Why **DevOpsSec** Offers a Better Model for Secure Cloud Applications

DATA SECURITY CONTINUES TO BE A PRIMARY CONCERN AMONG BUSINESS AND IT LEADERS CONSIDERING CLOUD INITIATIVES. In a 2014 IDG survey, 56 percent of the participating IT managers said they cannot embrace the cloud more fully until service providers can guarantee adequate security. The biggest concerns involve an ability to enforce corporate security policies at provider sites, controlling access to data in cloud-hosted environments and the ability to audit providers.

A rapidly evolving threat landscape has exacerbated those concerns. Security vendor Symantec's *2015 Internet Security Threat Report* shows that attackers are moving faster than ever while enterprise response times have not kept pace[1]. The opportunistic attacks of the past have been replaced by highly targeted and persistent attacks.

The data breaches at high-profile brands have received a lot of attention by virtue of their massive size and scope, but organizations across all industries have been affected by the trend, including businesses in supposedly secure sectors such as financial services and the airline industry.

Part of the challenge is that security often lies at the end of the IT delivery chain. Software development teams create applications and systems and then toss them over the fence to be "secured," says Bil Harmer, security expert and advisory board member to cloud-based business intelligence and big data analytics firm GoodData.

Security is rarely an inherent part of the software development process. Instead, it is often bolted on, almost as an afterthought at the very end of the process. "Security or privacy has to be by design. You can't build it in afterward," Harmer says.

The continuing lack of communication between security, development and operations teams has hampered organizations' ability to deal with new and emerging security threats. "We are still in the 'waterfall' process, that handoff process, the conveyor belt process—if you will—from decades ago," Harmer says.

For information security to improve, the enterprise needs to become more agile so developers can understand evolving risks and threats as they adopt new technologies.

Rise of the DevOps Team

In the early 2000s, a new form of software development emerged. Agile development came from a belief that software isn't done until it is delivered to the customer and meets its expectations for availability, performance and speed of change. Unlike the traditional waterfall approach to software development, in which code is built to a predefined set of requirements, the agile model accommodated the notion that requirements can evolve continuously and are best addressed through a collaborative approach. The agile method brought development, operations and QA teams together for the first time, enabling a tighter coupling of requirements and design through "DevOps."

DevOps is much more tuned to a SaaS application development and delivery model than the waterfall approach, but security

CSO
Strategic Marketing Services

GoodData

remains the one missing piece of this agile approach. Organizations throw code through sprints and scrums and deliver multiple releases daily or even hourly, with little assurance that the software is secure. Rather than building security into the code, most organizations continue to wrap Web application firewalls, intrusion detection systems and antivirus software around the code after the fact. They still take "feeds" from the ops logs to analyze them for patterns or indicators of attacks. The myriad systems required to manage security after the fact can create problems, because every handoff from one system to another is a potential point of failure.

The DevOps software development model has helped organizations reduce time to market and improve their ability to respond according to user feedback and changing business needs. Organizations can derive even bigger benefits by merging security with DevOps—an approach dubbed DevOpsSec.

Security by Design

DevOpsSec emphasizes the use of automated penetration tests and code analysis tools earlier in the lifecycle, so developers can identify and fix potential security issues as they surface—effectively embedding security into the development process. With DevOpsSec, all the items that need to be tested for security issues are completed by the time the product gets to the staging and deployment stage. The approach is very different from attempting to find and patch security flaws in an already completed product.

Importantly, the DevOpsSec approach also enhances an organization's ability to respond to potential problems in production systems. Since software is built in collaborative fashion between engineering, operations and security teams, the DevOpsSec team can respond quickly to initial alerts and mitigate security risks before they turn into full-blown problems. Building cloud applications like GoodData's business intelligence and data analytics platform with security as part of the design is the key to reducing risk to organizations and their data. It ensures more-secure code and enables much quicker incident response and mitigation.

Such security capabilities are crucial for MediGain, an online medical revenue cycle management firm. It uses GoodData to deliver a best practices analytics service to several hundred midsize physicians' offices, ambulatory centers and hospitals around the United States. MediGain has interfaced GoodData's BI and data analytics platform with all the various practice management tools used by the company's clients, says Ian Maurer, director of IT and Business Intelligence at MediGain.

Because all the client data is covered under HIPAA regulations, security is critical, Maurer says. GoodData ensures that all personally identifiable data is deidentified before it reaches the GoodData platform. Mandatory user filter (MUF) technology ensures that sensitive data belonging to different clients is kept properly segregated at all times when accessing the GoodData analytics system.

Breaking Down Silos

Implementing a DevOpsSec approach requires enterprises with long-established development processes to break down the fiefdoms and silos associated with these traditional development processes, Harmer says. In a typical organization, divisional heads, department leaders and sometimes even C-level executives will need to collectively agree on the restructuring that may be required to implement a DevOpsSec model.

Getting Started with DevOpsSec

A successful approach often requires the following changes:

1. STRUCTURE

- Integrate application security into the development group to ensure that it is tested in the QA phase.
- Merge security operations with the broader operations group.
- Make infrastructure security part of the system architecture group.

2. DATA MODEL

- Don't keep all of your data in one place.
- Make the attack vector more complicated.

3. MIND-SETS

- Educate employees so they understand that security is about more than just throwing technology at a problem.
- Adopt a "trust but verify" approach to cloud solutions; insist on more transparency for security issues from cloud service providers.
- Foster better communications between security, development and engineering teams.

Merging development, security and operations teams gives organizations a way to embed and test security earlier in the development lifecycle. It also helps enable quicker incident response by bridging the communication gap that usually exists between these groups in a typical waterfall development environment.

A DevOpsSec model is easier to implement in a startup environment than it is in a mature development organization burdened with ingrained development processes. But by engaging the right stakeholders and decision-makers, it is possible to build a successful DevOpsSec model that can mitigate many of the security concerns regarding enterprise cloud adoption.

GoodData helps companies innovate and evolve rapidly to meet changing business demands, with trustworthy business intelligence. As a multi-tenant, cloud-based solution, GoodData's HIPAA-compliant, end-to-end analytics platform offers a high degree of security for enterprise businesses and ISVs.

[1] www.symantec.com/security_response/publications/threatreport.jsp