The Road to Secure Software Development

DevSecOps can help agencies create secure and innovative applications while achieving the ultimate goal of better mission outcomes

AS SOFTWARE becomes more sophisticated, it plays an increasingly important role in all aspects of government operations. However, given the complexity and intertwined nature of modern software, any vulnerability could have wide-ranging consequences, which makes security of vital importance.

In announcing its 2022 State of Application Security report, Forrester Research stated: "Applications are once again the top cause of external breaches, and software supply chain concerns added complexity to a challenging year." Similarly, Verizon's Data Breach Investigations Report for 2022 states that system intrusions, miscellaneous errors and basic web application attacks represent 81% of breaches in the category of public administration.

The federal government has taken notice. A number of recent policy directives address issues related to the software supply chain, and key agencies are leading a governmentwide effort to promote secure software development.

ADDRESSING CONCERNS ABOUT CYBERSECURITY AND THE CUSTOMER EXPERIENCE

Secure, modern software is at the heart of agencies' ability to provide a digital experience that mirrors that of the commercial world. Such software helps the government operate more efficiently and successfully while increasing public satisfaction and trust in government. In a recent pulse survey of FCW readers, 91% of respondents said concerns about cybersecurity and the customer experience were pushing their agencies to reconsider how they handled software development and delivery.

The Executive Order on Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government states that "the federal government must design and deliver services in a manner that people of all abilities can navigate. We must use technology to modernize government and implement services that are simple to use, accessible, equitable, protective, transparent, and responsive for all people of the United States."

Furthermore, securing the software supply chain is an integral element of the Executive Order on Improving the Nation's Cybersecurity and subsequent guidance from the Office of Management and Budget (OMB) on secure software development practices, released late last year. Chris DeRusha, federal chief information security officer and deputy national cyber director, wrote at the time that "the guidance, developed with input from the public and private sectors as well as academia, directs agencies to use only software that complies with secure software development standards, creates a self-attestation form for software producers and agencies, and will allow the federal government to quickly identify security gaps when new vulnerabilities are discovered."

OMB's guidance directs agencies to use the resources provided by the National Institute of Standards and Technology (NIST) — specifically the Secure Software Development Framework and the Software Supply Chain Security Guidance — to create a foundation for secure software.

DevSecOps by the numbers

Sources: FCW, Verified Market Research, Verizon

73%

FCW survey respondents who said their agencies are developing or implementing a DevSecOps strategy

55%

FCW survey respondents who said entrenched processes prevent widespread adoption of DevSecOps at their agencies

$41.7B

Projected value of the global DevSecOps market in 2030, up from $3.7 billion in 2021

81%

Breaches targeting public administration organizations via system intrusions, miscellaneous errors and basic web application attacks

DEVSECOPS, AI AND ZERO TRUST

A key methodology for achieving the government's goals is DevSecOps. This set of tools and best practices brings together the development, security and operations teams to collaborate on software that incorporates security every step of the way. DevSecOps provides agencies with a clear roadmap for building and testing, deploying, and monitoring applications, as well as continuously delivering updates. By boosting efficiency and easing the security burden on developers, DevSecOps also has a positive effect on the employee experience, which can help agencies retain talented professionals.

In FCW's survey, a total of 73% of respondents said their agencies were developing or implementing a strategy for using DevSecOps, and 9% have fully embraced the methodology.

Gartner defines DevSecOps as "the integration of security into emerging agile IT and DevOps development as seamlessly and as transparently as possible. Ideally, this is done without reducing the agility or speed of developers or requiring them to leave their development toolchain environment."

Much of DevSecOps' potential comes from the opportunity to automate security reviews and testing. Artificial intelligence can quickly root out code with known vulnerabilities and untangle complex dependencies between software and systems, allowing developers to focus on innovation while the security team seamlessly achieves compliance with government mandates.

NIST's DevSecOps resources page states that "by integrating security practices and automatically generating security and compliance artifacts throughout the process," DevSecOps can reduce vulnerabilities and malicious code, mitigate the potential impact of vulnerability exploitation throughout the application development life cycle, and address the root causes of vulnerabilities to prevent recurrences.

The General Services Administration's DevSecOps Guide has the stated goal of Safer Software Sooner. It goes into great detail on strategies and metrics for activities that include logging, monitoring and alerting; patch management; platform governance; and application development, testing and operations.

Last September, the National Security Agency, the Cybersecurity and Infrastructure Security Agency, and the Office of the Director of National Intelligence released Securing the Software Supply Chain: Recommended Practices Guide for Developers. The document's goal is "to serve as a compendium of suggested practices for developers, suppliers and customer stakeholders to help ensure a more secure software supply chain."

In addition, the government's emphasis on building zero trust architectures can complement DevSecOps. In a recent blog post, Forrester researchers wrote that "a robust application security architecture incorporates zero trust's core principles of least privilege access and comprehensive security monitoring. Any discussion about protecting applications in production through API security, container security or workload security will naturally include zero trust requirements."

A COMPLEX INTERPLAY OF PEOPLE, PROCESSES AND TECHNOLOGIES

Verified Market Research has forecast that the global DevSecOps market will expand from $3.7 billion in 2021 to $41.7 billion by 2030, which represents a compound annual growth rate of nearly 31% from 2022 to 2030. Nevertheless, the firm's researchers noted that one of the chief obstacles to widespread adoption is people, not technology. "[Because] people have already become deeply accustomed to current development processes, it can be hard to break the system and adopt new tools and technologies," they wrote.

Indeed, DevSecOps requires a complex interplay of people, processes and technologies, with cultural barriers being the most challenging to overcome. Given government's traditionally siloed activities and risk-averse nature, it can be difficult to encourage teams to work together and share some level of accountability for the end product.

When asked about the obstacles that prevent widespread adoption of DevSecOps at their agencies, 56% of FCW survey respondents cited lack of employees with the right skill set and 55% cited entrenched processes. Lack of appropriate technology was next on the list at 44%, followed by a limited understanding of the methodology's benefits at 41%.

The wealth of government guidance can help agencies overcome the cultural and technological challenges to building a strong, innovative DevSecOps culture, but it's worth remembering that DevSecOps is not the final destination.

In a recent interview with FCW, Sean McIntyre, director of the Solution Delivery Service at the Federal Aviation Administration, offered this advice for his colleagues at other agencies: "Have faith that you can breathe new life into old applications by applying DevSecOps principles. At the same time, always take the view that DevSecOps is not the goal, it's the enabler of the goal, and try to emphasize that fact in every discussion you have on the subject at every level of your organization."

The ultimate goal, McIntyre said, "is greater mission value in less time with less toil." ■

Industry-leading DevSecOps tools and expertise

FCW recently spoke with sales directors Seamus Bergen and Rich Savage at Carahsoft about the company's commitment to giving agencies the flexibility and choice they need to achieve mission success with DevSecOps.

HOW CAN IT LEADERS MAKE THE BUSINESS CASE FOR DEVSECOPS AT THEIR AGENCIES?

Savage: Software is at the heart of modernization efforts in the government. The ability to release software more quickly and securely is mandatory to staying relevant in the Digital Age, so every agency needs to become a software agency.

Bergen: Software is not just a tool anymore. It's an asset, and agencies need to utilize it in a manner that helps them meet their missions. It is not about the old infrastructure way of maintaining hardware. Agencies are using software now to run their operations and achieve their goals and missions.

WHAT STEPS CAN AGENCIES TAKE TO ENSURE SUCCESSFUL ADOPTION AND ONGOING USE OF DEVSECOPS?

Bergen: Coming in with the right mindset is essential. DevSecOps is a culture change that involves fundamentally changing your approach to developing applications. You are now integrating the security aspect from the very beginning. It is an iterative process in which agencies are always introducing security measures, tying in operations, and developing code quickly and efficiently while iterating on that process. So the first step is ensuring your organization can make that adjustment to facilitate and support the effort.

Savage: Tools, talent and culture are critical to the success of software delivery groups. You can have the best tools in the world, but if you don't have talented people who are trained to use them, then those tools are almost meaningless. You can have the best people in the world, but if they're not using the right tools, they won't be successful. And then you could have the right tools and the right talent, but if you don't have the right organizational culture — one that allows people to experiment and learn in an agile type of way — the three elements won't line up to enable a successful DevSecOps implementation.

HOW DOES CARAHSOFT HELP AGENCIES EMBRACE MODERN, SECURE SOFTWARE DEVELOPMENT?

Savage: Thanks to our robust partner ecosystem, Carahsoft has the largest portfolio of DevSecOps companies in the industry. We know that no two software development groups use the exact same tools, so we offer a wide spectrum of choices to help our public-sector customers develop their own strategies for software modernization. It is also extremely important for agencies to have access to enterprise-grade, secure software development tools that have already been vetted to run on government networks. The ability to procure those tools through the appropriate contract vehicles is another important benefit of working with Carahsoft.

Bergen: The best approach to DevSecOps is one with an open mind. There are a lot of variables that one must decide on when implementing these approaches, and some factors are influenced by current state and investments. Here at Carahsoft, we have the necessary expertise and a comprehensive portfolio of tools so agencies are not limited in their options. To expand on what Rich said, the acquisition of DevSecOps solutions can be a bit tricky because of the flexibility that's required and because of the iterative nature of DevSecOps. We might start off thinking an agency needs X, but as we get to know that agency's situation and goals, it might turn out that Y is a better approach. We develop contracts that allow for that flexibility so we can ensure the government gets the solutions and value it needs.

Carahsoft will be hosting a DevSecOps conference in Washington, D.C., in August. Go to carah.io/devsecopsconference for details.