SECURITY COMPASS WHITEPAPER

How You Can Ensure Secure Cloud Migration

Security Compass

Secure cloud migration is a significant challenge for organizations

Cloud migration is a business priority for financial institutions. The benefits can be transformational: faster reactivity, better time to market, improved customer satisfaction, increased productivity, and new cloud-enabled business initiatives. However, risk management and regulatory oversight from institutions like FINRA, the OCC, and OSFI — particularly after the Capital One breach — mean that Financial Institutions need to incorporate security into the entire lifecycle of cloud migration. Gartner suggests that the Cloud Security Architect role can help organizations navigate the complexity of a secure cloud migration. However, this role suffers from the near ubiquitous security talent shortage.

Current testing tools address part of the cloud security problem

Vendors have responded to the challenge of cloud security with a number of tools. Cloud access security brokers (CASB), Cloud security posture management (CSPM), and (CWPPs) all serve key roles in helping secure cloud system access, infrastructure, and workloads.

This however, addresses only a piece of the holistic challenge of secure cloud migration. The applications that are deployed on this infrastructure, particularly "cloud native" applications that take advantage of services, pose a risk to the enterprise. For example, a common but serious flaw in code called Server-Side Request Forgery (SSRF) may have played a key role in at least one well-known cloud breach.

Existing application security tools, meanwhile, play a key role in finding security vulnerabilities but only cover a subset of the kinds of risks a cloud security architect needs to evaluate for a given system. Financial regulators continue to expect financial institutions to perform more rigorous processes like risk assessments, threat modeling, developers' security training, and the establishment of secure coding standards to ensure cloud systems have security & privacy built-in. Yet following these processes, which can take upwards of 20 days to complete in some cases, threatens to erode the very agility that cloud migrations offer.

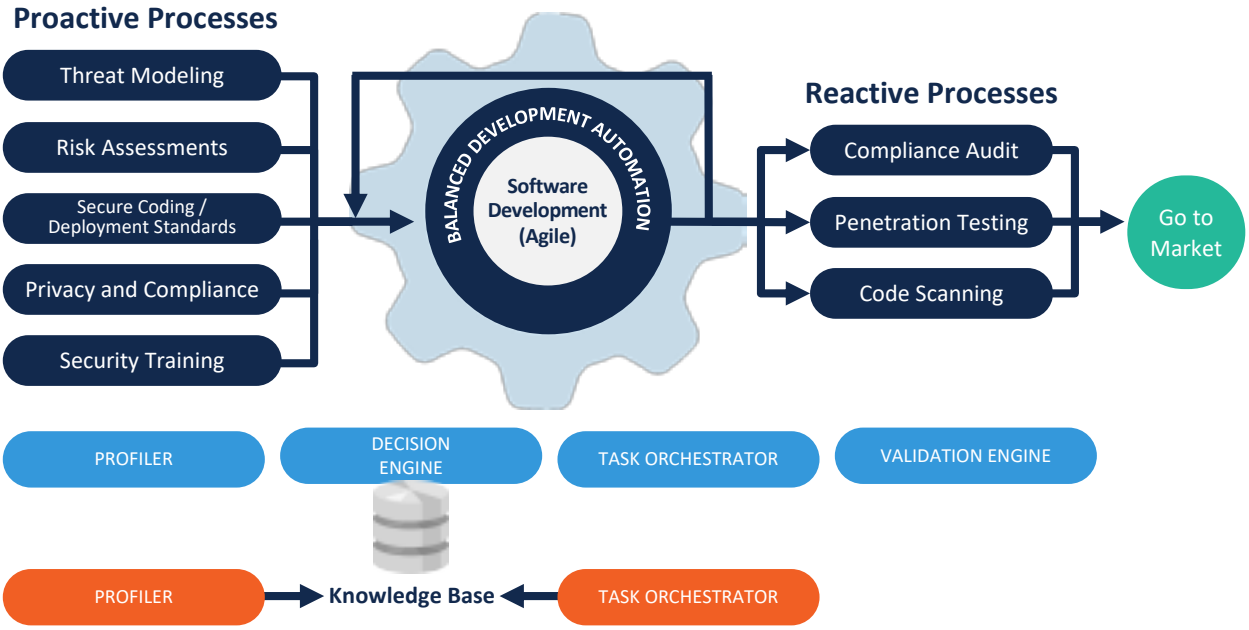
Understanding Balanced Development Automation

Going fast and relying exclusively on security tools that find defects after code has been written is not tenable for financial institutions; the approach sacrifices meeting regulatory requirements in favour of speed. This approach is "fast & risky." On the other hand, following all the processes to embed security & compliance into the design of software sacrifices speed & agility, which is a difficult proposition for business leaders to accept. This approach is "slow & safe."

> **"Balanced development" is the philosophy that organizations must work to preserve business agility while building systems that are secure & compliant. One goal cannot be achieved in a vacuum without the other.**

Balanced Development Automation (BDA) tools help to ensure security and speed by automating key parts of the proactive processes that currently slow down financial institutions.

How BDA tools work:



- Describe a cloud app and classify app according to risk
- Receive hardening and coding standards, mapped to regulatory requirements
- Integrate directly into issue trackers
- Dev teams consume content and create project
- Line 2 can produce reports and review the application portfolio holistically
- Integrate with CPSM and SAST tools

How BDA helps in cloud migration

The role of a BDA tool is to help organizations scale and automate slow, inconsistent, and siloed processes and deliver a consistent set of tailored tasks for teams like development, DevOps, and cloud.

For a cloud migration, the processes & best practices that BDA tools can help automate include:

- **Risk assessments:** BDA tools can help automate translating a description of a system to known information security & compliance risks and corresponding countermeasures.
- **Threat modeling:** Similarly, BDA tools can take a description of a system architecture and define well-known code-level & deployment security issues and corresponding countermeasures.
- **Privacy by design:** Based on the system description, BDA systems can suggest concrete steps to integrate privacy into design of a system.
- **Secure configuration standards:** BDA systems have best practice standards for secure cloud deployments from major Infrastructure as a Service (IaaS) vendors as well as container technologies like Docker & orchestration tools such as Kubernetes. BDA vendors ensure these standards are always kept up-to-date. This allows implementation teams to create infrastructure that incorporates security best practice by design, which they can later verify with CPSA tools.
- **Secure coding standards:** BDA systems include coding snippets across a wide variety of programming languages & frameworks, including cloud native systems. BDA vendors ensure these standards are always kept up-to-date. This allows development teams to write code that incorporates security best practices, which they can later verify with scanning tools.
- **Security training:** Embedded inside of BDA tasks are training instructions and video snippets for junior developers, as well as DevOps and operations teams to learn security & compliance best practices specific to the task at hand.

Using BDA has several advantages over manual approaches:

- **Speed:** By automating & consolidating these processes and best practices, organizations can save 80-90 percent of the typical elapsed time in more manual processes.

- **Integration:** BDA tools can integrate into tools your teams are already using. For example, security & compliance tasks can be delivered directly into Jira or Microsoft Azure DevOps.

- **Consolidation:** Consolidating the above into a single system drastically reduces overhead for line 2 operations teams which allows them to focus on delivering business value.

- **Self Sufficiency:** Giving DevOps teams a tool that they can operate on their own allows the business to rapidly migrate systems to the cloud and build cloud security & compliance expertise through just-in-time training. Over time this reduces the burden on experts.

- **Cost:** Using a system means less reliance on building out a team of costly, scarce experts in several domains.

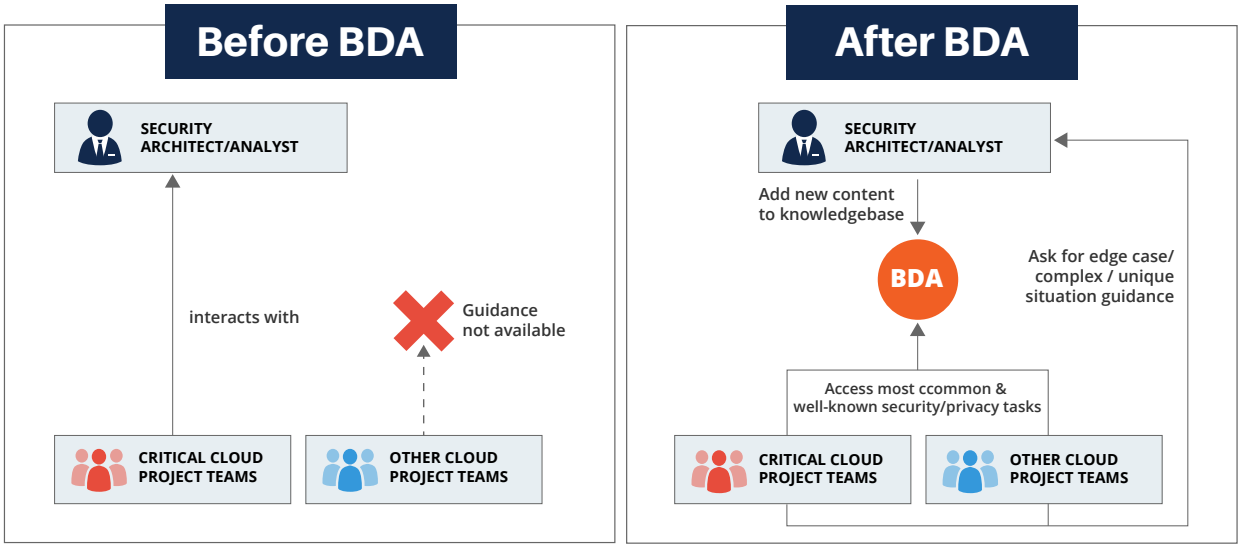
- **Consistency:** BDA systems will deliver a consistent set of results with the same input. Human experts may produce different results based on their relative experience.

- **Auditability:** Every task completed by a developer has an audit trail. Line 2 teams can easily generate reports to satisfy line 3 and external audit requirements.

Two lines of support model

BDA systems have several advantages over an entirely manual approach. Being automated, however, means that there are some limitations to what they can produce. For example, they cannot replicate the nuanced knowledge of a security architect or analyst in identifying very domain-specific threats or risks to a particular application such as potential ways an attacker might manipulate data to transfer funds between accounts on an online banking platform.

Fortunately, hooks for "human support" can be built right into the BDA tool analogous to a multi-tiered support model. The BDA system acts as the first line of support, where development and DevOps teams interact with the system to get specific security & compliance tasks. The BDA system can then use triggers to define when a human expert needs to get involved to add additional contextual analysis. For example, if a system stores particularly sensitive data, the BDA tool can automatically send an email to the privacy team and track whether or not they have assessed the system for specialized risks.



Can you risk your competitive advantage?

Despite the category name being launched this year, BDA tools are not new. Large organizations around the world have been making use of vendor and in-house developed BDA tools for years. Half of the ten largest banks in the U.S. use BDA tools to more rapidly produce software, including cloud applications.

Financial institutions that do not embrace balanced development in cloud migration will either put their brand at risk by being "fast & risky" or erode their competitiveness by being "slow and safe."

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.

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