AUTUMN 2021

DevSecOps: how to seamlessly integrate security into DevOps

Adaptavist

DevSecOps: how to seamlessly integrate security into DevOps

Contents

Introduction

A better approach to software security

Security is fundamental to the success of any software, the organisation that makes it, and the businesses and individuals that use it. But, in the past, security processes were sidelined. These once-manual activities were often left to the last minute, took too long, held up features from being delivered, and failed to protect effectively against the growing swathe of vulnerabilities.

DevSecOps is the integration of security into DevOps processes. It automates and replicates code scans and tests to make security verification a continuous part of the software development life cycle (SDLC). It harnesses many DevOps practices to ensure internal requirements and compliance with industry standards are built-in and considered at every step of the development process.

In this ebook, we'll take a look at how security fits into DevOps, the security challenges that DevOps poses, and why security should be so much more than an afterthought. Then we'll look at the steps you can take to start integrating security into your DevOps processes.

Part one:

How does security fit into DevOps?

What is DevSecOps?

In the past, security has been treated as a secondary system – an afterthought that gets incorporated at the end of the SDLC. This means most security vulnerabilities aren't addressed until development is almost complete – or worse, after release. DevSecOps requires a significant shift in thinking, ensuring everyone is accountable and takes responsibility for security. With a 'security-first' mindset, it's easy to see that security, part-automated and with minimal disruption to operations, should be integrated into the DevOps toolchain as a standard practice.

DevOps has introduced processes like continuous integration (CI) and continuous delivery (CD) into the SDLC, ensuring code is actively tested and verified along the way in an agile development process. DevSecOps relies on continuous security audits and vulnerability testing to make sure security is part of the product, rather than just bolted on once it's been built.

With the rise in open source – 99 percent of audited codebases contain some amount of open source – vulnerabilities are widespread. Last year 24 percent of developers confirmed or suspected a security breach tied to open source. Manual management just isn't viable, with thousands of new releases happening every day. According to Forrester's The State of Application Security 2021 report, organisations are unable to react quickly enough to rectify these breaches. In fact, 50 percent of those surveyed spent a week or longer remediating known OSS vulnerabilities in their code.

Luckily, the software industry is shifting left with DevSecOps. With security processes becoming more automated and being handled directly by the development team, deployment can speed up safely, supporting the rapid-release cycles now common across the industry.

Why is DevSecOps so important?

The clue is in the name. Security is necessary to ensure software is safe and fit for purpose. We all depend on technology, and security breaches are a very real threat to the way we do business, govern, communicate, and enjoy our day-to-day lives. No one is immune – from large organisations and the public sector to small businesses. And a security breach can have serious repercussions for organisations, leading to the loss or abuse of intellectual property, loss of revenue and unforeseen costs relating to the breach, not to mention reputational damage.

A security-focused, continuous delivery SDLC helps promote collaboration and ensure security professionals and their work is not forgotten about. It means more efficient cycle times where insecurities are not discovered at the last minute, requiring costly iterations, but are built into the product from the get-go. Sure, there might still be unexpected issues at the last minute, but the chance is a lot less likely. Moving away from traditional security measures enhances your credibility and builds trust with your customers too.

Facing security challenges in a DevOps culture

Organisations want to make sure their software is secure, but the pace of change has meant many have failed to adapt their security strategies to match IT infrastructure and development culture.

DevOps demands that batches of code are pushed and modified over much shorter time frames, outpacing the speed security teams can keep up. Here are a few other security considerations that DevOps poses:

- Containerisation and DevOps go hand in hand, making software easier and faster to deploy, requiring fewer resources, and making management easier. But they also pose negative security risks to organisations, due to misconfiguration and other inherent weaknesses. That's why it's so important that organisations implement runtime container security protections in all phases of development, testing, and production.
- Dynamic cloud-based environments mean that even small breaches can quickly escalate into catastrophes – think organisation-wide operational failures and vulnerabilities.
- DevOps teams have a wide-ranging toolset that's highly integrated and can change to meet project needs. This means more risk of compromised account details, SSH keys, and API tokens if the right security controls aren't in place.

It's clear to meet the demand of DevOps, traditional security methods just don't cut it, which is where DevSecOps steps up. Let's take a closer look at some of the big challenges security and development teams are facing and how a DevSecOps approach can help solve them.

Challenges facing security teams

Security teams are dealing with a two-pronged assault: they don't have time to do their job, and even when they do, it's hard to work with the development team to make sure the work is done correctly.

The first issue exists because the rapid nature of DevOps is at odds with the slower security architecture review process of the past. These time-consuming, manual tasks can cause significant delays to the process. But DevSecOps offers another way. With the help of security management tools, lots of the threat modeling and review process can be automated. A faster, more consistent process means both internal standards and industry compliance are accounted for every time a change is made.

The second issue arises because of poor communication and a lack of developer knowledge of how to handle security requirements. DevSecOps builds security needs into the SDLC, utilising platforms that create work tickets for developers as part of their everyday workflow. That way, security is prioritised side by side with functional needs, and threats are addressed earlier and can be resolved quickly with fewer cost implications.

Challenges facing developers

In addition to the workflow issues outlined above, developers are also faced with increased pressure from automated testing. Scanning tools that deliver application security testing (AST) are used after source code has been compiled. If a scan finds a large number of issues, it's the development team that shoulders the burden, with a significant amount of risk and cost to the schedule if the architecture needs to change.

But AST tools alone are not enough. Security platforms can help define which tests are required so developers can build custom tests that account for each application's unique vulnerabilities, rather than relying solely on scanners, ensuring any issues are addressed earlier in the SDLC, making the testing stage less precarious and painful for developers.

In part two, we'll look at how you can start integrating security seamlessly from the beginning of your SDLC, promoting the collaboration and continuous feedback DevOps calls for, while enhancing security and agility.

Part two:

How to integrate security into your DevOps processes

A security solution to suit your needs

The most important consideration when it comes to implementing DevSecOps, is that there's not a one-size-fits-all solution. What works best for you will depend on your organisation, architecture, and tech stack. For those more accustomed to a traditional security approach, this might come as a bit of a shock – but rest assured, the benefits become apparent pretty quickly.

That being said, taking the leap from DevOps to DevSecOps is not as simple as adding a security team to the mix. Security needs to become an intrinsic part of every team and process across the organisation. By doing so, you'll be sure to eradicate this bottleneck from your continuous delivery pipeline. To help your DevSecOps integration to thrive, there are a few key points to consider. In this section, we take a look at each in turn to help you get on the right track.

Shift Left

Fact: security has to start much earlier in your DevOps processes. By implementing security policies from the start – engineering them into design and deployment, and incorporating testing tools into development – rather than relegating it to the end of your SDLC, you'll keep costly mistakes to a minimum.

It’s much easier and cheaper to fix issues earlier in the life cycle, so how do you make it happen? Integrate code analysis tools and automated custom tests during development – and then keep security top of mind through deployment and production. You’ll catch and then eliminate security flaws far sooner, and save your people a lot of hassle in the process.

Automate

You’re already reaping the rewards of automation with DevOps, and there’s no reason your security efforts should be any different. If you want controls and testing to take place early and often, then you’re going to need to lean heavily on automated processes at regular check points before deploying to production.

An end-to-end automation and orchestration platform is integral to this approach, giving you greater visibility and control. The automatic tools in your arsenal can help with status and dynamic code analysis, software composition analysis, vulnerability and penetration testing, and privileged credentials management.

Loop

Automated security processes are only beneficial if they're done continuously and throughout the SDLC. Your automated pipeline then becomes a closed loop where testing, feedback, and remediation are always happening. CI/CD tools that integrate seamlessly with your security scanning and testing solutions can help ensure best practice, while regular checkpoints track changes, test for flaws, and make sure improvements are taking place.

Optimise

Automation is nothing without streamlined processes with clearly defined security requirements. A unified approach from the outset is key to prevent security being sidelined. Everyone should be on the same page about security requirements, so setting out what's needed during the design and architecture stages of a project is key.

It's a good idea to approach security as you would any other feature that needs testing. Make it part of the other metrics you're keeping track of, decide what standards you're working towards, develop a repeatable method, and make sure you document it. This way, your DevSecOps efforts will be transparent across the organisation, helping unify teams and ensure process improvements.

Be Aware

Everyone who joins your DevOps team should have a basic understanding of secure coding and the mistakes to avoid. But building a deeper knowledge of security implications into your organisation will help avoid potential pitfalls and ensure commits and releases stay on track without avoiding vital testing or compromising software security.

You should encourage early and often collaboration between security engineers and DevOps teams. This will help eliminate siloed team practices, increase communication, and enable security responsibilities to be shared across the development process. That way, threat models can be built to meet the demands of features and devs and ops know what's expected of them from the outset.

Think Differently

For security to establish itself as an intrinsic and vital part of how your organisation builds software, you need to address the culture that surrounds it. You have to help your DevOps team embrace security and do it well. That means a cooperative environment where trust is paramount; a functioning feedback loop, and a clear commitment to ensuring your people have the training they need.

This culture shift requires developers and operations to take joint ownership of security and be accountable, rather than assuming it's someone else's responsibility. One way to help this happen is appointing security champions during the transitional phase, providing a go-to person for any issues or concerns and a role model for what is expected of the rest of the team. By addressing culture in this way, security will stop being a function and evolve into a mindset across the whole organisation.

The next step in DevOps

By its very nature, DevOps should include the entire SDLC – that means security too, but traditional approaches and siloed teams have meant a more slapdash, last-minute approach has become the norm in some organisations. By explicitly including 'Sec' in the name of your approach, your organisation is acknowledging how much it values security, and how it is a core pillar of the way you work.

DevSecOps is not a catch-all. It won't eliminate risk completely. But that's okay. Striving for perfection is at odds with the speed DevOps demands. Security will never be perfect, but with a DevSecOps mindset – continuous assessment and greater visibility – your security stance will be head and shoulders above the competition. And you'll be able to make changes as required, adapting to the needs of your users, industry standards, and technological advancements.

Security experts are more essential than ever, but DevSecOps puts the onus on all technology personnel to play their part to ensure speed and security go hand in hand. With best practice in place, problems are caught earlier, resolved more effectively, and risk is significantly reduced.

Take the next step

Want to discuss how you can integrate or improve security with your existing DevOps practices? Get in touch with our experts today.

Find out more

Adaptavist

We help organisations transform to continuous change being their business as usual. We do this by supplying technology, providing advice, and delivering change through modern, iterative approaches to development, deployment, and application lifecycle management.

Adaptavist is Atlassian's largest platinum partner, supporting more than half of the Fortune 500. We are uniquely placed to provide our experience, expertise, and insight to help your business.

Whether you want training for your team, to build a software platform for your company, or to automate your existing tooling, we can help you. If you want to unlock the full power of Atlassian and transform your business at scale, get in touch with our team today.

Learn more or get in touch:

adaptavist.com

ATLASSIAN Training Partner

ATLASSIAN Platinum Solution Partner ENTERPRISE

ATLASSIAN Platinum Top Vendor