- On-board "Architect" feature guiding the threat modeler (Patented)
- Threat Model Chaining and Nesting (Patented)
- Threat Model Security Controls (Patented)
- Automated threat model generation from third-party diagram files (Patented)

Modern Threat Modeling Methodology

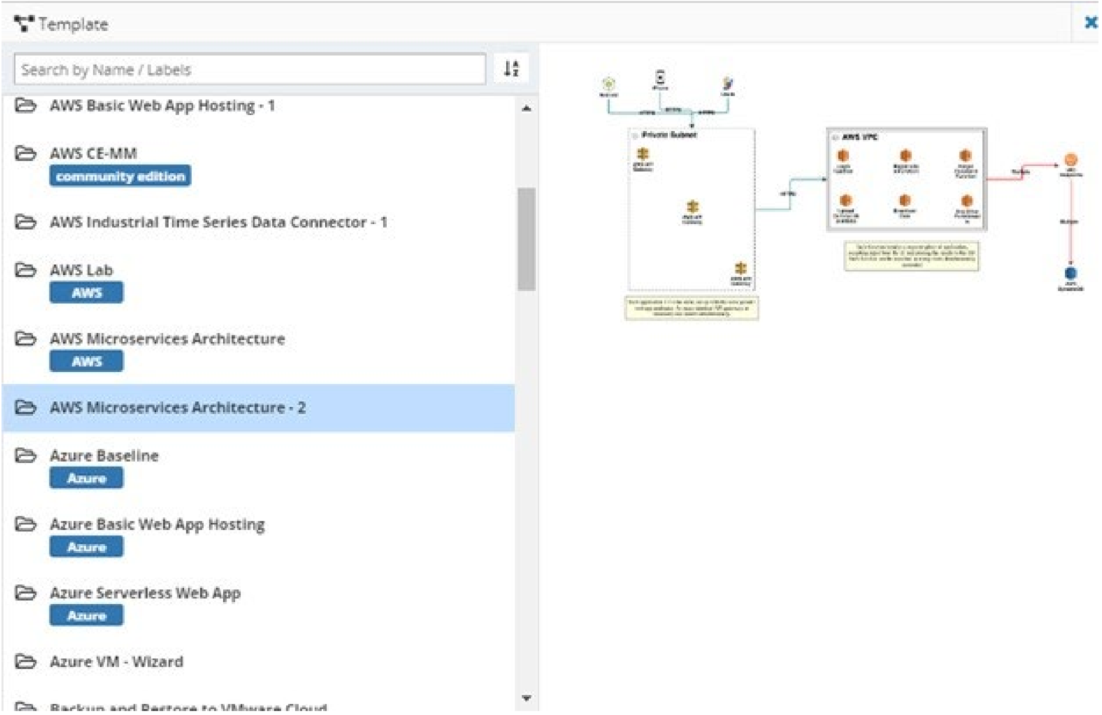


Continuing the theme of innovation goes beyond the technical features and functions of the platform and also encompasses the realm of threat modeling methodology. Rather than be bound to the outmoded Data Flow Diagramming (DFD) methodology dating from the 1970s, ThreatModeler leverages the modern Process Flow Diagramming (PFD) methodology.

ThreatModeler has published a white paper on the many advantages of PFDs vs DFDs and below are some of those benefits highlighted in the paper:

- PFDs Provide a Holistic View
- PFDs Mesh Well With the Modern DevSecOps Process
- PFDs Facilitate Collaboration and Speed
- PFDs View the System Through the Eyes of the Attacker
- PFDs Aid in Identifying Potential Attack Vectors
- PFD Threat Modeling Driving Testing and Red-Teaming
- PFDs Help to See the Infrastructure
- PFDs Aid in Standardization
- PFDs Suited to Agile Development

Pre-Built Templates and Components


Template

Search by Name / Labels

- AWS Basic Web App Hosting - 1
- AWS CE-MM community edition
- AWS Industrial Time Series Data Connector - 1
- AWS Lab AWS
- AWS Microservices Architecture AWS
- AWS Microservices Architecture - 2
- Azure Baseline Azure
- Azure Basic Web App Hosting Azure
- Azure Serverless Web App Azure
- Azure VM - Wizard
- Backup and Restore to VMware Cloud

ThreatModeler comes with 1000 common architecture components complete with their respective threats and mitigations out-of-the-box, ready for you to use in your threat models, coupled with a vast and growing library of pre-built templates of common architectures. ThreatModeler's aim is to get you up and running with minimal friction, as fast and painlessly as possible from the very beginning - planning and design.

Threat Research Center

Continuing the theme is ThreatModeler's Threat Research Center, comprising eight full-time security practitioners responsible for providing this vast array of components, templates and much more including:

- Researching industry security best practices covering a vast array of technologies.
- Researching emerging technologies for which there is no current public threat modeling documentation.
- Dissecting and reverse-engineering regulatory standards to ensure security and privacy compliance.
- Building vast complex rule sets feeding the rules engine ensuring any combination of architectural choices informs the threat model.
- Following threat intelligence feeds for new attack techniques and their respective mitigations.
- Compiling effective training for all security skill levels, including no skills.
- Writing test cases for pentesting and red teaming.

Product Steering Committee

Many product roadmaps are fueled with competing customer feature requests and ThreatModeler's Product Steering Committee is responsible for diligently analyzing these; however, ThreatModeler goes further. Customers that invest in the Enterprise Site License are allocated their own seat on this committee, which means a true partnership forged between ThreatModeler and you, exploring and aligning our visions and needs as we travel together.

Freeing Your Data for Pipeline Integration

CODE
PLAN
RELEASE
DEPLOY
BUILD
OPERATE
TEST
MONITOR

With an ethos of setting your data free, it is no wonder ThreatModeler comes with such an expansive API. Your data should be free to integrate upstream and downstream with whatever software you choose to be part of your automated DevOps pipeline. ThreatModeler gives you that freedom. If you can do it in the GUI, you can do it through the API, and so much more.

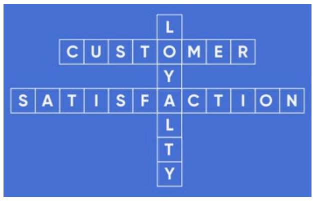
The Most Advanced Threat Modeling Cloud Technology

Without a shadow of a doubt ThreatModeler is leagues ahead of all others in the Cloud arena. And much of this innovation and technology is patented. This goes much further than Threat Modeling has gone before. From automatic integration with your cloud for continual scanning of your environment and automatic diagramming, to validating security requirements are in place (patent pending) and in the near future, deploying securely through Infrastructure as code. There is no other solution like ThreatModeler that can transition you to the cloud securely from the start and ensure you stay that way with automated checks.

White Glove Post-Sales Support

An automated threat modeling solution should be the key tool in the security maturity transition journey. That involves a lot more than just selling you the platform. For true success, ThreatModeler will appoint a dedicated project manager and ensure close and regular contact to ensure smooth deployment in your operational environment. We want this to be a success and to work with you for the long term and will do everything in our power to ensure that happens.

Some Favorite Customer Quotes



“I can’t even envisage our transition to the cloud without ThreatModeler Cloud. It integrates with our AWS services like Config and Security Hub, analyzes our security posture and makes recommendations!”

“We saved time measured in years transitioning to the cloud with ThreatModeler.”

“ThreatModeler helped us grow and scale our threat modeling practice.”

“We were struggling to collate all of our security know-how into one place in a coherent way. Although this knowledge base is very specific to our organization, ThreatModeler proved to be the ideal place to host it and is now available to anyone that has the rights to access it. This has helped a great deal in driving towards security consistency, and spreading and communicating knowledge broadly.”

“It was the ability to integrate ThreatModeler with our pre-existing pipeline tools that sold us. Not just Jira and Jenkins but others as well through the API.”

> **"ThreatModeler has enabled Intuit to launch our products into the AWS cloud and in Kubernetes in a manner that allows us to discover and resolve issues proactively. Using ThreatModeler, we’re able to consider security issues holistically over our microservices architecture. This allows us to launch in the cloud and in container- based systems with greater confidence."**
>
> **- Tom Holodnik, Security Architect, Intuit**