Deloitte.

Platinum
Business
Partner

2020

Unleashing the potential of containerized solutions

using IBM Spectrum Scale and Protect Plus

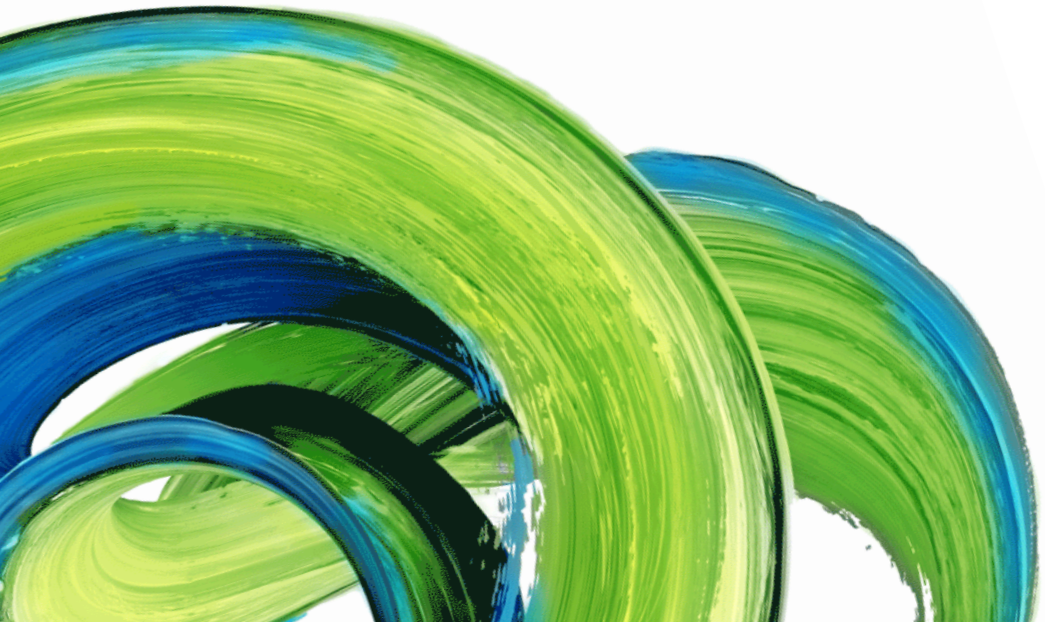
Many organizations face the dilemma of maintaining their traditional IT systems and staying up to date with the pace of digital transformation. This is driving trends such as hybrid cloud environments, cloud portability, and containerization.

As the cloud-adoption rate increases, many organizations are leveraging the principles of DevOps to solve the numerous challenges associated with traditional IT systems that are deployed on-premises and in private clouds.

Modern development best practices are leading to building applications that are divided into smaller microservice-based containerized pieces.

As a result, modern business applications have become highly distributed across traditional data centers, private clouds, and public clouds, making hybrid multi-cloud a reality. These applications are designed to scale quickly to support dynamic workloads.

Currently, organizations are leveraging the principles of DevOps combined with storage management technologies to solve many of the challenges associated with traditional IT systems deployed on-premise and in private cloud. Most organizations are embracing a containerization with heterogeneous cloud migration strategy to build a hybrid cloud environment. This approach includes cloud portability, auto-scalability, dynamic storage array provisioning, and container security – tools that can accelerate and optimize cloud storage across all protocols including file, block, and object storage.



Modern hybrid multi-cloud environments are architected differently today. The focus has shifted from connecting existing environments to building cloud-native apps that are portable across environments. These apps are a collection of small, independent, and loosely coupled micro services that are deployed in containers.

Container-based apps and their deployments provide a consistent computing environment. They package the same operating system and the associated dependencies to abstract all hardware requirements across multiple platforms. Containers are managed and run with an orchestration engine like Docker, Kubernetes or Red Hat OpenShift Container Platform (OCP) that abstracts all app requirements. This creates an interconnected and consistent environment where apps can be moved from one cloud to another without maintaining a complex map of Application Programming Interfaces (API) that break every time apps are updated, or cloud providers are changed. DevOps and TechOps allows development and operations teams to work collaboratively across integrated environments using a microservice architecture supported by containers.

A modern Software Defined Storage (SDS) based storage infrastructure is another key component of these hybrid multi-cloud computing platforms, in addition to the portability provided by containers. Together they play a critical role as the need to connect storage systems of multiple cloud environments with a degree of workload portability, orchestration, and management among them is increasing exponentially. SDS for containers allows enterprises to store data in any environment and move that data between them as desired.

IBM Spectrum Software Defined Storage solutions are continuing to play a crucial role in tackling the challenges and opportunities for this acceleration and optimization of container-based solutions for a variety of use cases in hybrid multi-cloud environments.

Business drivers

Technology and engineering organizations have realized that while the traditional way of doing technical operations can be made efficient with tools, processes, and automation, there is a fundamental shift in thinking required to react to today's challenges.

In this paradigm, development, operations, and security are separate entities collaborating to achieve common objects while guided by their own individual missions.

This is where pragmatic DevSecOps thinking can help shift to a proactive and ideally with the right tools even a predictive approach to problem solving. With the adoption of AI-centric, infrastructure-compatible technologies on the rise (such as IBM Spectrum), self-healing infrastructure is not as far-fetched for organizations to achieve as it once was. Deloitte distills DevSecOps down in terms of six capabilities, described below.

DevSecOps distilled: Six capabilities

CONTINUOUS INTEGRATION (CI)

Build, unit test daily
- Automates build, unit test
- Integrates source code with technical quality
- Metrics to manage technical quality

AUTOMATED TEST (AT)

Automate functional, performance testing
- Frequent regression testing
- Resolves defects early
- Metrics to manage functional quality

CONTINUOUS DEPLOYMENT (CD)

Test deployment daily
- Automates deployments and releases
- Runs deployment scripts and deployment validation tests
- Issues resolved early

DevSecOps is a culture shift, driven by shared vision, and is more than a technical solution.

DevSecOps delivers business value and mission IT with speed and quality. It joins "dev" and "ops" to maximize uptime.

IT organizations will learn new concepts, adapt leading practices and disciplines.

Process changes and metrics to provide indicators of success will be needed.

Enablers to success? Leaner technology platforms and investment in automation.

SOFTWARE DEFINED INFRASTRUCTURE (SDI)

Automates infrastructure provisioning
- Builds complete infrastructure from source code repository
- Tight control over all computing environment configurations

CONFIGURATION MANAGEMENT (CM)

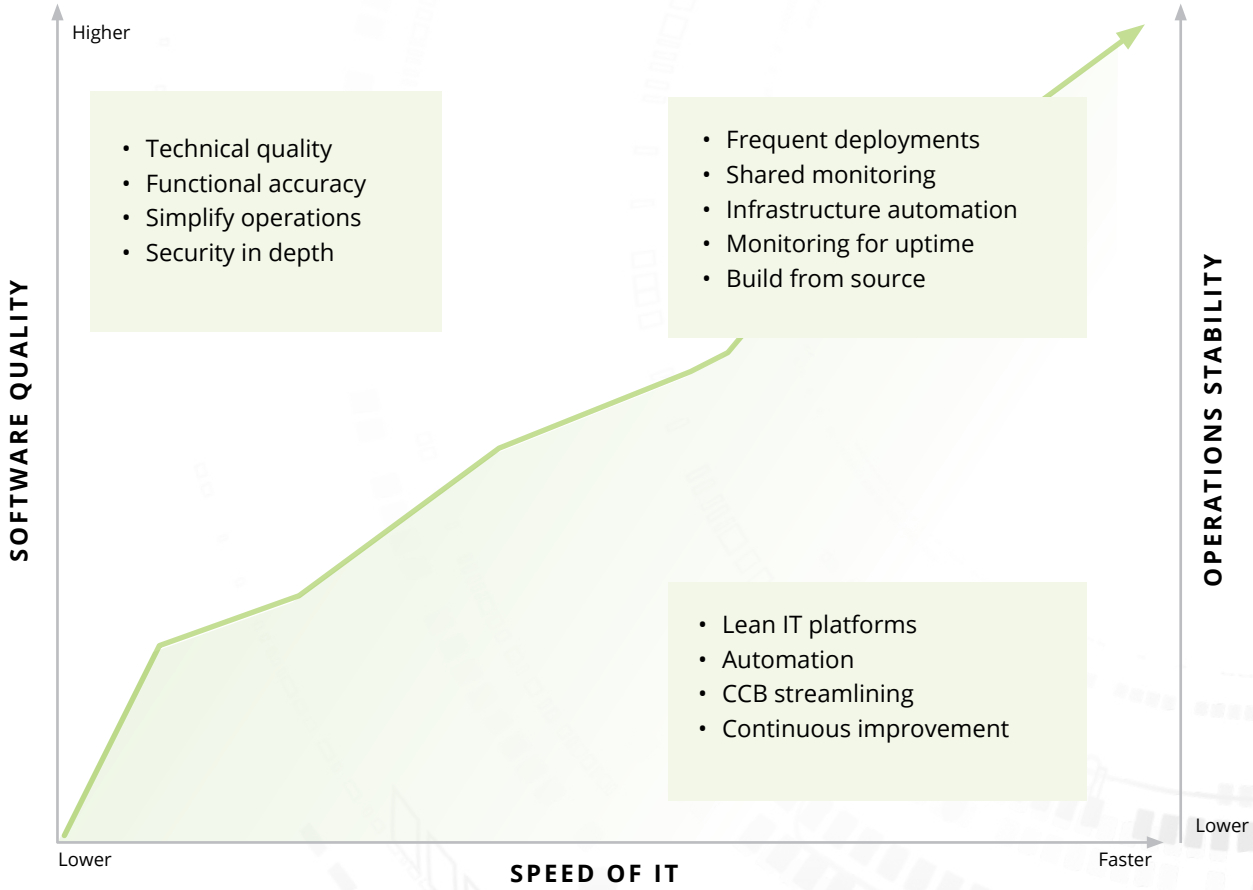
Foundation for DevOps
- A merge of "dev" and "ops" best practices
- A capability to strengthen when starting DevOps

CONTINUOUS MONITORING (MTR)

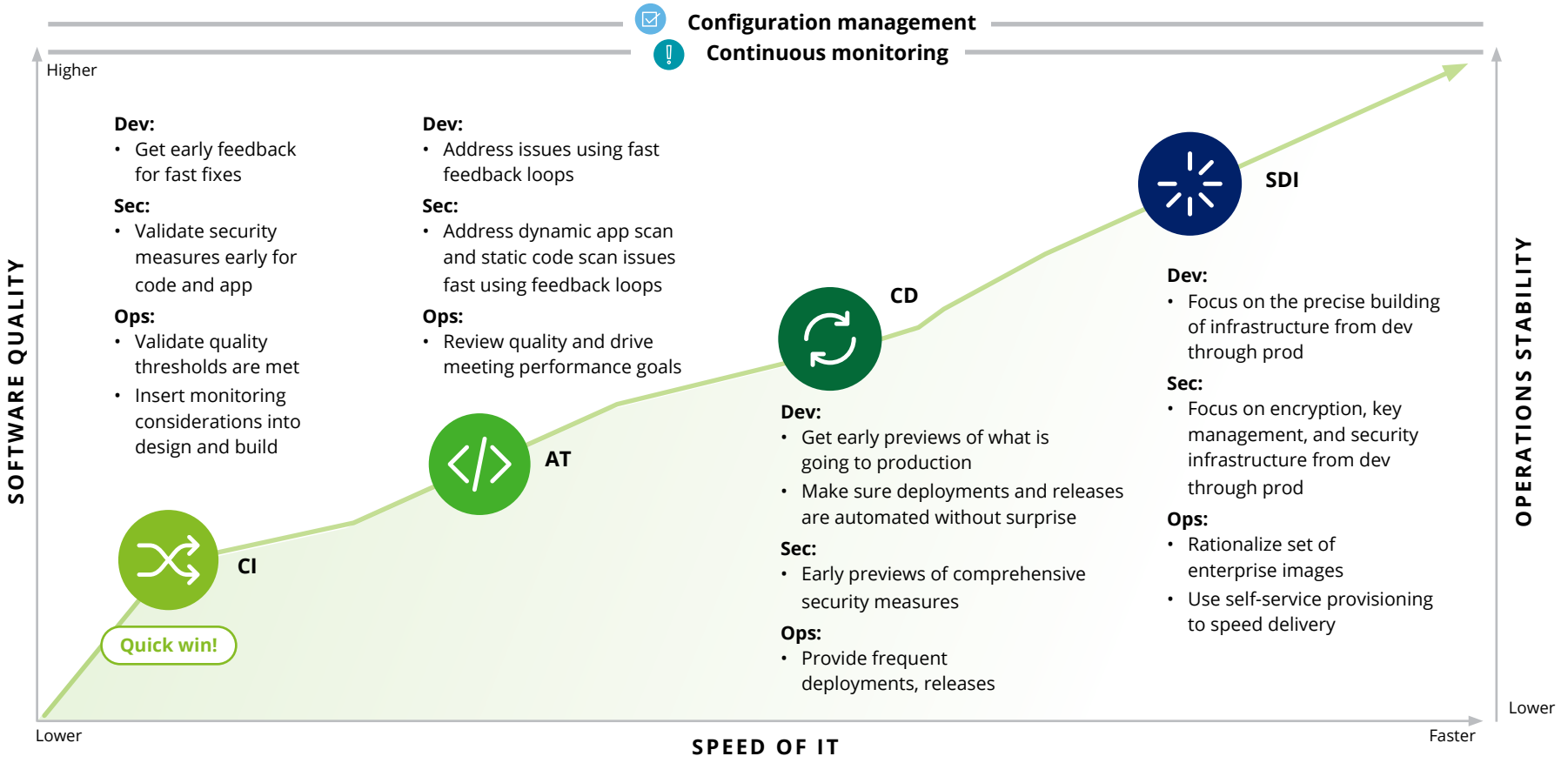
Monitor to take action
- Adopts "ops" monitoring disciplines to "dev"
- CI, AT, CD, and SDI generate metrics that can indicate action

In our experience, a typical journey for an organization looks as illustrated. It is important to note that DevSecOps is not a goal; instead it is a constant pursuit of improvement and evolution. Embedding security in all six capabilities, as opposed to treating it as a separate capability, is more likely to result in achieving realistic outcomes.

DevSecOps Journey: Defining the dimensions



DevSecOps roadmap: Strategize together, cross over best practices, create a DevSecOps culture



Based on this typical journey, a reasonable roadmap to achieve DevSecOps looks as illustrated. In this figure, the Software Defined Infrastructure (SDI) capability is on the far right and does require some maturity to achieve, with the other capabilities having been mastered to a reasonable level by the team in an existing IT infrastructure. There is a case to be made for new applications and systems where starting with the full vision upfront is often easier than trying to retrofit a system with active release cycles in production. Therefore, a lot of organizations consider new payloads or systems with fewer production release cycles to be candidates for DevSecOps pilots.

A typical organization with a large, complex ecosystem of technologies and business priorities often finds the adoption of the SDI capability to be significantly daunting. However, once achieved the outcomes of stability and higher quality (as well as speed in delivery) gained make it a prime target for CIOs and CTOs to consider as a business goal. With the advent of serverless technologies and most organizations adopting public cloud infrastructure in some shape or form, it is tempting to think that all existing workloads could transition to serverless architectures with ease.

Unfortunately, many enterprise systems are not candidates for pure serverless architectures due to:

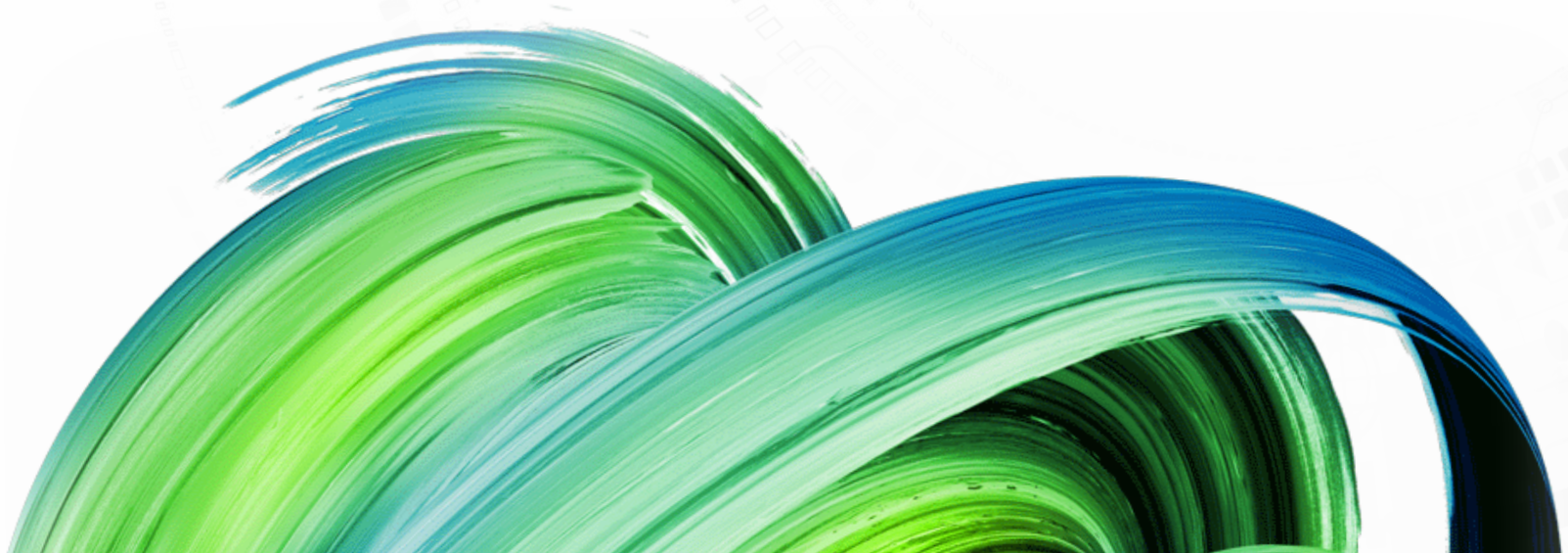
- Legacy architectures
- The nature of complex COTS integrations
- Significant investments in commercial application server technologies
- Legacy database engines

This is where containers lend a hand in easing the journey of DevSecOps for such large systems while allowing organizations to leverage cloud as necessary based on business decisions including regulatory compliance, data gravity, and integration complexity. Organizations that are used to relying on vendor support to decrease risks around uptime, patching support, and integration support (while still having a desire to adopt Open Source projects when it comes to SDI) can use IBM Red Hat OpenShift Container Platform (OCP).

Traditionally, virtual machines revolutionized compute resource distribution in datacenters. Today, containers are doing this at a more granular level with the application context even more tied in than before. When using the term SDI in today's context, it often gives IT executives the illusion that optimization is not needed. In actuality, the demands on performance, uptime, and business application adoption have only increased, with data being the wheel that is constantly accelerating the demand.

At the center of a good SDI strategy is storage, as it is the ultimate driving force that needs to scale with data, be it edge data or core data. Containers continue to become the norm for a lot of COTS vendors as well as application owners to package their solutions. Most enterprises will ultimately need a tool that bridges the optimization gap between a container platform like OCP and the myriad of storage options such as on-premise and public cloud providers. Such a solution should ideally continue to work with the non-containerized systems just as efficiently, otherwise it will simply add to the already complex IT landscape. This is where IBM Spectrum suite offers some unique products that reduce implementation complexity, especially when it comes to OCP based solutions as well as integrating with various public cloud providers, IBM cloud, and on-premises infrastructure.

While a container platform like OCP itself offers great options in terms of utilizing the full capabilities of underlying container and Kubernetes stack, it ultimately relies on the way the storage management solutions are configured. This is where the next level of optimization for a OCP type platform can be done using IBM Spectrum suite of products. IBM Spectrum Scale and IBM Spectrum Protect Plus can provide significant efficiencies to DevSecOps in organizations.



Why consider IBM Spectrum Scale for container optimization?

When it comes to large complex processing such as heavy data analytics, AI projects, IoT, or real time transactional systems, an organization needs a container infrastructure that can scale rapidly and be deployed with low latency. This is where combining a container technology such as OCP with IBM Spectrum Scale can provide significant ease of management, performance efficiency, and embedded security.

IBM Spectrum scale[1] provides containers with native storage access, including the ability to use data clustering provided by the high-performance Spectrum Scale nodes for on-premise architectures. By offering global access to object storage as a file from within a container, it reduces the complexity of the container image, allowing for easier persistence management of data vs. the container image. This also comes in handy when dealing with log file retention and using the IBM Spectrum Scale's native policy engine to archive to tape/cloud as needed within a hybrid infrastructure.

IBM Spectrum Scale offers a Kubernetes single management pane to tackle storage for all containers. This reduces operations overhead and allows for developers to focus on application development without worrying about the constraints and limits on localized disks. The native integration of IBM Spectrum Scale, with the OpenShift console, combined with a self-service mechanism for the enhanced Container Storage Interface (CSI) Operator dynamically provisions storage, making this an attractive option for DevSecOps teams looking to focus on removing the internal barriers and speed of delivery for their systems.

[1]IBM Storage for Data and AI Solution Brief - IBM Spectrum Scale Container Native Storage Access

Key considerations: IBM Spectrum Scale for container optimization

- **Optimize container resources**
- **Data accessible outside Kubernetes**
- **Policy-based archive to tape/cloud**
- **Self-service dynamic provisioning**
- **Enhanced access to storage and resources**
- **Scale container native storage without compute and data nodes**

Why consider IBM Spectrum Protect Plus for container optimization?

An efficient DevSecOps strategy must also address data replication speed, backups, and Disaster Recovery (DR). These components need an easy to manage policy-driven profile that allows for teams to secure data while having controls that don't prohibit business. IBM's Spectrum Protect and Protect Plus allows for the management of data directly into the Spectrum platform. This allows quick and efficient data backup to occur, including container images as well as the application data.

Having a unified capability to backup and restore this information simplifies operational procedures for refreshing non-production environments, as well as provisioning just-in-time data copies rapidly. This allows for short-lived use cases to still take advantage of full data sets that often need to be production sized for business use. These environments can be provisioned and disposed of quickly, without modification of the core business data profile changing. The built-in security measures, including pervasive encryption that addresses data protection concerns around sensitive data, can access monitoring and controls, especially when combined with containerized deployments. All of this is happening at speed without sacrificing compliance. And IT resources aren't having to jump through special controls and processes to meet the business demand.

Through the IBM Spectrum Protect Plus Kubernetes Backup Support capability, organizations can natively back up persistent volumes directly into the Spectrum suite. Container data can be rapidly backed up and replicated on-demand. Highly scalable workloads for non-production environments that have aggressive parallel release schedules mandating multiple environment sets and container profiles, Spectrum Protect Plus lets organizations confidently enable self-service for data sets and use policy engines to reclaim resources upon the DevSecOps pipeline being delivered.

This is crucial for busy DevSecOps teams who don't want to spend time on extensive resource reclamation exercises and need to do more with less due to either on-premise infrastructure constraints and/or imposed cloud resource limits. Spectrum Protect Plus provides out of the box de-duplication capabilities that can be further automated with policy driven actions.

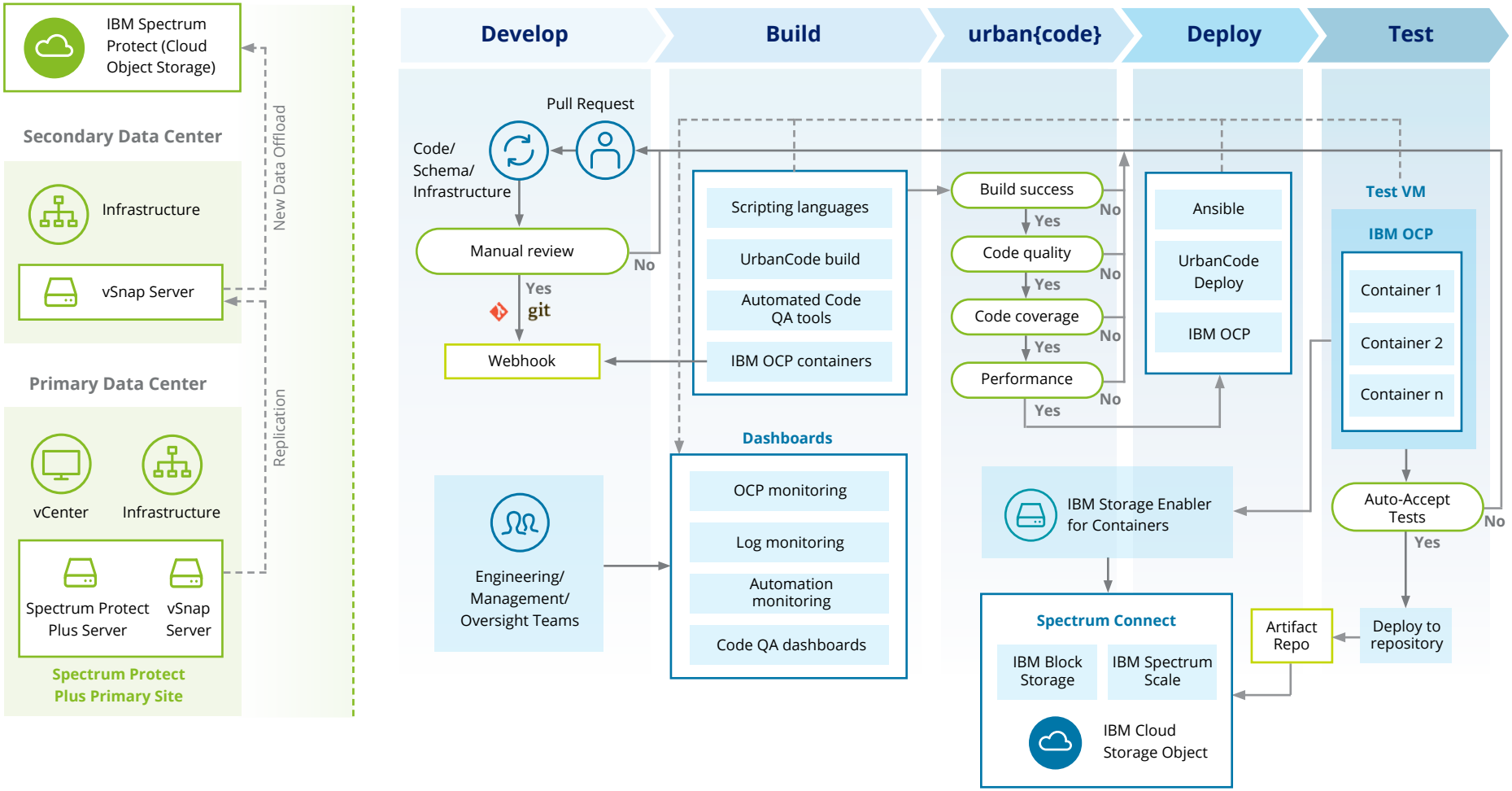
Additionally, as part of restore profiles when dealing with production data for non-production use, the teams have flexibility in setting profiles within Spectrum Protect Plus based on workload requirements. For instance, a development troubleshooting environment may not need the same Input Output Operations per Second (IOPS) profile and could likely work just as well on slower storage devices, whereas a performance test profile request may need to model production like performance of the system and utilize a higher IOPS profile.

By utilizing Spectrum Protect Plus profiles in combination with Kubernetes namespaces and the single pane management interface, an organization can use good guardrails that reduce inefficiencies without sacrificing time to delivery of features. These capabilities can be a game changer for DevSecOps teams across large research and development platforms, AI or IoT initiatives, or big transactional computing platforms.

Key considerations: IBM Spectrum Protect Plus for container optimization

- **Service level agreement driven policies for backup including frequency and retention**
- **Kubernetes services for multiple types of backup and support**
- **Role based access control to protect persistent data in containers**
- **Advanced encryption, network security and install package verification features integrated into Kubernetes Backup Support**

Architecture use case: A sample deployment architecture with IBM Red Hat OCP



The figure above represents a sample deployment architecture with IBM Red Hat OCP being used for the runtime. The diagram focuses on a DevSecOps perspective and how a typical OCP chain built on a typical Gitflow CI/CD pipeline uses Jenkins for orchestration. This architecture is representative of a typical AI application, IoT application, or even a large heterogeneous transactional application ecosystem. The containers consist of a combination of Open Source custom components and some COTS.

The containers themselves are optimized by Spectrum Scale to support rapid provisioning and allow such a system to scale as needed even in a hybrid cloud environment. Then the Spectrum Protect Plus enables the secondary data center/Disaster Recovery site as well. Important to note are some of the underlying components of the Spectrum Protect Plus suite include (at a minimum) a vSnap server and IBM Protect Plus Server that serves as the console. Similarly, IBM Spectrum Scale includes the IBM Spectrum connect server, the IBM Storage Enabler for containers, and IBM Spectrum Scale server including the console.

Conclusion

Traditionally, many organizations made their IT decisions in silos: on-premises versus cloud, storage speed versus size versus reliability, and divergent application optimization strategies. In today's constantly connected world, with shorter decision windows, decisions like these are no longer independent.

As organizations make decisions in the context of the overarching principles of cloud and optimization, they should carefully consider storage technologies. Scalability, security, and performance continue to reign as key drivers in the world where AI, Cloud, and Cyber take front and center stage. As organizations continue to migrate from traditional implementations to modern hybrid approaches for hosting, applications, and storage, they need to look for ways to support both traditional IT as well as digital transformation.

Using modern storage solutions like the IBM Spectrum suite in combination with container platforms like IBM Red Hat OCP, organizations can take advantage of wielding applications and data scalability with higher efficiency, while continuing to utilize existing on-premise and cloud assets. Ultimately, the drivers such as organizational IT infrastructure assets, data gravity, software assets, regulatory landscape, and business criticality will drive demand for workload profiles.

Using containerized technologies in combination with solutions like IBM Spectrum SDI suite allows for flexibility and optimizing capital expenditure spend.

How technologies like IBM Spectrum suite combined with IBM Red Hat OCP can help your business

Avoid costs

- Avoid unnecessary data replication by using Automated File Migration for local data caches
- Avoid management complexity with more self service and automated policies

Increase efficiency

- Increase availability and automate error handling further
- Increase infrastructure sharing

Grow business

- Focus on innovation over enablement
- Adapt to different data workloads faster
- Reduce time to market for new features and functionality

Authors and contributors

Hemang Dholakia
Managing Director
Deloitte Consulting LLP
hdholakia@deloitte.com

Venu Bommenani
Technical Architect
Deloitte Consulting LLP
vbommenani@deloitte.com

Mike Zawacki
Technical Architect
Deloitte Consulting LLP
mzawacki@deloitte.com

Amitava Kumar
Technical Architect
Deloitte Consulting LLP
amitavkumar@deloitte.com

Rinku Sinha
Digital Architect
Deloitte Consulting LLP
rinsinha@deloitte.com

Bob Miller
IBM Alliance Solution Architect and Legacy Transformation Lead
Deloitte Consulting LLP
robmiller@deloitte.com