

Public-private partnerships ensure ‘innovation flowing both ways’

THIS CONTENT HAS BEEN PROVIDED BY SONATYPE



Dr. Stephen Magill,
vice president
of product
innovation,
Sonatype



There's a well-worn stereotype that government can't innovate as fast as industry, and that's why it relies on public-private partnerships to update its technologies, because it can't on its own. But if you dig a little deeper, it turns out that the innovation ecosystem that exists between the public and private sectors is more complex than that, and involves far more give and take.

"There's always been this technology exchange between the federal government and industry, with innovation flowing both ways," said Stephen Magill, vice president of product innovation at Sonatype. "There's high profile examples of these government developed technologies that spawned commercial activities. So GPS is one example of that. Another is what you see in rocket technology, where initial work was all government funded happening at NASA. Now there's a lot of innovation happening at companies like SpaceX and Blue Origin. We've seen the same thing happen in the software security field as well."

For example, software security technologies like static application security testing and dynamic application security testing originated as government funded research projects. Government requirements around high levels of security and

assurance tend to develop earlier than within industry due to the nature of the mission at federal agencies, especially within the Defense Department and intelligence community. That's because government agencies face a higher risk of compromise from well-funded bad actors like adversarial nation states.

But those technologies that originate out of the needs of agencies and the research they fund to meet those requirements also spawned a large, thriving industry of software security companies and vendors. Those technologies then become widely available, and quickly adopted by the rest of the private sector. Soon every software company cared about security, which sparked further innovation, which then makes its way back into government. The same cycle is currently repeating with secure software development and DevSecOps.

"Government has the ability to spawn investment in new areas via government research programs, things like DARPA, and other research arms and DoD. NASA and DHS also have large research programs, so there's that ability to push the forefront and drive innovation," Magill said. "And then, as is always the case with research, some of those bets pay off big time, and some end up being a dead end. But those ones that really gain traction, I think then industry becomes the place where it really develops into a robust capability. In many cases, that capability then flows back to government. There's a sense in which government is often the incubator of some of these ideas, which is underappreciated."

That's why practically every government agency currently has a group experimenting with DevSecOps, and some of them are seeing real success with it, like the Air Force's Platform One program. These groups are delivering software faster and under budget. That's especially impressive considering that government often has more than just cloud-based software systems to think about; agencies have complex radio systems, vehicles and aircraft and other physical component systems that have to be integrated seamlessly. That's a tougher environment than most private sector organizations face.

Factor in the fact that governments also rarely have a single pipeline to manage for their development. While industry can set a single template for all its software development, federal agencies often have contractors contributing as well. That means those agencies essentially have multiple different development teams, with different processes, tools, infrastructure and environments operating on the same project. That makes governance a much more complicated proposition.

But that's where that back-and-forth ecosystem comes into play again, because one of government's main roles in that dynamic is to set standards and develop frameworks. Federal guidance like the recent cybersecurity executive order helps ensure everyone is on the same page, and provides methods for alleviating some of those governance issues.

"If you don't have that level of control over the development process, you need a way to check the final product," Magill said. "And so things like a software bill of materials give you that visibility that lets you say, 'I have this product that's coming out at the end of the process, and I have visibility into enough of how it was constructed to check security of components.'"

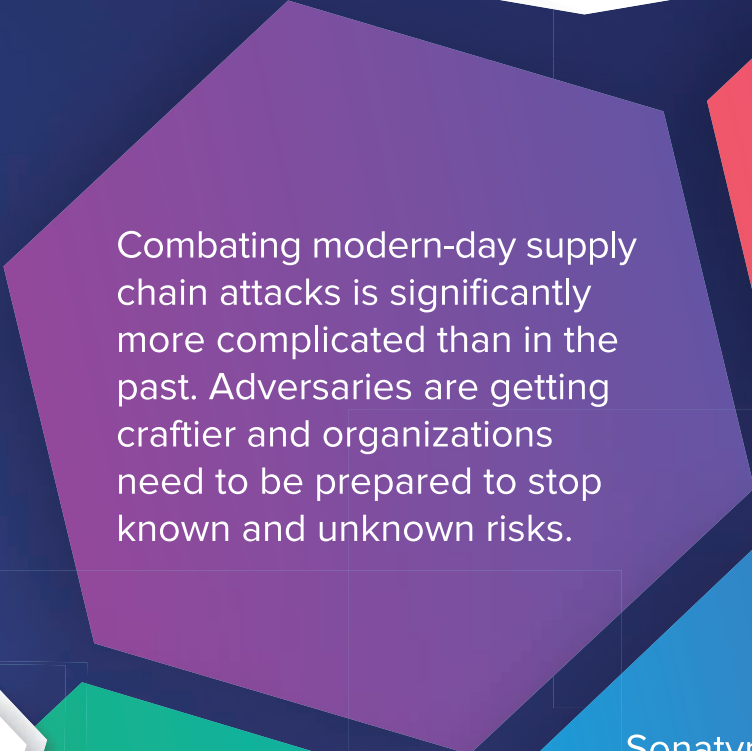
As government sets these kinds of standards, industry adopts and propagates them. This creates a kind of innovation feedback loop where government innovates, and industry runs with it, while government sets parameters on which direction to run in. You see this dynamic play out across various industries currently, including 5G and internet of things. Even technologies used to test weapons systems which can't safely be tested physically are being adapted to test self-driving cars.

"It's not something you hear often, that the government's innovating beyond industry. I want to push back on that a bit," Magill said. "There really are places where government has spawned innovation. And once something takes off in industry, and there's a large market for that technology to grow, then things can accelerate and take off. But there is a vital role government innovation plays in that advancement of software and technology."

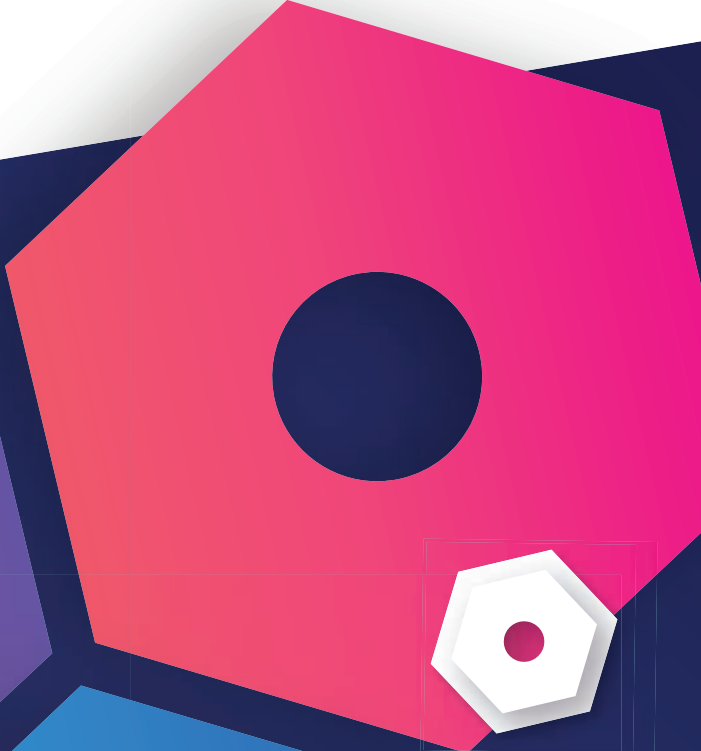


Code smarter. Fix faster. Be secure.

Software supply chain security should feel like a no-brainer.



Combating modern-day supply chain attacks is significantly more complicated than in the past. Adversaries are getting craftier and organizations need to be prepared to stop known and unknown risks.



Sonatype's Nexus platform provides precise intelligence for delivering uncompromised applications. It continuously, and automatically, identifies and remediates open source risk across every phase of the software supply chain.



Learn more about how to protect your software supply chains at sonatype.com.