Agile security in cloud DevOps

It's 2020, and no one disputes two key trends:

01 Cloud is the default solution for almost every new, critical IT project

02 DevOps software development practices are needed to remain competitive in the marketplace.

Cloud has acted as a powerful enabler for agile philosophies in DevOps, untethering them from legacy IT environments and bridging the gap between agile theory and practice. Most large organizations still have a way to go on their cloud and DevOps journey, and among the challenges they face is understanding what it means to manage cybersecurity risks when building software at DevOps speed and cloud scale.

We have all heard the conventional wisdom about the security team and the DevOps team. The pace of DevOps and occasional lack of discipline makes the security team worried, while the DevOps team perceives the security team as slow, inflexible and outdated. And yet, the business desperately needs to rapidly develop new services without exposing themselves to cyber attacks, and the consequences for business reputation and customers trust which follow.

We know the challenges with cloud, DevOps and security. We know what we want to avoid and how we want them to interact in the future. What we need is a set of guidelines for achieving the vision.

Journey	Tired	Wired	Inspired
Cloud	Building new applications in data centers	Developing new applications in the cloud using legacy architecture patterns used in data centers	Creating new applications using cloud native serverless computing, data and object storage services
DevOps	Following Waterfall development patterns with infrequent deployments	Configuring a Continuous Integration/Continuous Delivery (CI/CD) pipeline tool differently for each development team	Transforming the development lifecycle through centralized pipelines and powerful Infrastructure as Code capabilities
Security	Reducing risk by applying security when software code is in production with penetration tests	Minimizing risk by automated scanning of code for vulnerabilities before deployment	Decreasing risk by using automated, low friction scrutiny that is risk calibrated and easily auditable building on integrated security in DevOps processes

Harnessing the potential of cloud to provide a flexible, responsible and scalable business environment also requires us to change our approach to security. The right strategy for becoming a high performing, secure software development organization in the cloud begins with identifying the necessary risk reduction functions to build software. Start examining the Software Development Life Cycle (SDLC) and determine your list of desired capabilities, controls or behaviors across the separate phases. Once identified, the question turns to how best to deliver those outcomes in the cloud. Don't be afraid to tear up some of the old rule book as you do — new ways of working demand new thinking.

Creating the ”golden road”

Step back and imagine you wanted to ensure your organization could identify and react to potentially malicious activity in your applications. Would you create a separate data lake of relevant logs for each of your applications, apply different detection rules, and expect effective detection and response activities? No, because decentralized monitoring is unlikely to deliver mature, consistent capabilities at speed.

For the same reason, when organizations migrate to the cloud, technology leaders should take the opportunity to align their development teams on a common Continuous Integration/Continuous Delivery (CI/CD) pipeline. This 'golden road' practice of embedding this CI/CD pipeline has multiple advantages.

Want Static or Dynamic Application Security Testing (SAST/DAST)? Fuzzing? Want to generate software bills of materials (SBOMs) to have an inventory of open source software in your environment, or the ability to scan containers? A common CI/CD pipeline facilitates a single place for applying these security capabilities before deployment in a consistent, predictable manner. It prevents the manual set up of 'one off' scans that increase costs, time expenditures and slow down developer teams that need to move at DevOps velocity.

An automated CI/CD pipeline is a developer's dream. In the same way that no one looks forward to a security checkpoint in the airport, manual or face to face security team involvement before deploying new code to production is something many developers will go out of their way to avoid. If you can provide this enhanced experience, developer teams should be more motivated to embed security.

The “low friction” approach

The golden road — an automated CI/CD pipeline — is a big change in security mindsets but also offers the potential for a 'shift left' to embed security controls directly into the development life cycle and supporting tooling. The effort to embed all the controls into an agile cloud DevOps process matters — from the code libraries embedding security functionality, to the automated vulnerability and code quality checks, to the controlled rapid and incremental release of production code. It can answer the challenge of keeping technology secure, but also the need to meet product deadlines and optimize costs, which are the priorities of DevOps teams working on business and consumer applications. The mindset shift is critical: it lets security work fluidly in the new cloud environment — and allows for a rethinking of old principles.

New territories

The security team is playing in new territories. Applications designed by DevOps teams to harness the potential of cloud technologies look different in production than legacy applications and are more likely to take advantage of serverless technology, containers and microservices. These technologies can sometimes be unfamiliar to security teams with a whole new lexicon of security components from sidecar proxies, to API gateways and service meshes. Managing the security of the new generation of cloud-native applications will require new skills and an understanding of new architectures.

Nevertheless, security does still boil down to a few key primitives such as asset management and access controls for example. These primitives can be embedded effectively when linked to cloud DevOps processes and a compliance environment which exploits the rich configuration controls offered in the cloud environment.

New rules

The rules are changing. For organizations well on their cloud DevOps journey and ready for another opportunity to reduce risk, chaos engineering is an option for change. Chaos engineering is the practice of introducing failures into production systems to identify weaknesses in complex systems. Taking a leaf from their peers in Site Reliability Engineering teams, the security organization should consider conducting these controlled experiments to identify unknown risks in cloud production systems. Although most security professionals instinctively avoid deliberately introducing failures into live applications, if done right, such tests can provide insights that no development test can —

and really test the interactions between the cloud components that work together to create a resilient system.

New roles

While cloud technology is alluring, leaders can't forget the role of individuals. With security checkpoints and manual code reviews now a legacy of old development models, security teams with less engineering background can focus on or realign to design the security guardrails used by the DevOps teams while providing essential complementary services such as threat modeling, security champions programs and bug bounty programs. Each service is a low friction method for preventing or detecting vulnerabilities in your DevOps teams' cloud applications.

The above changes may seem radical, but keeping in mind the guiding philosophy: when security 'shifts left' in the product lifecycle in cloud environments, security teams can profoundly impact the actual security of the product with less business friction.

There is no threshold for 'achieving DevSecOps' — it's a mode you only realize you're operating in when you look back on the road behind you, and it may take many organizations the better part of this decade to get it right. The most powerful business transformations come from incremental progress over time, letting you embed the culture, building the right processes and ways of working throughout the organization, changing mindsets along the way.

Once the security team is confident that controls are being embedded into application development, they can begin to play a more strategic role. They can start to focus on bigger challenges, such as securing the business rather than just the applications.

For instance, a customer-facing team may assume that new cloud applications they're rolling out to customers need to be secured using a traditional password authentication security template. It might be the job of security to challenge those initial assumptions and help design a new, seamless authentication model that improves the customer experience while still integrating with fraud controls elsewhere in the business to reduce risk.

A pipedream? Perhaps — but some organizations are getting to the stage in which security isn't just part of DevOps — it's part of the company's brand. And in the cloud environment, where development teams can operate with the speed and scale to meet demand, the need for security to be part of the DevOps process is greater than ever.

Caleb Queern
Director, Cyber Security
KPMG in the US
E: cqueern@kpmg.com

Walter Risi
Partner, Cyber Security
KPMG in Argentina
E: wrisi@kpmg.com.ar

Martijn Verbree
Partner, Cyber Security
KPMG in the UK
E: martijn.verbree@kpmg.co.uk

Kyle McNulty
Associate, Cyber Security
KPMG in the US
E: kylemcnulty1@kpmg.com

Dani Michaux
Partner Cyber Security
KPMG in Ireland
E: dani.michaux@kpmg.ie

Katherine Robins
Partner, Cyber Security
KPMG in Australia
E: krobins@kpmg.com.au

David Ferbrache
Global Head of Cyber Futures
KPMG in the UK
E: david.ferbrache@kpmg.co.uk

Dimitrios Petropoulos
Director, Cyber Security
KPMG in the UK
E: dimitrios.petropoulos@kpmg.co.uk

Deepak Mathur
Director, Cyber Security
KPMG in the US
E: deepakmathur@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Designed by Evalueserve.
Publication name: Agile security in cloud DevOps
Publication number: 137040-G
Publication date: October 2020