WHITEPAPER

# Complete Guide to Using SD Elements for Cloud Migration

Security Compass

# We're all moving to the cloud

Companies of all sizes are accelerating their digital transformation efforts to streamline IT operations and lower overhead. According to IDG's 2020 Cloud Computing Survey, 92 percent of organizations have an IT environment at least somewhat in the cloud today. This makes sense. Moving to the cloud alleviates organizations from the burden of purchasing, expanding, and maintaining physical infrastructures such as servers, storage, and network devices.

For all its benefits, moving to the cloud can also introduce new threats and risks. Organizations that simply reinstall internally hosted applications on cloud platforms open themselves up to well-established weaknesses that adversaries can exploit. One consistently exploitable attack vector is server misconfigurations. With applications in the cloud, a misconfigured cloud storage bucket can expose sensitive data to anyone looking for it (even if you are Microsoft).

- Personal data of 198 million voters was exposed on an unsecured Amazon Web Services S3 bucket.
- A cloud storage bucket managed by the defense and intelligence contractor Booz Allen Hamilton exposed classified geospatial intelligence.
- Nissan leaked source code and other intellectual property through a Bitbucket Git server with the default credentials of admin.

How common is this? The 2021 Verizon Data Breach Investigation Report found that within the Information industry (including software publishing and data processing) misconfigurations were by far the leading error in breaches, far surpassing programming errors by developers.

## Threats change when you're moving to the cloud

To be clear, a cloud environment is not inherently less secure than an internally managed environment. Cloud service providers (CSP) have the resources (spread across their customer base) to harden their environments, monitor for threats 24x7x365, and employ extensive security controls. However, not every deployment includes all those services across all applications.

The problem goes beyond configuration issues and requires a different approach to securing applications and infrastructure. Cloud providers use a "shared responsibility" model for security. They provide and manage the hosting facilities, physical hardware, and network infrastructure, while cloud users deploying applications are responsible for secure coding. Other aspects of application security, however, vary with the CSP and its pricing model. Some may provide firewalls and identity and access management (IAM) services, while the user is responsible for firewall rules and managing the IAM permissions.

When building applications that will run on a CSP platform, organizations must consider these additional responsibilities and understand clearly whether the CSP employs appropriate controls for each application. The European Network and Information Security Agency

(ENISA) publication "Cloud Computing. Benefits, risks and recommendations for information security" describes almost two dozen discrete risks across policy and organizational, technical, and legal categories. These include:

- **Governance:** Cloud providers monitor and manage the hosting facilities, leaving the application developers dependent on the policies, procedures, monitoring, and reporting of the cloud provider. Organizations deploying applications subject to regulatory oversight must be sure the CSP can provide detailed reporting and logging information needed for standards such as PCI DSS. Similarly, if a critical application requires special host configurations for hardening, the CSP must be able to support such configurations and change management procedures.

- **Multi-tenancy and Isolation Failure:** Two defining features of the cloud are shared resources and multi-tenancy. By sharing computing resources across multiple users clouds allow rapid scaling without requiring application owners to maintain permanent resources for peak capacity. If not managed properly, this can lead to "guest-hopping" attacks where one tenant has access to another tenant's resources or data.

- **Insecure or Incomplete Data Destruction:** Many regulatory standards and organizational policies require the secure destruction of data that is no longer needed. In a cloud environment, that data may be on shared resources including disks, databases, and other storage devices. "Wiping" these resources is often not an option.

- **Changes of Jurisdiction:** Many providers maintain facilities in multiple geographic locations to provide redundancy and continuous operations in the event of outages or a natural disaster. Data is subject to laws and data disclosure regulations in each of those jurisdictions. Tracking this in secure coding standards for each application can be challenging.

## Translating regulatory standards into actionable security controls

Forward-looking organizations understand they need to account for changing responsibilities and technology stacks and apply controls to safeguard data and systems. To ensure proper security, many organizations have processes in place for classifying applications. Many also have secure coding standards and controls to account for critical applications and regulatory demands.

Simply having policies, however, does not ensure that those policies are followed and enforced across each application and system. Translating regulatory standards into actionable security controls is complicated for a single project. Manual and homegrown tracking systems suffer from several shortcomings.

- **Consistency of identifying risks:** Manual methods are only as effective at identifying risks as are the employees reviewing the applications and systems. An individual or team with less experience is likely to miss threats obvious to more experienced individuals or teams. A team under pressure might take shortcuts that would not be advisable in the absence of that pressure. Consistency can be difficult even when using written questionnaires, as answers to

questions may not be clear or may require narrative answers, complicating the assessment process.

- **Consistency in applying controls:** Standardized controls help organizations scale their security programs. However, manual assessments often result in inconsistent controls for any given threat. Written policies can help, but remembering each use case and correctly mapping "official" controls is dependent on the diligence and experience of each employee.

- **Scalability:** The shared responsibility model for the cloud can be different for each application and cover the infrastructure, metastructure, infostructure, and applistructure layers of the environment. While a team of senior security, compliance, and development professionals can conduct an effective threat model or risk assessment, these resources are scarce in even the largest organizations. When attempting to assess hundreds or thousands of projects and CSP policies, manual tracking methods quickly break down.

- **Auditability:** Reporting for current security posture can be difficult with manual methods that rely on spreadsheets or shared documents. Without adequate change control features, these provide poor evidence of compliance with corporate policies and regulatory standards.

## Balanced Development Automation

SD Elements' Balanced Development Automation platform solves the problem of complicated regulatory standards, "shared responsibility" models, and secure coding guidelines — at scale. It provides a centralized platform to automate threat modeling and assessments and translate threats into clear, actionable controls that can be implemented by the DevSecOps team.

- **Consistent:** SD Elements starts with a survey to describe the software project for development, governance, and/or security teams. This includes the technology stack and frameworks, deployment environment, shared responsibility models, and dozens of regulatory standards to which the application may be subject. From this, SD Elements generates a complete list of known threats to those characteristics of the project.

- **Cloud aware:** SD Elements understands the cloud environment and its threats. It translates the threats inherent to the project's technology stack and deployment environment into controls to satisfy secure coding standards for each project. This includes:

  - **Cloud services configurations:** Each service in a cloud deployment, installation, and maintenance requires specific configurations to minimize risk. SD Elements anticipates these threats, provides mitigating controls, and assigns controls and test validation plans to personnel. Threats and controls include Identity and Access Management (IAM), Storage Services, Domain Name Services (DNS), Notification Services, Key Management Services, and Load Balancing.

- **Mapping to regulatory standards:** To ensure compliance and simplify audits, SD Elements' content library includes standards and controls from all over the world, and translates these requirements into actionable tasks, including code samples and test plans.

- **Support for cloud frameworks:** SD Elements supports security frameworks and standards. This includes the Cloud Security Association's Cloud Controls Matrix (CCM). The CCM provides over 130 security controls across 16 domains, including application and API security, audit assurance, encryption and key management, and data security and information lifecycle management.

- **Scalable:** SD Elements automates threat modeling for applications moving to the cloud, allowing consistent and accurate assessments. While time-consuming manual threat models are warranted for an organization's most critical applications, up to 90 percent of the threats to an application are a function of the programming language, frameworks, and other aspects of the application's technical stack.

- **Auditable:** SD Elements provides a centralized and controlled environment for recording all activity regarding the threats, controls, and mitigation efforts for each software project. If an auditor requests a demonstration of which controls 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 having to interrogate software engineers.

# How to use SD Elements

### Profile your application

SD Elements' survey tool automatically characterizes the technical stack of an application including all cloud attributes. If your company has common or standard technology stacks, you can create "Profiles" which automatically apply a predefined set of answers to a project's survey.

For example, you can create a profile named "Acme AWS App," which automatically includes specific AWS services, Java and Java EE, a database management system, and other components to the stack. This greatly decreases the time required by your DevOps team to start modeling their projects in SD Elements.

### Classify the application and apply policies

You can configure SD Elements to classify your cloud applications based on a risk level derived from the information gathered in the project survey. You can also mirror your own risk classification scheme with advanced formulas in SD Elements.

Each classification can be associated with one or more "policies." These policies define the level of rigor your team should apply to implement security and compliance measures. For example, you can specify that you want developers to focus only on high-priority tasks that are in scope for GLBA or ISO 27001.

## Create automations & notifications

SD Elements provides your DevOps teams with a self-service interface. However, there may be times when you want to involve a security architect, enterprise architect, or compliance expert. For example, you may want to have a privacy expert involved in any project that manages sensitive personal information.

SD Elements enables this through "tasks." In this example, the task would require a privacy expert's review whenever "Sensitive PII" is selected in the survey. You can then have that privacy expert "subscribe" to the project and be notified every time a project is created that requires their expertise.

## Integrate SD Elements into your workflow

SD Elements supports extensive integrations. A common integration is to synchronize SD Elements tasks automatically with issue trackers like JIRA or Microsoft Azure DevOps, allowing DevOps teams to consume content directly from their tool of choice.

SD Elements also integrates with Application Security Testing tools such as Veracode, Checkmarx, and Fortify to verify and/or close tasks automatically if scans indicate the required work has been completed.

In addition, you can configure CI/CD tools such as Jenkins to fail a build if the mandated minimum subset of tasks from SD Elements are not completed and/or verified.

## Workflow

Once initial setup is complete, a project team responsible for migration can use SD Elements to help ensure they meet minimum security and compliance requirements.

### Step 1: Information gathering

Select a profile and then answer more specific questions about the application's intended use and technical stack to generate a tailored set of tasks for the project, based on the application's inherent risk classification.

### Step 2a: Expert assessment

Tasks will be added according to the rules-based logic and classification scheme you configured during the initial setup. Tasks can include sample code and recommended test plans.

### Step 2b: Manual additions

If you set a trigger to involve an expert because, for example, the project will handle sensitive PII, that expert can review the list of relevant tasks and, if required, add their own specific recommendations following a manual assessment of the application.

### Step 3: Recommendations

SD Elements exports the tasks into issue tracking systems like JIRA or uses the native interface to assign tasks to DevOps teams.

### Step 4: Validation

When desired, SD Elements can import test results from scanners to automatically validate whether tasks have been completed.

### Reporting and Auditability

SD Elements includes reporting for several supported regulations including PCI-DSS, HIPAA, PIPEDA, GLBA, GDPR, and other privacy-related standards, along with any custom regulations you add to the system. These reports provide evidence of compliance with corporate policies and regulatory standards, including information about whether tasks are completed, who completed them, and when. When synchronizing with an issue tracker, reports also include links to the specific ticket.

SD Elements also produces a Problem Summary Report showing all issues the system identified, and data about relevant countermeasures.

## Stay Safe. Go Fast.

Moving applications to the cloud can be a daunting project for DevOps teams. New threats and challenges require a different way of thinking about security, and the shared responsibility model requires a clear understanding of the capabilities and controls of the cloud providers.

SD Elements' Balanced Development Automation platform provides teams with the ability to accelerate time to market while ensuring that threats and appropriate security controls are identified and applied consistently. With SD Elements, organizations can build applications nearly as fast as if they were developed without any security or compliance — yet inclusive of critical security controls.

SecurityCompass

Security Compass

# Go Fast. Stay Safe.

Security Compass, a leading provider of cybersecurity solutions, enables organizations to shift left and build secure applications by design, integrated directly with existing DevSecOps tools and workflows. Its flagship product, SD Elements, allows organizations to balance the need to accelerate software time-to-market while managing risk by automating significant portions of proactive manual processes for security and compliance. SD Elements is the world's first Balanced Development Automation platform. Security Compass is the trusted solution provider to leading financial and technology organizations, the U.S. Department of Defence, government agencies, and renowned global brands across multiple industries. The company is headquartered in Toronto, with offices in the U.S. and India. For more information, please visit www.securitycompass.com.


**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