Infosys®
Navigate your next

DEVSECOPS - ENTERPRISE VALUE CATALYST FOR DISTRIBUTED PRODUCT TEAMS

Infosys® | Knowledge Institute

Contents

Enterprises deliver safer, quicker, and reliable business value to customers through technology. With rapid advancements, software delivery must remain agile, resilient, and secure. DevSecOps is helping businesses to shorten the cycle time, from initiating a business idea to delivering to end customers. Subsequently, specialized disciplines such as NetOps for networks, DataSecOps for data engineering, MLOps for machine learning, NoOps for operations, and EdgeOps for edge computing have come into the frame. This discipline started for application development, but now has spread enterprise wide and caters to workloads developed by hybrid teams. Further, shift left site reliability and AI/ML backed insights augment these approaches. Organizations can now effortlessly collaborate and detect problems early in the value stream through intelligent observability within technology portfolios.

COVID-19-induced disruptions have pushed enterprises toward rapid digitization at scale. This was particularly driven by their IT landscape in response to the challenges of the remote workforce and related interruptions.

IT teams need to be agile to adopt new technologies, transform legacy systems, and respond to fast-changing customer needs. DevSecOps and cloud technologies help enterprises better align cross-functional teams, reduce time to market, and streamline engineering and operations processes. This ability to collaborate effectively across functional boundaries, and to ensure customer-focused product delivery, has a substantial impact on business growth, according to our Agile Radar analysis.

Post-pandemic, enterprises need to reexamine collaboration, automation, security, compliance, governance, observability, and analytics across key dimensions for resilient and agile IT operations. These key dimensions include application technologies, packages, data, testing, infrastructures, and networks.

Almost all enterprises have faced challenges with a remote workforce. In addition to volatility in demand for products and services, unprecedented threats and attacks from malicious actors and security incidents have plagued the open-source world. All this has affected enterprises' security, compliance, and governance protocols.

Organizations must safeguard systems and data using end-point security automation solutions, best-in-class authentication and authorization mechanisms, and touchless automation (a paradigm wherein data is verified without human intervention). They must secure their IT supply chain by tightening source code development practices and validating application vulnerabilities early in the testing life cycle. This requires considering antifragility aspects in application development and following chaos engineering principles. For instance, during application resiliency testing, turbulent conditions can be created to highlight failure points. Further, DevSecOps can help organizations implement compliance at scale by codifying cloud infrastructure compliance policies while provisioning infrastructure on the cloud using codified policies with automation across the DevSecOps pipelines. Further, zero-day vulnerabilities such as Log4Shell are pushing organizations to adopt DevSecOps for rapid software rollout.

Enterprises must be ready 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 life cycle. Further, their applications will have to be more resilient and integrated with DevSecOps tools and technologies to ensure higher predictability and client value.

THE DEVSECOPS EVOLUTION CONTINUUM

The concept of combining development and operations (DevOps) gained traction between 2008 and 2009, when businesses worked to collapse boundaries and automated 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 life cycle (SDLC) ecosystem evolved, open-source point tools paved the way for task orchestration (automating the arrangement, coordination, and management of complex systems) 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 only limited solutions were available. These pipelines were implemented primarily using open-source tools on on-premises/private cloud infrastructures.

Horizon 2 (H2): Over the past 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 environmental 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 the DevSecOps concept. Solutions have emerged in this horizon for legacy technologies like mainframe, proprietary technologies such as SAP and Siebel, and evolving technologies like robotic process automation (RPA) and ML. All this is characterized by the codification of pipelines, software configuration, infrastructure, and security.

Horizon 3 (H3): Enterprises embrace an ecosystem approach and adopt a framework with end-to-end platforms that provide cloud-agnostic DevSecOps automation as a service. They focus on scaling DevSecOps adoption through low code/no code (LC/NC) approaches, utilizing inbuilt and continuous security. With auditing, compliance, visibility, and governance becoming prominent, observability capabilities and flow metrics in DevSecOps platforms will see a significant uplift. Application of AI/ML-based insights in the DevSecOps life cycle for enhanced efficiencies in CI, CT, CD, security, application life cycle management (ALM), value stream management (VSM), monitoring, and self-healing areas will increase. Site reliability engineering (SRE) has entered the game.

This will 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). With AI/ML spreading across the enterprise landscape, release time, reliability, and efficiency of ML models will enhance with ML operations (MLOps) practices.

We have identified sixteen key trends across the following eight subdomains:

Enterprise-scale CI/CD

Security and policy compliance

DevSecOps for packages

DataOps

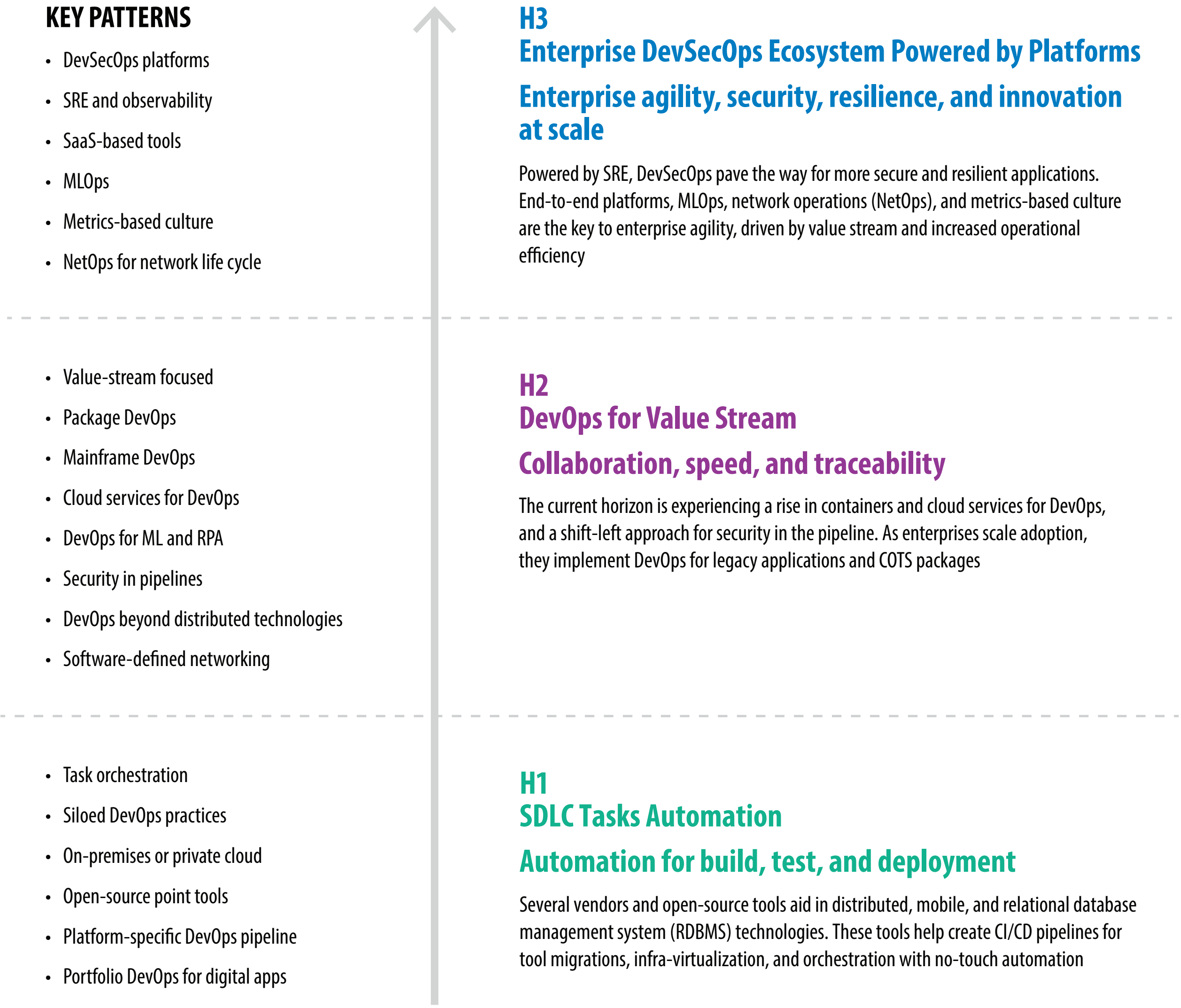
AI/MLOps

NetOps

ALM

QA DevOps

Figure 1: Three horizons (H1, H2, and H3) in DevSecOps



KEY PATTERNS

- DevSecOps platforms
- SRE and observability
- SaaS-based tools
- MLOps
- Metrics-based culture
- NetOps for network life cycle

H3

Enterprise DevSecOps Ecosystem Powered by Platforms

Enterprise agility, security, resilience, and innovation at scale

Powered by SRE, DevSecOps pave the way for more secure and resilient applications. End-to-end platforms, MLOps, network operations (NetOps), and metrics-based culture are the key to enterprise agility, driven by value stream and increased operational efficiency

- Value-stream focused
- Package DevOps
- Mainframe DevOps
- Cloud services for DevOps
- DevOps for ML and RPA
- Security in pipelines
- DevOps beyond distributed technologies
- Software-defined networking

H2

DevOps for Value Stream

Collaboration, speed, and traceability

The current horizon is experiencing a rise in containers and cloud services for DevOps, and a shift-left approach for security in the pipeline. As enterprises scale adoption, they implement DevOps for legacy applications and COTS packages

- Task orchestration
- Siloed DevOps practices
- On-premises or private cloud
- Open-source point tools
- Platform-specific DevOps pipeline
- Portfolio DevOps for digital apps

H1

SDLC Tasks Automation

Automation for build, test, and deployment

Several vendors and open-source tools aid in distributed, mobile, and relational database management system (RDBMS) technologies. These tools help create CI/CD pipelines for tool migrations, infra-virtualization, and orchestration with no-touch automation

Source: Infosys

Figure 2. Key trends across domains

Enterprise-scale CI/CD	**Trend 1.** Modernization drives demand for cloud-based DevOps **Trend 2.** DevOps scales across the enterprise to drive agility
Security and policy compliance	**Trend 3.** End-to-end integrated DevSecOps pipelines aid enhanced security **Trend 4.** Codification of security and privacy controls enables a shift left
DevSecOps for packages	**Trend 5.** Increased DevSecOps adoption in the SAP ecosystem **Trend 6.** End-to-end, inbuilt platform capabilities strengthen
DataOps	**Trend 7.** DataSecOps enhances data efficiency **Trend 8.** AI and ML products integrate with DevSecOps
AI/MLOPS	**Trend 9.** AI models deployed at the edge for better customer experience **Trend 10.** Integrated MLOps practices enhance AI capabilities
NetOps	**Trend 11.** Organizations shift to intent-based networking (IBN) **Trend 12.** Open-source, closed-loop AIOps drive cognitive and intelligent next-gen OSS
ALM	**Trend 13.** OKRs help track decisions and product value **Trend 14.** NoOps brings extreme automation and abstraction to IT infrastructure
QA DevOps	**Trend 15.** Hyperautomation offers faster and more efficient testing **Trend 16.** Real-time and automated security integrate with DevSecOps

Source: Infosys

ENTERPRISE-SCALE CI/CD

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. The integration was primarily done for distributed, mobile, and 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. Other tools gaining popularity are container DevOps, using container management technologies like Kubernetes; cloud-agnostic DevOps, using Terraform; cloud-native DevOps, using services like Azure DevOps; and AWS Developer or Platform as a service (PaaS) tools like OpenShift.

Enterprise-scale DevOps adoption continues to rise. Centralized DevOps platforms and reusable frameworks are playing key roles in standardizing adoption and optimizing costs. DevOps tools have better features such as software as a service (SaaS) tools, end-to-end tool capabilities, and abstraction levels in container management platforms. During enterprise adoption, key team changes like creating unified DevOps or SRE teams lead to process changes.

Trend 1: Modernization drives demand for cloud-based DevOps

Organizations are increasingly migrating their existing applications to the cloud or using cloud-native development to build new applications. This allows firms to speed up software deployments and generate significant revenues from launching new business models, boosting the usage of cloud-based commercial or open-source tools for cloud DevOps. Advanced configuration and container management, orchestration tools, and technologies like Ansible, Chef, Puppet, and Kubernetes are driving cloud DevOps adoption. Further, 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, enable easy configuration of end-to-end pipelines through DevOps.

A manufacturing company was experiencing frequent downtime due to more than 2.5 million visits per day to its global website. The company partnered with Infosys to create more than 90 declarative CI/CD pipelines for its site and subsystems using Azure DevOps and Azure Resource Manager. The client achieved zero downtime and a 90% reduction in provisioning and deployment time.

Trend 2: DevOps scales across the enterprise to drive agility

Many businesses are implementing DevOps after realizing its benefits in specific applications. However, this requires efforts beyond setting up CI/CD for every application. Unplanned DevOps scaling can have adverse effects such as higher tooling and infrastructure costs, more effort by application teams in setting up CI/CD, and unstandardized implementation. Organizations must form a DevOps center of excellence (COE), which defines and advocates DevOps practices and guidelines. Reusable frameworks, a centralized DevOps platform, dashboards, and analytics are also crucial. Enterprise DevOps adoption goes beyond distributed technologies. All systems that are part of a value stream adopt DevOps to gain time to market benefits. Therefore, we are seeing DevOps developed for mainframes, customer relationship management applications, custom off-the-shelf products, middleware, and business process management. Vendors are also providing DevOps features as add-on tools within their products.

A U.S. automobile manufacturer faced availability and scalability challenges with its existing DevOps solutions, including noncompliance to standards, rising costs of tools, and infrastructure and security concerns. The client collaborated with Infosys to build an enterprise-scale multi-cloud platform, using AWS, Terraform, Kubernetes, and other tools, to reduce DevOps costs, achieve standardization, and eliminate currency complexity.

SECURITY AND POLICY COMPLIANCE

Enterprises use security tools throughout all life cycle stages for faster delivery and enhanced security. Tools 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) enable this left shift in security testing.

Command line interface (CLI) or application programming interface (API) integrates CI/CD pipelines with security testing tools. Configuring incremental scans in the pipelines, no-touch gating of results using custom scripting, and identifying and reducing false-positive reports support these integrations. Docker tools such as file scans, image scans, registry scans, and container security tools are part of the continuous security checks for applications using container security.

Centralized platforms, reusable frameworks, and dashboards drive the enterprise scaling of DevSecOps. Concepts like compliance-as-code and policy-as-code and security testing tools strengthen security. DevOps teams must collaborate with security subject matter experts (SMEs) to successfully adopt secure coding practices, security as requirements, and security as notices of findings and recommendations (NFRs).

Trend 3: End-to-end integrated DevSecOps pipelines aid enhanced security

Security issues and cyberthreats, specifically for B2B or B2C applications, are continuously rising. 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, so scans should be run outside the pipeline or nightly batches, and custom scripts should 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 promising tools include features that improve integration, such as incremental scanning capabilities to reduce scan time and AI-based tools to identify false positives and automate issue remediation. Docker tools also incorporate container security into the CI/CD pipelines.

An industry leader in brokerage and wealth management experienced a bottleneck in its underlying network of shared services. Due to manual security testing, it could not achieve an early time to market for end-user applications. The client partnered with Infosys to implement an end-to-end DevSecOps solution to improve speed and quality. Now it has reduced release management effort by around 88%, quadrupled the release frequency, and saved $3.3 million annually.

Trend 4: Codification of security and privacy controls enables a shift left

Businesses are looking at reusable frameworks and centralized DevSecOps platforms to successfully scale its adoption enterprise wide. By implementing a consolidated security dashboard in the pipeline, they collect defects 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 encouraging DevSecOps adoption, which reduces the load on underlying infrastructure and efforts to maintain tools. Open-source tools help reduce cost concerns attributed to several licenses needed for enterprise-scale adoption. Enterprises are implementing organizational change management tactics such as enabling secure coding practices for developers, changing mindset, and integrating security as a 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. Increased trust and collaboration between security SMEs and application teams also help here.

A large telecommunications provider was facing estimated fraud losses of $490 million per year, which was expected to increase by nearly 38%. The client, in partnership with Infosys, adopted a holistic people, process, and technology approach, and implemented enterprise-scale DevSecOps for over 1,000 applications. This increased feature delivery by 40% and eliminated almost $1 million in fraud losses within the first seven months of implementation.

DEVSECOPS FOR PACKAGES

At the onset, enterprise resource planning (ERP) packages like SAP, Oracle, and Salesforce did not adopt DevSecOps. In fact, they provided little to no inbuilt platform support to customers. SAP's version releases and configurations were tied to its complex change and transport system. If not properly tested, an organization's SAP transport could harm performance or even shut down the production environment. At the same time, Oracle's ERP relied on custom tools and applications to manage and monitor its environments. While Oracle had some CI/CD capabilities, it still could not adopt the full DevOps concept. Salesforce utilized manual deployment scripting and basic environment management tools, it had no version control or branching.

However, as their businesses and technologies matured, these ERP providers began integrating these tools into CI/CD pipelines, 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. For example, SAP Business Technology Platform (SAP BTP) has scaled up SAP's DevOps and integration capabilities. It also built versioning and branching capabilities with abapGit and GitHub integration.

Trend 5: Increased DevSecOps adoption in the SAP ecosystem

There is constant demand for upgradation and quicker time to market with SAP's core business platform. As a package of offerings, SAP has worked to build self-contained tools for ALM. With the advent of DevOps, SAP has kick started its agility journey by launching Activate Methodology. It is embracing open-source tool sets to amplify life cycle management capabilities. Riding on DevOps' value, security considerations are now built at the beginning of the design stage and through production deployment. Code vulnerability, general data protection regulation compliance, and information life cycle management have become key design considerations for enterprise applications. Various SAP tools like IDM, ILM, GRC, CVA, and Onapsis help manage different security requirements throughout the development life cycle. SAP has enhanced its operations support system (OSS) integration through SAP BTP. Cloud connectors of SAP BTP provide a seamless integrated DevOps in SAP. DevSecOps-enabled SAP Project delivery ensures faster and more frequent deployments. It makes systems more secure, reliable, and efficient. Native tool sets like SAP's Focused Build, Solman change request management, CTS+, and SAP TAO are now widely used in DevSecOps deployments in conjunction with abapGit. These integrated tool sets are being amplified by OSSs like Jenkins and partner tools like Virtual Forge CodeProfiler, Rev-Trac, Infosys DevOps Platform (IDP), Jira, Rally, and more.

A leading luxury automobile manufacturer deployed five production releases in a month with 85% first-time right accuracy, utilizing Infosys' IDP, Jira, and HP ALM test management tools. Over two years, the client achieved a 40% increase in sprint velocity and 100% automated regression testing.

Trend 6: End-to-end, inbuilt platform capabilities strengthen

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

A leading North American financial services company, in partnership with Infosys, built a sophisticated DevSecOps framework with high automation. Inbuilt platform capabilities combined with third-party tools provided deep insights and integrated tracking of DevSecOps processes.

DATAOPS

Data architectures are continuously evolving and becoming volatile — moving from traditional data warehouses and data marts to data lakes and now lake houses. Alongside, 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.

H2 has seen much movement toward public cloud adoption and cloud-native DevOps adoption. Organizations are exploring varied technology stacks with multiple technology-specific automations aligning into DevSecOps. Historically, traditional data platform tools embraced custom CI/CD capabilities to integrate into enterprise DevSecOps adoption. However, DevSecOps pipelines have now gained momentum with 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 and Data Mesh adoption. Collaborative data management built with DataSecOps-enabled data pipelines and digitized data governance will allow faster analytics. Data Mesh adoption with hub-and-node structure will happen through centralizing the foundational elements and decentralizing their adaptations based on specific data domain needs.

Trend 7: DataSecOps enhances data efficiency

Companies are exploring and adopting DataOps across various data tools and data stakeholders to deliver faster business value. We also see digitized data governance and containerization through automation and self-service tools for greater focus on value delivery. As part of digitized data governance, components like data lineage, data security, data quality, and environment abstraction will integrate with data and logic tests. This will support in self-service and higher-quality data services delivery.

Enterprises must organize 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 by building pipeline-as-code with end-to-end integration across the data fabric. Modern technologies will help integrate DataOps and accelerate this journey.

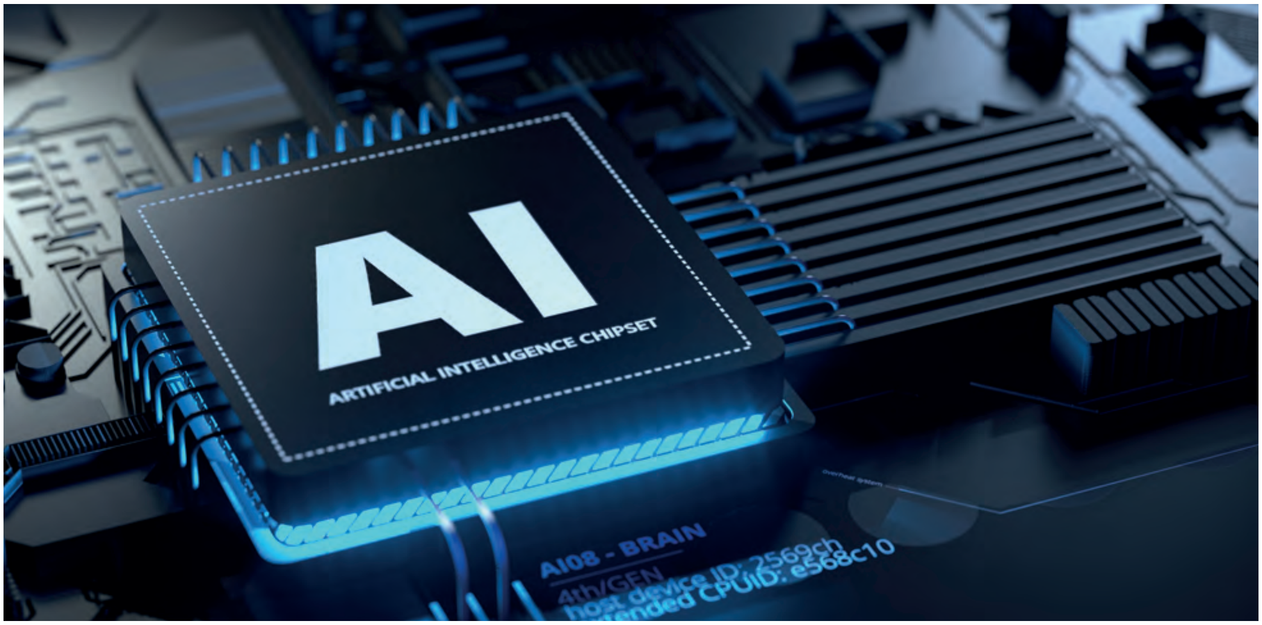
A large food and beverage company wanted to become data-driven and agile. However, long delivery cycles and dependence on engineering for data discovery challenged its vision. The company partnered with Infosys to successfully adopt agile processes and enrich data governance through a phased approach on DataSecOps. The client reduced data discovery time by 90% and achieved 10-times-faster user acceptance of features deployed.

Trend 8: AI and ML products integrate with DevSecOps

The AI/ML model's life cycle 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 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 gained momentum. Other products, such as Amazon Macie, Pachyderm, and TensorFlow, are also being explored and tested.

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

AI/MLOPS



Organizations use DevOps to employ CI/CD in developing large-scale systems. While similar concepts apply for AI-based systems, MLOps is surfacing as a way 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: AI models deployed at the edge for better customer experience

Enterprises are increasingly deploying AI models at the edge. And that too for the latest use cases. To deliver a transformative experience, diverse sensing devices in near-real time are deployed.

The various available frameworks (such as NVIDIA DeepStream, Triton, OpenVino, Azure Edge) and hardware options (such as Intel Edge VPUs, FPGA, NVIDIA Jetson, and Google's Edge TPU) will soon be joined by additional choices. Hence, solutions should evolve with technology and adhere to open community-driven standards.

With trending Internet of Things (IoT)/smart devices, deploying models for autonomous and low-powered devices would bring significant new MLOps challenges. Customers will have to evaluate multiple frameworks, hardware devices, and deployment models to implement a future-proof solution. They will also have to address privacy, device management, security, federated deployments, and implementation of open standards across devices.

A Fortune 500 oil and gas company wants to capitalize on opportunities from alternative energy sources. It has partnered with Infosys to pilot an AI-enabled business model based on video analytics and IoT, involving autonomous stores. In the current pilot phase, the project is expected to provide a frictionless checkout experience to customers. It involves real-time AI inferences using video analytics on 50-plus cameras and signals from more than 100 IoT sensors installed in a store.

Trend 10: Integrated MLOps practices enhance AI capabilities

Companies are standardizing MLOps practices to scale AI adoption. Having quickly identified use cases and conducted early experiments on AI applications, they are realizing the need for an end-to-end pipeline from data sourcing and for model training, deployment, and monitoring. Enterprises are also looking at creating a central model repository and adopting trustworthy AI practices.

Technologies like Azure ML, AWS SageMaker, Airflow, Kubernetes, Databricks Delta Lake, NVIDIA Triton, MLFlow, and products like DataRobot and Iguazio, are emerging as sources for model management, deployment, and managing training data. Meanwhile, various customers are indicating the need for online and offline feature storage for ML data management and model monitoring.

With multiple technology options available to realize the architectures, solutions and program road maps are evolving to cater to the specific implementation and priorities of individual organizations.

A large North American telco wanted to standardize its MLOps architecture to enhance AI development life cycle management. Infosys helped the client develop a platform that standardizes model deployment, monitoring, and governance. The platform works on Azure and technologies like Delta Lake and Spark. By implementing an end-to-end architecture for MLOps with an eye on cloud-native principles, the customer anticipates replicating it across different business lines and multiple cloud providers.

NETOPS

Network operations 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: Organizations shift to intent-based networking (IBN)

Current network conversions focus on programmability, which is achieved by software-defined networks (SDNs) and network function virtualization (NFV). SDNs 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.

IBN caters to business cases such as network slicing and server security rather than to individual tasks. The IBN controller takes care of the right changes to the network to manifest the intent.

> A tier-one U.S. telecommunications company launched over 50 headend locations (master distribution centers for converting television signals to cable transmission), supporting over 10,000 cable modem customers using the latest DevOps technologies. By virtualizing its locations, the client achieved 50% savings in capital and operating expenditures. It also reduced the duration of service and site launches from a month to less than a week, accelerating time to market by 75%.

Trend 12: Open-source, closed-loop AIOps drive cognitive and intelligent next-gen OSS

Monitoring and service assurance solutions traditionally used legacy tools to manage and operate a network. With telcos leveraging 5G, IoT, and edge-computing use cases to drive monetization, network response and reliability become the linchpin of the service level agreement. The latest trend is moving toward real-time, intent-driven solutions, mostly distributed and cloud-enabled. A wide range of open-source platforms, including ELK Stack, Prometheus, and Grafana, are used for data analytics. These systems are matured and widely deployed by customers in production.

AI/ML smart service assurance offers cognitive network planning, topology discovery, and automated recovery to create a zero-touch, closed-loop assurance system effectively. Open-source big data solutions like Hadoop, Spark, and TensorFlow, along with workflow engines like Camunda, are used for data correlation and issue remediation. These solutions are also used for fault prediction to avoid impact on business services; for capacity management to prevent service degradation; and for automated feedback loops to improve service assurance continuously.

A U.S. telecom company partnered with Infosys to develop a rule-based alert management framework. By using this framework, the company was able to do AI/ML-based probable root cause analysis and automated recovery. The client reduced its alarm volumes by nearly 85% and lowered operating expenditure significantly.

ALM

Application life cycle management has seen remarkable changes from an agility perspective. What started with individual team adoption has reached a program-level paradigm, with ALM tools supporting multiple agile and cloud-based frameworks. Businesses are adopting a flow-based value stream with a customer-centric view of what flows across the SDLC. The documentation, project management, traceability, metrics, and collaboration elements built into the ALM tools provide end-to-end visibility of the software release process and its impact on business outcomes. This is further augmented by the tooling support for design thinking, digital prototypes, LC/NC 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 development and operations teams to a hub-and-spoke model, where the "hub" provides centrally managed services and the "spoke" consumes services, eliminating the need for a DevOps enablement team. Organizations are starting to follow a no operations (NoOps) model, where an integrated DevOps team of full-stack engineers collaborates closely to implement extreme automation — all while taking care of development and infrastructure needs, thus eliminating the need of a separate operations team.

Trend 13: OKRs help track decisions and product value

Organizations are extensively using objectives and key results (OKRs) to define and set goals, and to achieve outcomes. A set of key results defines the measurable outcome for these objectives. While OKRs have been in use for a while, the systems to relate these key results to the stated objectives in a near real-time manner were lacking. Here, VSM gets into the picture.

VSM ensures the flow of business value is accelerated all the way from the ideation stage to the actual delivery of desired outcomes. Organizations are using ALM tools to establish and track these flow metrics, providing visibility on delays in the release process and highlighting the impact on desired outcomes. By gathering relevant data across tool chains, cross-functional teams, and value streams, the VSM platform gives a unified view of the progress of value delivery to the end customer. Associating the relevant flow metrics with the desired key results helps provide clear visibility of the likelihood of achieving the key results and hence the business objective.

A U.S.-based global logistics provider wanted to reimagine customer journeys and improve business outcomes. It partnered with Infosys to use design thinking to boost product-oriented delivery and scale operations. The company, in collaboration with Infosys, built a flow that included setting strategic OKRs, cascading them to product levels, and regularly monitoring and evaluating them. The benefits included the doubling of shareholder value and a two-week release cycle.

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

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

Businesses with a traditional approach and legacy systems are less likely to move in this direction, while those with scalable infrastructure and on-demand, automated deployment and monitoring features can prosper from a NoOps approach.

A leading oil and gas company wanted to accomplish a federated, cloud-based DevOps model by implementing a hub-and-spoke architecture. The company collaborated with Infosys to develop a self-service Azure platform that started the shift toward NoOps, where teams would manage the infrastructure elements. The hub ensured the implementation of right policies. With automation, more than 250 spokes and approximately 1,000 resource groups were created in 18 months. Also, Azure policy-driven compliance and audits (more than 300 policies applied at different access levels) were implemented. The company was able to repurpose its operations staff on newer areas like SRE, which are also embedded within the teams.

QA DEVOPS

The proliferation of an agile enterprise and DevOps has helped reshape the software testing function at each step of the agile life cycle. 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: Hyperautomation offers faster and more efficient testing

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

The test automation evolution began with the automation of user interface, API, and database layers using open-source tools such as Selenium and Appium. With accelerated 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, enterprises use hyperautomation to improve cycle time and the process. Hyperautomation technologies are raising test automation's maturity level through RPA tools like UiPath, Appian, and Automation Anywhere; LC/NC tools like Tricentis and Katalon; and AI, ML, and NLP advances and autonomous testing tools like AutonomIQ.

> A leading health care firm wanted to adopt an AI-led cognitive automation solution, which combines the best automation approaches with AI to deliver superior results. The company, in partnership with Infosys, developed a solution with three key focus areas: eliminate test coverage overlaps, optimize efforts with more predictable testing, and move from defect detection to defect prevention.

Trend 16: Real-time and automated security integrate with DevSecOps

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. This evolved into a shared responsibility, with everyone playing 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 an 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 with the implementation of AI/ML for security defense and risk prediction, and with automated vulnerability assessment and management. AST now includes 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 U.S. company, in collaboration with Infosys, built a threat intelligence database to suppress false positives. The client achieved 25% faster time to market, 100% code coverage and OSS components, and a 50% reduction in common vulnerabilities.

Glossary

Abbreviation/Acronym	Full Form
AI	Artificial intelligence
AIOps	Artificial intelligence operations
ALM	Application life cycle management
API	Application programming interface
AST	Application security testing
AWS	Amazon web services
BTP	Business technology platform
CD	Continuous delivery
CI	Continuous integration
CLI	Command line interface
COE	Center of excellence
COTS	Commercial off-the-shelf
CT	Continuous testing
CVA	Code vulnerability analyzer
DAST	Dynamic application security testing
DataOps	Data operations
DevOps	Development and operations
DevSecOps	Development security and operations
ERP	Enterprise resource planning
FPGA	Field programmable gate arrays
GCP	Google cloud platform
GRC	Governance, risk, and compliance
IAST	Interactive application security testing
IBN	Intent-based networking
IDM	Identity management
IDP	Infosys DevOps platform
ILM	Information life cycle management
IoT	Internet of things

Abbreviation/Acronym	Full Form
LC	Low code
ML	Machine learning
MLOps	Machine learning operations
NC	No code
NetOps	Network operations
NFRs	Notices of findings and recommendations
NFV	Network function virtualization
NLP	Natural language processing
NoOps	No operations
OKRs	Objectives and key results
OSS	Operations support system
PaaS	Platform as a service
QA	Quality assurance
RASP	Runtime application self-protection
RDBMS	Relational database management system
RPA	Robotic process automation
SaaS	Software as a service
SAST	Static application security testing
SCA	Software composition analysis
SDLC	Software development life cycle
SDN	Software defined network
SME	Subject matter expert
SRE	Site reliability engineering
TAO	Test acceleration and optimization
TPU	Tensor processing unit
VPU	Vision processing unit
VSM	Value stream management

Advisory Council

Mohammed Rafee Tarafdar
SVP and Unit Technology Officer

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

Nabarun Roy
SVP, Group Head, Quality

Alok Uniyal
VP, Quality

Gautam Khanna
VP, IP Deployment and Commercialization

Naresh Choudhary
VP, Reuse and Tools - Head, Quality

Ashok Kumar Panda
AVP, Delivery Head

Amit Karoliwal
Director, Product Architecture, EdgeVerve

Priti Budhia
Senior Unit Quality Head, Quality

Contributors

Adarsh Mehrotra

Amit Gaonkar

Anaga Mahadevan

Anjali Dadaram Chavan

Anoop Alazhathu

Aswin Kumar

Dhiraj Dhake

Harleen Bedi

Kannan Narayanan

Kaushal Desai

Kedar J Mankar

Krishna Kanth B. N.

Mir Riyaz Ahmed

Mitul Gupta

Mohit Jain

Namrata Chandra Prakash Ramnani

Palani G. Sankar

Prasanna Ghanekar

Priti Budhia

Ranjit G A

Ruby Batra

Saurabh Vasant Muley

Senthil Kumar Shanmugam

Smitha Sidharthan P.

Sujatha M.

Surya Prakash G.

Varun Jain

Producers

Ramesh N
Infosys Knowledge Institute
ramesh_n03@infosys.com

Abhinav Shrivastava
Infosys Knowledge Institute
abhinav.s08@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 or email us at iki@infosys.com.

Infosys®
Navigate your next

For more information, contact askus@infosys.com

Infosys.com | NYSE : INFY

Stay Connected