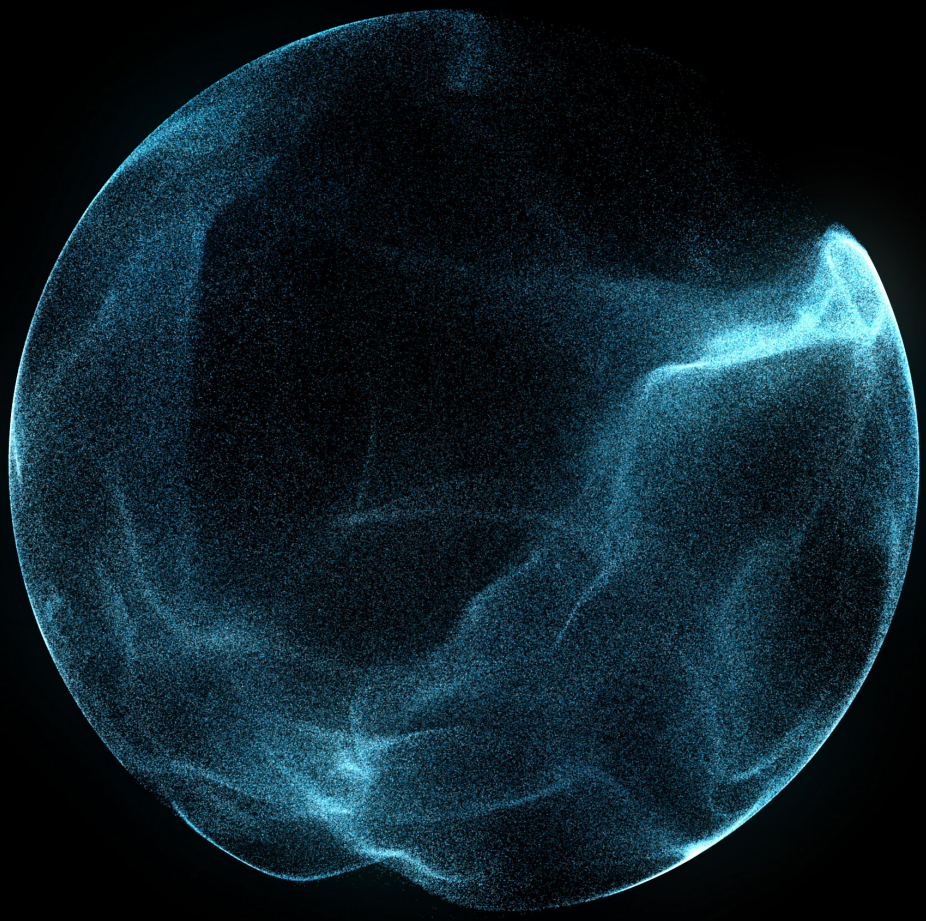
Deloitte.



One cloud does not fit all

Building, managing, and securing multi-cloud environments

MAKING AN IMPACT THAT MATTERS since 1845

More than a decade into cloud adoption we are now seeing an interesting phenomenon emerge that is analogous to the "server sprawl" that the IT industry experienced in the 1980's and 1990's. This has led to the creation of multi-cloud environments where organizational data and applications are spread across multiple cloud vendors, thus increasing profitability and access to services. However, without a planned design and governance model, such environments can lead to increased risk, where users and applications are now spread across several clouds without the means to centrally view, secure, or manage these environments effectively.

Some are calling this phenomenon "cloud sprawl", which can create many challenges for the IT organization when it comes to designing, monitoring, and securing all the cloud usage across the enterprise. In this paper we dig deeper into various facets of designing, building, managing and securing cloud environments with respect to three major aspects:

- Design and architecture with a focus on cloud strategy
- Management and operations with a focus on interoperability, portability, storage, and tools for effective delivery
- Cloud security with a focus on automation to maintain visibility across multiple environments, and reduce risk through the application of zero trust principles

Doug Schneider
Managing Director

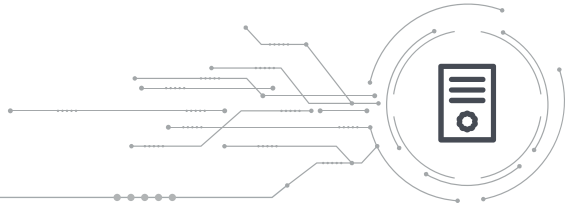
Doug Schneider is a Managing Director in Deloitte Consulting LLP's Government & Public Services practice and serves as Deloitte's Cloud Native leader. He is advancing cloud native and multi-cloud capabilities with a focus on industrializing DevSecOps as Software Factories for Government.

Doug's 25 years of experience spans public and private sector technology delivery and transformation engagements. He assists his clients to improve their software delivery organization and engineering culture by adapting industry leading software practices.

Design and architecture

In a multi-cloud environment, cloud strategy becomes a continuous process and thus cloud design and architecture similarly need to be able to evolve continuously. A continuous cloud architecture is therefore the foundation of a sound, long-term, multi-cloud strategy. A Continuous Cloud Architecture (CCA) describes the business logic and data framed as end user software products. Designing common cloud solutions with the openness to adopt cloud SaaS offerings, agencies can reduce costs, become timely and let go of low-level operations and maintenance (O&M) risks. Other benefits come in the form of lower O&M costs compared to a separate cloud-per-agency-silo approach. Platforms that are multi-cloud are integrated upfront regardless of who the vendor is and narrow the usage of cloud tools per the CCA guardrails. The benefit is multi-cloud reach, avoiding sprawl, and a shorter lead time to deliver user needs.

The benefits of a CCA as part of an agency multi-cloud strategy are compelling. A CCA assists agencies to prioritize and make decisions based on the current divisions of IT responsibility in balance with agency end-to-end mission goals. Without a CCA, moving to cloud could result in just adding over time, versus keeping a lean inventory of best-fit integrated cloud technologies. The age of decade-long investments in fixed systems is giving way to regular evaluation, selection and migration – the advantage is the end of legacy systems and the high-cost, high-risk worries of today.



Dave Savino
Managing Director

David Savino is a Managing Director in Deloitte Consulting LLP's Government & Public Services practice and serves as Deloitte's Cloud Managed Services leader. He focuses on assisting his clients with the modernization of their IT infrastructure programs. Dave brings 20+ years of IT management experience in both the federal and commercial sectors and is currently supporting clients in the Civilian, State and Local, and Defense sectors.

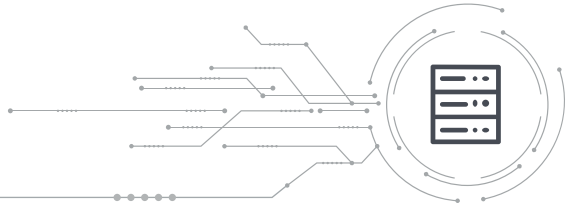
Management and operations

Cloud Operations
Cloud operations have rapidly become a hot topic with nearly every IT organization as they begin to restructure their workloads for the cloud. In the multi-cloud world, three considerations become key to successful operations: interoperability, portability, and storage. Ensuring interoperability with existing data centers, Software as a Services (SaaS) applications, multiple cloud service (IaaS) providers, and other entities can be a challenge. Equally important for many IT organizations is avoiding over-reliance on a single vendor – so data and workload portability is another key factor in cloud operations. Lastly – because storage is "easy to add" almost everywhere in cloud, it is vitally important to keep an informed view of storage needs versus storage costs.

Interoperability: Ensuring proper interoperability between your cloud platforms and other systems (be they data center, SaaS, or other third-party services) is a vital part of cloud operations. Interoperability considerations greatly affect the operational cost of a cloud deployment. Without the right levels of interoperability, it is possible to more than double the operational overhead of maintaining a multi-cloud platform.

Portability: Portability covers two aspects of deployed application systems: migration between an existing data center and the cloud and migrating between Cloud Service Providers (CSPs). When planning a cloud migration of any variety the data and applications on the source systems need to be easily shifted into the cloud. If migrating between two CSPs, planning should be done in the first migration to cloud, so that successive migrations to other CSPs can be made smoothly. To maximize portability, consider the use of containers with a supporting container system such as Kubernetes, or properly sized virtual machine deployments. While CSPs have similar service offerings for various aspects of an application such as API gateways and internal and external connections, translating an application from one CSP to another can be difficult if all the needed features are not present on the target CSP. In short, careful planning around even the very first migrations from data center to cloud can help to alleviate problems down the road with portability within a multi-cloud environment.

Storage: Ability to access and share data across multiple CSPs is critical and requires careful planning of data access and security. Keeping a close eye on storage is a crucial requirement that makes up the whole of cloud operations, as storage can quickly become one of the largest cost drivers for any cloud workload both in terms of hard dollars and the time and attention required to manage. A fundamental aspect of every multi-cloud deployment is the need for storage. Whether it is a drive attached to a virtual machine or a bucket various resources can access, storage can be a difficult to manage.



Doug Bourgeois
Managing Director

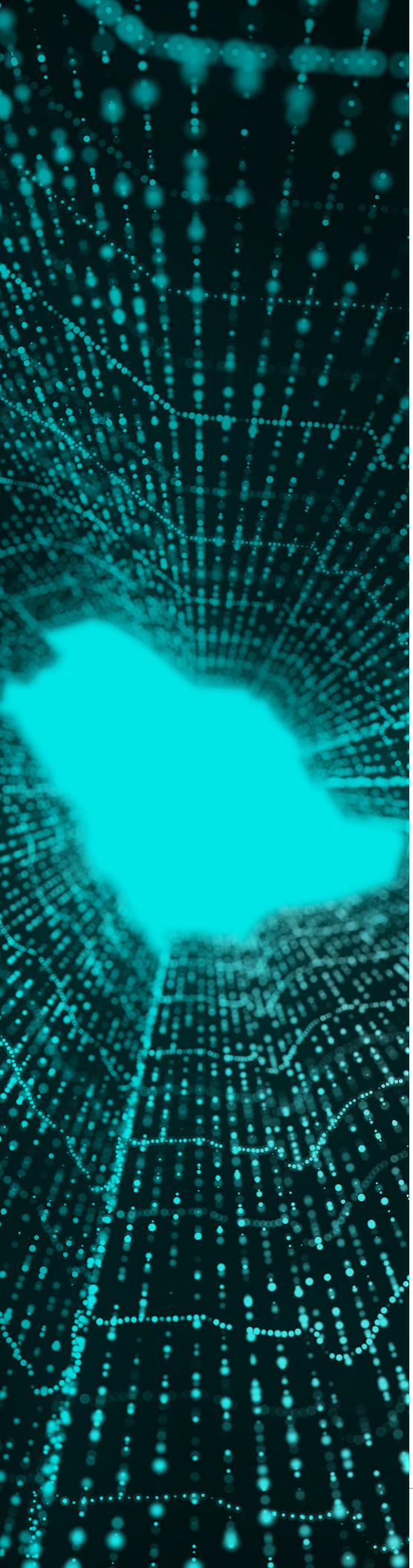
Doug Bourgeois is a Managing Director in Deloitte's Government and Public Services practice, focusing on cloud computing and shared services. He previously led multiple cloud and secure mobility projects at VMware, where he served as vice president of End User Computing and previously as a chief cloud executive for a public sector agency.

Tools for effective delivery

Mission teams have begun to realize the benefits of cloud and are now consuming cloud faster than many IT organizations can handle. When a variety of mission groups migrate applications to multiple clouds, these applications often do not follow standardized processes or governance. A key reason is that current policies that govern government IT are typically not designed for cloud and modern service delivery approaches, and as a result, are often bypassed. To combat the resulting cloud sprawl, an integrated platform that enables DevSecOps, Infrastructure as Code (IaC), automated Cloud governance, and agile deployments and orchestration can offer significant benefits that meet the speed of the mission.

In addition to that, an effectively designed multi-cloud management solution needs to categorize functions and capabilities into a framework that consists of common security policies and governance. These policies could be enforced by integrating the cloud security management and enforcement capabilities across each layer of the cloud management stack as well as extending them into the cloud service provider environment. The cloud management stack consists of seven integrated layers with each one providing a specific set of capabilities, which are complementary to the overall solution. Each layer that comprises a comprehensive multi-cloud management solution is summarized below:

- **The Business Management** layer facilitates informed decision making. This layer includes the tool set that provides transparency and control over the costs and quality of IT services, enabling the decision-makers to align IT with the mission by comparing the costs of workloads between the private cloud and multiple public clouds.
- **The Service Management** layer provides a common unified portal to allow users with role-based authorization to request IT services across clouds. It includes a workflow management and automation capability to implement a service catalog and governance that spans the entire multi-cloud operational environment in a manner that is streamlined for the user.
- **The Operational Management** layer offers a single pane of glass command and control panel, which provides operations staff cloud administration, performance monitoring/ tuning, risk mitigation, and troubleshooting capabilities.
- **The Automation** layer provides consistent deployment and management of IT services while reducing manual processes, helping limit human error, and ensuring policy compliance. This often means integration and support of Infrastructure-as-Code technologies such as Terraform and configuration management tools such as Ansible.
- **The Orchestration Platform** layer enables the automation of complex IT tasks to adapt and extend service delivery and operational management across clouds and with existing IT investments. The orchestration platform is the engine by which vulnerability scans are conducted at the right time in the life cycle, agents are installed on workloads, data is automatically entered into an external CMDB, and more.
- **The Application Programming Interfaces (APIs)** layer is extensible. It includes the capability to recognize the most common APIs and can interact with IT management and an organization's private cloud as well as the major CSPs that have achieved a FedRAMP security authorization.
- **The DevSecOps** layer allows the solution to be forward facing, with the ability to incorporate the required tools to enable the operations of a continuous integration and delivery pipeline. This requires entire workflows being triggered from a code repository commit and applies to both Infrastructure-as-Code and application code in a cloud agnostic approach.



DevSecOps in the multi-cloud environment

By Doug Schneider

Most government agencies do not need the high frequency of DevSecOps deployments that commercial startups must have to compete in the marketplace. However, agencies are interested in the DevSecOps byproducts of greater automation that include cost savings, continuous security, transparency, and the ability to trust a fast deployment cycle when responding to urgent events (pandemics come to mind). A DevSecOps culture intersects with multi-cloud in several ways. These intersections include automation and integration of security and optimizing a common backplane for O&M. Integration is not only the run-time components for end users, but also the DevSecOps toolchains and pipelines. For example, a multi-cloud approach for authentication and access control must integrate across clouds and be maintainable versus the cost and overhead of Federating multiple Identity and Access Management solutions.

DevSecOps automation speeds software delivery, removes human error and provides better transparency of the security and quality to meet user needs. DevSecOps is sometimes referred to as *SecOpsDev* to highlight shifting security-left in the lifecycle by implementing zero trust architecture and securing the software supply chain as the agency cloud foundation. Leading agencies are creating multi-cloud, security-first landing zones with cybersecurity operations that detect and push security events versus just periodic auditing. Securing multi-cloud landing zones and architecting for secure data sharing is not trivial and worth addressing upfront on the path to multi-cloud. CSPs provide cloud technologies lowering the effort for authorization and maintenance. Selecting, extending and connecting CSP technologies must be on the list for agencies adopting multi-cloud.

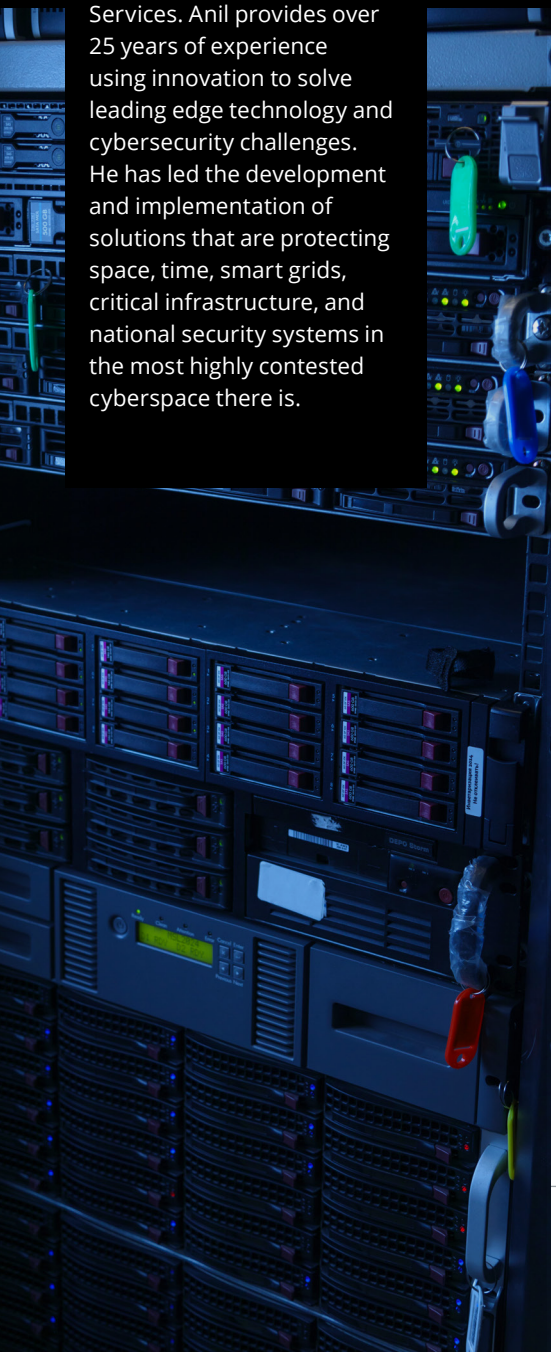
DevSecOps in multi-cloud goes beyond simply scanning application code but includes validating that security controls are always in place with the system. Implementing common security controls in cloud workloads that move or are extended across environments is difficult with only native solutions. Agencies moving to multi-cloud for application portability have to plan for how security controls will travel with the workloads that move from one cloud to another. This includes advanced data discovery, tagging, and classification capabilities along with network and identity segmentation to control communication amongst application components.

The *Ops* in *SecOpsDev* highlights the upfront operate and maintain aspects, seeking a common backplane to manage scale, cost and resolve/prevent incidents across environments. A common, multi-cloud backplane provides advantages in operating a mix of CSP containerization, serverless and managed services to monitor and trace execution across CSPs using integrated views for Service Level Agreement management.

DevSecOps for multi-cloud has intersection points that matter upfront when designing your strategy and architecture. Integration across CSPs with durable interface points avoids vendor lock-in, and enables making changes downstream. Shifting left on Security and Operations is paramount when considering moving to a multi-cloud approach that's cost effective and avoids more costly redundant silos of operations.

Anil Ramcharan
Principal

Anil Ramacharan is an Advisory Principal in Deloitte's Government & Public Services practice, focusing on Cyber Risk Services. Anil provides over 25 years of experience using innovation to solve leading edge technology and cybersecurity challenges. He has led the development and implementation of solutions that are protecting space, time, smart grids, critical infrastructure, and national security systems in the most highly contested cyberspace there is.



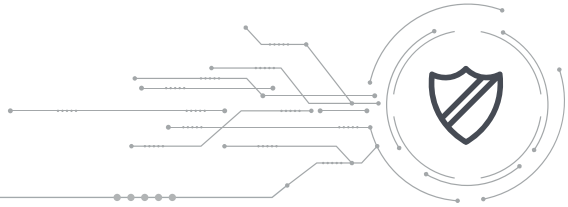
Security

Implications of security in multi-cloud environments

The reality for cybersecurity leaders at many organizations going through commercial cloud migrations is that their IT agencies are not migrating to just one cloud provider, but several across a variety of cloud delivery models (i.e., infrastructure-as-a-service, platform-as-a-service, software-as-a-service). This multi-cloud environment represents a new set of complex challenges and risks to the cyber risk profile of their enterprise. New architectures and capabilities need to account not just for extending compliance, protection, and operations out of an on-premises data center(s), but for enterprise users, assets, and data moving in and out of different CSPs with a different set of security responsibilities and tools. Despite these challenges, if managed effectively a multi-cloud environment can bring new opportunities for greater cybersecurity.

Each CSP is responsible for the security "of the cloud", but each customer remains responsible for what's "in the cloud". This includes the configuration of individual services and use of the security services and tools that CSPs provide as options for customers to use. Unmanaged CSPs connected to the network and services being used that aren't visible and managed by the organization is the new "Shadow IT" for enterprises. Organizations will need to maintain visibility into all the CSPs and cloud services in use, how those services are being used, and the configuration of those services.

Manually maintaining visibility and managing configurations across CSPs is a time-consuming process that can introduce errors. Automation becomes key for enabling customers to manage and enforce cloud service configurations and enterprise security policies across a diversity of CSPs. Customers can go one step further and apply zero trust principles to cloud native network, compute, storage, logging, and other functional services across CSPs to manage risk while reducing costs and providing the agility that enables developers to move at the pace of missions and business.



Conclusion

Operations and security in a multi-cloud environment has its challenges. The key is to stay ahead in the game by taking the time to properly define and design your multi-cloud solution, and then select the right management and monitoring tools to fit your requirements.

At Deloitte, we see our role as a trusted advisor to our government and public sector clients to help them advance mission-critical operations. With over 4,500 employees with security clearances and more than 70 former senior government executives, our team of Deloitte professionals has a deep understanding of how to navigate the complexities of regulatory environments and help see the full cloud picture.

Get in touch

Thomas Beck
Principal
thbeck@deloitte.com

Dave Savino
Managing Director
dasavino@deloitte.com

Meghan Sullivan
Principal
msullivan@deloitte.com

Doug Bourgeois
Managing Director
dbourgeois@deloitte.com

Doug Schneider
Managing Director
douschneider@deloitte.com

Geetika Tandon
Managing Director
getandon@deloitte.com

Anil Ramcharan
Advisory Principal
aramcharan@deloitte.com

Deloitte.

Designed by CoRe Creative Services. RITM1053967.