REPORT REPRINT

Enterprise DevOps broadening across industry, companies

SEPTEMBER 30 2019

By Jay Lyman

Enterprises are increasingly looking to DevOps workflows and releases that combine software development and IT operations as they seek to modernize their infrastructure and leverage innovative technology. Our recently published VotE DevOps advisory report provides perspective on the state of enterprise DevOps today, and where the trend is headed.

Introduction

Enterprises are increasingly looking to DevOps workflows and releases that combine software development and IT operations as they seek to modernize their infrastructure and leverage innovative technology such as cloud computing and cloud-native software (containers, Kubernetes, serverless). Our recently published VotE DevOps advisory report provides perspective on the state of enterprise DevOps today, and where the trend is headed based on our survey of enterprise IT decision-makers and practitioners.

451 TAKE

DevOps is being driven by advantages that go beyond faster releases, including flexibility to quickly respond to changes in the market, managing larger-scale infrastructure with smaller teams, and enhanced teamwork. Nevertheless, there are still challenges that include cost, complexity and lack of skills. Our survey tracked the most important tools and components of DevOps. We are also researching DevOps migration to the cloud and how organizations are moving beyond on-premises and private cloud deployments, which represent a majority of DevOps today, and running DevOps in public clouds.

Context

Among the biggest changes in enterprise DevOps – the joining of software development and IT operations for faster releases, efficiency and to effectively leverage cloud computing infrastructures – has been the top-down adoption of DevOps methodology and technology. This has been driven largely by digital transformation, for which DevOps can be a starting point or a building block.

In addition to the involvement of more management and leadership in DevOps, our VotE: DevOps 2019 survey shows a number of other stakeholders – security, central IT admins, data analytics and science teams – that are critical to successful DevOps implementations, particularly as they span more broadly across enterprise organizations. Data processing and analytics shows up in our survey among the top applications released with a DevOps process.

Security professionals and teams are consistently cited as a primary stakeholders, in addition to developers and IT operators, as the Secure DevOps trend (DevSecOps) rapidly evolves. Our research indicates security is increasingly seen more as a requirement and enhancement, and less as something that will simply slow down DevOps teams.

Our survey showed heavy crossover between DevOps and cloud-native software such as containers and Kubernetes. Enterprise DevOps teams were heavy users of containers (60% at full or some adoption) and Kubernetes (30% at full or some adoption), and most respondents (90%) said cloud-native is somewhat or very important to their DevOps releases. While most enterprise DevOps today is occurring on-premises or in private clouds, survey respondents expressed a strong interest in managed services, and we expect the share of DevOps using cloud infrastructure will grow over time as we track it, based on what's happening with enterprise workloads in general.

Top-down adoption of DevOps growing along with pace of releases

DevOps has grown beyond a bottom-up trend driven primarily by developers. In today's DevOps market, adoption is driven as much, or more, by company leadership, managers and central IT teams, which are focused on better serving developers, driving efficiency in IT operations, and creating enhanced value for their organizations. Seventy-nine percent of organizations are at some level of DevOps adoption, further illustrating the trend as an enterprise priority, as well as its maturity.

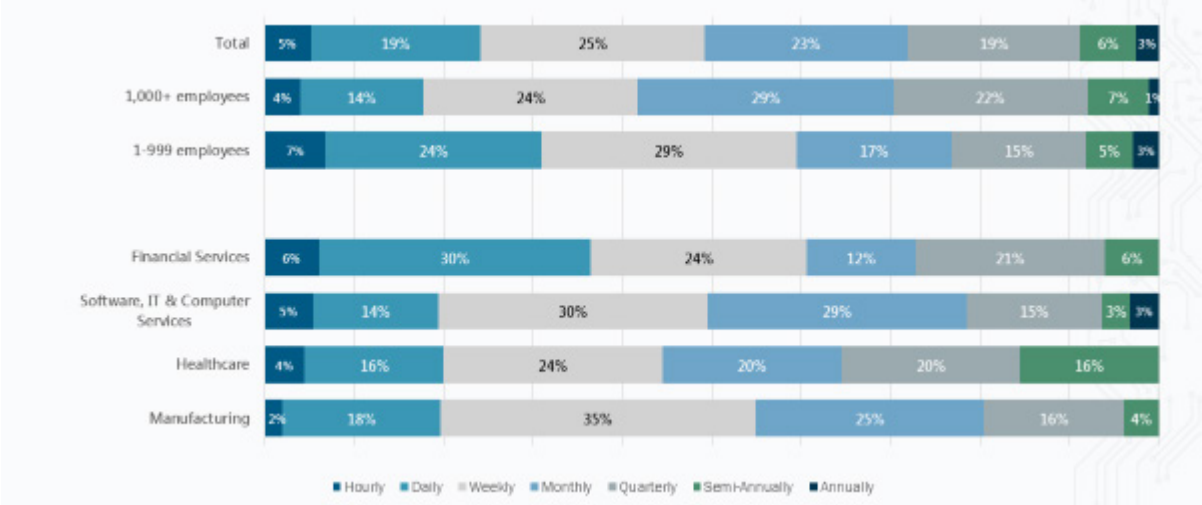
Team and business-unit adoption may be a waystation to broader, company-wide adoption, but only about a third of organizations not yet at full DevOps adoption plan to move to full adoption during the next year – most likely new technology adoption and digital transformation leaders. Indeed, we've seen a connection between DevOps and digital transformation, particularly because, in addition to faster releases and more efficient IT operations, DevOps embodies effective use of cloud computing resources and cloud-native software.

Our survey highlights how weekly, daily and hourly releases outnumber monthly, quarterly and semi-annual releases – a far cry from 10, five or even a few years ago, when monthly and quarterly releases were the norm for many organizations. Larger organizations with 1,000 or more employees are less likely than smaller companies to have weekly, daily or hourly releases, indicating faster releases may be more challenging for larger companies.

Figure 1: Quickening pace of releases

Source: 451 Research LLC

Q. In the last 12 months, how often did you deploy most software applications to production?



DevOps drivers, hurdles and culture

DevOps has always been about faster, iterative software releases enhanced by collaboration between developers and IT operators, but our survey revealed other drivers and advantages. Top among enterprise DevOps benefits is flexibility to quickly respond to changes. This highlights how organizations are interested in DevOps beyond single or multiple releases and teams, and seek to build readiness into their organizations to act upon new data, market changes and global events.

Efficiency is also a main benefit of DevOps, enabling organizations to manage larger-scale infrastructures and more frequent software releases with smaller, more efficient teams. The market demand for continuous updates and new features is a key driver, reflective of end users and consumers eager for new features and impatient with latency. Flexibility in developer tools, another key benefit of DevOps, highlights that, while organizations want to manage and sanction DevOps deployments, they are aware of the need to support developers and their choices for tools and technology.

According to our survey, cost is one of the primary barriers to DevOps deployment. The cost issue may essentially boil down to personnel and the expense of hiring DevOps champions and teams. Technical complexity ranks high on the list of DevOps barriers, consistent with the hurdles of other new technologies and methodologies, such as cloud computing and cloud-native. The security and compliance risks of DevOps also rank high as barriers to deployment.

These are legitimate concerns, given not all teams and releases can be blended and included in compliance with HIPAA, Sarbanes-Oxley, PCI, the General Data Protection Regulation, and other regulations. Digital transformation leaders rank technical complexity and concerns about governance, security and compliance risk as the top challenges of DevOps, while digital transformation learners and laggards say the biggest DevOps challenge is cost. Our survey shows cost, security/compliance and technical complexity also emerge as barriers to the expansion of DevOps to more of organizations' applications, releases and teams.

DevOps is very much about culture, which can be the basis for both synergies and challenges. Aligning priorities and objectives and fostering cross-discipline experience across development, IT operations, security and other areas were leading cultural synergies driven by DevOps. While some cultural challenges – such as overcoming resistance to change and aligning differing priorities for stakeholders and teams – diminish for organizations that have implemented DevOps for more than two years, other cultural challenges (promoting communication between teams not accustomed to working together, sharing responsibility for problems and demonstrating equity of benefits/costs) actually increase for organizations that have implemented DevOps for more than two years.

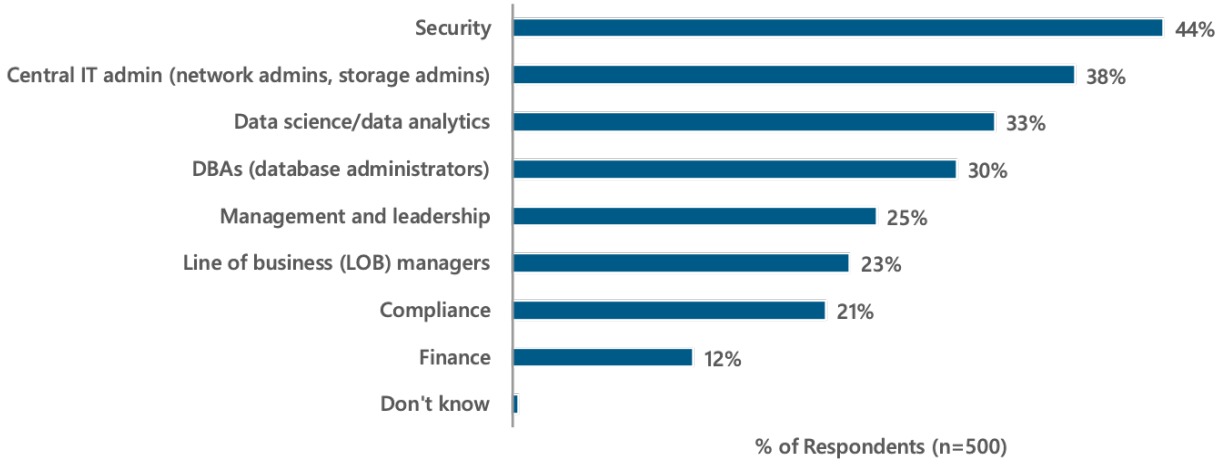
The stakeholder spread of DevOps

While DevOps has always centered on collaboration among software developers and IT operators, successful DevOps implementations pull in a range of additional key stakeholders as they spread across the organization. Security professionals and teams lead the pack of additional stakeholders (44%), in line with the evolution of the secure DevOps trend that has made integration of security tooling into DevOps processes a growing priority for enterprises.

Central IT administrators (network/storage) are also prominent among additional DevOps stakeholders, consistent with the prevalence of sanctioned DevOps deployments. Although database administrators have been notoriously left out of enterprise DevOps releases in the past, they, along with data analytics and data science teams, are among the key additional stakeholders. The presence of management and leadership as key stakeholders provides further evidence of the emerging top-down trend in DevOps adoption.

Figure 2: Stakeholder spread

Source: 451 Research, Voice of the Enterprise: Q1 2019 VotE DevOps survey
Q. Beyond developers and IT operations, who are the primary stakeholders in your DevOps implementation?



We see DevOps being used for a variety of applications, both internal and external. Our survey indicates the top types of applications deployed with a DevOps approach are data processing, analytics and BI – not surprising, considering these are among the top applications for the cloud and often represent new greenfield applications that are a good fit for DevOps.

IT/infrastructure optimization functions are also a top application type, given the importance of IT automation and efficiency to overall enterprise operations. Consumer-facing functions are not far behind, and this is consistent with anecdotal research that indicates once an organization can successfully implement DevOps for internal functions, it then leverages the same approach for external applications.

Growth of the Secure DevOps trend

Security, once viewed as a roadblock slowing down application development, is increasingly tied to quality, and thus baked in. The fact that security tooling is increasingly integrated, automated and intended for software releases has helped fuel this change. In addition, high-profile security incidents and breaches serve as a near-constant reminder that no organization wants to suffer the black eye of a security breakdown, particularly if it can be prevented or its likelihood reduced.

DevOps can enhance security, including software composition and open source analysis, logging or analysis of security events, source code protection, and vulnerability assessment. There is some variance by industry, such as financial services, which rates logging or analysis of security events as a greater security enhancement than software composition and open source analysis. In our survey, 53% of organizations say more than half of their DevOps processes include security elements. We expect this will increase as the Secure DevOps trend continues to evolve.

Critical tools and components of DevOps

Continuous integration/continuous delivery (CI/CD) software such as Jenkins and Bamboo are the most commonly used DevOps tools – not surprising, given these tools are often part of organizations' initial homegrown automation and DevOps efforts.

Monitoring, logging and alerting tools that are designed to provide visibility/observability, such as Datadog, New Relic and Splunk, are also top DevOps tools in use. Communications and collaboration tools such as Slack and PagerDuty, and API and code management tools like JFrog and Sonatype, are likely to be a part of enterprise DevOps processes, highlighting the importance of tools for both developers and IT operators, as well as combined DevOps teams.

Infrastructure automation tools such as Red Hat's Ansible, Chef, Puppet and Salt – among the original DevOps building blocks – are the next most likely to be included in DevOps, followed by build tools such as Gradle, Maven and Make and source code repositories such as GitHub and GitLab. Not far behind them are process automation tools such as Bitnami (acquired by VMware), Electric Cloud (acquired by CloudBees), Plutora and XebiaLabs, as well as test automation tools such as Quali, Rally and Selenium.

Our survey indicated heavy use of cloud-native software, including containers and Kubernetes, by enterprise DevOps teams, with 90% of them viewing cloud-native as very or somewhat important. DevOps-focused organizations identify containers and microservices as the most important cloud-native technologies. We have always seen a strong link between these two, and it also often represents the start of cloud-native in organizations that are primarily focused on leveraging containers to move beyond monolithic applications toward microservices.

Still moving beyond on-premises and private clouds to public clouds

Enterprise DevOps teams continue to implement DevOps processes in on-premises private cloud and non-cloud IT environments. However, IaaS/PaaS and SaaS are emerging as both environments in use and as primary environments for DevOps. Organizations that have implemented DevOps for more than two years are nearly twice as likely to identify IaaS/public cloud as a DevOps environment (35%), as opposed to those that have implemented DevOps for two years or less (18%).

This is consistent across all survey respondents and within those that are implementing DevOps using multiple environments. It is also in line with anecdotal research indicating most enterprises are still keeping their DevOps deployments 'behind the firewall' and are running them on top of on-premises and private cloud infrastructure that they control.

Managed services are extremely or somewhat important to enterprise DevOps, according to 97% of respondents. The study also indicates significant use of managed services, with more than 60% indicating they are part of their DevOps implementations. IaaS, SaaS and PaaS are among the leading managed services used in enterprise DevOps.

DevOps skills in demand

Organizations identify IT operations skills as the most essential for enterprise DevOps. We've always believed the bulk of DevOps-related disruption is happening on the IT operations side. IT operations skills aligned to DevOps environments emerge as the top essential skill and number-two-ranked expertise/personnel gap.

Domain experience – where professionals can carry what they've learned in development, IT operations, security or other areas to better support DevOps – is deemed essential, and emerges as the top type of skill identified as lacking. Management and leadership rank highly on the list of skills deemed essential for DevOps deployments, providing further evidence of the increasingly top-down adoption of DevOps.

Measuring and proving DevOps success

Our survey investigated how enterprises measure their DevOps success, and how that is used to spread DevOps across more of their organizations. Quality metrics such as defect rates and vulnerabilities lead the way. This is consistent with how DevOps feedback loops work, and highlights the growing importance of security in DevOps. Organizations are using business-level metrics as DevOps proof points, including customer satisfaction, customer experience and response times.

Application performance metrics, such as availability, latency and throughput, also emerge as key DevOps benchmarks, which, in practice, generate the raw material for the customer-facing business metrics. The ability to measure and document the value of DevOps – whether in terms of time-to-release, staff efficiency/productivity, or digital user experience – is particularly critical as organizations look to expand the DevOps approach more broadly across the organization to additional software releases and functional teams.

Figure 3: Measuring and proving DevOps success

Source: 451 Research, Voice of the Enterprise: Q1 2019 VotE DevOps survey
Q. How do you measure/prove the business value of DevOps implementations?