Infosys®
Navigate your next

DEVSECOPS: FUTURE-PROOFING DEVELOPER-TOOL ADOPTION FOR A HYBRID IT ECOSYSTEM

Infosys® | Knowledge Institute

Contents

DevSecOps evolution continuum	5
Enterprise scale CICD	8
Continuous Security	10
Adoption across ERPs	12
DataOps	14
Artificial intelligence/machine learning Ops	16
NetOps	18
Application lifecycle management	20
QA DevOps	22
DevSecOps for business agility and live engineering	24
Advisory council and contributors	25

Enterprises embrace digital technologies to deliver safer, quicker and more reliable business value to their customers. With rapid advancements in efficiency and technology consumption, software delivery must remain resilient and secure. DevSecOps (short for development, security and operations) helps enterprises embed security into their value delivery system while ensuring the consistency, governance, efficiency, scale and speed associated with the software development are not compromised. Our clients are rapidly adopting DevSecOps tools and technologies to reduce the overall cycle time – from when the business idea starts to when the software is in the end-customers' hands. This framework enables teams to establish reliability and intelligent observability within their application portfolios, making it easier to collaborate and detect problems early in the engineering lifecycle. Our report presents key macro trends, with an emphasis on tools and technology, across the DevSecOps architecture landscape in application lifecycle management, security practices, ERP packages, data and analytics, QA practices, software-defined networks and machine-learning operations.

Global enterprises are accelerating their digital and cloud transformation-led engineering journeys to evolve their IT landscape in response to the impact caused by the global pandemic. The outbreak has placed new challenges across businesses and forced a significant portion of the workforce to operate remotely. To effectively manage this sudden disruption, enterprises have no choice but to shift to higher digitization levels.

A digital business requires IT teams to move faster to adopt new technologies, transform legacy systems and respond to ever-changing customer needs. This accelerated business model requires integrating DevSecOps and cloud technologies into the IT value stream, which helps enterprises achieve closer alignment within multiple teams, faster time to market and streamlined engineering and operations processes.

Today, enterprises must re-examine **collaboration**, **automation**, **security**, **compliance**, **governance** and **analytics** across key dimensions such as application technologies, packages, data, testing, infrastructures and networks to make IT operations resilient and agile.

Almost all enterprises have faced challenges with a remote workforce. In addition to sudden surges and declines for products/services, they have seen unprecedented threats and attacks from malicious actors, which has affected their security, compliance and governance protocols.

To mitigate these risks, organizations must always look for ways to safeguard their workforce using end-point security automation solutions, best-in-class authentication and authorization mechanisms, as well as touchless automation. They must secure their IT supply chain by tightening source code development practices and validating application vulnerabilities early in the testing lifecycle, which requires embracing antifragility aspects in application development and following chaos engineering principles. They should also enforce organizational compliance policies while provisioning infrastructure on the cloud using codified policies with automation across the DevSecOps pipelines.

Enterprises must be poised to convert their siloed, process-based ecosystem into a live enterprise where intelligent feedback on performance and outcomes is delivered at every critical point in the engineering lifecycle. Furthermore, their applications will have to be more resilient and integrate with DevSecOps tools and technologies to assure higher predictability and client value.

DevSecOps evolution continuum

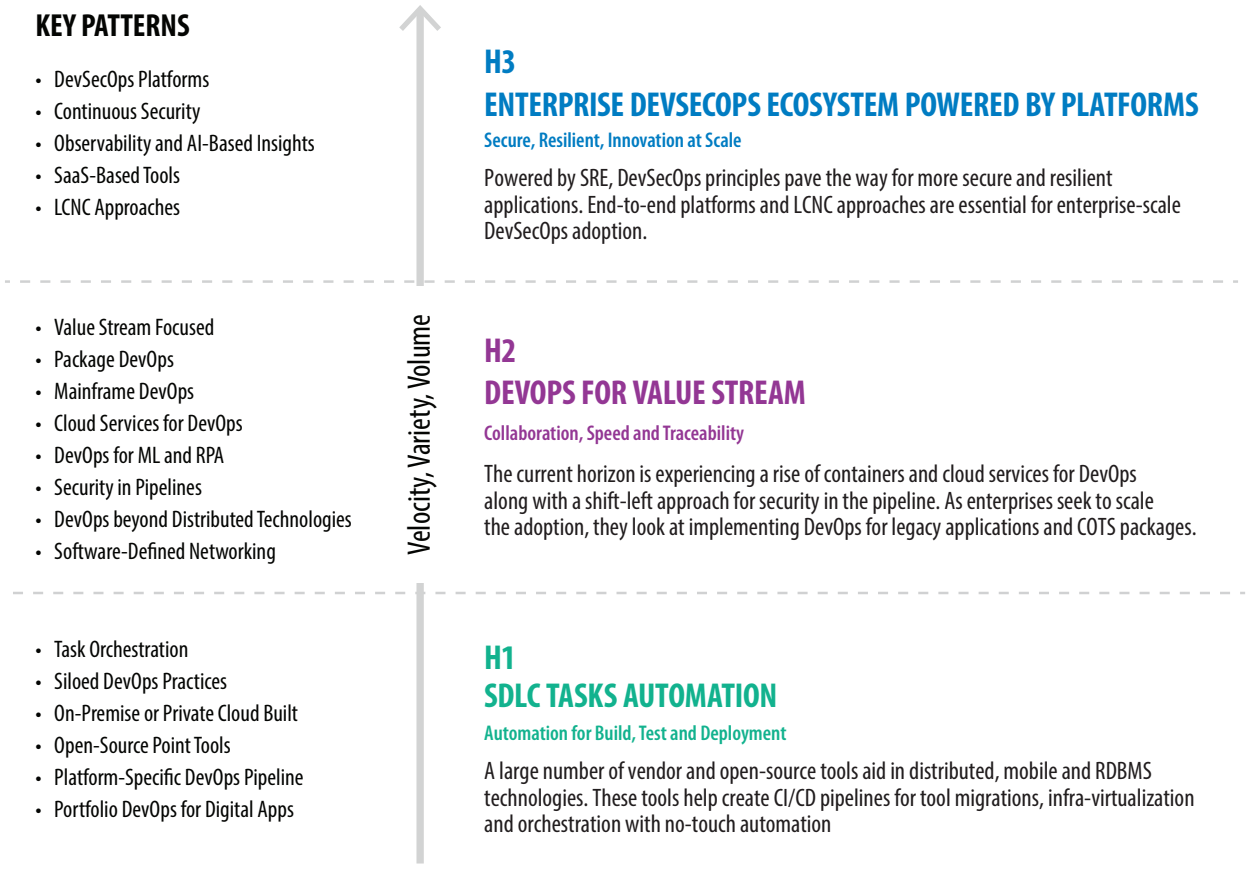
The concept of combining development and operations (DevOps) gained traction between 2008 and 2009 when businesses worked to eliminate the divide between the two teams and automate the repetitive steps in the software engineers' daily workflows. Infosys experts consider this to be the starting point of the three horizons in the DevSecOps journey.

Horizon 1 (H1): As the software development lifecycle **(SDLC)** ecosystem evolved, **open-source point tools** paved the way for **task orchestration** and the **DevOps pipeline**. This pipeline orchestrated mundane tasks for code-automated builds, tests and deployments. Engineering teams felt the need to integrate and deploy the code at high frequency, but limited solutions were available to fulfill this demand. These pipelines were primarily implemented on on-premise/private cloud infrastructures using open-source tools.

Horizon 2 (H2): Over the last few years, rapid advancements in areas like containerization, data analytics, artificial intelligence/machine learning (AI/ML), security tooling and cloud computing have elevated DevOps to complex orchestrations. These orchestrations involve **environment provisioning** and **commercial off-the-shelf (COTS) packages**, and a **value stream-focused** approach to enhance the maturity and efficiency of software delivery. Today, continuous integration (CI), continuous testing (CT) and continuous deployment (CD) have become mainstream, and team collaboration solutions are in place. DevOps now focuses on security and a DevSec Ops concept. Solutions have emerged in this horizon for legacy technologies like mainframe and proprietary technologies like SAP and Siebel, characterized by the **codification** of pipelines, software configuration, infrastructure and security.

Horizon 3 (H3): Soon, enterprises will embrace an ecosystem approach and adopt a framework with

Figure 1: Adapting to market dynamics: the three horizons



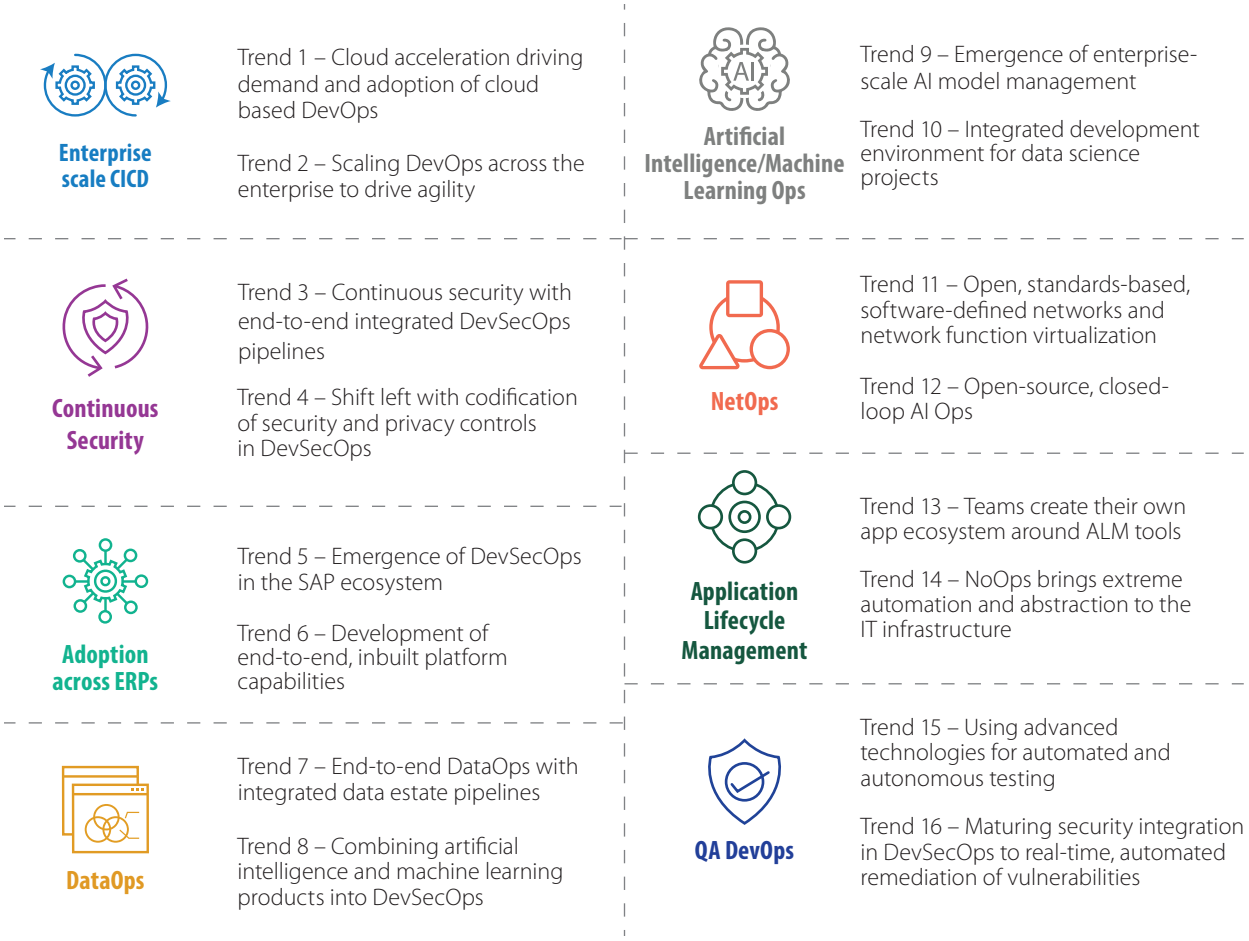
Source: Infosys

end-to-end **platforms** that provide cloud-agnostic DevSecOps automation as a service. They will focus on scaling DevSecOps adoption across the enterprise through **low-code, no-code (LCNC)** pipeline approaches utilizing inbuilt, continuous security. With audit, compliance, visibility and governance growing more prominent, **observability** capabilities and metrics in DevSecOps platforms will see a significant uplift. There will be an increased application of **AI/ML-based insights** in the DevSecOps lifecycle for enhanced efficiencies in CI, CT, CD, security, application lifecycle management (ALM), value stream management (VSM), monitoring and self-healing areas. **Site reliability engineering (SRE)** will enter the picture and complement DevSecOps principles to drive continuous deployments and production health. Application teams will also migrate their DevSecOps practices and pipelines to hyperscalers such as Azure, Amazon Web Services (AWS) and Google Cloud Platform (GCP). There will be an increased focus on team culture and collaboration to achieve the success of the complete value stream cohesively.

Let us explore the key trends across the following subdomains:

1. **Enterprise scale CICD**
2. **Continuous Security**
3. **Adoption across ERPs**
4. **DataOps**
5. **Artificial Intelligence/Machine Learning Ops**
6. **NetOps**
7. **Application Lifecycle Management**
8. **QA DevOps**

Figure 2. Key trends across domains



Source: Infosys

ENTERPRISE SCALE CICD

Initially, CI/CD used the wide availability of vendor/open-source tools for various lifecycle stages and integrated them with no-touch automation and infrastructure virtualization. This integration was primarily done for distributed, mobile and relational database management system (RDBMS) technologies.

With the growing adoption of DevSecOps to increase delivery speed, the focus is now shifting to CI/CD for all systems within the value stream, resulting in DevOps for packages, middleware and legacy technologies. CI/CD pipelines are being enhanced to include management tactics such as infrastructure as code, environment as service and pipeline as code. Self-service portals, dashboards and metrics are now a critical component of CI/CD implementations. Container DevOps that use container management technologies like Kubernetes, cloud-agnostic DevOps using Terraform, or cloud-native DevOps that avail cloud provider services like Azure DevOps, AWS Dev tools or PaaS platforms like OpenShift are also gaining momentum.

Enterprise-scale DevOps adoption continues to rise, and centralized DevOps platforms and reusable frameworks play key roles in standardizing adoption while optimizing costs. Better features such as SaaS tools, end-to-end tool capabilities or abstraction levels in container management platforms are available in DevOps tools. During enterprise adoption, key team changes are also occurring, like creating unified DevOps or SRE teams, which result in process changes.

Trend 1 – Cloud acceleration driving demand and adoption of cloud-based DevOps

We see increased cloud adoption as organizations migrate their existing applications to the cloud or use cloud-native development to build new applications. The result is an increased cloud DevOps trend using cloud-based commercial or open-source tools. Advanced configuration and container management, orchestration tools and technologies like Ansible, Chef, Puppet and Kubernetes are helping drive cloud DevOps adoption while cloud-native DevOps services like AWS Developer Tools, Azure DevOps, GCP Cloud Build, Azure and Lambda Cloud Formation are reducing installation and maintenance efforts required for DevOps tools. Many PaaS platforms such as OpenShift and Pivotal Cloud Foundry provide DevOps services to configure end-to-end pipelines easily.

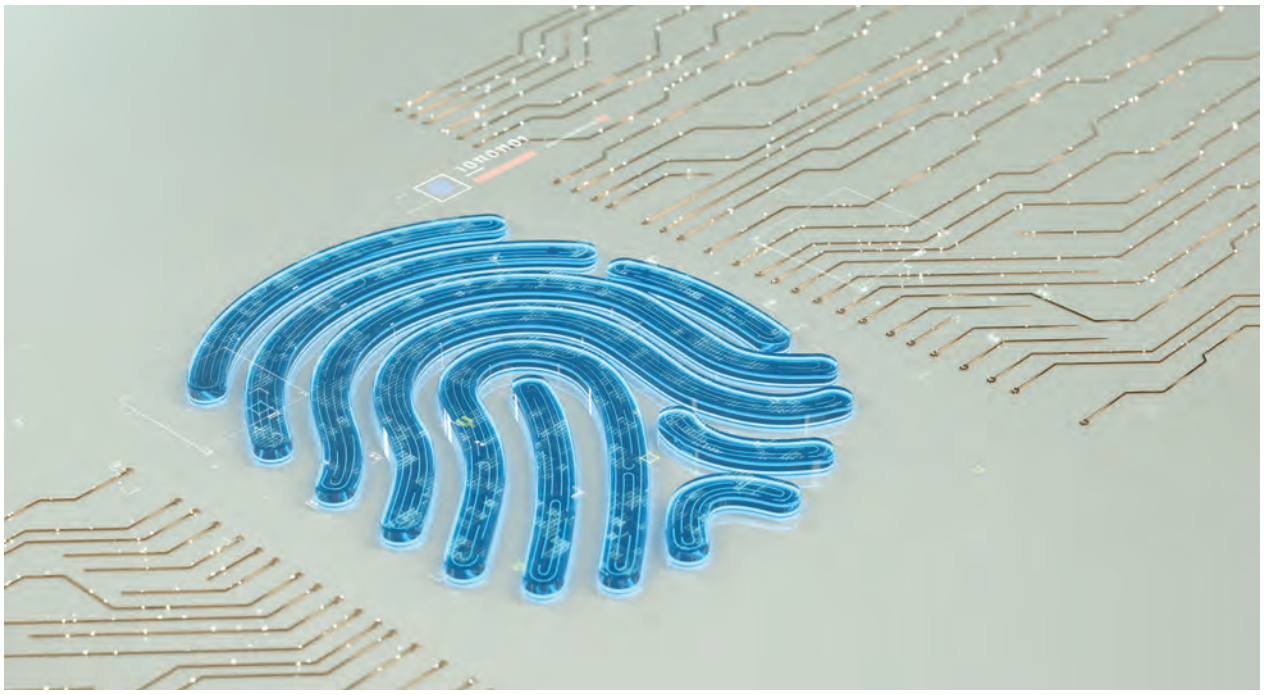
With more than 2.5 million visits per day to their global website, downtime was a big concern for a large, high-tech device manufacturer. To remedy the situation, they partnered with Infosys to create more than 90 declarative CI/CD pipelines for their site and its sub-systems using Azure DevOps and Azure Resource Manager. As a result, they achieved zero downtime along with a 90% reduction in provisioning and deployment time.

Trend 2 – Scaling DevOps across the enterprise to drive agility

Many businesses strive for enterprise-scale DevOps adoption once they see the DevOps benefits achieved in specific applications. However, scaling at an enterprise level needs more attention beyond setting up CI/CD for every application. Unplanned DevOps scaling produces adverse effects such as higher tooling and infrastructure costs, higher effort spent by application teams in setting up CI/CD, as well as non-standardized implementation. It is critical that organizations form a DevOps center of excellence (COE) which defines and advocates DevOps practices and guidelines. Along with that, reusable frameworks, a centralized DevOps platform, dashboards and analytics play key roles. Enterprise DevOps adoption goes beyond distributed technologies; all systems that are part of a value stream adopt DevOps to gain time-to-market benefits. This is why we are seeing DevOps developed for mainframes, customer relationship management applications, custom off-the-shelf products, middleware and business process management, and why vendors are now providing DevOps features within their products and as add-on tools.

An automobile manufacturer in the U.S. faced availability and scalability challenges with its existing DevOps solutions, including non-compliance to standards, rising costs of tools and infrastructure and security concerns. Infosys helped build an enterprise-scale, multi-cloud platform for them using AWS services, Terraform, Kubernetes and other tools to service 10 technologies and packages. With their centralized platform, their DevOps costs are reduced, standardization is achieved, and currency upgrades are easy.

CONTINUOUS SECURITY



To achieve fast delivery without compromising security, enterprises use security tools throughout all cycle stages rather than toward the end of a release. This left shift in security testing is enabled by tactics such as static application security testing (SAST), software composition analysis (SCA), dynamic application security testing (DAST), interactive application security testing (IAST) and runtime application self-protection (RASP) tools.

CI/CD pipelines integrated with security testing tools are orchestrated using command line interface (CLI) or application programming interface (API) integration capabilities. These integrations are supported by configuring incremental scans in the pipelines, no-touch gating of results using custom scripting, as well as identifying and reducing false positive reports. Docker tools like file scans, image scans, registry scans and container security tools are part of the continuous security checks for applications using container security.

The increased enterprise scaling of DevSecOps is driven by centralized platforms, reusable frameworks and dashboards. Concepts like compliance as code, policy as code and availability of security testing tools also help strengthen security. DevOps teams must collaborate with security subject matter experts (SMEs) to achieve success and adapt their processes to include secure coding practices, security as requirements and security as notices of findings and recommendations (NFRs).

Trend 3 – Continuous security with end-to-end integrated DevSecOps pipelines

This continuous trend to alleviate security issues and threats is more prevalent in B2B or B2C applications exposed on the internet. End-to-end DevSecOps pipelines include integration at all security phases of SAST, SCA, DAST, RASP and/or IAST in a no-touch fashion. Tool vendors offer easy CLI- and API-based integration capabilities for greenfield applications. Existing applications are more complex because scans must be run outside the pipeline or nightly batches, and custom scripts must be used to reduce false positives. Once the scans are performed to remove the huge backlog of issues, these tools are integrated into the pipeline. Many tools are emerging with features to improve integration, such as incremental scanning capabilities to reduce the time taken to scan, AI-based

tools to identify false positives and automated issue remediation. Container security is also incorporated into the CI/CD pipelines through Docker tools such as file scans, image scans, registry scans and container security testing.

An industry leader in brokerage and wealth management experienced a bottleneck in their underlying network of shared services. Due to manual security testing, they could not achieve early time to market for their end-user applications. They partnered with Infosys to implement an end-to-end DevSecOps solution to improve speed and quality, which resulted in a nearly 88% reduction in their release management effort, a four-times higher release frequency and $3.3 million in annual cost savings.

Trend 4 – Shift left with codification of security and privacy controls in DevSecOps

To successfully scale DevSecOps across the enterprise, businesses are looking at using reusable frameworks and centralized DevSecOps platforms. By implementing a consolidated security dashboard in the pipeline, they will collect defects found across all types of security testing tools, including SAST, SCA and DAST. With mature DevSecOps implementations, businesses are also defining metrics and setting up thresholds. The availability of SaaS-based security testing tools is opening the door to wider DevSecOps adoption by reducing the demand put on the underlying infrastructure and maintenance efforts of the tools themselves. As a result, we see encouraging effects. Open-source tools help reduce cost concerns attributed to the large number of licenses needed for enterprise-scale adoption. Enterprises are implementing organizational change management tactics such as enabling secure coding practices for developers, bringing in mindset change and integrating security as part of requirements and NFRs. Empowering DevOps teams on security aspects also reduces the additional load faced by current security SMEs due to frequent releases of fast-moving applications. A focus on building increased trust and collaboration between security SMEs and application teams only helps the cause.

A large telecommunications provider faced fraud losses close to $490 million, which were expected to increase by nearly 38% yearly. Adopting a holistic people, process and technology approach, the client implemented enterprise-scale DevSecOps for over 1,000 applications, which resulted in a 40% increase in feature delivery and the elimination of almost $1 million in fraud losses within the first seven months of the implementation.

ADOPTION ACROSS ERPs

At the onset, ERP packages like SAP, Oracle and Salesforce did not adopt DevSecOps. In fact, they provided little to no inbuilt platform support for their customers. SAP's version releases and configurations were tied to their complex Change and Transport System. If not properly tested, an organization's SAP transports could harm performance or even shut down the production environment. Oracle relied on custom tools and applications to manage and monitor their environment. While they had some CI/CD capabilities, they still did not adopt the full DevOps concept. Salesforce utilized manual deployment scripting and basic environment management tools but had no version control and branching.

But, as their businesses and technologies matured, these ERP providers began integrating their tools into the CI/CD pipeline, building up security measures and incorporating more capabilities directly within their ERP packages. In H3, ERP packages will provide a full spectrum of DevSecOps capabilities using native cloud and polycloud platforms. They will bring a higher level of automation with third-party tools, provide built-in branch management using version control software and integrated code quality management, and reduce overall defects and efforts for organizations.

Trend 5 – Emergence of DevSecOps in the SAP ecosystem

There is a constant demand for changes and quicker time to market with SAP's core business platform. As a package, SAP has worked to build self-contained tools to manage the application lifecycle. Now, with the advent of DevOps, SAP has kickstarted its agility journey by launching its Activate Methodology and embracing open-source toolsets to amplify its lifecycle management capabilities. Riding on DevOps' value, security considerations are now being built at the beginning of the design stage and through production deployment. Code vulnerability, general data protection regulation compliance and

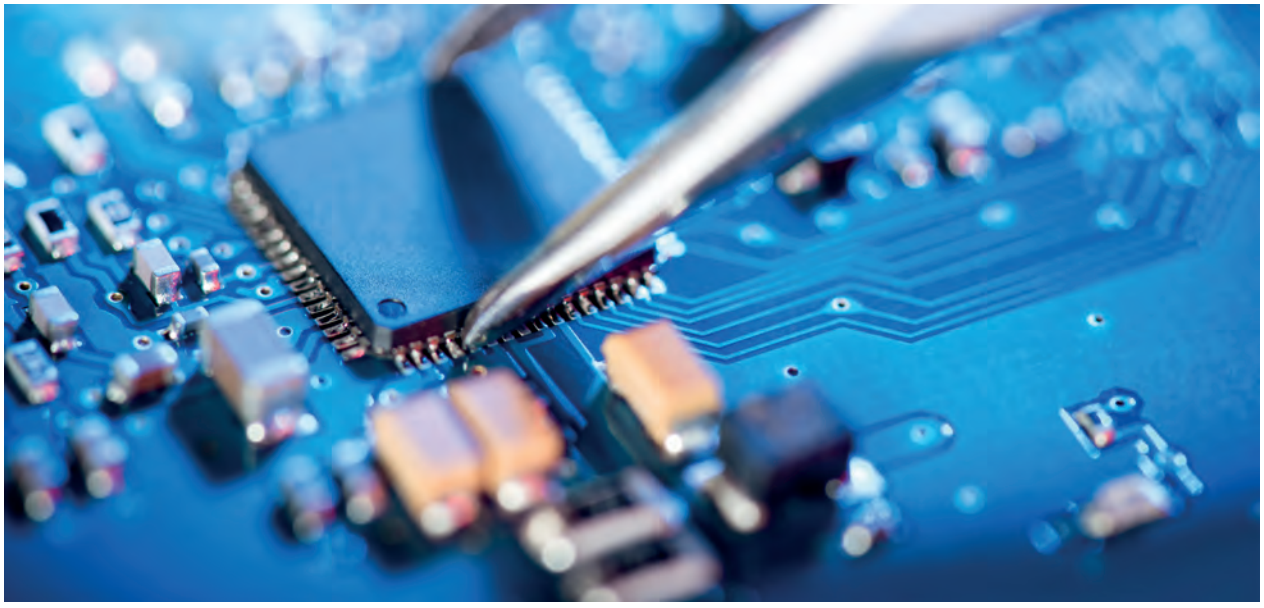
information lifecycle management have become key design considerations for enterprise applications. Various SAP tools like IDM, ILM, GRC, CVA, Onapsis and more help manage the different security requirements throughout the development lifecycle. Ever since SAP's Cloud Platform was reinforced with open integration, we see increased adoption of DevOps across SAP ecosystems. DevSecOps-enabled SAP Project delivery ensures faster, frequent deployments and makes systems more secure, reliable and efficient. Native toolsets like SAP's Focused Build, Solman change request management, CTS+ and SAP TAO are now widely used in DevSecOps deployments. These integrated toolsets are being amplified by operations support systems (OSSs) like Jenkins, partner tools like Virtual Forge CodeProfiler, Rev-Trac, Infosys DevOps Platform (IDP), Jira, Rally and more.

A leading luxury automobile manufacturer utilized DevOps to deploy five production releases in one month with 85% First Time Right accuracy aided by Infosys' IDP, Jira and HP ALM test management tool. Over two years, they achieved a 40% increase in sprint velocity and 100% automated regression testing.

Trend 6 – Development of end-to-end, inbuilt platform capabilities

DevSecOps is increasingly becoming the core element of Salesforce ecosystems. The Salesforce platform has long been known for its strong security capabilities and ability to govern the access of hosted data. However, certain dimensions of DevSecOps must be addressed by vendors, such as the lack of inbuilt version control of metadata. But as the platform continues to expand and evolve, Salesforce is renewing its attention on DevSecOps and maturing its current capabilities. New tools like Salesforce DX, scratch orgs, inbuilt data masking and DevOps Center aim to strengthen their platform further. The platform's rich set of APIs promotes partner framework adoption, and their open-source framework offers well-rounded, sophisticated DevSecOps capabilities for any size implementation.

Infosys worked with a leading North American financial services company to build a sophisticated DevSecOps framework with a higher level of automation. Inbuilt platform capabilities combined with third-party tools now provide the client with deep insights and integrated tracking of DevSecOps processes.



DATAOPS

Data architectures are continuously evolving and becoming volatile – from traditional data warehouses and data marts to data lakes and now lake houses. With this data platform agility, new tools are emerging with specific capabilities. Data platforms have moved from siloed CI and manual deployments across various data tools to pockets of enterprise CI/CD adoption.

In H2, there has been much movement toward public cloud adoption and cloud-native DevOps adoption. Organizations have explored varied technology stacks with multiple technology specific automation aligning into DevSecOps. Traditional data platform tools embraced custom CI/CD capabilities to integrate into enterprise DevSecOps adoption. Today, DevSecOps pipelines have gained momentum with the adoption of version control tool consolidation, data quality tools, digitized data governance and AI/ML models.

The significant shift in H3 will be enterprise consolidation into DataSecOps. Collaborative data management built with DataSecOps-enabled data pipelines and digitized data governance will allow for faster analytics.

Trend 7 – End-to-end DataOps with integrated data estate pipelines

Companies will explore and adopt the integration of DataOps across various data tools and data stakeholders to deliver faster business value. Along with this trend, we will see digitized data governance and containerization through automation and self-service tools to place a greater focus on value delivery. As part of digitized data governance, we will see the integration of components like data lineage, data security and data quality, and environment abstraction with data and logic tests to support self-service and better quality of data services delivery.

To benefit from this trend, enterprises must align their entire data estate into DataOps pipelines, break the silos of data teams and data products and create a fully integrated data factory view. They must also evaluate and standardize tools and processes across the entire data estate. Adoption of modern technologies will help integrate DataOps and accelerate this journey.

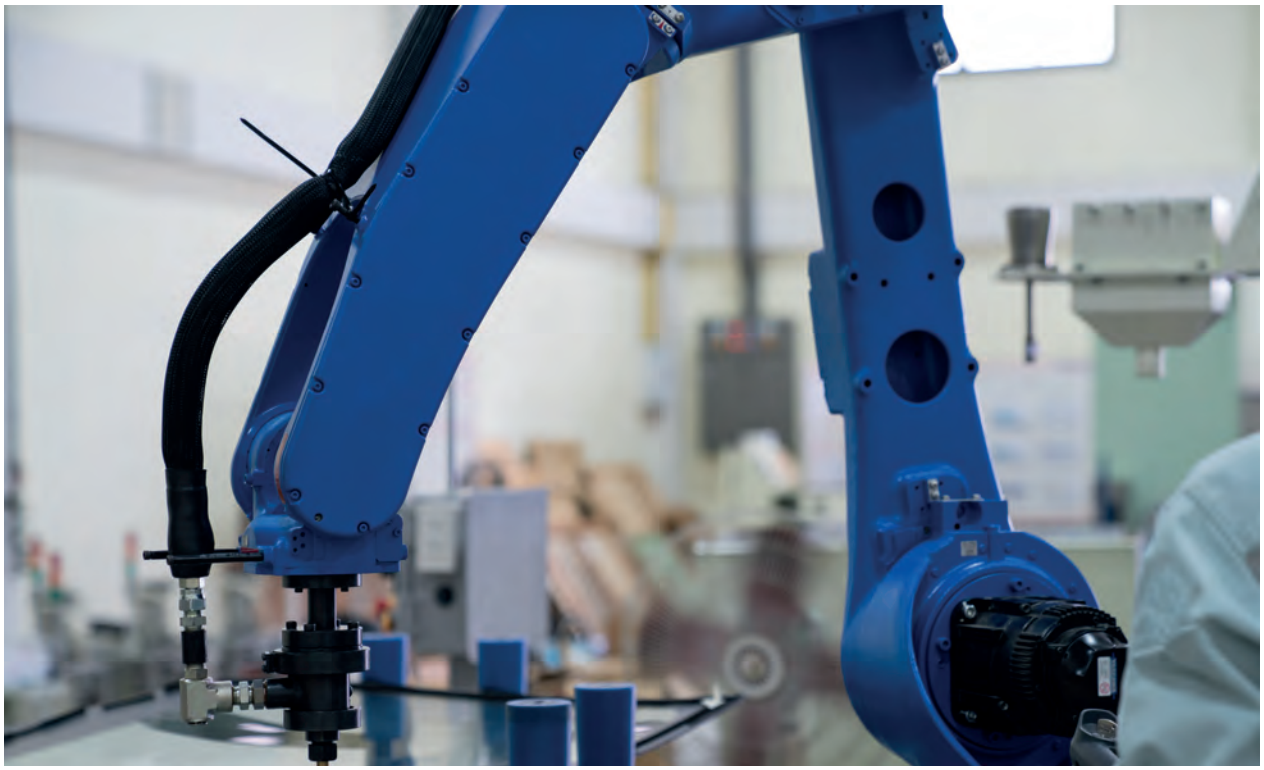
A large retailer adopted DataSecOps as part of their modernization into the public cloud. They explored and adopted new technology capabilities to deliver faster business value from their data.

Trend 8 – Combining artificial intelligence and machine learning products into DevSecOps

The AI/ML model's lifecycle involves various stages – from data collection, data analysis, feature engineering and algorithm selection to model building, tuning, testing, deployment, management, monitoring and feedback loops. To improve DevOps maturity, AI/ML models are being integrated into the DevSecOps pipelines to be standardized, fully managed and controlled. Configuration management tools, data security and data privacy tools and services for AI/ML models have also gained momentum. Other products like Amazon Macie, Pachyderm and TensorFlow are also being explored and experimented in DevSecOps pipelines.

A supply chain solutions company deployed AI and ML models on diverse platforms using an open-source software stack. This approach helped save 80% of deployment time, enabled elastic and containerized execution, thereby delivering better solutions for its customers.

ARTIFICIAL INTELLIGENCE/MACHINE LEARNING OPS



Organizations use DevOps to employ CI/CD in developing large-scale systems. While similar concepts apply for AI-based systems, ML Ops is emerging to handle specific demands of AI systems such as performance-tuning a model, periodic retraining, reproduction challenges, ongoing monitoring involving drift analysis and bias checks.

Trend 9: Emergence of enterprise-scale AI model management

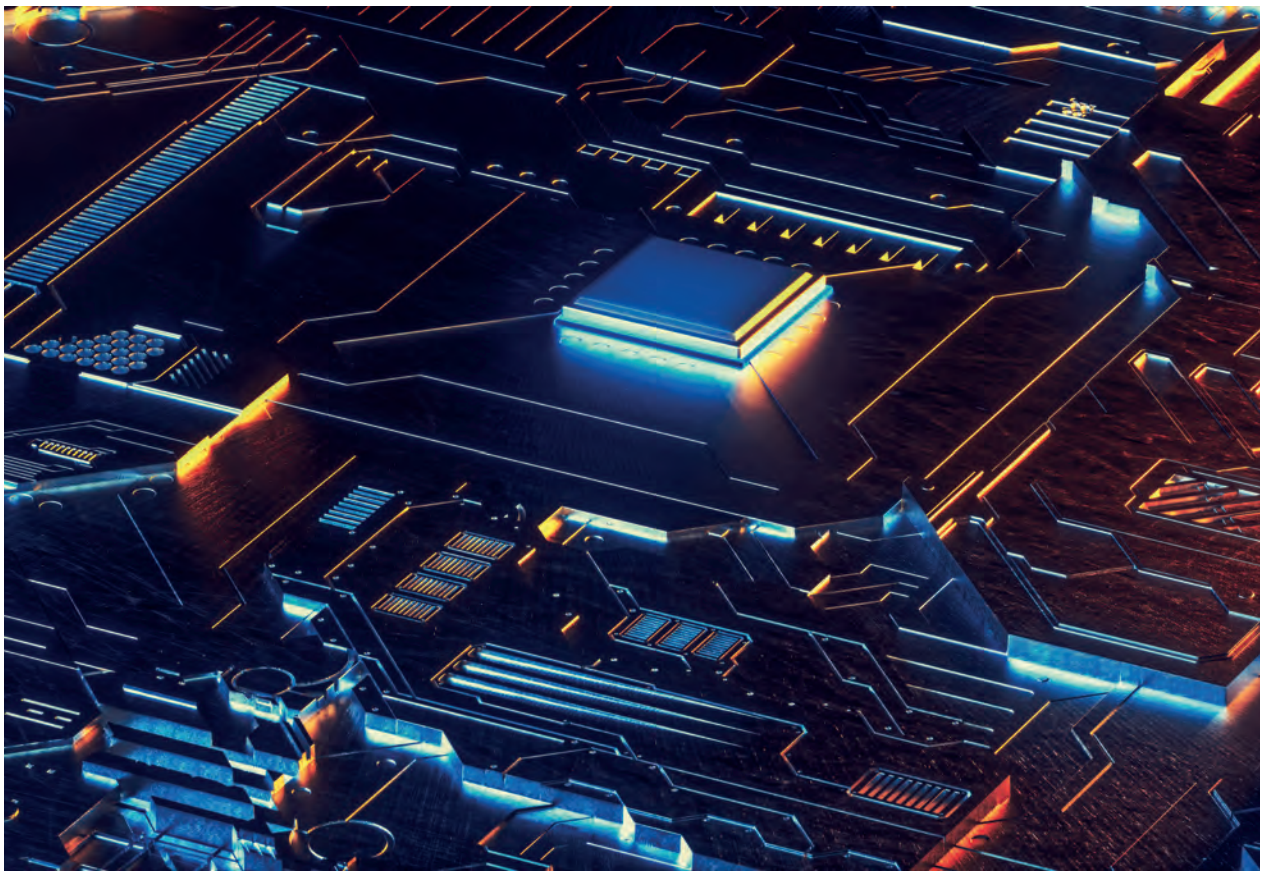
As AI initiatives graduate from proof of concept to enterprise deployment, organizations face challenges with the engineering complexity of model deployment, the ability to scale infrastructure efficiently and the lack of AI model visibility and governance. A few large organizations have started investing in the construction of an enterprise-scale AI model management framework. They are developing a repository of AI artifacts such as models, pipelines, features and datasets and managing a complete lifecycle of AI models that range from tuning and training to deployment and monitoring. This approach enables businesses to execute AI in a poly-compute manner and ensure AI governance through the detection of drift and bias, and the explanation and reproduction of AI prediction. While cloud providers offer fully managed model lifecycle management, the open-source community also contributes significantly to create frameworks such as Kubeflow on Kubernetes' containerized platform.

> Infosys partnered with a major U.S.- based finance organization to create a centralized AI platform for model training, management and deployment.

Trend 10: Integrated development environment for data science projects

Data scientists need different development environments, depending on the nature of data and their AI framework. Traditionally, data scientists have used various development tools to choose their desktop to develop ML models, but deploying and integrating them with their AI ecosystem has been a challenge. Organizations are now setting up environments where a data scientist can perform various tasks like data acquisition, profiling and pipeline development; obtain enterprise assets like datastores, models, Git and more; access different packages/frameworks; collaborate with other team members; integrate with a model management framework or deploy the model at scale – all within the same development environment and context of the AI project.

> A U.S.-based telecommunications company democratized AI by building an AI platform for their data scientists, data engineers and business analysts by partnering with Infosys. The new platform allows them to set up challenges, compete and collaborate across their organization, as well as integrate with AutoML tools.



NETOPS

Network operations (NetOps) is the practice of building agile networks. Traditional networks demanded reliability, performance and security, but these legacy systems were complex and hard-wired with little scope for automation. Today's networks require agility in **configuration**, **capacity** and **operation**. To achieve this high scalability, they must use ML algorithms for minimal disruption scheduling and analysis-based upgrades.

Trend 11: Open, standards-based, software-defined networks and network function virtualization

Current network conversions focus on programmability, which is achieved by software-defined networks (SDNs) and network function virtualization (NFV). SDNs help make networks flexible and create an agile networking landscape. NFV, with the help of cloud computing platforms, drives capacity scaling.

Together, these twin trends make automation and DevOps practices possible in the networking space. The broad technologies in NetOps include orchestration platforms like Cloudify, which drives zero-touch provisioning across multiple cloud platforms and edge devices; infrastructure as code based on templates using Terraform, Tosca and other standards; NFV where businesses deploy the entire virtual private cloud with just a click of a button using a DevOps pipeline; configuration management tools like Ansible and even open-source white box hardware which is deployed and configured in a completely automated manner.

With the emergence of technologies like multi-access edge computing, applications are moving closer to edge devices to get better throughput and scalability. Customers are also looking for flexibility in deploying virtual network functions, either on the edge device or in the edge cloud and across multiple public cloud platforms.

A tier-one U.S. telecommunications client brought efficiencies to their enterprise when they launched over 50 headend locations supporting 10,000-plus cable modem customers using the latest DevOps technologies. By virtualizing their locations, they saw more than 50% savings in capital and operating expenditures. They also reduced their service and site launches from a month to less than a week, leading to 75% acceleration for time to market.

Trend 12: Open-source, closed-loop AI Ops

Monitoring and service assurance solutions traditionally used legacy tools to manage the network and adhere to the agreed service-level agreement. But, with only a simple network management protocol in place, they had limited monitoring capabilities. The latest trend is moving toward real-time, intent-driven solutions, which are mostly distributed and cloud-enabled. A wide range of open-source platforms is being used for data analytics, including ELK Stack, Prometheus and Grafana. These systems are matured and widely deployed by customers in production.

On the horizon is AI/ML-based smart service assurance, which offers robotic cognitive automation, topology discovery and automated recovery to create a zero-touch assurance system effectively. Open-source big data solutions like Hadoop, Spark and TensorFlow, along with workflow engines like Camunda, will be used for data correlation and issue remediation. These solutions will also be used for fault prediction to avoid impact on business services, capacity management to prevent service degradation and automated feedback loops to improve service assurance continuously.

Using a rule-based alert management framework, a tier-one U.S. telecommunications company reduced their alarm volume by nearly 85%. This, along with AI/ML-based probable root cause analysis and automated recovery, helped the client make significant savings in operating expenditures.

APPLICATION LIFECYCLE MANAGEMENT

The area of ALM has seen remarkable changes from an agility perspective. What started with individual team adoption has become adoption at a program level with ALM tools supporting multiple agile and cloud-based frameworks. In the near future, we foresee businesses adopting a flow-based value stream and having a customer-centric view of what flows across the SDLC. Initially, there were documentation, project management, traceability, metrics and collaboration elements built into the ALM tools. We now have tooling support for design thinking, digital prototypes, LCNC platforms and link-sync via open APIs. This additional support allows for automated governance and compliance, deep analytics, high-quality, auto-generated user stories and acceptance criteria. The operating model construct has evolved from a DevOps COE that helped bridge the gaps between the Dev and Operations teams to a "hub and spoke" model, where the "hub" provides centrally managed services, and the "spoke" consumes services, eliminating the need of a DevOps enablement team. In the future, a NoOps model made up of full-stack engineering teams will own the development, promotion and upgrades for infrastructure and operations.

Trend 13: Teams create their own app ecosystem around ALM tools

Enterprises are moving to adopt ALM tools that help govern software development and ensure measurable agility in the delivery of business value to customers. An essential feature that facilitates this agility is the strong integration capability that the ALM tool provides, which helps enterprises extend capabilities and allows its integration with other enterprise tools.

Open APIs allow external applications to interface with the ALM platform via a bi-directional data exchange, reducing or avoiding manual intervention when updates are reflected. Increasingly, LCNC solutions will focus on a drag-and-drop approach for app creation, facilitating easier integration of legacy, mobile, package and new-age applications with the ALM tool. This trend will carve a path for robotic automation and alter the digital landscape to accelerate business agility.

Eventually, the integration capabilities of the ALM tool will help provide a unified view of value delivery from the business vision stage through the post-production monitoring stage. While enterprises should adopt these modern, open and connected technologies, any legacy applications that still exist in silos will be integrated with the ALM tools by way of adapters and wrappers.

A large telecommunications company based in Australia and New Zealand partnered with Infosys to set up more than 300 features for teams working with DevSecOps using tools like Jira for their B2B and B2C programs. To further drive quality into the SDLC, Infosys introduced an app on Jira using Text Analytics to provide user story views on the completeness, conformance and size. The benefits included a 10% to 15% reduction in defects and a more than 30% reduction in epic shifts in the first six weeks.

Trend 14: NoOps brings extreme automation and abstraction to the IT infrastructure

NoOps intends to eliminate human intervention in software management. It aims to allow operations teams to focus on more value-adding activities rather than spend time on mundane tasks. Hyperscalers that provide elements of the software, software-defined infrastructure and networks have contributed to NoOps becoming a reality. As enterprises adopt more automation, ALM tools adapt to support the further evolution from DevSecOps to NoOps. Enterprises first moved from siloed development and operations teams to an integrated Dev and Ops model where the team that builds the system also runs it. We now see enterprises changing to a NoOps model where maintenance and other tasks performed by the operations team will be fully automated, removing the need for a dedicated operations team. NoOps solutions will remove friction and increase the flow of valuable features through the pipeline, so that businesses are able to focus on early feedback, continuous learning and improvement. The NoOps approach will help derive AI-based intelligent inference of the metrics provided by the ALM tool and help in other aspects like corrective and preventive maintenance or scaling.

Businesses with a traditional approach and legacy systems are less likely to move toward a NoOps model. At the same time, those that employ a scalable infrastructure with on-demand, automated deployment and monitoring features are more apt to embrace and prosper from a NoOps approach.

A pharmaceutical client in the U.S. implemented full-stack agile pods to manage new application development, infrastructure and operations without any Ops support. Their NoOps adoption with self-sufficient pods is starting to deliver faster, better and more economical results.

QA DEVOPS

The proliferation of an agile enterprise and DevOps has helped reshape the software testing function at each step of the agile lifecycle. Quality engineers utilize programming skills, design patterns, advanced automation tools, AI/ML technologies and the cloud ecosystem to decrease cycle time across all QA aspects in the DevOps pipeline.

Trend 15 – Using advanced technologies for automated and autonomous testing

Hyperautomation (using AI to drive decision making) is emerging as a leading strategic technology trend that integrates robotic process automation (RPA), AI/ML, intelligent business management software and other emerging technologies to increase automation levels in enterprises. This trend is influencing software test automation evolution as different tools, frameworks and custom-developed solutions continue to help increase automation penetration and efficiency.

The test automation evolution began when user interface, API and database layers were automated using open-source tools such as Selenium and Appium. With the accelerated adoption of an agile culture, a digital business and DevOps, technologies such as AI/ML capabilities, zero-touch automation pipelines and self-healing automation scripts have made testing smarter. As a result, teams have optimized their automation strategies to adapt faster and operate more effectively.

In the test automation domain, we see enterprises use hyperautomation to improve both the cycle time and the test automation process, as well as validate other processes that have been automated using hyperautomation tools. Hyperautomation technologies are raising test automation's maturity level through RPA tools like UiPath, Appian and Automation Anywhere, LCNC tools like Tricentis and Katalon and AI, ML and NLP advances and autonomous testing tools like AutonomIQ.

Infosys partnered with a leading health domain firm to adopt an AI-led cognitive automation solution called Intelligent Automation, which combines the best automation approaches with AI to deliver superior results. The solution's focus is three-dimensional: eliminate test coverage overlaps, optimize efforts with more predictable testing and move from defect detection to defect prevention.

Trend 16: Maturing security integration in DevSecOps to real-time, automated remediation of vulnerabilities

DevSecOps introduced security earlier in the SDLC, expanding collaboration between development and operations teams in DevOps to include security teams. Security testing tools were introduced but were not integrated with continuous testing pipelines. It evolved into a shared responsibility, where everyone had to play a role in building security into the DevOps CI/CD workflow. Later, DevSecOps integrated application security testing (AST) tools into the CI/CD process. SAST tools (e.g., Micro Focus Fortify) were used to identify coding errors and design flaws leading to exploitable weaknesses; DAST tools (e.g., Micro Focus WebInspect) helped automate black box security testing to mimic how a hacker interacts with a web application or API and, finally, SCA tools (e.g., Black Duck) were implemented to identify known vulnerabilities in open-source and third-party components. These integrations within the CI/CD pipeline accelerated the identification and remediation of security vulnerabilities earlier in the cycle.

The trend has matured further by implementing AI/ML for security defense and risk prediction, as well as automated vulnerability assessment and management. AST tools now include two additional tools: IAST to detect runtime vulnerabilities and provide detailed insights to developers and RASP to identify threats and support self-protection.

A high-tech company in the U.S. built an AI-based threat intel database to suppress false positives by partnering with Infosys. This has resulted in a 25% faster time to market, 100% code coverage and OSS components, and a 50% reduction in common vulnerabilities.

DevSecOps for business agility and live engineering

The quest for digitization will drive businesses to embark on enterprise-scale engineering transformations. At the core would be an ecosystem-led live engineering approach to DevSecOps that revolves around an end-to-end, centralized platform that caters to the needs of the entire IT landscape, including ERP/COTS packages, networks, infrastructure, QA, data, AI/ML and custom applications. Such an ecosystem would not only unify the engineering and support teams to create a business-aligned value stream, it would also play a key role in standardizing and scaling DevSecOps adoption to optimize costs and provide insights across the live enterprise.

Advisory Council

Mohammed Rafee Tarafdar
SVP and Unit Technology Officer

Shaji Mathew
EVP and Service Offering Head, Health, Insurance & Life Sciences

Nabarun Roy
SVP, QLTY

Nitesh Bansal
SVP, Service Offering Head

Alok Uniyal
VP, QLTY

Gautam Khanna
VP, IP Deployment and Commercialization

Naresh Choudhary
VP – Reuse and Tools - Head, QLTY

Hasit Trivedi
AVP, AI & Automation

Amit Karoliwal
Associate Director – Product Architecture, EdgeVerve

Priti Budhia
Senior Unit Quality Head, QLTY

Contributors

Abayavidya Rengahari

Adarsh Mehrotra

Alok Uniyal

Amit Gaonkar

Amit Karoliwal

Amlan Sahoo

Anaga Mahadevan

Anil Kumar Nandivada

Anjali Dadaram Chavan

Anupama Rathi

Ashok Kumar C S

Ashok Kumar Ratnagiri

Ashvin Agaram Janardhan

Aswin Kumar

Chetan Ramamurthy

Deepak Gupta

Dhiraj Dhake

Dipu Sreekumaran

Dr. Mandeep Walia

Harish K B

Harleen Bedi

Jasdeep Singh Kaler

Kannan Narayanan

Krishna Kanth B. N.

Lakshmi Narayanan Kaliyaperumal

Lakshminarayana Indraganti

Madhanraj Jeyapragasam

Manas Kumar S

Manish Jain

Manjunath DK

Mir Riyaz Ahmed

Mitul Gupta

Namrata Chandra Prakash Ramnani

Palani G. Sankar

Prasanna Ghanekar

Prashant Burse

Priyapravas

Raghunandan Shrinivas Terdal

Rajesh Kumar Vissapragada

Raktim Singh

Renu Sudhakaran

Ruby Batra

Sachin Kaushik

Saurabh Vasant Muley

Senthil Kumar Shanmugam

Shilpa Aphale

Sumit Goyal

Udaykumar Gupta

Vaibhav Gupta

Viral Thakkar

Producer

Ramesh N

Infosys Knowledge Institute
ramesh_n03@infosys.com

About Infosys Knowledge Institute

The Infosys Knowledge Institute helps industry leaders develop a deeper understanding of business and technology trends through compelling thought leadership. Our researchers and subject matter experts provide a fact base that aids decision-making on critical business and technology issues.

To view our research, visit Infosys Knowledge Institute at infosys.com/IKI.

For more information, contact askus@infosys.com