Mastek™

ENSAT

What is **DevSecOps**

Recent Trends in **DevSecOps**

DevOps v/s **DevSecOps**

Short Intro on **Mastek's** Offerings on **DevSecOps**

DevSecOps

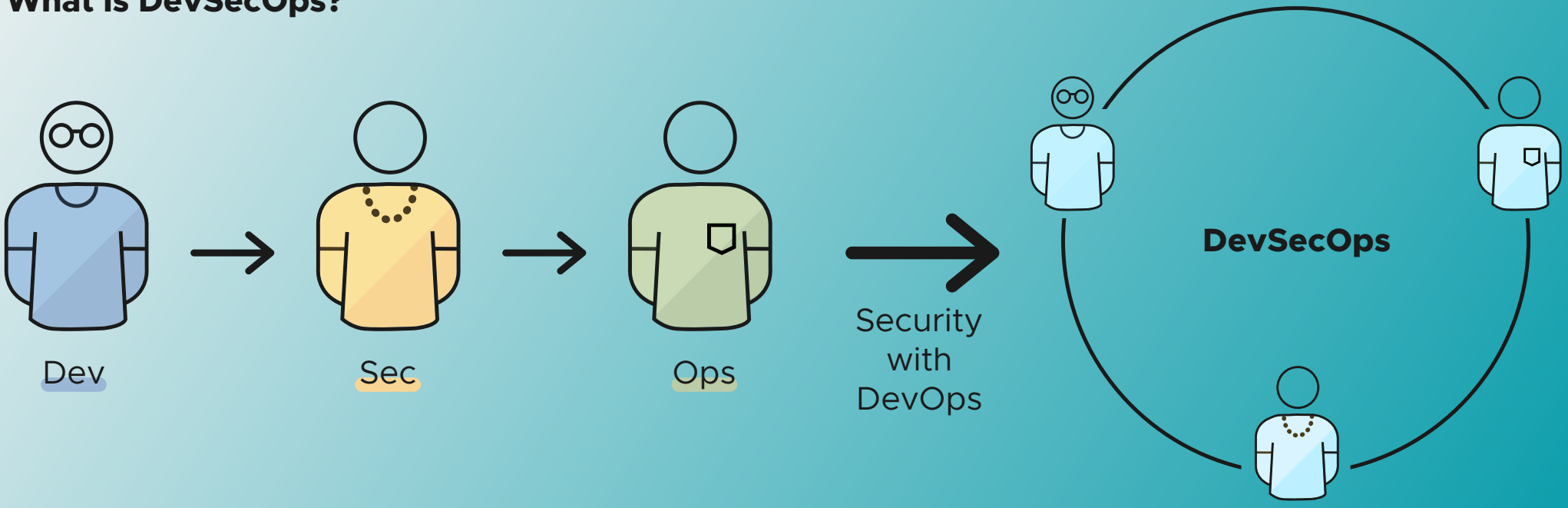
Do you practice DevOps?

It is time to take complete advantage of its agility and responsiveness by including security as an integral part of the entire app life cycle.

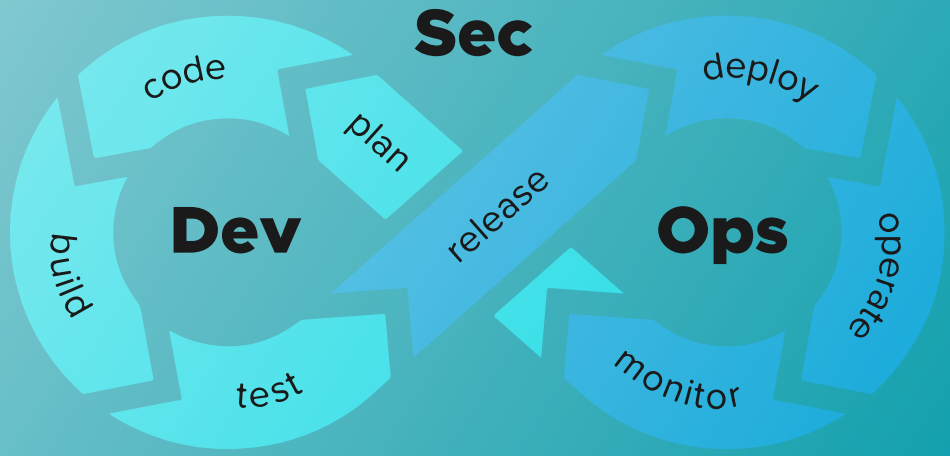
Integrate automated security in your DevOps practice.

Many organizations aim to shorten their system's development life cycle and provide continuous delivery with high software quality. Where DevOps combine a system's software development and IT operations, IT security plays an integral role in completing the entire life cycle of any application.

What is DevSecOps?



DevSecOps is a framework that integrates security to any application and infrastructure that is built on the methodology of DevOps and ensures that an application is less vulnerable and ready to use. Thus, DevSecOps - development, security, and operations - automating the integration of security at every phase of a software development lifecycle, from initial designing to integration, testing, deployment, and software delivery.



A definition of DevSecOps by Gartner states -

“DevSecOps is 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.”

Recent Trends in DevSecOps?

As the world witnessed record breaches in 2017, leading IT initiated the integration and automation of security practices throughout their software development life cycle to better fortify applications and protect their data.

A recent **2020 survey by GitLab** on Mapping the DevSecOps Landscape says:

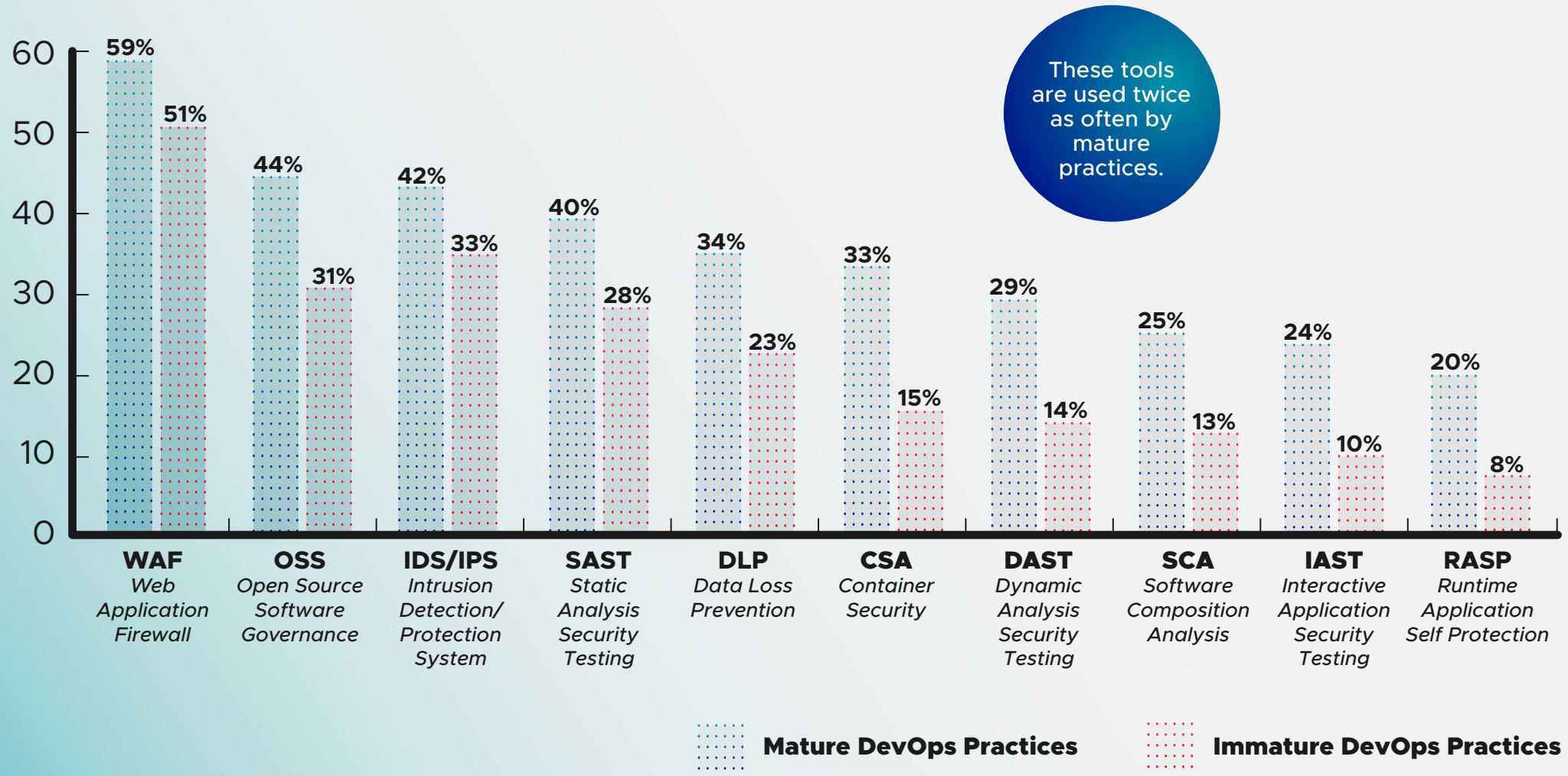
- ***CD (continuous delivery) is real***
  Nearly 60% deploy it either multiple times a day, once a day, or once every few days. That's up from 45% last year.

- ***As per the survey's top Development findings***
  DevOps = faster releases
  If you're a developer, DevSecOps just works. Nearly 83% of them report they're releasing code more quickly.

- ***As per top Security findings***
  DevSecOps = changing roles
  Security can be found on cross-functional teams and working closely in collaboration with developers, both of which represent a significant change from the past.

  It further said: After what seemed like an eternity of being outsiders looking into software development, security pros now report their roles are beginning to change. **Nearly 28% reported being part of a crossfunctional team focused on security** (perhaps really putting the "sec" in DevSecOps).

  Let's have a look at **DevSecOps Community Survey 2020** by Sonatype in which experienced IT professionals from all over the world took part.



Mature DevOps teams properly integrate automated security tools almost two times more often than immature development practices.

Market Overview

CAGR **31.2%**

- Growing need for highly secure continuous application delivery will drive the growth in DevSecOps market.
- Increase focus on security and compliance to help in adoption of DevSecOps solutions.
- Resistance to adopt new tools and technologies may restrain the growth of the market.

The DevSecOps market size is expected to grow from USD 1.5 billion in 2018 to USD 5.9 billion by 2023, at a Compound Annual Growth Rate (CAGR) of 31.2% during the forecast period. The growing need for higher secure continuous application delivery and the increased focus on security on security and compliance are the major growth factors for the DevSecOps market.

Let’s understand the Importance of DevSecOps and its Benefits.

The methodologies of DevOps and DevSecOps have many similar aspects such as the use of automation and continuous processes to create collaborative development cycles. However, while DevOps prioritizes delivery speed, DevSecOps shifts security to the left. It is an integration of automated security with an organization’s DevOps practice. It validates all the components of a codebase without slowing down the development lifecycle. The goal is to promote the fast development of a secure codebase., all organizations having a DevOps framework should strive to adopt the DevSecOps.

Imagine a top functionality car without seatbelts and an auto-lock system. Would you prefer to buy it?

Even though the car is developed with top-notch functions and mechanisms, you still have your doubts, because security sits on top of your priority list while buying any car, considering the chances of accidents, however a top model car it may be.

Similar is the case while developing a software application, where a car is an application and integrating security into its infrastructure is just as important as having a safety belt to your car seats. Your DevOps framework requires automated security integrated with its development and operational functions, to protect your application from any kind of cyber accidents and hacks that may occur. The DevSecOps methodology helps identify security issues early in the development process rather than after an application is set for customers to use. It aims is to address the need for proactive, customer-focused security that anticipates rather than reacts to data breaches or other cyberattacks.

Organizations that have implemented the DevSecOps framework have benefited from numerous advantages:

Speedy Recovery
In case of any security incident, an application's recovery is enhanced by utilizing templates and pet/cattle methodology.

Improved Security
With increased code coverage and security automation through the use of immutable infrastructure, the overall security is improved by reducing vulnerabilities and insecure defaults

Secure by Design
DevSecOps ensures automated security review of code, automated application security testing, educating and empowering developers to use secure design patterns.

Cost Reduction
As the security issues get detected and are fixed during the development phase. It also increases the speed of application delivery

Boost in Product Sales
In a DevSecOps world, proactive and preemptive threat hunting, and continuous detection and response to threats and vulnerabilities mean that there are fewer major incidents and more mitigations. This helps in cutting down any bad publicity, and therefore can potentially increase sales

Everyone is responsible for Security
DevSecOps fosters a culture of openness and transparency from the earliest stages of development. It also enables a culture of constant iterative improvements with its ability to measure several things which can be seen by everyone.

If you are contemplating a major DevOps transformation or a modest improvement to your current software delivery pipeline, it is important to assess where you stand, how far you have already progressed, and what challenges remain.

ACCELERATE GTM with **MASTEK's 5-Week Implementation** of Azure DevSecOps

Mastek's 5-week implementation of Azure DevSecOps

Mastek has an extensive experience in Automated Infrastructure Provisioning, Migration Services, Integrated Security, Governance, and Quality Engineering to accelerate DevSecOps with Microsoft Azure.

We adopt a maturity roadmap for the transformation of an organization's DevOps framework. Using our iterative DevACT (Assess, Consult, Transform) framework, we partner with you in building a DevSecOps roadmap with maturity assessment, chart your best route forward and support your transformation across people, processes, and technology.

We provide a framework for incremental, comprehensive transformation, supporting your organization on its DevSecOps journey by understanding, exploring, practicing, maturing and then innovating the best suited roadmap to mature your DevOps framework.

Mature Your DevOps Framework with Mastek's DevACT Approach!