TECH DOSSIER

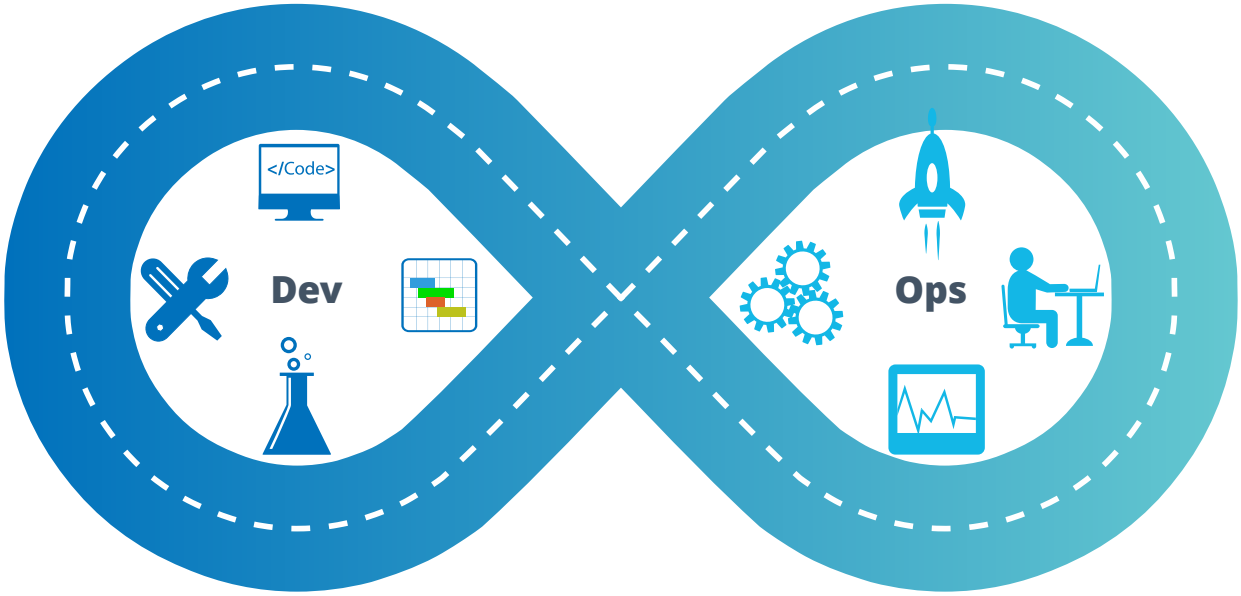
3 REASONS:

Why DevOps is a Game-Changer for Security

Meeting the speed of DevOps with effective cybersecurity requires new InfoSec approaches that include built-in security, automation, and proactive prevention.

tenable™

IDG
STRATEGIC MARKETING SERVICES



The DevOps model drives digital transformation and the rapid delivery of new software products and services. It replaces a traditional, linear development approach by emphasizing cross-functional collaborations, integrated tools, and automated workflows.

In fact, DevOps represents a kind of cultural revolution in which the creation and deployment of software and services happen at an extremely accelerated pace. That said, this process has largely taken place outside the purview of information security (InfoSec) and often without its knowledge or involvement.

As a result, security teams have struggled to keep pace or, even more seriously, have not been engaged at all. Even when they are engaged, security teams tend to slow the overall development process with their own linear approaches and mindsets.

Yet DevOps presents InfoSec with the perfect opportunity to move from a reactionary response to one where safeguards, proactive testing, and prevention are automatically integrated throughout the development lifecycle.

This article explores the intersection of DevOps and InfoSec. Specifically, it offers three reasons why security organizations will benefit by combining these two practices.

REASON 1: **Built-in Security**

BUSINESS VALUE CHECKLIST

Built-in DevOps security leads to measurable gains and organization-wide benefits. Businesses can:

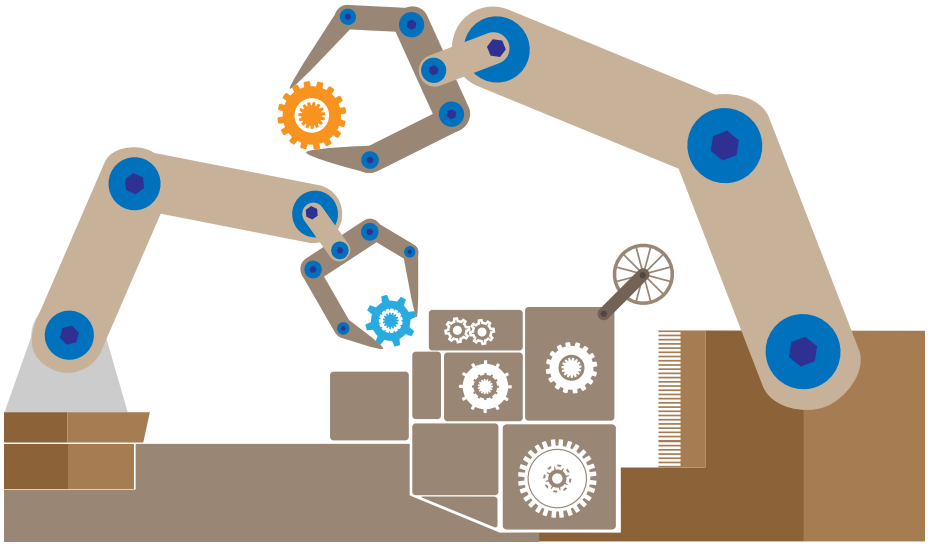
- √ **Reduce operational costs**
- √ **Improve DevOps efficiency and code quality**
- √ **Strengthen security posture**
- √ **Speed time to market**

The practice of integrating security into DevOps is quickly gaining momentum. By 2021, secure DevOps processes will be embedded in 80% of rapid development teams, up from 15% in 2017, according to Gartner's "10 Things to Get Right for Successful DevSecOps" report.

In response, InfoSec teams should shift from a reactive approach to one that incorporates built-in security controls throughout the development process. With integrated security tools in place, developers never have to leave their continuous deployment toolchain environment. Moreover, organizations are eliminating the risk that developers will simply choose to bypass separate security tools. Built-in security ensures the quality and integrity of products and software that are constantly evolving, and it reduces operational costs by fixing defects early in the software development lifecycle.

Built-in security testing enables developers to move fast, confident that mistakes and vulnerabilities will be resolved before deployment. By collaborating, and integrating security at multiple points in DevOps workflows, InfoSec teams can assess integrity with each new iteration, and leave behind labor-intensive manual testing.

REASON 2: **Automation**



BUSINESS VALUE CHECKLIST

Automation optimizes limited resources, ensures development accuracy, and enables continuous monitoring to:

- √ Accelerate delivery times
- √ Reduce operational costs
- √ Lower project risk
- √ Improve code quality

Many organizations with strong DevOps processes generate dozens—sometimes hundreds—of iterations a day of software and services. Moreover, developers constantly run QA tests during builds covering unit, API, and integration testing to improve code quality. In these fast environments, manual testing and the linear model for security are simply inadequate. For example, traditional one-time gating and penetration testing delays deployments, and decelerates high-velocity development cycles.

Automation compensates by ensuring that high levels of security exist across all areas of DevOps, not only as a seamless part of a developer's integrated development environment (IDE), but also within the continuous integration and continuous development (CI/CD) toolchain. For example, security testing can become another quality control that's incorporated into QA. Automation guarantees that application security is an inherent part of the build process and facilitated by DevOps itself as software evolves.

When you consider the limitations of outdated processes like gated checks, or the alternative of no security at all, then it's clear why automated security is crucial to the DevOps process.

REASON 3: **Proactive Prevention**

BUSINESS VALUE CHECKLIST

Proactive prevention ensures that protections are in place throughout the DevOps process, helping to:

- ✓ Increase productivity
- ✓ Deliver more secure products and services
- ✓ Increase consumer confidence and brand equity
- ✓ Improve overall security posture

In general, InfoSec teams spend inordinate amounts of time identifying and remediating security vulnerabilities. The process of applying security protections in the final stages of development, or patching vulnerabilities after deployment, are both time-consuming and resource intensive. This challenge is often compounded by the tedious process of identifying individual application and asset owners—especially in the case of microservices, which frequently involves many owners.

By integrating InfoSec early in the DevOps process, many vulnerabilities can be prevented, and cybersecurity teams can ensure that defects cannot be exploited in production. Taking such an approach reduces operational costs by proactively addressing security rather than responding on a case-by-case basis and putting out fires.

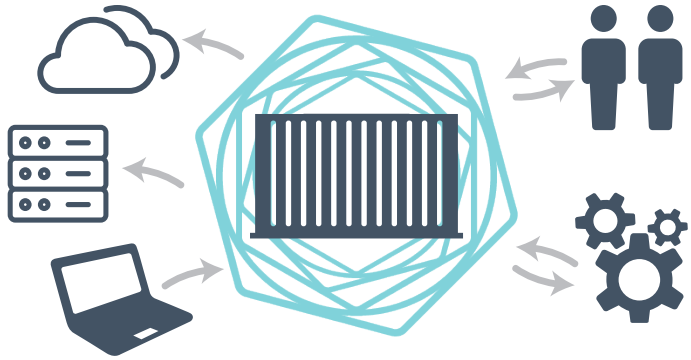
Moreover, being proactive can also negate time-consuming and costly incident response efforts. Finally, preventing potential vulnerabilities enables InfoSec leaders to implement higher-value programs that more effectively support compliance, and improve risk management.

Putting reasons in action: securing application containers

DevOps teams are rapidly adopting containers to enable the continuous development of new applications and services. In fact, containers are one of the hottest innovations in enterprise IT, with 40% annual growth in adoption, according to the IT monitoring service Datadog.

> "If a container has a vulnerable piece of software and the security team is in a DevOps model, they can work quickly, fix the container image, and the next time that container gets spun up, it is secure."
>
> — MANNIE ROMERO
> Executive Director
> Office of the CISO, Optiv

Containers are transformational packages that dramatically accelerate and simplify application development and deployment while lowering operational costs, increasing innovation, and speeding deployments. Standalone, lightweight, and efficient, containers enable seamless portability across different computing environments through write once, run anywhere capabilities.



In addition to greater consistency and more streamlined processes, containers also offer developers increased agility. Yet these extremely short-lived assets can be quite difficult to secure using current vulnerability management techniques. For cybersecurity teams, it requires nearly constant environment scanning with no guarantee of detection. The lack of container IP addresses or logins for credentialed scans further complicates the security process and renders traditional testing ineffective. Finally, remediation or patching is impossible once a container is deployed, requiring a completely new approach to cybersecurity.

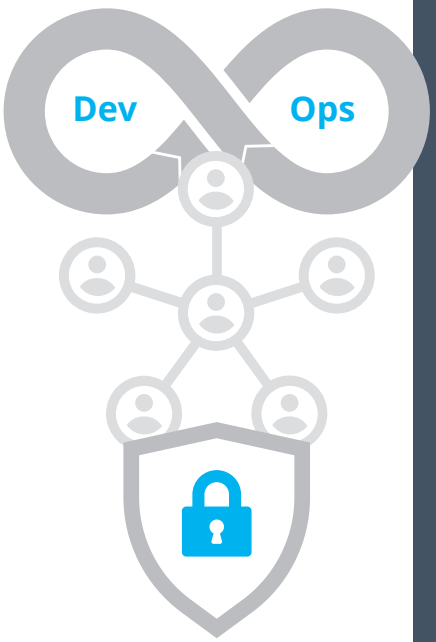
A principle means of reaching these new security objectives is leveraging secure DevOps principles. These include moving security testing closer to the beginning of the software lifecycle, adopting automation where possible, and focusing on the actual container image itself.

For example, developers can reduce risks and ensure higher degrees of protection by performing vulnerability and malware checks of container images and certifying compliance at build time. In this secure DevOps model, security tests live in the CI/CD and take less than a minute to complete. These kinds of methodologies are the result of a new IT mindset that emphasizes the primacy of an immutable infrastructure where components are replaced and redeployed rather than changed in place.

Toward that end, adopting a comprehensive container security platform offers an effective means for gaining greater visibility into container images and integrating security into the DevOps pipeline.

A platform approach includes container security solutions that provide the guardrails to keep developers within a certain risk posture, and enforce corporate policy. Having the right platform in place guarantees that developers never have to leave their CI/CD systems and that every build is protected.

Moreover, a container security platform ensures that testing becomes a fundamental part of DevOps processes without impeding development velocity.



Taking a New Approach to Organizational Security

The increased speed of IT brought on by digital transformation is fundamentally changing how IT security, developers, and corporate end users think and work.

But greater connectivity and faster production can also lead to increased risks. Ensuring effective safeguards requires an organization-wide cultural shift and a new mindset in which cybersecurity becomes the responsibility of all stakeholders. Consider these recommendations for how you can increase security awareness and commitment:

DevOps Teams

- Embrace security training to understand cyber risks
- Incorporate InfoSec within small, cross-functional teams
- Move security tasks further left in the DevOps toolchain
- Encourage communication across teams and silos
- Designate responsibility for security testing directly to developers
- Ensure that developers never leave their toolchain environment

InfoSec Teams

- Perform continuous risk- and trust-based assessments
- Approach application security testing as a continuous improvement process
- Reduce operational risks by breaking down large projects into smaller, simpler changes
- Participate in DevOps scrums and planning cycles
- Embed a security champion model throughout the organization, especially in DevOps
- Prioritize remediation to focus on securing high-level risks, even if that means allowing for low-risk vulnerabilities to persist

Conclusion

In terms of delivering solutions and services both faster and securely, organizations will achieve higher performance levels when they seamlessly combine InfoSec with DevOps.

Embedding security into the CI/CD pipeline, automatically programming controls, and adopting a preventative security posture are all critical to that integration.

InfoSec teams will find that DevOps processes can become part of the solution to cybersecurity challenges, ensuring more thorough and responsive approaches. And faster development speeds, as well as an increase in the quality of products and services, will improve the company's competitive position.

NEXT STEPS:

To learn more about secure DevOps and container security, visit the Tenable Container Security Resource page: tenable.com/secure-insights

Tenable™, Inc. is the Cyber Exposure company. More than 23,000 organizations of all sizes around the globe rely on Tenable to manage and measure their modern attack surface to accurately understand and reduce cyber risk. As the creator of Nessus®, Tenable built its platform from the ground up to deeply understand assets, networks and vulnerabilities, extending this knowledge and expertise into Tenable.io™ to deliver the world's first platform to provide live visibility into any asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, large government agencies and mid-sized organizations across the private and public sectors.

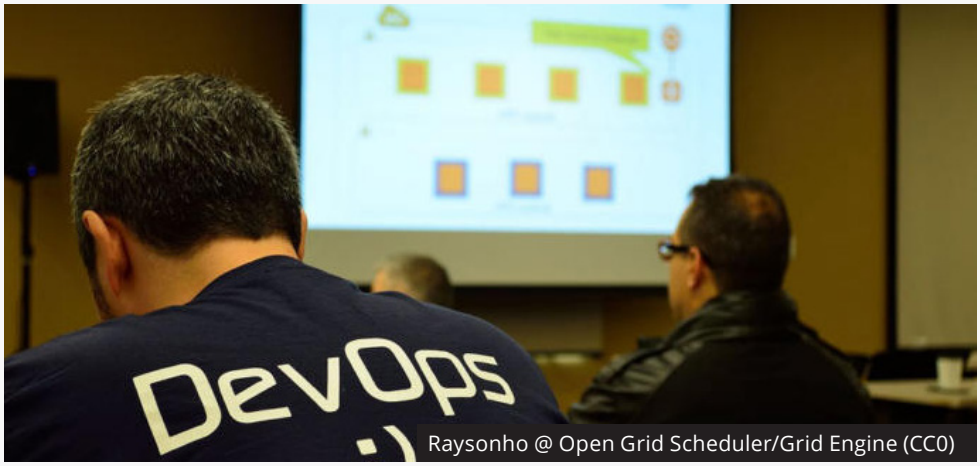
tenable™

IDG STRATEGIC MARKETING SERVICES

ADDITIONAL READING FROM IDG

The impact of DevOps on your bottom line

During Cybersecurity Awareness Month and beyond, DevOps is a philosophy to which security practitioners should pay attention.



Raysonho @ Open Grid Scheduler/Grid Engine (CC0)

By Rick Howard, Contributor, *CSO* | September 2017

DevOps is the most important innovation to the IT sector since the invention of the personal computer. Nearly everyone I have talked to in my travels, these past few years, says they are building their own DevOps shop. But when you probe them about what they are actually doing, most say they are deploying applications to the cloud. That is not exactly what DevOps is.

To put it in a nutshell, DevOps combines the cultural and technical philosophies of software development, quality assurance, and IT/InfoSec operations into a single system of systems that is managed as a whole. The purpose is to deliver applications and support services at a much higher velocity. With traditional software development processes and standard InfoSec and IT tool maintenance updates, it sometimes takes weeks, months and even years for organizations to roll out a new application, update an old application, install a patch to a machine, or add enhanced prevention controls derived from new intelligence. The DevOps mantra is to roll out ten deployments/ changes a day. That sounds good when you say it fast, but it is tough to find the edges of this new philosophy when you start to think about the implications.

To read the rest, click here.

ADDITIONAL READING FROM IDG

Learning to love DevOps

Security professionals need to embrace DevOps and use it to their advantage. The DevOps Handbook offers an up to date guide for this process.

By Frederick Scholl, Contributor, *CSO* | December 2016

To be honest, I'm not falling in love with DevOps yet. DevOps doesn't really seem to have a built in place for security, but we security professionals can't bail out. IT has never really had a home for security. So how to make lemonade out of lemons?

I first heard the term "DevOps" while finishing Gene Kim's book "The Phoenix Project". I had enjoyed Phoenix, especially after a stint managing information security at a large manufacturing firm. I heard that Gene was working on a new book on DevOps. But DevOps seemed to be a deep dive down into the weeds. Who would have thought it would go mainstream...an idea catching the wave of both demand and supply. The demand for more reliable systems that can keep up with customer needs and the supply of full featured cloud development and operations platforms.

DevOps did catch the wave, pulled along by its supporters' initiatives and creativity and pushed along by the acceptance of the cloud. Google Trends still shows a healthy growth of interest as of this writing. So I had some catching up to do. The good news was that I had been a long-time believer in the application of lean manufacturing concepts to information security. So I knew the concepts behind DevOps.

To read the rest, click here.