Business Case for Automating Threat Modeling, Risk Assessment and Secure Coding Requirements

The long-run competitiveness of businesses depends on the security of their digital products — especially given the rising number of breaches leading to brand damage and penalties.

SecurityCompass

The Ongoing Dilemma: Speed vs. Safety

For too long organizations have faced a dilemma in building software, go fast and deliver required functionality to market quickly while sacrificing security. Or stay safe by performing manual threat modeling, risk assessments and secure coding practices while slowing down development. The key question most organizations have is — how can we become "Fast and Safe"?

This is not just a technology issue. It is a competitive issue.

Many organizations are choosing the fast and risky approach to build digital products faster while sacrificing security. Others are doing all the right things by infusing security and compliance but can only build products at a snail's pace and end up losing to irresponsible competitors.

In this cost savings guide, we will address the challenges faced by organizations that have adopted the "Fast and Risky" approach and want to move away from it to minimize the associated risks (and brand damage), and also those that have been taking the "Slow and Safe" approach and want to speed up time to market with safety.

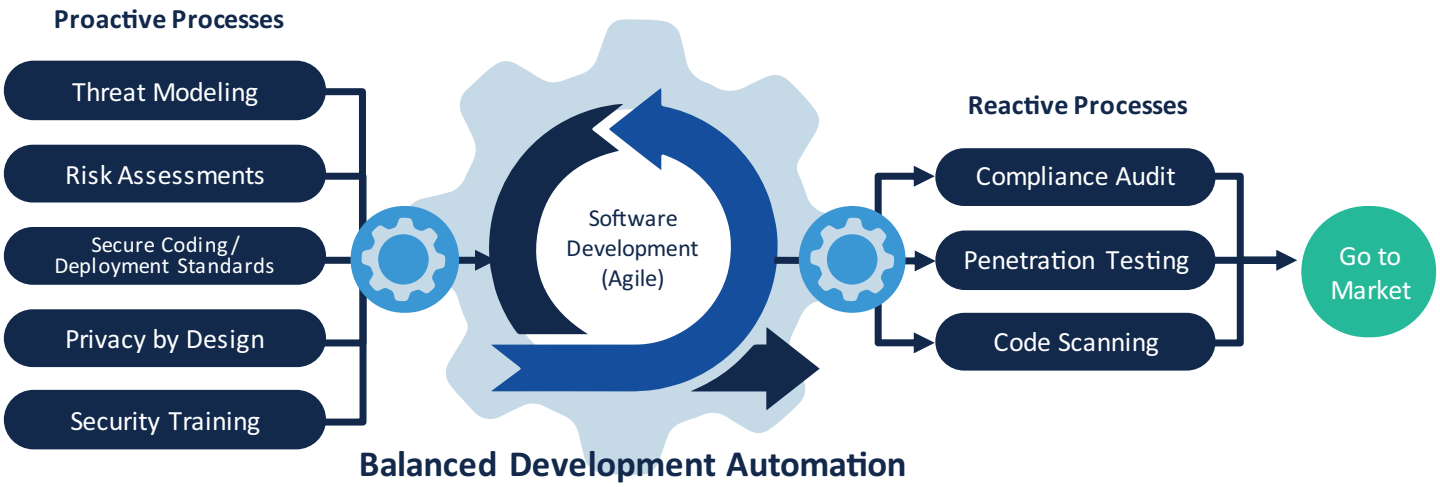
FAST AND SECURE DEVELOPMENT IS NOT A TECHNOLOGY ISSUE, BUT A COMPETITIVE ONE.

Improve Time to Market While Staying Safe

Speed and security can work in unison.

Organizations can go “Fast and Safe” by using a new approach, balanced development automation, that helps them accelerate software releases while improving product security. It operationalizes security and privacy policies and regulatory standards, turning them into actionable controls or tasks which guides engineering through every step of development. Using this approach, developers can get security/privacy instructions as they write code.

Balanced development automation allows your organization to build secure products nearly as fast as if they were being built without security or compliance at all, and as safely as if it were painstakingly built under the guidance of human experts.



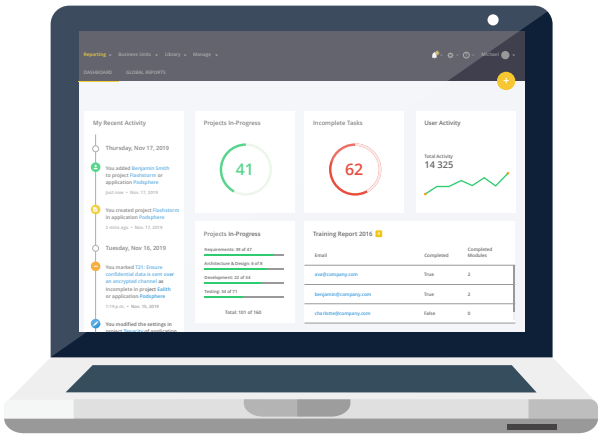
HOW BALANCED DEVELOPMENT AUTOMATION WORKS

Balanced development automation helps organizations accelerate software releases while improving product security. It works by automating key portions of your proactive security processes such as threat modeling, risk assessment, and privacy by design reviews, and infusing secure development and best practices into your workflows. The system acts like a guide through every step of development, delivering security and compliance instructions for that part of the work. When the project is finished, the system can compile insights about what was done and what wasn't, so that your business leaders can get a view into risks across all applications.

Balanced development automation makes sure software gets built right in the first place. Ultimately, it enables you to push software to customers faster while giving you confidence that it is also safe.

SD ELEMENTS

SD Elements is the world's first balanced development automation solution. It enables enterprises to deliver secure and compliant software quickly and reduce costs. That's why leading organizations across the world trust our solution to balance safety with time to market.



Snapshot of our client base:

15 of the largest banks in North America and Latin America.

12 of the largest technology companies focused on software development, chip manufacturing, and payment processing.

U.S. Federal Government agencies such as the DOD, the U.S. Navy, the U.S. Air Force, and the SEC.

Multiple clients across varied industries such as Health Care, Telecom, Automotive, Retail, and Energy.

WHY CLIENTS ADOPT SD ELEMENTS

Our clients have witnessed one or more of the following quantifiable benefits from implementing SD Elements within their organization:

COST SAVINGS

SD Elements accelerates proactive security processes and brings down timelines from 5 to 30 days to 1 to 2 days which significantly saves cost.

1

IMPROVES TIME TO MARKET

As a result of increased efficiency in performing threat modeling and risk assessments, and in generating secure coding requirements faster.

2

EXPEDITES REGULATORY COMPLIANCE

By providing near real-time traceability of security controls that have been implemented, compliance gets easier.

3

SAVES REMEDIATION COSTS

By identifying and addressing security weaknesses early in the development process, our solution saves the need for remediation.

4

REDUCES CONTENT UPDATE COSTS

SD Elements keeps an organization's security best practices up-to-date, thereby eradicating the need to maintain a research department.

5

In addition to the direct cost savings noted in the previous section, SD Elements also introduces new capabilities and benefits:

- Enables your organization to utilize security experts only for high-value security work by freeing up their time from manual processes
- Drives efficiency in proactive security processes which is particularly valuable when security teams are mandated to do more with the same budget
- Provides your organization a better understanding of corporate risk and compliance posture related to applications
- Reduces your risk of brand damage by decreasing the number and severity of security flaws in applications
- Improves your team's secure development knowledge as they implement automatically-generated controls, and consume just-in-time training
- Improves relationship and collaboration between Security and Development teams to implement security measures, while also reducing duplicate efforts and the need for meetings and in-person conversations
- Drives consistency in your proactive processes, thereby improving the accuracy of reporting
- Simplifies the audit process as our solution helps you with transparency and reporting
- Implement consistency in data between disparate systems as a result of automated integrations

Cost Savings Framework: SD Elements Implementation

Processes to proactively embed security and compliance in software development vary by organization, and thus, results for adopting a balanced development automation solution like SD Elements will also vary. To drive consistency and efficiency in process and outcomes, SD Elements distills key activities common in some proactive processes, such as threat modeling and secure coding, into four steps:

1. **Information Gathering:** SD Elements guides users in a systematic way so that projects are onboarded efficiently. It gathers information about your project, such as its technology stack, deployment infrastructure, security testing tools, and compliance requirements.
2. **Expert Assessment:** SD Elements analyzes the information and correlates it with regulations, policies and best practices in the knowledge base.
3. **Recommendations:** SD Elements makes intelligent decisions on risks, controls, just-in-time training and even code samples specific to your technology and industry, and can deliver these directly to your issue tracking tools. It also rapidly classifies your project into relative risk grouping to help your teams manage projects by potential risk.
4. **Validation and Reporting:** SD Elements tracks controls, and can also validate the status of certain tasks automatically by capturing updates from security testing tools. This gives you a near real-time view into the risk status of your projects, and the controls in scope for each, at any time in the project life cycle.

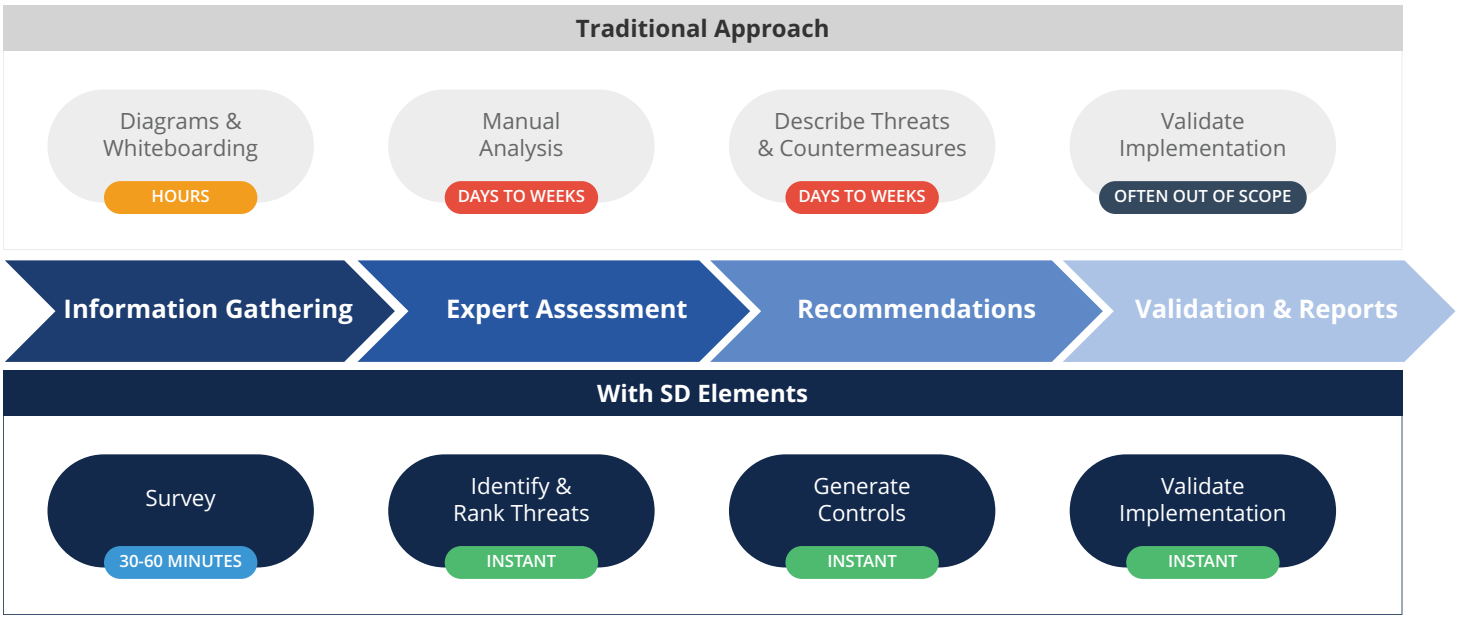
SD Elements drives quantifiable benefits in four use cases: threat modeling, compliance, secure development, and risk assessment. In the following section, the key steps in certain use cases are summarized in the context of the four-step framework discussed above to help your organization think about and model the potential and actual value of SD Elements.

THREAT MODELING

Many companies are now faced with a dilemma — do they hire additional experts or outside consultants to address their threat modeling backlog, or adopt a new way by automating key activities in threat modeling to help reduce overall risk?

Our research suggests that most organizations currently perform threat modeling using tools such as whiteboards or automated diagramming tools that require security expertise. Sounds familiar? While these tools may seem practical, they are very difficult to scale and require substantial human capital to use and maintain.

SD Elements distills the key steps in threat modeling to streamline and accelerate the process:



Client Spotlight

80% Reduction in Threat Modeling Time

Our client in the financial services sector reduced their threat modeling time for select, high-risk applications from 5 days to 1 day with SD Elements. The solution also improved collaboration and helped align the application security and development teams early on in the software development life cycle.

SECURE SOFTWARE DEVELOPMENT

Many organizations write code and then identify vulnerabilities using code scanners or penetration tests. Based on their risk tolerance, they make a decision to either:

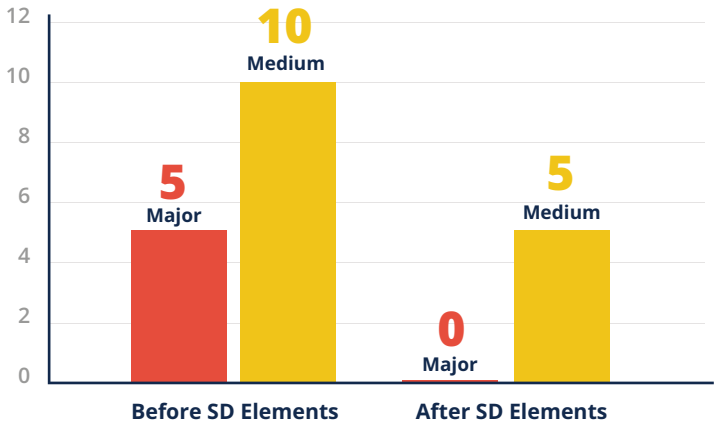
1. Remediate the vulnerabilities, which means spending a significant amount of time and thus delaying product releases.
2. Or accept the risks, which means allowing products with critical vulnerabilities to be released.

Because of the rising number of breaches and concerns about data privacy, more and more organizations are “shifting security left” and ensuring code is developed securely from the beginning.

Client Spotlight

92% Reduction in Vulnerabilities & Cost of Preparing Guidelines

Based on a Forrester Total Economic Impact study commissioned by Security Compass in 2015, a leading financial institution reduced high risk vulnerabilities by 100% and medium risk vulnerabilities by 50% using SD Elements. Our client witnessed significant cost savings from their investment in software security:



After the implementation, they now average only five medium-level vulnerabilities per project, which is down from five major and 10 medium vulnerabilities earlier. They are avoiding millions in remediation costs now.

1. For 75 major applications, they registered savings of $75,000/project leading to an overall cutback of more than $5.6 million.

2. Of the total savings, they attribute 40% to SD Elements, resulting in a benefit of more than $2.2 million annually and a total of more than $6.7 million over three years.

The use of SD Elements freed up 40% of the security professionals' time, resulting in savings equivalent to 14 FTEs, and allowing them to work on other security initiatives. At an average burdened salary of $150,000, this translated to savings of $840,000 per year.

Further, based on a study conducted by Security Compass in 2019, SD Elements addresses at least 92% of the vulnerabilities found in penetration testing reports. Using SD Elements early in the process as a proactive security measure significantly reduces vulnerabilities that eradicates the need for remediation later.

COMPLIANCE

Regulatory standards and internal corporate policies are constantly updated and complex to understand. Managing these requirements with disparate spreadsheets, email, and file storage solutions can get difficult as you scale your application portfolio.

SD Elements translates complex standards into easy-to-understand tasks, and provides continuous visibility into the status of controls and evidence of adherence to compliance requirements.

Client Spotlight: U.S. Federal Government

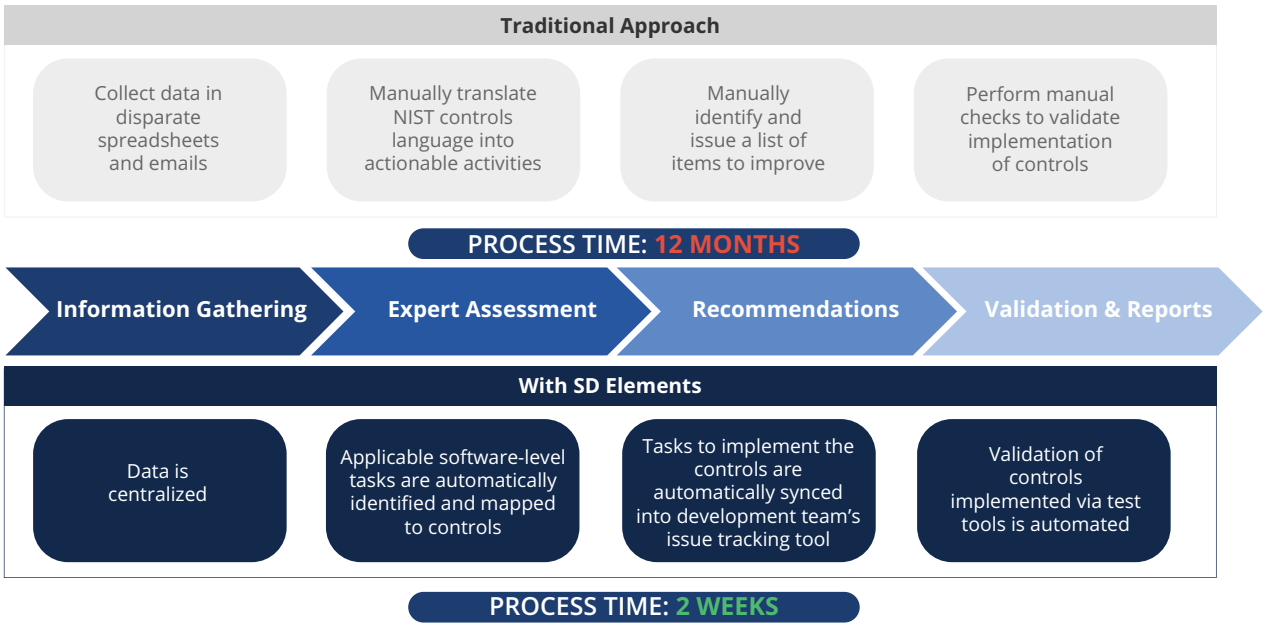
96% Reduction in Compliance Process Time

Security is critical for application development across the U.S. federal government agencies to prevent cyberattacks. Naturally, the federal government has a strict framework for authorizing applications that operate on their network and entities have to obtain an Authority to Operate (ATO). However, the ATO process can take months as organizations have to identify all possible risks and monitor controls.

SD Elements helps your organization manage the ATO process by supporting all three ATO pathways – RMF Now, Fast Track ATO and Ongoing Authorization or Continuous ATO (cATO).

U.S. Department of Defence Software Factory

Key aspects of the software factory's process to build an ATO package are summarized as follows:



With SD Elements as a key enabler, the software factory was able to reduce the time required to obtain an ATO from 12 months to 2 weeks — achieving an **operational efficiency of roughly 96%.**

Further, SD Elements allows the DOD software factory to achieve cATO for ongoing software delivery by enabling the assessment team to easily trace compliance with security standards.

SD Elements is used by other federal government agencies and programs in a similar manner, tailored to each assessment teams' requirements and technology stack.

RISK ASSESSMENT

Risk assessments are a core part of risk management in an organisation. As digital transformations continue to grow, so will the need for risk assessments, delivered at a pace that matches the speed and scale of development. This presents a challenge as scaling risk assessments requires the expertise of scarce and exhausted subject matter experts.

Risk assessments also rely on the knowledge and experience of the assessors, which can result in inconsistent results and lead to an incomplete view of risks. Moreover, risk assessments are typically manual and can take weeks, and in some cases months, to complete. Basically, it is an expensive process that slows time to market.

With SD Elements, organizations can streamline risk assessment processes, such as the identification of weaknesses and controls and automated delivery of controls to the issue tracking tool.

The benefits for the customer? Savings in time and costs, increased velocity of assessments (i.e. number of assessments in a given period), and improved quality and consistency of risk assessment outcomes.

Client Spotlight

90% Reduction in Risk Assessment Time

Key aspects of the risk assessment process used by a client in the financial services and insurance sector are summarized as follows:

1. An insurance and financial services client reduced their risk assessment time from 10 days to 1 day by automating some of their security processes with SD Elements. By automating more processes later in the cycle, they're expecting to reduce the time taken from 28 days to 1 day, which is a significant drop by 96%.

2. This has not only increased their ability to scale their process and meet their internal policy requirements for risk assessments, but has also resulted in a simplified process and increased velocity.

Gaining Buy-In from Business Leaders

Creating a program that balances speed of software delivery and risk management is a critical competitive differentiator for businesses. Most organizations do not have an existing budget to pay for this initiative and often have to reallocate budget from other areas. We are listing some strategies our clients have used to gain buy-in for SD Elements.

Use Agile or DevOps program funds: Many organizations fund large-scale Agile and/or DevOps initiatives. SD Elements automates proactive processes, which is a critical success factor to these initiatives in security conscious and/or heavily-regulated companies. Our clients have been successful in using discretionary funds from these programs to invest in SD Elements.

Reallocate contractor, services and/or headcount budget for proactive security processes: Many organizations contract out or hire security analysts, architects, and consultants to perform proactive processes such as threat modeling, risk assessments, privacy by design, etc. Reallocate part of this budget for tools that automate these processes so that you are getting wider reach from your experts rather than having to hire more of them.

Look at your mix of proactive vs. reactive security processes: Most organizations have line items for several different reactive security testing processes. Contrast the budget you have allocated to “reactive” security testing tools vs. “proactive” security (i.e. before code is written). More and more companies are looking at balancing these activities by critically reviewing their reactive tools, for instance, how much value are you getting from dynamic analysis tools? How much overlap do you have between various tools? The end result may be a shift to proactive tools like SD Elements.

Use security awareness budget: Many organizations have separate budgets for security awareness training. SD Elements contains both instructions on security practices and embedded training videos with Just-In-Time Training (JITT). Security Compass can also bundle in e-learning offerings, including standard security awareness training. Companies can leverage the security education budget to pay for SD Elements.

Use compliance budget: Some organizations have more flexibility with allocating budgets to meet compliance needs. Consider your current compliance status with respect to security & privacy by design as they relate to PCI, GDPR, CCPA, FFIEC requirements, etc. If you are “out of compliance” , use this to obtain funding for SD Elements as it will be a more cost-effective option, in most cases, than using additional personnel/contractors.

Use GRC budget: Governance, Risk and Compliance (GRC) programs are often large and multi-faceted. Their primary value is better risk management. Considering the business value of SD Elements related to improved time to market and traceability of risk/compliance, find out if GRC budget can be trimmed back to invest in SD Elements. SD Elements can be positioned to provide the “operational/day-to-day” components of DevSecOps that feeds data into your GRC solution via configurable integration.

Introduce a chargeback model to the Line of Business: Large software development projects are often expensive. The true value of faster time to market through proactive process automation is of benefit to the business. Consider having each line of business pay for SD Elements for their applications. The cost for one application is typically a small fraction of their budget.

Convince the C-Suite to Invest in Cybersecurity

If you want to learn how you can put a strong business case for embedding security that drives real-world results, please connect with us. We are also working on a new guide to help you frame budget issues, identify key metrics, calculate company specific savings and return on investment for implementing a more mature DevSecOps program. Get in touch with us to learn more.

Security Compass

Go fast. Stay safe.

Security Compass, a leading provider of cybersecurity solutions and advisory services, enables organizations to adopt balanced development automation for rapid and secure application development. With their 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. In addition, they offer advisory services on how organizations can embrace emerging technologies like cloud to strengthen their security posture. Security Compass is the trusted solution provider to leading financial organizations, technology enablers, and renowned global brands. The company is headquartered in Toronto, with offices in the U.S. and India. Follow Security Compass on Twitter @securitycompass or visit them at securitycompass.com to learn more.

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

CALIFORNIA
995 Market Street
2nd Floor
San Francisco, CA
USA 94103

NEW JERSEY
621 Shrewsbury Avenue
Suite 215
Shrewsbury, New Jersey
USA 07702

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

1.888.777.2211
info@securitycompass.com
www.securitycompass.com

@SECURITYCOMPASS
SECURITY COMPASS