



CASE STUDY

Automating Threat Modeling at Charles Schwab



charles
SCHWAB

About

Investment services leader Charles Schwab Corporation offers brokerage, banking, and financial advisory services.

Through its subsidiaries, including Charles Schwab & Co., Inc. and Charles Schwab Bank, the firm delivers a wide range of investment products and banking services designed to meet the diverse needs of its clients.

The company is dedicated to a client-centric approach, prioritizing the security of client information by continuously updating its technology, training personnel, and refining protocols to protect against emerging threats.

Manual Threat Modeling Process

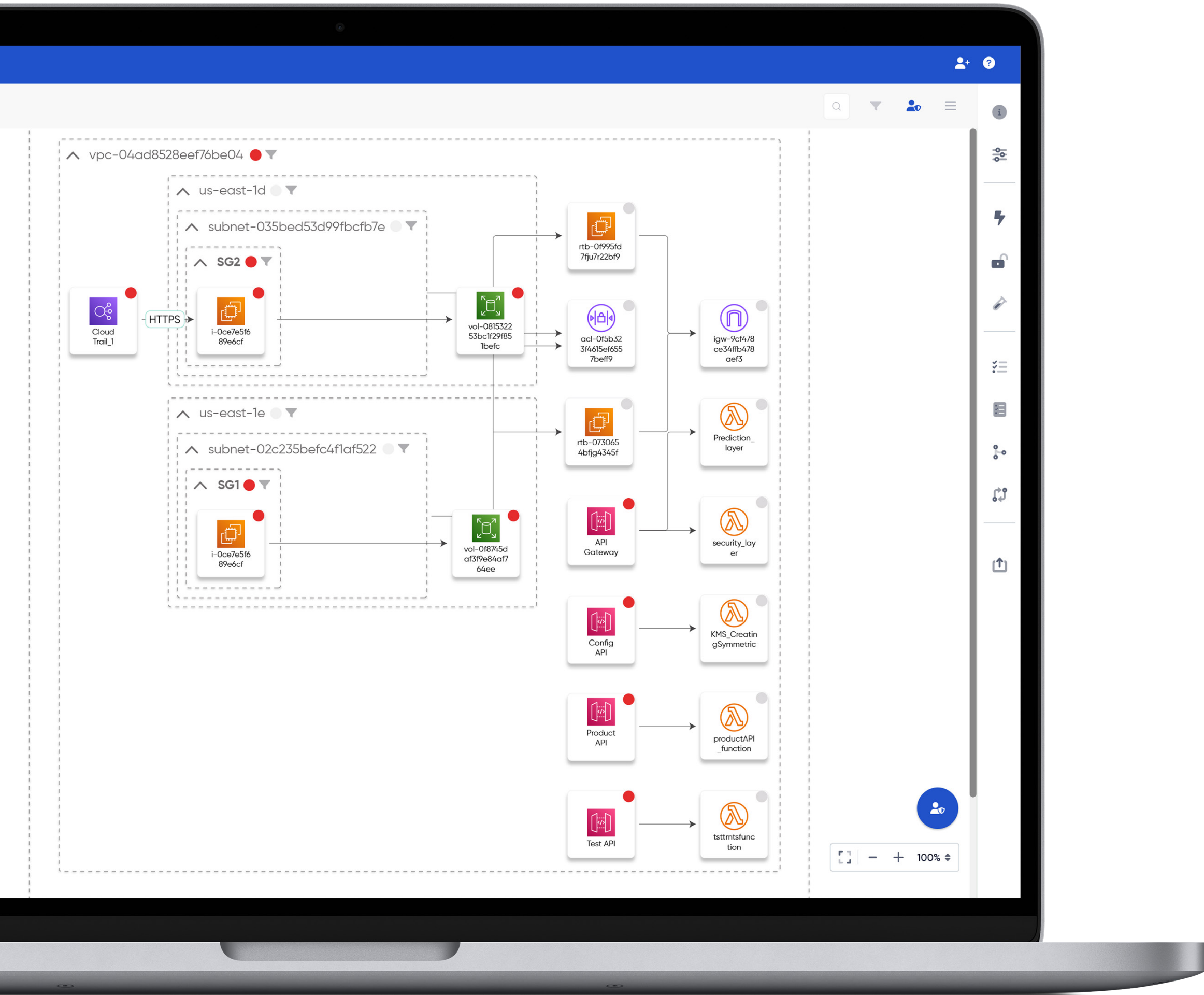
Charles Schwab was following a manual threat modeling process. The process was slow, repetitive, and highly dependent on the security team and, hence, did not integrate with their agile development practices. This also required Solution Architects to be dependent on security teams' expertise for identifying threats and security requirements.

- **Manual process** | Resource-intensive and repetitive manual threat modeling.
- **Security team dependency** | Heavy dependency on the security team to threat model.
- **Agile integration issues** | Cumbersome to incorporate threat modeling into the agile development cycle.
- **Challenges in shifting left** | Inability to scale and keep up with the demands of shift-left approach to security.

Challenges

- **7-Step process** | Conducted during the design phase and updated with architectural changes.
- **Support needed** | Solutions Architects require extensive support and hand-holding from the security team.
- **Frameworks used** | Utilizing STRIDE to identify threats and DREAD to score risks.
- **Inefficiency** | The process is laborious and repetitive, especially for more complex applications.





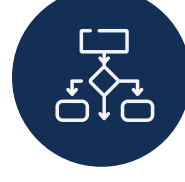
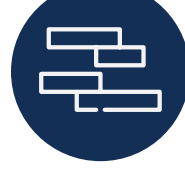


Transformative Solution

ThreatModeler is an automated threat modeling platform that Charles Schwab chose to alleviate the current challenges and roll out a scalable comprehensive automated Threat Modeling Practice to increase security posture of applications, platforms, and infrastructure. The move had their Architects and Developer Community independently drive threat modeling, ensuring that security requirements were baked into every software release.

Why ThreatModeler?

There were four major reasons why ThreatModeler was chosen by Charles Schwab:

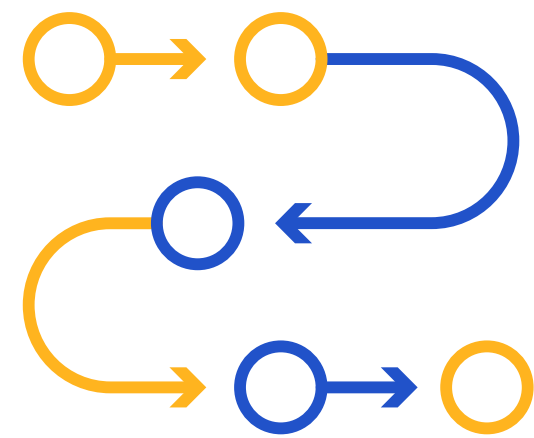
- 
Intuitive interface | Easy-to-use interface allows Solutions Architects to drag and drop components, then create connections in a visual threat model.
- 
WingMan™ | AI-driven feature that predicts and provides suggestions for the next components, making the learning curve quicker and the confidence to create threat models much higher.
- 
Threats automatically generated | ThreatModeler produces a list of threats and security requirements and it also generates descriptions of each threat and mitigation strategies in detail.
- 
Integrates with project management software | Integration with project management software used by the organization made the process seamless.

Key Benefits



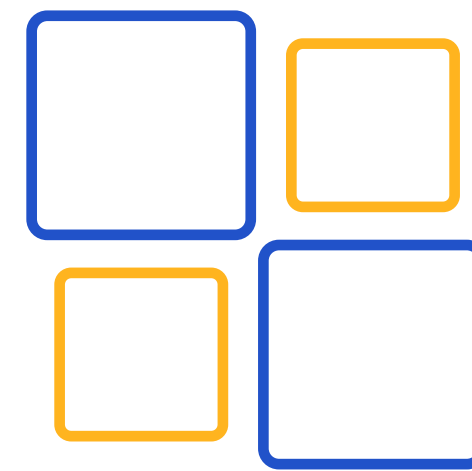
Proactive Security

Threats are mitigated during the design phase.



Streamlined Process

Segregation of duties and approval process is efficient.



Reusable Components

Leads to both time savings and improved consistency.



Self-Service Model

Minimizes dependency on the security team.

Outcomes and ROI

The main focus for Charles Schwab was to make threat modeling painless for the Solutions Architects and to get widespread adoption within the Architects Community. ThreatModeler helped accomplish this through the following:

Shift-Left security

- Integrated threat modeling into development life cycle.
- Security requirements specific to solutions are added into backlog.

Scaling threat modeling practice

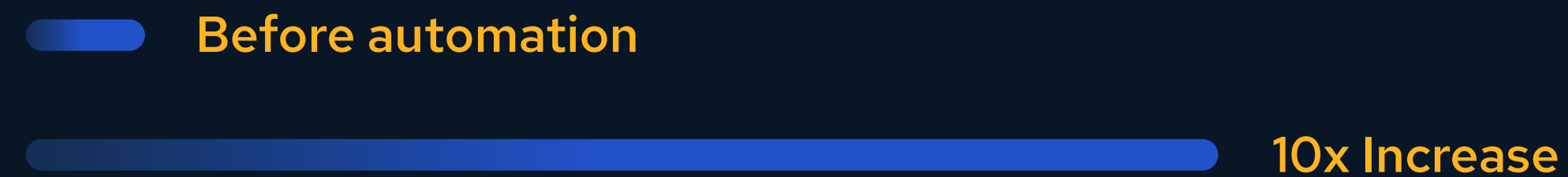
- Threat modeling performed at scale and by Architects with first-hand information about the solution.
- Increased efficiency in threat modeling with custom reusable components.

Improved oversight

- Approval workflow to confirm accuracy of threat model.
- Integrated with organization's governance processes.



Threat Models Completed



Year-on-Year Growth in Threat Models Created



Impact and Scalability

ThreatModeler's implementation at Charles Schwab established a self-service threat modeling practice within the organization. It has taken a lot of burden off the shoulders of security teams by allowing them to focus on more strategic initiatives.

Security requirements have become an integral part of development, resulting in informed architectural decisions and a proactive approach to security. This shift has had significant positive impacts on their Infrastructure and Application security.

- **Self-service onboarding** | Threat Models are created by technology teams who have first-hand information about the architecture and design of the application. Security teams are no longer a bottleneck allowing to scale threat modeling efforts independent of security resources.
- **Early security integration** | Security requirements are identified early in the development life-cycle, and mandated to be included in every release to bolster security resulting in avoidance of costly redesign of solutions.
- **Strategic focus** | Automation allows Security Architects to focus on strategic initiatives that improve the overall security posture of an organization and proactively mitigate emerging threats.

Financial Impact

- **Financial benefits** | Automated threat modeling reduced the time of spent by Solution Architects and Security Architects helping them invest on other priorities. Risk-based approach to scope applications for threat modeling helped prioritize effort on higher risk applications.
- **Lower remediation costs** | The reduction of rework and associated remediation costs by identifying and treating threats at the design phase was minimized.
- **Improved compliance** | The platform guaranteed the uniform application of security requirements in projects and strengthened adherence to security standards.





The ThreatModeler platform provides security teams with an extensive library of components and allows codifying custom threats and security requirements in the Threat Framework. Now, all our Solution Architects can use the drag-and-drop user interface to threat model and automatically get the same benefits of having a Security Architect by their side to point out solution-specific threats and security requirements.



Johnson Michael

Director of Enterprise Security Architecture



The ThreatModeler platform provides integration capabilities for single sign-on and allows adding security requirements directly to the application team's backlog for threat mitigation in future releases. Now, our security team can track outstanding security requirements both within and outside of the ThreatModeler platform, enforcing compliance.



Amy Hire
Director of Application Security



Streamline your threat modeling process

Contact Us