Building a Business Case For Secure Application Development

SecurityCompass

The Dilemma:
Application Security or Software Delivery Speed

Technology is changing at a rapid pace, making it necessary for organizations to constantly innovate and introduce new features to their products. While delivery speed is important, compromising on application security can have a disastrous impact on your business.

Organizations are under intense pressure to balance software delivery speed with security. Doing both is not easy — so many must choose between speed and safety. If you choose security, you will likely extend the development life cycle and delay product releases. On the other hand, without embedding security in your applications, you are, or your customers are at risk of a data breach.

This continuous tussle between security and speed makes it difficult for security teams to sell their case to business leaders. In this guide, we will help you to build a strong business case for automating security activities that reduces cost while minimizing risks.

Fast & Safe Application Development

How can you be both fast and secure?

Developer-centric Threat Modeling (DCTM) enables organizations to build software as safely as if being built with guidance from security experts and nearly as fast as if they were being built without security guidelines at all. By automating key portions of proactive security processes, such as threat modeling and preparation of secure code guidelines, organizations can not only improve product security but also accelerate software releases. It's a win-win.

What Matters to Your Audience

To sell the benefits of proactive software security using Developer-centric Threat Modeling, you need to assess what matters to the business leaders with ultimate responsibility for the decision. If you talk about compliance with your CTO, you will likely be redirected to the CISO.

DATA-DRIVEN DISCUSSIONS

Defining performance metrics and talking about the impact through numbers can really make a difference to your discussions with the C-suite.

Pain points of technology executives

- Developer productivity declines from unwieldy and inconsistent secure software guidelines (e.g., spreadsheets and missing or unnecessary security controls)
- Excessive time required to demonstrate compliance with internal security and risk policies and external standards and regulations
- Delays in product release and higher development costs due to software vulnerability remediation time and effort
- Enforcement and scalability of secure coding guidelines
- Technical debt and risk from releasing unsecured software

Pain points of risk executives

- Productivity of scarce security resources
- Lack of visibility into the security and compliance state of software across the entire software portfolio
- Costs and scalability of implanting and enforcing secure coding guidelines
- Lack of security culture
- Demonstrating adherence to internal and external security policies and compliance standards

Measure Results From Security Investments

Nothing can help better to achieve buy-in than showing results from your current or past projects.Identify the metrics that will help you to make a strong case. For a CFO, you can talk in terms of cost savings and ROI. Your CISO would want reports on the risk posture and compliance status. TheCTO, on the other hand, has a focus on the overall effectiveness of technology — so talk about the impact of security on growth.

Key Metrics to Track

- Cost savings
- Compliance reporting
- Remediation costs
- Time savings

Specific Use Case Metrics

We are using four use cases to talk about the metrics and the quantifiable benefits you can realize by using Security Compass to proactively build security into software. Based on internal analysis and client data, we have collated these metrics from the use of our SD Elements platform.

THREAT MODELING

Traditional threat modeling processes are time-consuming, inconsistent, and can be applied to only critical applications. When you automate these processes, you can benefit significantly and scale this to your entire application portfolio.entire application portfolio.

80% **Reduction in Threat Modeling Time**

SECURE SOFTWARE DEVELOPMENT

Many organizations write code and then identify vulnerabilities that can be expensive and delay releases. By "shifting security left" and ensuring code is developed securely from the beginning, you can realize:

90% **Reduction in Time to Create Security Requirements**

COMPLIANCE

Regulatory standards and internal corporate policies are constantly updated. Automation can quickly translate complex regulations into simple tasks for developers. How much time can you save?

96% **Reduction in Compliance Process Time**

Your Business Case: Driving Profitability and Growth

In most discussions, the value of security is limited to ensuring compliance with regulatory guidelines for avoiding a data breach. To gain buy-in from business leaders, security teams need to drive home the point that lack of security can impact the bottom line.

We all know security breaches can lead to irreparable damage but quantifying this damage can make a difference. Product release delays happen quite frequently because of software vulnerabilities, but are you bringing the cost of delays to your discussions?

Average financial cost of a breach

US$4.24

MILLION

Cost difference where remote work was a factor

US$1.07

MILLION

Time taken to identify and manage a breach

287 DAYS

Source: 2021 Cost of a Data Breach Report, IBM

We just need to change our vocabulary to focus on the business value that security brings.

Focus Area

- Faster time to market
- Improved developer productivity
- Quantifiable cost savings
- Deliver more secure software
- Portfolio-wide visibility to risk

Gaining Buy-In from Business Leaders

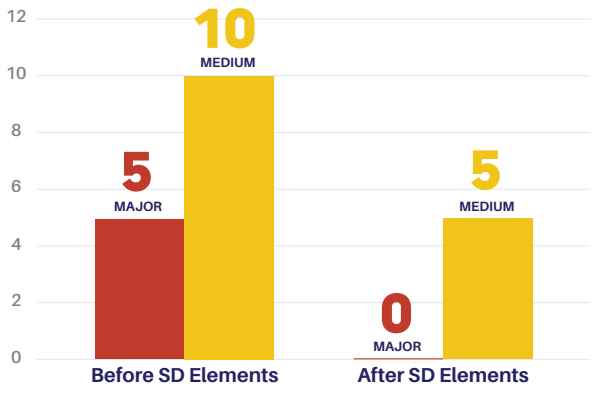
Creating a program that balances the speed of software delivery and secure development is a critical competitive differentiator for businesses. But convincing the C-suite is not always an easy feat especially in times of increased competition. We are listing some strategies our clients have used to gain buy-in for SD Elements.

- Reallocate contractor, services, and/or headcount budget for proactive security processes.
- Consider allocating your budgets from reactive security testing programs to proactive software security.
- Your current compliance budget can be easily directed toward proactive software security programs that ensure compliance.
- In heavily regulated industries, organizations fund large-scale DevOps initiatives in which security is a critical success factor.

Impact of Proactive Software Security

Proactively integrating security into software development minimizes vulnerabilities in your products. This not only makes your products more secure from the beginning but also reduces the time and money spent on remediation of flaws.

Based on a Forrester Total Economic Impact study commissioned by Security Compass, the composite organization realized significant cost savings. These figures can be cited as a major benefit for proactive security.



Reduced high-risk vulnerabilities by 100% and medium-risk vulnerabilities by 50% using SD Elements.

Overall cost savings for 75 applications: US$5.6 million
Freed-up 40% of security experts' time

Based on a 2019 study by Security Compass, SD Elements reduces 100% of the high-risk vulnerabilities and 92% of medium-risk vulnerabilities found in pen tests.

Building security early in the process has become more important today as digital transformations take every industry by storm and customers become more aware of security. Maintaining your competitive edge is as important as your brand image; therefore you must balance speed with safety.

If you want to learn more about how you can benefit from proactive software security, please download our cost savings guide. We would be pleased to share cost savings data from our engagements and provide you an ROI template to calculate benefits. Get in touch with us.

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 howorganizations 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