WHAT IS DEVSECOPS? DEVSECOPS EXPLAINED

The explosive growth of public cloud spending -- $128 billion in 2017, reaching $266 billion by 2021[1] -- coupled with the continued adoption of DevOps continues to shape how organizations deliver innovative solutions to their customers. The ability to design, build, and deploy iteratively at an ever-increasing velocity has not only transformed responsiveness but also sharpened competition. As businesses rush to the cloud, and as cloud service providers roll out more services using new technologies, security becomes increasingly complicated. Security and compliance is as relevant to the cloud as it was (and is) to the data center, if not more so when one considers the scale, speed and complexity which the cloud enables. Enter DevSecOps.

As the name suggests, DevSecOps is the practice of integrating automated security tasks within DevOps processes. It is about going fast ***and*** safe, refusing to accept that the two are mutually exclusive. DevSecOps is about creating a #SecurityFirst culture, where security is a part of

everyone's job: from Developers, to IT Security (of course) and IT Operations alike. Originally a paradigm focused on secure software applications, its scope has since expanded to include security and compliance of cloud services and resources which those applications use. But before we dig in, let's first examine the historical model under which developers and security teams previously operated.

According to some sources, adoption of DevOps software development practices has reached 84% among the enterprise segment[2], those businesses with over 1,000 employees. While software development has transformed itself with the adoption of the Agile Manifesto to produce high-quality code at a faster clip, in many ways IT security practices remained in the waterfall world. In this waterfall model, software security checks are performed at the end of the software development process, if at all, right before the application is to be released to production. As you might well imagine, when priority is placed on code creation instead of security testing, Parkinson's Law[3] (or maybe Murphy's Law?) dictates that development work will consume the time up until the release date. Less thought than necessary is given to security during the development process. And if the release date is to be kept, often there is no time left to fix security issues. Remediation of security concerns, identified at the proverbial 11th hour, requires that the production release date be delayed, aggrieving the development team and line of business owners alike. Unsurprisingly, dev teams and line of business owners become conditioned to circumvent the IT security team, shipping code to production with or without security scans, regardless of the results. DevSecOps seeks to change this dysfunction by making security agile - by continuously delivering security during the software development process. It achieves this goal through a combination of new tools and processes that enhance security of (1) the application software, and (2) the cloud resources which these apps use.

First, to secure the application software itself, security checks are run earlier and more frequently during the software development process, where violations are 10x to 20x less expensive to resolve than at the production release step[4]. By continuously delivering security alongside the continuous delivery of software, security problems are identified before they become hopelessly entangled in the application and therefore more difficult (and costly) to resolve. For example, when an application developer checks-in a new code snippet, a scan can be automatically initiated at build time to check for known vulnerabilities, such as those which might originate from the use of 3rd party libraries. In this way, the developer is testing incrementally along the way for both functionality and security. This combination of automation and continuous delivery of security during the development process makes security scans much less disruptive than a single "big bang" security scan at the end of the development cycle. And of course, just as a developer would fix a compile error, he can fix the security issue as soon as it is flagged. In this manner, fewer application vulnerabilities find their way into production. But that's not the end of the story.

These applications use cloud services and resources, such as storage, serverless compute functions, and database searches. A well-known cloud service provider (CSP) has over 100 such services available. Each **instance** of these services must be correctly configured by the customer for

them to be secure. Benchmarks published by the Center for Internet Security (CIS) detail best practices for configuring these resources securely. Gartner recently projected that through 2020, 95% of cloud breaches will be of the customer's own doing[5], by such things as misconfiguring permissions of cloud storage. A quick online search of cloud data breaches over the last 12 months will support their assertion. As developers ship incremental application enhancements at a weekly, daily, or even hourly continuous delivery cadence - and where IT Operations provide self-service resource provisioning and configuration to those developers - there must be a mechanism to manage the security and regulatory compliance of all these cloud resources or one risks running afoul of regulatory mandates such as PCI DSS, HIPAA, or the EU's upcoming GDPR[6].

In summary, to return maximum value to the organization, a flexible DevSecOps paradigm will not only seamlessly embed security and compliance scans into DevOps processes, but also find and fix security and compliance concerns in cloud services. And it will achieve these ends at a pace which mirrors that of DevOps. The business will innovate more quickly because security is integral to the process, not a hindrance to it. The result will be less risk of data breaches, more secure applications, and continuous security monitoring of cloud resources and services. Implemented well, DevSecOps can deliver a sustainable competitive advantage.

[1] IDC, July 2017, https://www.idc.com/getdoc.jsp?containerId=prUS42889917?

[2] RightScale 2017 State of the Cloud Report?

[3] "Work expands to fill the time available for its completion.", Cyril Parkinson, article in The Economist, 1955?

[4] Code Complete, McConnell, Microsoft Press, ISBN 0735619670?

[5] "Gartner Predicts 2016 and Beyond: Cloud Security"?

[6] The European Union's General Data Protection Regulation becomes effective May 25, 2018, and impacts any business having customers within the EU. Fines for non-compliance can reach €20M or 4% of annual global sales, whichever is greater.?