Security Compass

SD Elements in the Modern Enterprise

SD ELEMENTS: FROM POLICY TO EXECUTION

January 2019

CONTENTS

SD ELEMENTS - FROM POLICY TO EXECUTION 3

INTRODUCTION 4

COST SAVINGS AND RISK REDUCTION 5

TECHNOLOGY 6

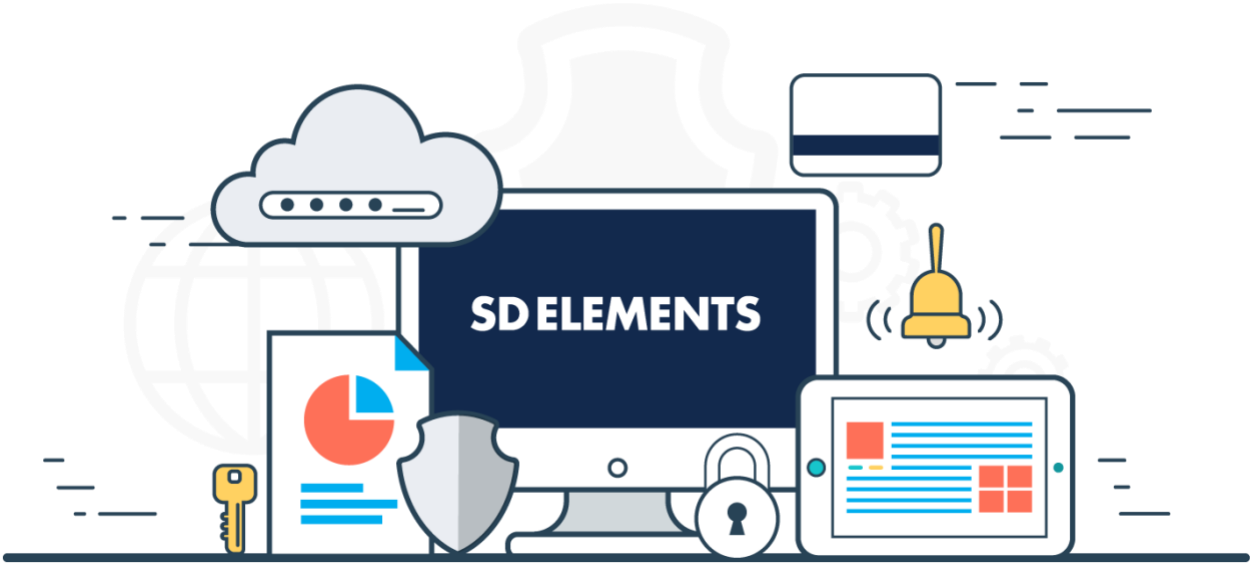
USE CASES FOR SD ELEMENTS 7

WHOLE APPLICATION PORTFOLIO COVERAGE 9

ENTERPRISE DELIVERY SERVICES 9

WHY SECURITY COMPASS 10

SD ELEMENTS - FROM POLICY TO EXECUTION



SD Elements manages requirements throughout the software development lifecycle, for every application in an enterprise's portfolio. Common 'Use Cases' for SD Elements include:

- Managing Security Activities in SDLC
- Application Security: "Shift Left" and "Build Security In"
- Privacy: Data Protection by Design and Default
- Compliance
- Scalable, Modern Threat Modeling
- Quality Assurance
- Just-in-Time Training
- Force Multiplier for Security Architects and Privacy Engineers
- Deployment Security for AWS, Azure, Docker, etc.

INTRODUCTION

"SD Elements manages requirements for applications." This simple statement has many implications for the modern enterprise.

Security & privacy are critical. What kind of assurance do you have that your software is secure?

Scan-and-fix isn't working. Once you find a security flaw in your software, how do you systematically prevent defects from reoccurring?

How can you **systematically build security & privacy** into software in a way that scales?

Application requirements are no longer the exclusive territory of the software engineering organization. Stakeholders from across the business have various interests for keeping applications secure, private, and compliant with regulatory requirements.

Used by some of the world's leading financial institutions and technology companies, SD Elements is a scalable policy-to-execution platform that helps multiple teams build, coordinate, and manage application security, privacy, and compliance controls. These controls can then be applied to applications residing in different parts of the business (Products, IT Apps, Third Party Applications, and M&A targets).

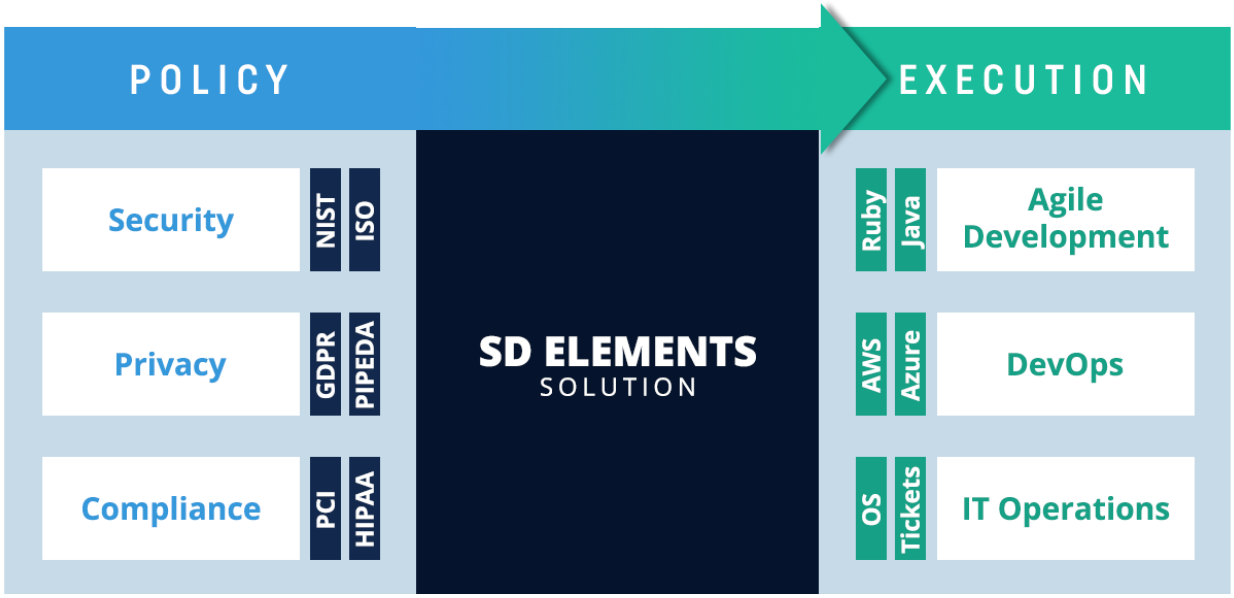


Figure 1: SD Elements orchestrates the requirements of many stakeholders and facilitates collaboration with application owners across the business (including in-house developed applications and third-party applications).

SD Elements accelerates the pace of engineering, improves collaboration between teams, enables faster SDLCs like Agile and DevOps, and decreases risk. SD Elements helps solve difficult security, privacy, and compliance challenges faced by many organizations:

Business Alignment
SD Elements helps prioritize security & risk needs alongside business needs.

Risk Management
SD Elements provides a clear view of the application, network, and operational risk.

Privacy & Compliance
SD Elements enables businesses to build-compliance-in and achieve privacy by design.

Collaboration Between Teams
SD Elements facilitates bi-lateral communication between business, security, and risk & compliance teams.

Security & Awareness Skills
SD Elements scales the distribution of expertise and training to many teams.

Shift Left
Build in security and address privacy at the earliest opportunities. Avoid remediation work and costs.

COST SAVINGS AND RISK REDUCTION

Accelerated Development

Historically, managing "Non-Functional Requirements" has burdened software engineering teams with long to-do lists and provided no practical guidance for completing the identified tasks. In contrast, SD Elements accelerates development by pairing requirements with specific solutions, language-specific "How-Tos," code samples, and test cases.

Reduced Risk

There is a common misconception that scanning with SAST and DAST is sufficient to ensure application security. While these tools are good at verification, research shows significant gaps in scanner coverage. SD Elements starts much earlier in the SDLC and helps teams identify which activities must be performed and what mitigations must be implemented to build safe, secure, and compliant software. Not only is the coverage better, but the guidance is provided at a more appropriate time (before the application is written).

Saving Money via Build vs. Buy

Developing and maintaining a homegrown system to manage application requirements is very costly. Custom features and enterprise integrations need to be continually added and maintained by a development team. Knowledgebase content must be developed and then frequently updated by highly-paid and often unavailable experts in software security, compliance, privacy, and operational security.

On the other hand, by leveraging SD Elements, your team can immediately access years of existing development, plus several dozens dedicated software engineers and subject matter experts who continuously improve the platform and the knowledge base. It is possible to build a customized solution on top of SD Elements using the extensive APIs and enterprise integrations. We can even help you.

TECHNOLOGY

SD Elements is fully equipped to support the key capabilities of an application security program.

An Extensive Knowledge Base

The knowledge base includes significant content for application security, privacy, compliance, and operational security (such as AWS, Azure, and Docker). It can easily be customized to your business needs and technology frameworks.

An Expert System

A brief questionnaire, paired with simple and customizable rules, automatically identifies the controls required for each application.

Application Lifecycle Management (ALM) Integration

The required controls (and their solutions, HowTos, and code samples) are synchronized bi-directionally and in real time with ALM tools (such as Jira). The guidance itself accelerates the software engineering process, while the ALM integration removes any workflow friction.

Validation Workflow and Scanner Integrations

Integrations with security testing tools (e.g., SAST and DAST tools like Checkmarx, Veracode, Fortify, WhiteHat, AppScan) automate validation of each control and support DevOps and CI/CD pipelines. Controls that didn't or can't be automatically validated are highlighted by SD Elements. Test requirements are compiled by SD Elements for manual verification of these controls by QA, security, or audit teams.

Audit and Compliance Reporting

It is easy to generate reports against published security, privacy, and compliance frameworks (GDPR, PCI, ISO 27001, NIST 800-53, etc.) and to build custom policies based on the needs of your business.

API

SD Elements is an information brokerage platform that coordinates activities, shares knowledge, provides oversight, and automates numerous workflows. The REST API and service-oriented architecture ease integrations and leverage your existing investment in tools like RSA Archer, SIEM, Defect Tracking, and so on.

Risk Reporting

The Risk Dashboard feature provides quick visual summaries and reports about the applications and projects in your organization so you can quickly see their compliance status with the risk policies that your organization has set as a corporate standard.

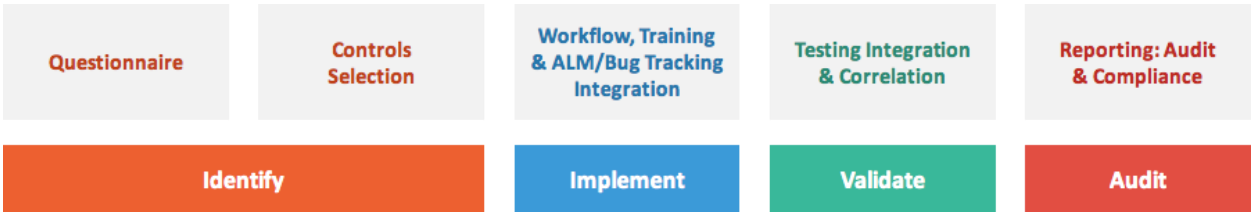


Figure 2: SD Elements workflow enables complex orchestration and collaboration between stakeholders.

USE CASES FOR SD ELEMENTS

Managing Security Activities in SDLC	Many organizations risk-rank applications using SD Elements and then apply appropriate SDL activities (architecture review, threat model, privacy assessment, penetration test).
DevOps Enablement	SD Elements automates many of the repeatable security and compliance activities (such as threat modeling and requirements management) in the SDLC, allowing these practices to fit into rapid and continuous release cycle methodologies. It is also proven to drastically reduce the number of findings from SAST+DAST "scanner" tools, allowing the release to keep moving without having to deal with hours of remediation work.
Application Security: "Shift Left" and "Build Security In"	Prevent application security vulnerabilities from being introduced and reduce your engineering teams' workload by providing tailored and actionable guidance early in the SDLC.
Privacy: Data Protection by Design and Default	It is not enough to build an application which protects your customers' data — we are now required by law (e.g., EU GDPR's Article 25) to demonstrate that the system implements "Data Protection by Design and Default." SD Elements tracks the determination of which privacy controls are in scope for each application, the implementation of each control, and the verification each control. It creates an audit trail and a "system of record" which allows you to demonstrate due diligence and "Data Protection by Design and Default."
Compliance	An application may need to adhere to a dozen compliance standards, but there is no need to go through a dozen audits. SD Elements can present the security and privacy posture of an application in the taxonomies the auditors need and reduce their impact on development teams by de-duplicating requirements.

Threat Modeling	Manual threat modeling is a strong best practice but it is time-consuming and it requires expert resources. SD Elements streamlines the process by automating the repeatable domain-agnostic threats (the "low hanging fruit"), allowing your team to focus on higher-level analysis.
Quality Assurance	QA and Test teams can leverage standardized testing guidance, ensuring a high level of consistency and cross-training among the teams. This guidance can be customized according to your technology stack.
Just-in-Time Training	Computer-Based Professionally-Developed Training micro-modules on specific topics are delivered directly to the developers who need them, accessible through the ALM, at the exact moment they are required.
Force Multiplier for Security Architects and Privacy Engineers	Finding it difficult to hire security experts? Allow your existing experts to accomplish more by leveraging automation. They can tailor the SD Elements Questionnaire, Rules, and Knowledge-base to virtually attend to product planning, feature planning, and sprint planning meetings.
Deployment Security	Do your teams use AWS, Azure, or Docker Containers? SD Elements provides deployment and hardening guidance for applications built on these platforms.

WHOLE APPLICATION PORTFOLIO COVERAGE

SD Elements supports application requirements for many different kinds of applications.

In-House Development
'Shift Left' to build security and privacy into your applications. Support Waterfall, Agile, DevOps, CI/CD, and any mix of these across your enterprise.

3rd Party COTS and SaaS
Vendor Risk Management traditionally has a blind spot when it comes to managing application security and privacy risk.

Contracted Application Development
Ensure that security, privacy, and policy requirements are addressed in contracts with outsourced development teams.

Mergers & Acquisitions
Quickly assess technical debt and risks from new applications being introduced via M&A activity.

ENTERPRISE DELIVERY SERVICES

We offer a proven implementation methodology to ensure successful adoption of SD Elements. Working together with your team, we help develop processes and integrate tools, so that you can meet the compliance standards in a cost-effective manner. These are categorized into the following high-level services:

- **Process Design & Project Planning:** in this stage, a project plan is created and success metrics are established. Executive buy-in is obtained and change management planning is done. Process design is facilitated, teams and champions are identified, and a rollout plan is created.
- **SD Elements Enablement** (i.e., Technical Implementation)
    - Configuration of roles (global and project-specific), business unit workflow options, notification settings, custom statuses, and risk policies. Enterprise integrations setup including SSO, ALM, SAST, DAST and CI/CD (e.g. Jenkins)
    - Localization of Corporate Content (addition of custom content if required): remove or hide unused content, apply corporate terminology, review and update 'Frequently Customized' tasks, create custom compliance to report against required tasks, and add organization-specific content for process tasks.

- **Training of Subject Matter Experts/End Users on Our Solution:** we train for 5 different roles, including System/Server Admin, Software Admin, Content Admin, Project Admin or 'SD Elements Process Champions' (# of persons scales with # of applications), and End Users (teaching a self-serve model for using eLearning, documentation, and in-app tips).

- **Organizational Change Management:** we create user guides and FAQs, offer onboarding assistance for ~5 apps (which includes an introductory demo of SD Elements, answering the survey with our clients, an initial review of compiled controls for the project, and syncing outstanding work to their ALM).

WHY SECURITY COMPASS

Security Compass believes in a world where people can trust technology, and it is our mission to help customers proactively manage cybersecurity risk, without slowing down business.

Contact us at info@securitycompass.com

Security Compass

securitycompass.com

twitter.com/securitycompass

linkedin.com/company/security-compass

