ThreatModeler
Security starts here

# V.A.S.T. Methodology

## Visual, Agile, Simple Threat Modeling

**Only VAST scales threat modeling enterprise-wide, overcoming the flaws and implementation challenges inherent to other threat modeling methodologies.**

### Key Outcomes of Using VAST Include:

- Integration with Agile and production tools, forming the basis of a collaborative, comprehensive threat modeling process that leverages the skills and strengths of key stakeholders organization-wide.
- The ability for organizations to automate and scale threat modeling across the entire DevSecOps portfolio (thousands of threat models) for an accelerated framework of continuous delivery.

## 3 Foundational Pillars that Scale a VAST Threat Modeling Practice

As an organization expands its technology stack, new threats arise. Where other methodologies are not built to secure at scale, VAST's pillars support exponential growth, enabling a self-service threat modeling practice:

### Automation

Complex technology ecosystems require automation to save on time-cost and eliminate repetitive, manual threat modeling, reducing time to update a model from hours to minutes. VAST addresses sustainability and the ongoing updates required from design to post deployment.

### Integration

VAST is the only threat modeling methodology created with the principles of Agile DevSecOps, boosting the short-term sprint structure of continuous improvement and updates. Through VAST, threat modelers integrate with CI/CD tools to deliver consistent, accurate security outputs.

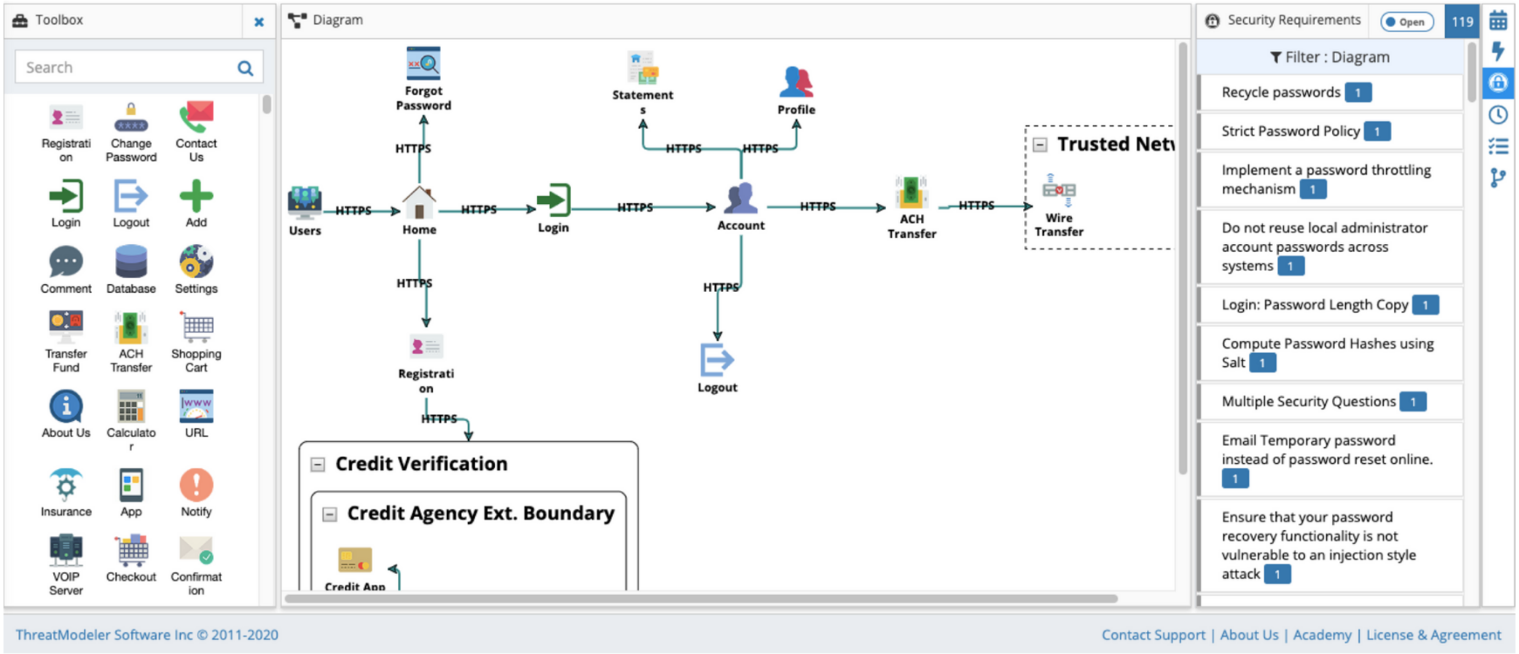
### Collaboration

Scalable threat modeling requires stakeholder collaboration and buy-in. VAST emphasizes Agile collaboration tools for use by teams, to communicate security controls and issues broadly. More people across the organization can get involved, maintaining a collaborative, dynamic security mindset.

## ThreatModeler is the Most Advanced Threat Modeling Platform on the Market and Leverages Process Flow Diagramming (PFD) With the VAST Methodology

VAST methodology ensures contextualization between all elements for accurate threat mitigation at scale. Through VAST, the entire attack surface is visualized (all threats cumulatively) with a focus on reducing the attack surface (as opposed to mitigating individual threats).

This holistic view is opposed to zoning in on components in isolation and mitigating individual threats (as in STRIDE). This leads to a reduction of false positives and false negatives as well as the implementation of actionable security controls that address real threats.



Recycle passwords 1

Strict Password Policy 1

Implement a password throttling mechanism 1

Do not reuse local administrator account passwords across systems 1

Login: Password Length Copy 1

Compute Password Hashes using Salt 1

Multiple Security Questions 1

Email Temporary password instead of password reset online. 1

Ensure that your password recovery functionality is not vulnerable to an injection style attack 1

## Apply VAST Methodology and Execute PFD-Based Threat Modeling Seamlessly with ThreatModeler's Automated Platform.

### Reduce Security Debt. Maximize Efficiency and ROI.

PFD-based threat modeling represents the mature visual decomposition of modern applications and underlying infrastructure, providing deeper contextual information about specific components – not just component types. PFDs were designed specifically to illustrate the attacker's perspective and path to data targets within an architecture framework, supporting complete threat identification at scale.

This enables teams to make precise security recommendations in the design stage, preventing costly threat remediations in the long run that might have been otherwise missed, and eliminating the need for rebuilds or reconfigurations.