

WHITEPAPER

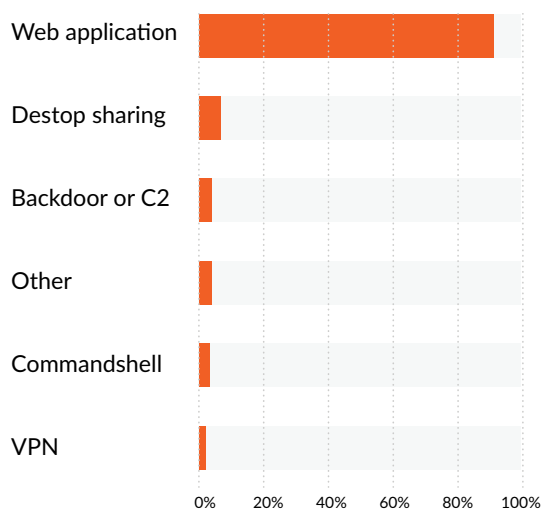
# How **SD Elements** Automates and Scales Threat Modeling for DevSecOps



# The imperative for automated threat modeling in a DevSecOps world

Cybercriminals can face a variety of defenses when attacking a network. As a result, they attack applications with increased frequency. Coding errors, misconfigurations, and poor tracking of security requirements and their associated controls can make applications an attractive target.

Whether the attacker’s goal is to steal sensitive data or disrupt operations through a distributed denial of service attack, web applications offer the simplest attack vector. The [2021 Verizon Data Breach Investigations report](#) cited web applications as the attack vector in over 90% of the data breaches researched. The [Forrester State of Application Security 2021 report](#) is more succinct, stating “web applications are the most common form of external attack.”



The 2021 Verizon Data Breach Investigations report

# The role of threat modeling in reducing risk

Relying on tests to identify vulnerabilities is simply not enough. Security professionals know they can accelerate development, better secure systems, and reduce unnecessary security rework through threat modeling.

Threat modeling works to assess risk and ensure that necessary defensive controls are in place to protect applications from adversaries. By identifying threats and mitigations – ideally before building or modifying an application – developers can add appropriate controls as part of the normal development cycle. As the National Institute of Standards and Technology (NIST) [recommends](#), “Addressing security requirements and risks during software design (secure by design) helps to make software development more efficient.” It is unsurprising then, that [threat modeling is a top priority for organizations](#).

Threat modeling has traditionally been a manual process driven by specialized security and software architecture professionals. Threat modeling teams can spend weeks mapping an application’s data flow, diagramming “trust boundaries,” and prescribing mitigations for implementation by development teams. As a result of the time required to build threat models, the bandwidth and availability of security and software architecture professionals limit the ability to extend threat modeling capabilities beyond the most critical applications.

Rapidly changing technology and threat

landscapes demand a new approach. Attackers know they can target less critical applications to gain a foothold in an organization, and scaling manual threat models is not an option. As with much of modern software development, automation is required to expand threat modeling capabilities across an organization's software portfolio.

## Challenges of threat modeling solutions

Security and development professionals on the front lines of threat modeling activities face the following challenges when they relying on manual and diagrammatic solutions to identify threats and appropriate mitigations:

- **Lack of an automated process to identify the appropriate threat mitigations for the components being modeled.** To recommend preventive mitigations for a particular system component, such as encryption and identity and access management policy, most solutions still require human expertise. The expansion of regulatory requirements further complicates this issue.

- **Integration with the secure development process.** In a DevSecOps environment, security and development tools must work together in an automated manner to minimize blockage in the pipeline. Some threat modeling solutions lack integration with common development tools, like Jira, while others work only with security tools produced by the same vendor.
- **Lack of support for major cloud platforms.** As organizations move their applications to the cloud, they want to avoid vendor lock-in. Support for multiple cloud infrastructures is a requirement.
- **Limited security expertise.** Understanding which threats are most critical and which mitigations are most effective is crucial. A good threat modeling solution must be "self-service": simple for developers to use with minimal support from security





## The SD Elements platform

SD Elements is a breakthrough solution that automates threat modeling. SD Elements greatly reduces the time and effort required to identify weaknesses and mitigations, allowing organizations to develop secure and compliant software more rapidly. It provides an ultimate “shift left” and scalable approach to threat modeling by identifying weaknesses attackers target and appropriate mitigations across software portfolios.

SD Elements uniquely goes beyond the traditional scope of threat modeling in three ways:

- SD Elements is developer-centric, automatically describing preventive controls in the form of detailed instructions, short Just-in-Time training videos, and code samples so developers can effectively implement the controls and reduce security, privacy, and compliance risk.
- SD Elements integrates security guidance into development workflows, including market-leading development tools like Jira, Digital.ai (formerly VersionOne), and Azure Boards. Integrations with security testing tools expedites the verification of control implementation and security testing guidance helps focus manual testing efforts.
- SD Elements’ content library includes dozens of regulatory standards and best practices frameworks globally and translates these into easy-to-follow instructions for development, assurance, and deployment teams.

## How SD Elements automates threat modeling for DevSecOps



**Figure 1** High-level view of how SD Elements automates threat modeling

SD Elements is purpose-built for DevSecOps. It provides a fast, consistent, and scalable approach to threat modeling that is effective irrespective of the security expertise of the team.



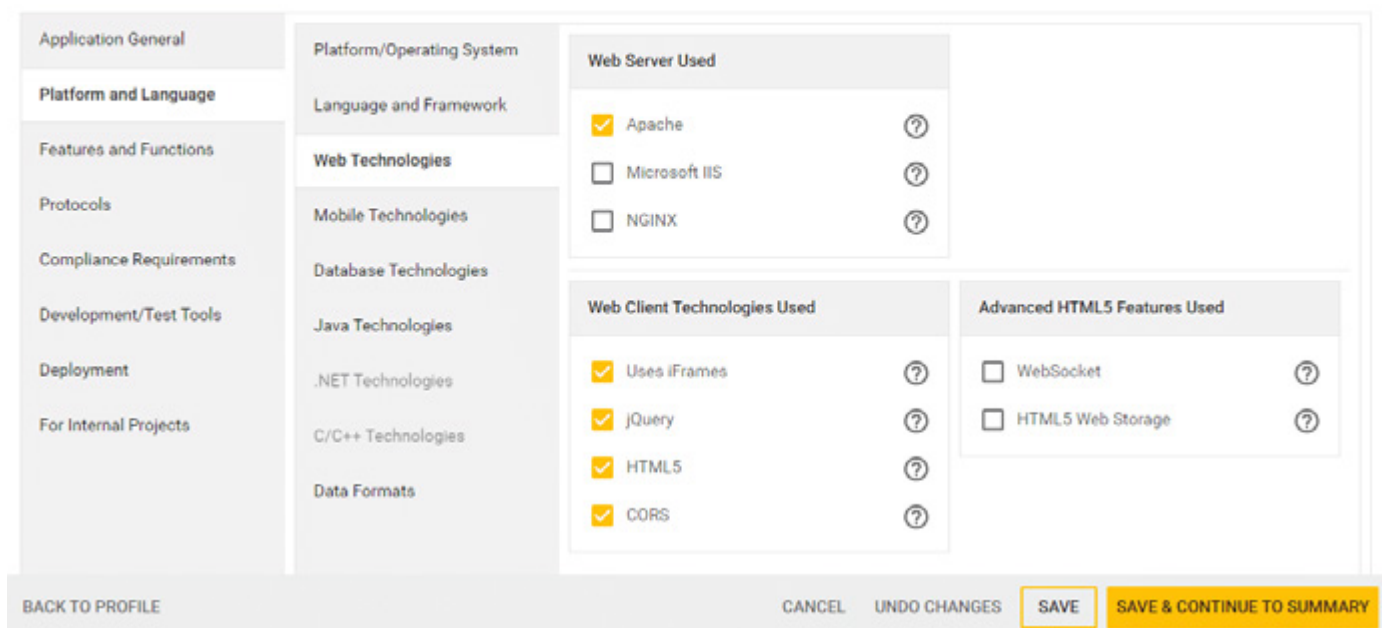
## Identify Weaknesses That Attackers Can Exploit










The SD Elements platform uses a survey that allows diverse stakeholders in compliance, security, privacy, software development, and operations to more easily contribute to the information gathering process. A standardized survey guides users through the information process in a systematic way, so systems consisting of applications, APIs, IoT devices and/or embedded systems, referred to as Projects in SD Elements, can be onboarded efficiently.

### 2. Project Survey

[Export Survey History](#) 

Model the application by customizing the **Android App** settings below. If you complete the project settings but are unsure of certain answers, you can make assumptions and then change the project settings at a later time.



Application General	Platform/Operating System	Web Server Used	Web Client Technologies Used	Advanced HTML5 Features Used
Platform and Language	Language and Framework	<input checked="" type="checkbox"/> Apache 	<input checked="" type="checkbox"/> Uses iFrames 	<input type="checkbox"/> WebSocket 
Features and Functions	Web Technologies	<input type="checkbox"/> Microsoft IIS 	<input checked="" type="checkbox"/> jQuery 	<input type="checkbox"/> HTML5 Web Storage 
Protocols	Mobile Technologies	<input type="checkbox"/> NGINX 	<input checked="" type="checkbox"/> HTML5 	
Compliance Requirements	Database Technologies		<input checked="" type="checkbox"/> CORS 	
Development/Test Tools	Java Technologies			
Deployment	.NET Technologies			
For Internal Projects	C/C++ Technologies			
	Data Formats			

BACK TO PROFILE      CANCEL    UNDO CHANGES    **SAVE**    **SAVE & CONTINUE TO SUMMARY**

**Figure 2** Survey in SD Elements

Completing the survey characterizes the project, its technology stack, deployment infrastructure, and relevant regulatory or internal security and privacy standards. A survey can be completed as early as the design phase and updated as more information becomes available or as new features are added. This supports a self-service approach, and complements the rapidly changing DevSecOps environment.

According to the [Software Engineering Institute](#), 90% of reported security incidents result from exploits against defects in the design or code of software. SD Elements goes above and beyond this to reduce the attack surface. It quickly generates a consistent set of defects or weaknesses not only in the architectural components (i.e. the software code specific to the programming language and framework and the application infrastructure), but also in the SDLC activities including deployment and operation of the system. These are all presented as Problems in the platform.

Magellan 3.1 Problems		☰ 🔍
Risk Rating	Problem	<input type="checkbox"/> Show only On-Boarding Policy tasks
10	P203: Missing Authentication for Critical Functions	
10	P209: Cleartext Storage of Sensitive Information without Access Control Mechanisms	☰ 1
10	P216: Clear Text and Unencrypted Transmission of Information	☰ 1
10	P1170: Lack of a secure process for outsourcing	☰ 1
10	P1171: Lack of a process for identifying applicable compliance regulation	☰ 1
10	P1172: Lack of a process for identifying critical assets	☰ 1
10	P1173: Lack of a process for dynamic application testing	☰ 1
10	P1180: Lack of process for collecting and protecting sensitive data	☰ 1

Page: 1 ▾ Rows per page: 8 ▾ 1-8 of 134 < >

**Figure 3** List of Problems or weaknesses identified by SD Elements

As the survey is updated, SD Elements automatically adjusts the threat model and recommended controls. Users can also model only what will or has changed in the model using the Release Project feature, and SD Elements will rapidly identify incremental security and privacy controls. If desired, security can customize the survey and controls to match internal security policies.

### Identify and Prioritize Security and Privacy Controls

The SD Elements platform automatically identifies specific and actionable security and privacy controls for development, security, and operations teams to address the weaknesses enumerated through the survey. This allows consistent controls regardless of which personnel modeled the project.

Status	Priority	Task
🕒	10	T42: Avoid relying on untrusted data for server-side selection
🕒	10	T76: Do not hard code passwords
🕒	10	T186: Use recommended settings and the latest patches for third party libraries and s...
🕒	9	T61: Disable default accounts or change all default passwords
🕒	9	T335: Sanitize user input before passing to NoSQL operators

**Figure 4** List of automatically-generated controls based on Survey responses

### ***Cross-platform support***

Unlike language or platform-specific threat modeling tools, SD Elements supports **hybrid development environments** and all major **cloud infrastructure platforms** including Amazon Web Services, Microsoft Azure, and Google Cloud Platform. This allows teams that use multiple programming languages, and deploy applications on-premises and in cloud environments, to identify and mitigate security weaknesses quickly, thus reducing the likelihood of successful attacks.

### ***Compliance ready***

Overlapping regulatory standards and internal corporate policies are constantly changing and complex to understand. The **SD Elements Content Library** covers over 40 distinct regulations and standards including the OWASP Top 10, OWASP API Top 10, NIST 800-53, and FedRAMP. SD Elements determines which standards and regulations are applicable based on survey responses; it automatically deduplicates overlapping controls, prioritizes, and maps them. SD Elements uses open APIs to provide programmatic access to our library of content and services to provide maximum flexibility when building your DevSecOps vision.

### ***Continuously updated***

Regulatory requirements change frequently, as do internal policies and the threat space. To keep you protected without investing in an in-house team, SD Elements' content library is continuously updated by security experts at Security Compass. As new content on security weaknesses and mitigations are added to the content library, SaaS users are automatically notified and have the option to accept the latest content updates applicable to a project.

Security and compliance teams can modify or add controls to SD Elements to address internal policies, critical cybersecurity concerns, and unique regulatory matters. Other domains such as infrastructure security, accessibility, legal requirements, and vendor/supply chain management are also supported.



## Simplify Mitigation

Identifying weaknesses that threats target is only the first step. Applying controls to eliminate these weaknesses is also necessary, and often a challenge for organizations. SD Elements integrates with leading development tools to simplify mitigation.

Gartner® reported that “three out of four software engineering teams report that they experience development friction, defined as unnecessary time and effort they must exert to achieve their objectives.”<sup>1</sup> Further, almost half of the software engineering personnel surveyed reported experiencing friction in meeting architecture and security requirements.

SD Elements makes this process frictionless by delivering preventive controls and prescriptive security guidance specific to your projects through native integrations with leading issue tracking tools to automate creation of tickets and enable bi-directional synchronization of ticket statuses.

### Specific and actionable tasks

Security and privacy controls are presented as Tasks in SD Elements. Tasks include an explanation of how the weakness can be exploited by attackers to help raise security awareness, how-to instructions, short, contextual training videos, and detailed code samples – all to make the implementation of security and privacy controls much easier for development and operations teams. Test plans for validating control implementations are also available.

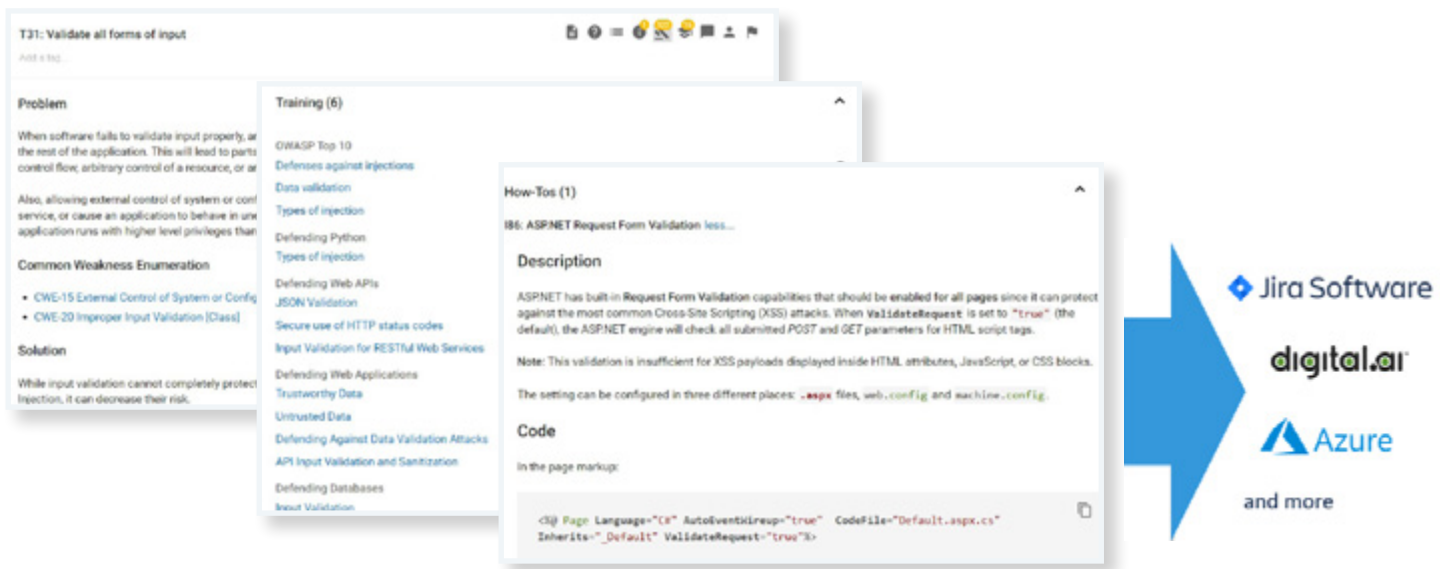


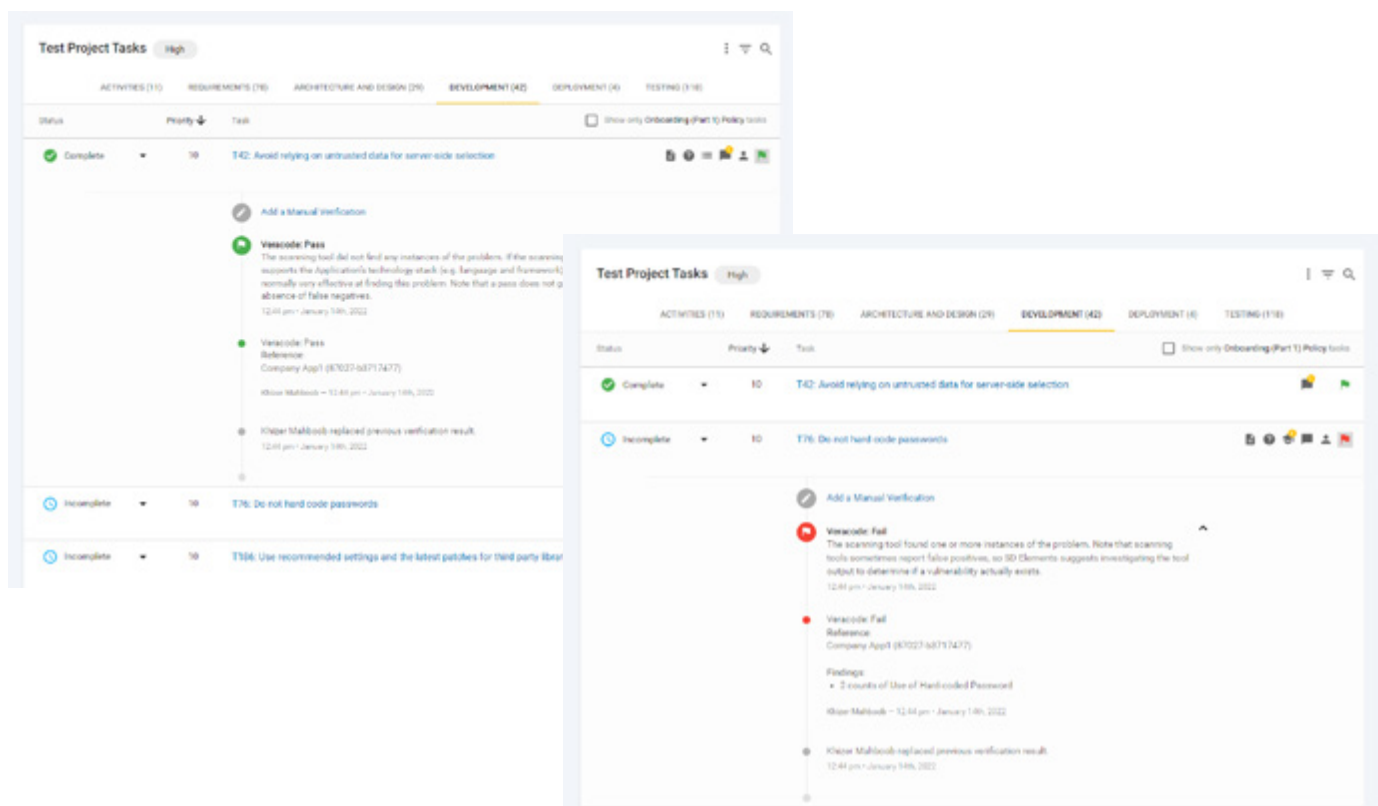
Figure 5 Task and its components

## Risk policies

SD Elements makes the process of embedding security and privacy into the design, architecture, and deployment of projects manageable by leveraging Risk Policies. This feature allows teams to control the number and scope of controls per sprint or phase based on compliance priorities and/or inherent risk.

## Streamline Verification

Verifying the proper implementation of assigned controls can challenge security and compliance teams. Mapping output from security scanning tools and manual tests with specific controls is difficult and tracking open issues with spreadsheets is unreliable.



**Figure 6** Integration with static and dynamic analysis tools

SD Elements solves this by automatically verifying control implementation. It can import results from scanning tools to automatically verify whether security controls have been fulfilled and prioritize open issues. It can also identify which controls the tools cannot verify and expedite manual testing of those controls through its security testing guidance.

## Deliver Reporting for All Stakeholders

SD Elements delivers stakeholder-specific reporting to teams. It provides a centralized, controlled, and auditable environment for recording all activity regarding a project's weaknesses, controls, and mitigation efforts. Teams can quickly generate reports on the weaknesses identified in a system by SD Elements and the completion status of controls. The executive dashboard reports on key controls metrics such as the status of risk mitigation across the organization and risk professionals can view compliance specific reports for PCI-DSS, HIPAA, PIPEDA, GLBA, GDPR and **other privacy related standards**, along with any custom regulations you add to the system.



## SDELEMENTS

# HIGH PRIORITY COMPLETION STATUS REPORT

Application: Mobile Banking  
 Project: Payments Application  
 Prepared on: Aug 5, 2020

## Section 2: Requirements

ID	NAME / TITLE / NOTES	PRIORITY	STATUS	LAST MODIFIED BY	LAST MODIFIED	VERIFICATION	LAST VERIFIED BY	ASSIGNED TO
T21	Ensure all data in transit is encrypted using a secure TLS channel	5	Complete	Chloris Lee	Nov 11, 2019	...	...	...
T60	Use coded and approved cryptographic algorithms, parameters, and key lengths	5	Incomplete	...	...	...	...	...
T34	Use standard libraries for cryptography	5	Not Applicable	Chloris Lee	Aug 27, 2020	...	...	...
T49	Profile and remove debug capabilities and redactions, and prepare application for release	7	Incomplete	...	...	...	...	...

## Section 3: Architecture & Design

ID	NAME / TITLE / NOTES	PRIORITY	STATUS	LAST MODIFIED BY	LAST MODIFIED	VERIFICATION	LAST VERIFIED BY	ASSIGNED TO
T176	Apply principles of privacy when handling personal information	5	Complete	Chloris Lee	Nov 11, 2019	...	...	...
T14	Enforce the principle of least privilege	5	Complete	Chloris Lee	Nov 11, 2019	...	...	...
T521	Protect the Digital network infrastructure with a Network Key	5	Incomplete	...	...	...	...	...

**Figure 7** Executive dashboard in SD Elements (left); Completion status of controls identified by SD Elements (right)

If an auditor requests a demonstration of which applications and issues were in scope, who implemented them and when, who validated them and when, and what notes were attached to those activities, teams can generate a report without software engineers. Keyword searches can quickly show which controls relate to specific security weaknesses.

# Integrating Threat Modeling with DevSecOps

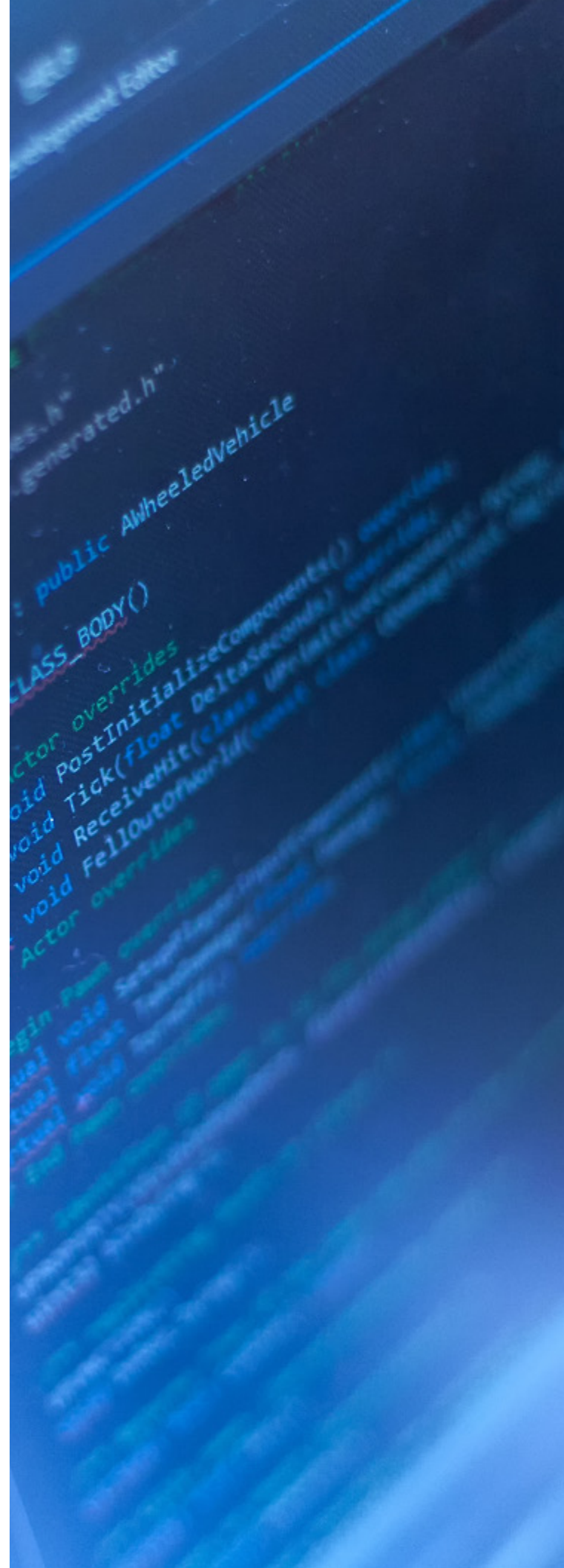
Teams leverage SD Elements to kickstart and scale their threat modeling programs. By automating the identification of risky designs across their portfolios and applying consistent controls, they reduce the likelihood and impact of successful attacks. For high-risk systems, the security and privacy controls and test guidance identified by SD Elements provide a starting point to help focus manual threat modeling activities with security experts.

## Learn More

[Contact us](#) today to learn how SD Elements can help you automate and scale your organization's DevSecOps threat modeling process.

---

1 Gartner, "Reduce Friction to Boost Software Engineering Team Productivity", Applications and Software Engineering Research Team, Published 25 May 2021. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.



# SecurityCompass

## Go Fast. Stay Safe.

Security Compass, a leading provider of cybersecurity solutions and advisory services, enables organizations to build more secure software faster. Our flagship product, SD Elements, the company helps automate significant portions of proactive manual processes for security and compliance that improves time to market for new technology. Security Compass is the trusted solution provider to leading financial organizations, technology enablers, and renowned global brands. Security Compass is headquartered in Toronto, with offices in the U.S. and India. Follow Security Compass on Twitter @securitycompass or visit us at securitycompass.com to learn more.

**1.888.777.2211**

**info@securitycompass.com**

**www.securitycompass.com**

 **@SECURITYCOMPASS**

 **SECURITY COMPASS**

### OFFICES

#### GLOBAL HEADQUARTERS

1 Yonge Street  
Suite 1801  
Toronto, Ontario  
Canada M5E 1W7

#### TORONTO

390 Queens Quay W  
2nd Floor  
Toronto, Ontario  
Canada M5V 3A6

#### NEW JERSEY

621 Shrewsbury Avenue  
Suite 215  
Shrewsbury, New Jersey  
USA 07702

#### CALIFORNIA

600 California Street  
San Francisco, California  
USA 94108

#### INDIA

#4.07  
4th Floor, Statesman House  
Barakhamba Road, New Delhi  
India 110001