Summary Insights: The Keys to Mainstreaming Next-Level DevSecOps

RFG Perspective: As organizations transition toward mainstream DevSecOps adoption, the DevSecOps method of application development still faces opposition due to technical obstacles and business pushback to change. Business and IT executives must acknowledge these obstacles to DevSecOps adoption – and they must address them so that developers will be able to deliver more consistent and secure code. Otherwise, cyberattacks and ransomware attacks could become more frequent – and more damaging to a firm's brand – than ever before.

The naming of corporate champions who support DevSecOps is gaining support in many organizations. These corporate champions will accelerate DevSecOps adoption enterprise-wide – something that would protect applications and corporate data across the entire organization. Technology can help here: Code security can be improved through the modernization of aging applications, often by using automated scanning of older code and standardization of code. But these technical goals can be greatly enhanced by refreshing or adopting new corporate policies for moving to DevSecOps best practices.

Business executives should pay attention to the technical issues regarding application modernization and deployment. They should put more energy into coordinating with IT executives to ensure that their organization's DevOps practices integrate better security software into their future releases of application programs, thereby limiting future financial losses and damage to the firm's brand and reputation.

On July 14, 2021, Robert Frances Group facilitated an RFG 100 videoconference entitled: **"The Keys to Mainstreaming Next-Level DevSecOps."** This videoconference examined the business and technical roadblocks preventing DevSecOps from becoming the primary development methodology adopted throughout the enterprise.

For DevSecOps to scale and to achieve mainstream status, enterprise stakeholders must collaborate and iteratively refine cooperative efforts to produce the best customer experiences related to software development. For most organizations, DevOps and DevSecOps initiatives began at the grassroots level, with each group in the enterprise setting its own procedures and standards and selecting their own tools. Some groups brought Security into the process, while others did not. Because the development process is often a grassroots effort, there is often a lack of

46 Kent Hills Lane, Wilton, CT. 06897; (203) 429 8951;
http://www.rfgonline.com/; *Contact: inquiry@rfgonline.com*

commonality among developer groups across the enterprise. This situation is one of the inhibitors to considering DevSecOps to be the primary development process for the entire enterprise.

For most enterprises today, CIOs and senior IT executives acknowledge that agile development and waterfall development processes are the only authorized software development lifecycles (SDLC) for their organization. This situation needs to be turned around, because executives must consider, understand, and emphasize the business value of switching to a DevSecOps methodology.

Rapid Changes in Business Models Require Faster Software Development

Why is programmer productivity so very important for today's businesses, as they emerge from the COVID-19 related business slowdowns? As one IT executive put it: "Every company is becoming a software company." The context here is that business relies on software and – given the centrality of software functionality to today's businesses – time-to- market with the security guardrails in place is imperative.

Unlocking the full potential from DevSecOps requires stakeholder incentivization. Once accepted, DevSecOps can become a competitive advantage to the corporation and individual participants alike. But this requires both a cultural shift and executive leadership to succeed.

Key Questions for the DevSecOps Discussion

To discuss the adoption of DevSecOps in organizations, RFG 100 panelists considered the following key questions now facing business customers:

1. What cultural changes need to occur before DevSecOps can become mainstream within an enterprise?
2. Is this process considered to be DevOps or DevSecOps – and who belongs on the team? What personas or roles should be involved in decision-making?
3. What organizational learning is needed to understand, and support, DevSecOps?
4. How does one obtain buy-in from all appropriate parties so that a true DevSecOps organization can be built?

5. What phases and milestones should be part of the transformation to DevSecOps?
6. What are the critical success factors to making DevSecOps the prime method for all future development?

The panelists for this videoconference were:

- David Giambruno, CEO, Nucleaus
- Brook Schoenfield, Master Security Architect, True Positives
- Aruneesh Salhotra, Global Head of Application Security, Nomura Securities
- Don D'Angelo, senior architecture manager and SVP of a major U.S. financial institution

Taking Inventory of DevSecOps Readiness

For DevSecOps adoption to take place consistently throughout the enterprise, IT executives must evaluate the state of readiness to leverage DevSecOps in their company. They must take stock of the assets they have in-place for DevSecOps adoption. Key elements of this cross-organization inventory include the following:

- **Support from business executives:** Business executives will have to align with IT executives regarding the importance of have a consistent approach to development, no matter where applications are developed in the enterprise. This is essential to adopting mainstream DevSecOps policies and practices.

- **IT Skillsets:** Evaluating the DevSecOps skillsets available to join the team.

- **Application Portfolio:** Taking inventory of the types of applications that are being developed, or modernized, across the entire organization.

- **Security support:** What software releases and updates are in place right now – and do they currently support the latest software tools and security standards? Should they be updated, to provide the strongest level of protection from security attacks, including cyberattacks and ransomware?

- **Business cycle times are accelerating.** Cycles for development and deployment of new applications has accelerated in the age of hybrid cloud. Applications must be built and deployed in weeks and months, rather than in years. To speed development, customers are turning to automation and code-

scanning to find gaps in policies, practices, and security – so that these gaps can be addressed quickly.

Why is DevSecOps Needed Now?

Customers must take stock of the technical assets that are already in-place for DevSecOps adoption – and evaluate the state of readiness to leverage DevSecOps in their company. The RFG100 panel discussion surfaced the following as the primary considerations for those seeking to adopt DevSecOps methods:

- **Creation of universal standards.** Standardization of code prevents many types of human errors introduced by developers/programmers as they type in individual lines of code. For many organizations, each development team has created its own code and process standards.

- **Application development cycles must be improved.** To keep pace with rapidly changing business environments, application development must move quickly, usually on a CI/CD cycle of continual updates, as needed.

- **Using automation to scan code more quickly.** The introduction of automation and AI-based scanning tools will accelerate the pace of application code reviews and repairs. When applied across the organization, these techniques result in dramatic improvements in cycle times.

- **Leveraging "snap" storage copies.** Storage technologies that take snapshots of software images are linked to programmer productivity. Having the ability to "snap" code in container repositories, so that exact golden images of the code can be used again and again, allows customers to "scale" their infrastructure more rapidly.

An Approach to DevSecOps Solutions

Review applications to ensure consistent software-development practices: Due to merger and acquisition (M&A activity), many organizations inherit the infrastructure and processes of the smaller companies they acquire. As a result, large companies with M&A programs often inherit software that was developed using different policies and best practices than was used in their own IT

organization. Adoption of agreed-upon software tools will reduce the amount of security exposure that customers face.

Change the Culture: Customers must face the fact that business executives must reach consensus about the need to move to more secure DevOps – if only to protect the core business from cyberattacks, ransomware and identity theft. Business executives have broad influence over the corporate culture – and, due to their budgeting capabilities, they can allocate funds to improve software practices and secure software development.

Create a centralized DevSecOps Center of Excellence (CoE): Companies that have a centralized DevSecOps center of excellence can set consistent policies and development practices across the organization. They can use software toolkits that speed the review of older code for updates and security purposes.

Adopt CI/CD development cycles: CI/CD methods result in the continuous delivery of code, with pipelines and consistent tooling throughout the organization. This means that software will be reviewed, updated, and put into production frequently, and consistently – making security patches faster and easier to apply.

Use automation, where possible: Use pre-tested code, and use software automation tools to scan older code. Both approaches will speed the overall Dev/Test software development cycle, supporting acceleration of the overall DevSecOps software-development and deployment process. Learn which toolsets are gaining adoption in other companies – and evaluate them for possible use in your organization.

Cybersecurity needs to be embedded in your corporate culture: Customers need to have "champions" for DevSecOps practices inside the company or governmental organization. That's how they will be able to achieve "culture change" for the way applications are developed. This is being done to create a positive environment for DevSecOps adoption and to establish company-wide security standards.

Summary: "Mind the Gaps"

Organizations must become aware of the gaps in their current software portfolio – regarding performance, efficiency, and security – and they must address them – to

protect their applications and corporate data. As one of the panelists said: "Take stock of what you already have, find the gaps, and address them."

Here are some practical steps to take along your DevSecOps journey:

Apply automation to speed software development: Automation is key to speeding up software review processes, such as scanning code for security flaws. Without leveraging automation tools, the process of reviewing millions of lines of code in large applications can become too lengthy and costly to sustain.

Take a 360-degree view of your software estate. Look at all the key assets together. It will create a baseline for your in-depth review of your enterprise's software portfolio.

Assess your organization's security gaps: Get a true idea of your real level of vulnerability to software attacks. Look across your entire application estate to get a real-world view of how vulnerable to attack your organization may be.

Leverage ISV software, where necessary. Mitigate your company's security risks by adding third-party software tools, where needed, based on your security audit. IT executives need to be more proactive than the software vendors (ISVs) themselves if they want to ensure that their software development policies and practices are being updated without introducing gaps into new or updated applications.

RFG POV: Most IT organizations are still struggling with a corporate cultural paradigm shift from traditional SDLC processes to a set of DevSecOps processes that are more agile, and more secure, than earlier processes. Enterprises can achieve greater levels of success, while reducing costs, resources, and risks, if they can embrace the broad DevSecOps culture, and if they implement the required processes and standards enterprise-wide.

Bringing all the parties together for this level of change requires corporate and line of business (LoB) leadership to overcome the inertia and resistance that stem from a lack of consensus across multiple units within the organization. To improve this situation, business and IT executives must commit to driving change, while addressing any inhibitors that may arise.

46 Kent Hills Lane, Wilton, CT. 06897; (203) 429 8951;
http://www.rfgonline.com/; *Contact: inquiry@rfgonline.com*

Additional relevant research and consulting services are available. Interested readers should contact Client Services to arrange further discussion or interview with Mr. Cal Braunstein, CEO and Executive Director of Research. Jean S. Bozman, president of Cloud Architects llc, co-authored this report.

---

46 Kent Hills Lane, Wilton, CT. 06897; (203) 429 8951;
http://www.rfgonline.com/; *Contact: inquiry@rfgonline.com*