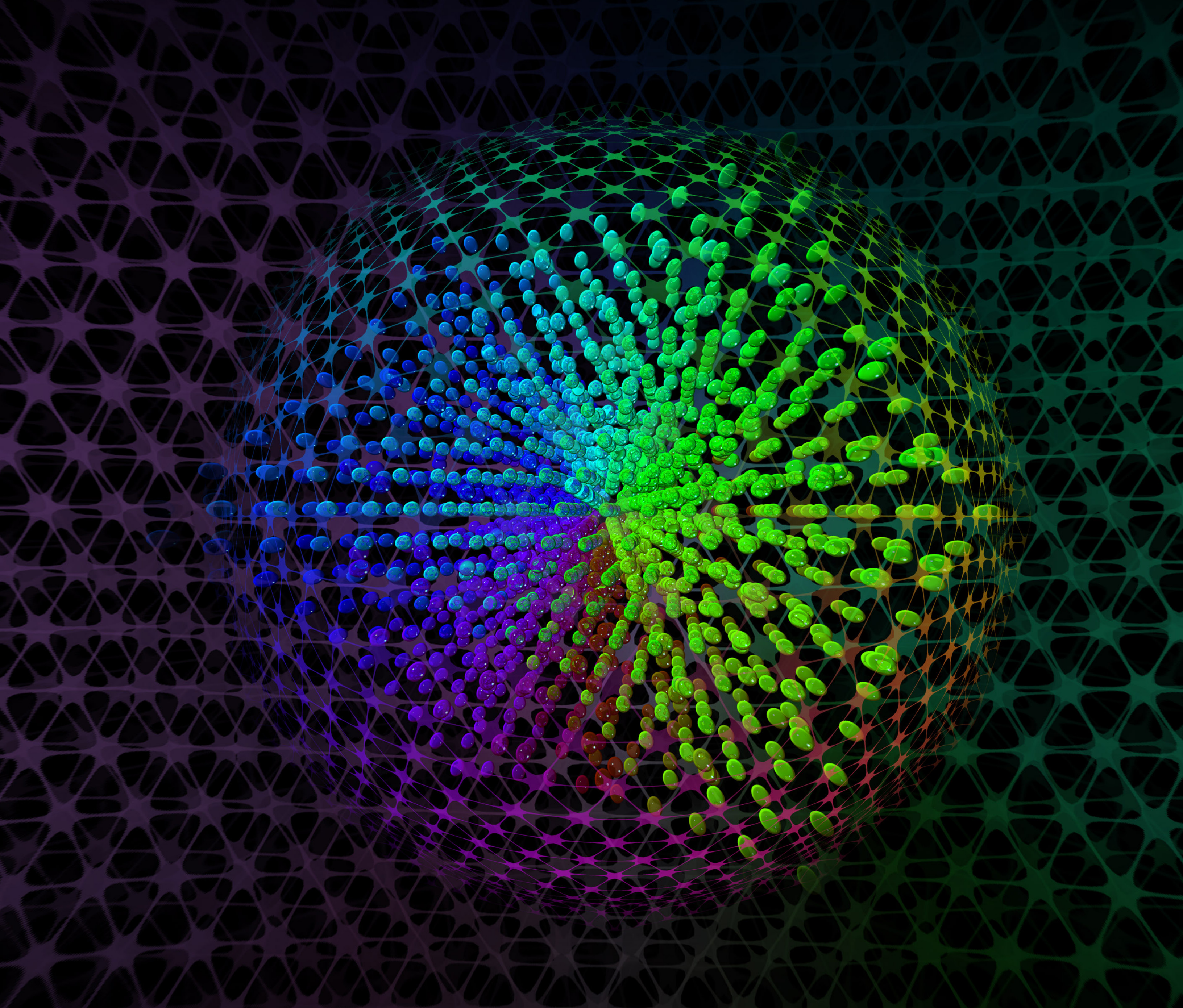
Deloitte.
Insights

A report from the
Deloitte Center for Integrated Research



The future of cloud-enabled work infrastructure

Making virtual business infrastructure work

About the Deloitte Center for Integrated Research

Deloitte's Center for Integrated Research focuses on developing fresh perspectives on critical business issues that cut across industries and functions, from the rapid change of emerging technologies to the consistent factor of human behavior. We look at transformative topics in new ways, delivering new thinking in a variety of formats, such as research articles, short videos, in-person workshops, and online courses.

Connect

To learn more about the vision of the Center for Integrated Research, its solutions, thought leadership, and events, please visit www.deloitte.com/us/cir.

Deloitte Cloud Consulting Services

Cloud is more than a place, a journey, or a technology. It's an opportunity to reimagine everything. It is the power to transform. It is a catalyst for continuous reinvention—and the pathway to help organizations confidently discover their possible and make it actual. Cloud is your pathway to possible. To learn more, visit Deloitte.com.

Contents

Cloud growth accelerated by COVID-19

COVID-19 HAS DRIVEN a fundamental shift in business-architecture assumptions. Overnight, many organizations have had to shift their cloud infrastructure strategies. In fact, in a Logic Monitor survey, 87% of global IT decision-makers agree the pandemic will cause organizations to accelerate their migration to the cloud, anticipating a decline in on-premises workloads by 2025.[1] That accelerated adoption has started already (figure 1).

Companies worldwide spent US$34.6 billion on cloud services in the second quarter, up roughly 11% from the previous quarter.[2] As Satya Nadella, CEO of Microsoft, states, "We've seen two years' worth of digital transformation in two months."[3]

Organizations that move quickly have an opportunity to rethink how technology is enabling virtual work, workforce, and workplace and to use infrastructure as a competitive differentiator.

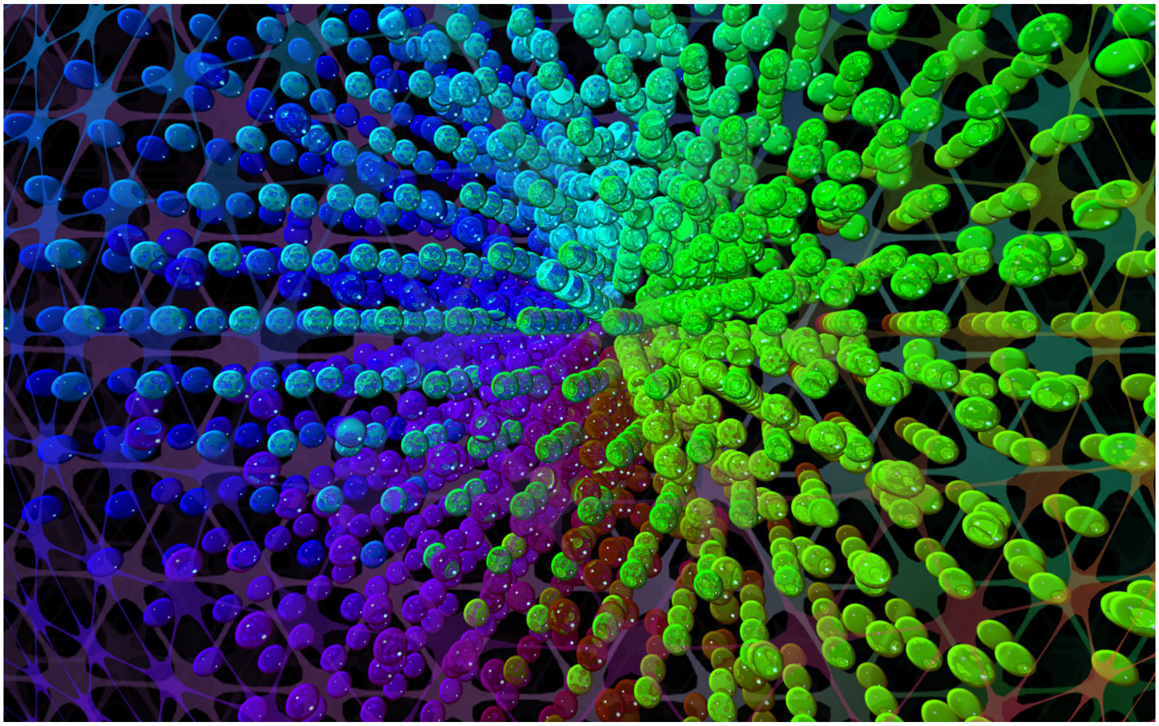


FIGURE 1

Cloud strategies accelerate in response to COVID-19

Before the COVID-19 pandemic	During the COVID-19 pandemic
CLOUD DEMAND **20%** of enterprises expected at least half of their enterprise workload/data to be in a public cloud within 12 months.[a]	CLOUD DEMAND **59%** enterprises expect cloud use to exceed plans due to the pandemic.[b] Queries for senior cloud executives in the digital realm have increased **224%**.[c] Half a dozen global financial institutions have announced new cloud initiatives since the start of the pandemic.[d]
REMOTE WORKING **3%** full-time employees reportedly worked remotely in January 2020.	REMOTE WORKING **64%** full-time employees reportedly worked remotely as of April 2020.[e] **81%** of the global workforce (2.7 billion workers) was impacted by stay-at-home orders as of May 2020.[f]
COLLABORATION TOOLS ~**20 million** Microsoft Teams daily active users in November 2019.[g]	COLLABORATION TOOLS ~**75 million** (almost quadrupled) Microsoft Teams daily active users by May 2020.[h]
INFRASTRUCTURE REQUIREMENT **17%** desktop users and **15%** mobile users accessed VPN in December 2019.[i]	INFRASTRUCTURE REQUIREMENT Microsoft Azure VPN connections grew **94%**. WAN peak traffic grew 40x since lockdowns were imposed in early March.[j] VPN connections grew **72%** from the prepandemic levels.[k]
CLOUD REVENUES The cloud market leaders experienced considerable growth in 2019. • **37%** growth for Amazon Web Services (AWS) in Q2 2019 • **22%** growth in Microsoft Intelligent Cloud revenue in Q3 2019 (includes server products, cloud services and enterprise services, revenue)[l]	CLOUD REVENUES Despite the economic recession, each major public cloud provider posted continued **double-digit** growth in 2020.[m] • **43%** revenue growth for Google Cloud Platform in Q2 2020 cloud revenue [n] • **29%** growth for Amazon Web Services in Q2 2020 [o] • **27%** growth in Microsoft Intelligent Cloud revenue in Q3 2020 [p]

Sources: Deloitte analysis and as given below:

a) Flexera, *Flexera 2020 state of the cloud report*, accessed August 19, 2020

b) Ibid.

c) James Bourne, "Cloud executive demand soars due to Covid-19, data shows," Cloud Tech, July 27, 2020

d) Patrick Jenkins, "Big banks look to the cloud to accelerate digital shift," *Financial Times*, July 20, 2020

e) Roy Maurer, "SHRM: Employers say remote work not here to stay," SHRM, May 5, 2020

f) International Labor Organization, "COVID-19 and labour statistics," accessed August 19, 2020

g) Venture Beat, "Microsoft Teams passes 20 million daily users, up more than half in 4 months," November 19, 2019

h) Moshe Beauford, "Microsoft Teams skyrockets to 75 million DAUs," *UC Today*, May 4, 2020

i) Rob Mardisalu, "VPN statistics and usage," The Best VPN, January 6, 2020

j) Mark Russinovich, "Azure responds to COVID-19," Microsoft Azure, June 16, 2020; Donna Goodison, "Microsoft Azure CTO Mark Russinovich gets technical about pandemic capacity," CRN, June 16, 2020

k) Verizon, "Verizon delivers network reliability during COVID-19 while accelerating 5G deployments," June 11, 2020

l) Microsoft, "Earnings release FY19 Q3," press release, April 24, 2019

m) Sean Michael Kerner, "AWS, Microsoft Azure, Google Cloud grow during COVID-19 pandemic," Channel Futures, May 11, 2020

n) Natalie Gagliordi, "Google's Q2 cloud revenue climbs over 43%," ZD Net, July 30, 2020

o) Emil Protalinski, "Amazon reports $88.9 billion in Q2 2020 revenue: AWS up 29%, subscriptions up 29%, and 'other' up 41%," Venture Beat, July 30, 2020

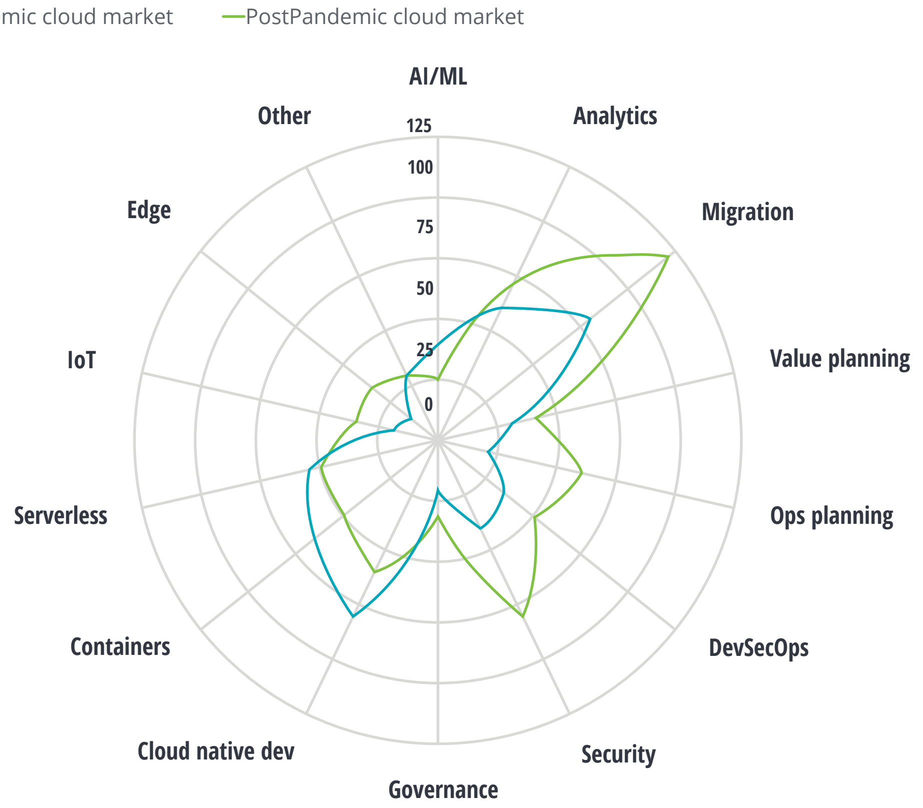
p) Microsoft, "Earnings release FY19 Q3," press release, April 24, 2019.

With most of the global workforce remote, major public cloud providers witnessed a huge surge in demand for their services. Such volumes stressed traditional infrastructure (e.g., virtual private networks) and forced organizations to lift and shift to the cloud quickly, leaving room for further optimization. Stay-at-home orders made it difficult, if not impossible, to access on-premise infrastructure highlighting a key infrastructure risk.[4] The vulnerability of tightly interlocked business and technology architectures to stress has become apparent.[5] For these reasons, we expect to see a shift in cloud strategies toward cloud migration, security, operations, value planning, and DevSecOps (short for development, security, and operations) as well as a retraction of cloud native, container, and serverless initiatives (figure 2).

As organizations respond to COVID-19 with a renewed cloud focus, they face **IT complexity**, **security risk**, and **operational efficiency** challenges. While some organizations are deprioritizing or delaying nonessential cloud migration plans,[6] resilient leaders and organizations have an opportunity to modernize their technology backbones with scalable cloud infrastructure.[7] When designing an approach, Deloitte's research has shown that the "magic mix" to resolving cloud complexity is having effective

FIGURE 2

COVID-19 is a corner stone in cloud strategy and planning



Source: Deloitte perspective based on several sources, including analyst input, clients, and thought leadership trends, among others.

tools (34%), approaches (34%), and people (32%).[8] For many organizations, this means reigniting cloud programs and employing new strategies across development and operations (DevOps), federated security, and multicloud solutions for heterogeneous infrastructures to optimize process, mitigate risk, and manage complexity. Organizations that move quickly have an opportunity to rethink how technology is enabling virtual work, workforce, and workplace and to use infrastructure as a competitive differentiator (figure 3).

FIGURE 3

Business challenges are accelerating cloud infrastructure solution uptake across work, workforce, and workplace

BUSINESS CHALLENGE	TECHNOLOGY AND OPERATIONAL CHALLENGE	TECHNOLOGY SOLUTION APPROACH
Technology complexity increases with shifting consumption and access models across heterogeneous infrastructure.	• **Physical data centers** can no longer be accessed due to remote **workplace** requirements. • **Remote-working volumes** stress traditional infrastructures, forcing lift-and-shift strategies that require greater operational efficiency.	• **Multicloud solutions** (not just strategies) will support virtual work, workforce, and workplace with a focus on operational efficiency tools and platforms for a full-stack solution • **Virtualized data centers** will enable centralized remote data access or distributed data management.
Security risks arise as tightly interlocked business and technology architectures show vulnerability to stress.	• **Physical infrastructure** becomes inaccessible due to stay-at-home orders, expanding access points and shifting the security perimeter. • **Heterogeneous technology** infrastructure and changes to the nature of work shift network access points and consumption.	• **Federated security** manages situational awareness and access points as contexts change and encourages information-sharing for real-time threat intelligence and remediation.
Operational efficiency requires resilient ways of working to quickly meet shifting business needs.	• **A distributed workforce** that can't physically be together impacts teams and ways of working across nonstandardized infrastructure, prompting companies to implement technology infrastructure changes.	• **DevOps** is a tried and true approach to achieving better value sooner, safer, and more painlessly from IT programs, and is seeing new developments in an increasingly distributed work environment.

Source: Deloitte analysis.

Multicloud solutions, not strategies, to support virtual work, workforce, and workplace

MULTICLOUD AND HYBRID *cloud strategies are now the norm*, with an industry study finding 93% of organizations using cloud infrastructure are employing a multicloud strategy, 87% of which are using a hybrid (public and private) cloud infrastructure model. As much as 85% of enterprises agree hybrid cloud is the "ideal" IT operating model, with 61% of respondents reporting the need for application mobility across clouds and cloud types as "essential."[9]

The next frontier in managing cloud complexity will likely be about building on that foundation by configuring tools, software, and technology to deliver a full-stack, multicloud solution.

As such, many organizations have moved beyond the initial challenge of selecting multiple cloud providers, determining what data to store in public or private cloud services, and managing interoperability across their multiple cloud infrastructures. The next frontier in managing cloud complexity will likely be about building on that foundation by configuring tools, software, and technology to deliver a full-stack, multicloud *solution*—whether that includes identity and access management, network monitoring, metadata management, or artificial intelligence for IT operations (AIOps) to manage workforce systems and platforms used to perform work.[10] Multicloud *solutions* should consider orchestration across these tools and technologies to manage data, resources, and workflows and help ensure the most efficient flow of data across the full solution architecture including storage, databases, platforms, and even security. Only then can the multicloud infrastructure efficiently and securely support business applications to drive value on an application-by-application basis.

In a COVID-19 context, what can be especially challenging for multicloud solutions is finding a good application fit for those technologies, quickly. The temptation is often to leverage whatever platform or service is in a hype cycle. However, moving to an application that is not a good fit for any new platform is typically going to fail. Organizations should first understand the application itself, understand the connected data, and the underlying architecture, and then assess if any of these new technologies is a fit. Kubernetes, an open-source project by Google to automate container deployment, management, and scaling, is an example. Flexera's annual cloud study shows businesses use an average of 2.2 public and 2.2 private clouds[11] and 20% of organizations are using Kubernetes in production or for development and testing.[12] But that doesn't mean others should rush to use Kubernetes. Instead, companies could do well to think about what cloud management resources are needed to support the underlying business application—in this case, remote work infrastructures and collaborative working environments—and work back from there to select the right tools that bring the right services (figure 4).

FIGURE 4

Developing IT infrastructure that powers the future of work, workforce, and workplace

NEW CHALLENGE →	WHERE WE WERE →	WHERE WE'RE GOING →	BENEFITS
DATA CENTERS			
• On-premise data centers face business continuity risk.	• Virtualize data centers for long-term workload-management gains.	• Build common data services with a single virtual database or by managing data in a distributed way.	• Eliminate redundancy and enable data understanding, API connectivity, and enhanced governance.
IT			
• Shifts in consumption across already heterogeneous infrastructure increase IT complexity.	• Embrace multicloud and hybrid cloud strategies that are now widely accepted as the optimal strategy.	• Develop *multicloud solutions* that focus on access, network management, operations, and end-point complexity for a full-stack solution. management, operations, and end-point.	• Achieve flexible consumption models with improved cost governance.
OPS			
• ITOps continues to evolve beyond CloudOps.	• Implement CloudOps.	• Extend CloudOps to include AIOps, which goes beyond reactive monitoring to automated response.	• Enable predictive monitoring.

Source: Deloitte analysis.

A few key considerations for managing multicloud infrastructure, perhaps even more important now in a pandemic-ridden world, include building common data services, managing heterogeneous infrastructures, resolving endpoint complexity, and embracing new methodologies in IT operations (ITOps) including AIOps.

- **On-premise data centers face business continuity risk:** Organizations' inability to access the workplace, including on-premise infrastructure, during the pandemic has made virtualizing the data center a hot-button issue for business continuity risk. If it is done right, there is historical evidence of long-term gains for organizations. For example, a fintech giant saved millions by moving tens of thousands of workloads into the cloud to reduce its data center footprint.[13] There are two paths to building common data services: one that **consolidates the data** into a single physical or logical database or database systems and another that **manages the data in a distributed way**, leveraging virtualization to look at all the data as a single database, even though they are different distributed databases, using different database models. Whichever approach the organization chooses, the idea is to have a single path to unique customer, sales, product, and other data. This approach can allow organizations to:

    - Eliminate redundancy for increased efficiency and managed infrastructure cost
    - Understand the database in great detail, along with the metadata
    - Select the right database technology to suit their needs, understanding that generally cloud-native databases are the best choice
    - Enable the database service with API or web services access
    - Implement governance, security, and management services

Virtualized data warehousing has allowed large retailers, such as The Home Depot, to react faster to consumer needs across its supply chain. The Home Depot tracks more than 50,000 items across 2,000 locations, analyzes what items are sold when and where in real time with the internet of things (IoT), the edge and the cloud, and course corrects accordingly.[14]

- **Heterogeneous infrastructure sees shifts in consumption and increased end-point complexity:** Organizations are no longer managing systems in a single data center. They're managing the mobile network, IoT devices, and the edge. Together they amplify data complexity (as in The Home Depot example). This trend toward a heterogeneous infrastructure already was underway, but COVID-19 has shifted consumption models across that network by changing where the workforce is and how work is happening. Those who already had cloud infrastructure benefited from being able to scale down workforce infrastructure costs for their unused infrastructure or increase resources in places where they saw more demand. After all, airlines, retailers, and insurance companies' business models and workforce needs were all impacted differently by the pandemic and, therefore, their data and infrastructure demands to support the workforce will all be different. For example, due to remote working, cloud consumption at Audi Business Innovation GmbH, a unit of Volkswagen AG-owned carmaker Audi, jumped 12% between March and April, with employees using more of the rented, remote computing power and software tools. Given the organization was in the cloud already, it was able to adjust consumption models and platforms with an expectation to reduce spend by 30%.[15] COVID-19 has changed the composition of what work organizations are sending to their off-premise data centers, how they're accessing networks via nonstandardized channels, and what volume of on-premise IoT, mobile, edge, and cloud data needs to be managed across the network with shifting access points. All of this can increase complexity.

Chances are the company's infrastructure already was a collection of many different platforms, some hosted on the cloud, and some on premises, so to manage the shift in device consumption due to the pandemic (workers at home on laptops and mobile phones, off the corporate network) organizations need to understand the interfaces, security models, and governance models and go from there. Managing heterogeneous infrastructure often starts and ends with taking an overall system inventory and then creating a management plan to implement cloud operations or cloud operations (CloudOps), which combines network, security, performance, device management, and help desk tasks, can streamline operational process design to a physical operating model inclusive of tools and technologies. Organizations can look to manage end-point complexity by reducing the number of endpoints under management, minimizing the number of system types (processor, operating systems, databases), and using management, governance, and automation tools to manage the remaining complexity.

- **Embracing new methodologies in ITOps including AIOps:** Given the need to focus on CloudOps,[16] one evolving area within CloudOps is AIOps. In cloud infrastructure monitoring, there has been an evolution from reactive monitoring to predictive monitoring, and now we are moving on to a new era of AIOps.[17] The use of AIOps and other modern monitoring and management tools provides the mechanism to create layers of automation that are able to react to events and launch corrective processes (such as spotting packet errors coming from a single network device and temporarily routing around that device until it's replaced). AIOps tools as well as other operations tools are able to analyze the data coming from all systems and devices to determine when something is failing—and they can do so before humans can. If configured properly, they can detect anomalous behaviors and launch corrective processes. Prior to the pandemic, several AIOps vendors were acquired by infrastructure automation organizations as part of a growing AIOps trend which we expect to continue.[18]

Federated security for the future of work, workforce, and workplace

WHILE COVID-19'S IMPACT on work, workforce, and workplace has forced IT to manage increasingly heterogeneous infrastructures with new tools and techniques, many infrastructures themselves are facing new security challenges, given that the where, what, and how of work has changed. As IT focus shifts to accommodate the new ways work is being done across altered workplace locations, the very *context* for security monitoring with an entirely new infrastructure composition—use of home internet, personal mobile devices, etc.—has changed. This has reinforced a need to focus on federated security strategies known for their success in managing distributed, heterogeneous infrastructure security across tiers, and driving *situational awareness*. Federated cloud *frameworks* allow organizations to deploy, integrate, and manage multiple cloud computing services.[19] They can help define and implement federated security protocols across the application, network and system layers, and the cloud security center. The focus should be on proactive defense monitoring (early warning, command, and control) and managing *access point attacks* against malware, advanced persistent threats and network intrusions across infrastructure tiers, data storage, trusted platforms, websites, and operating systems. All this should be done to help enable *dynamic threat information sharing*.[20] The US Department of Homeland Security, for example, created a cyber defensive and intelligence-sharing ecosystem that incorporated various defensive technologies (aspects of its moving target defense and cloud systems security) into federations of enterprises across a network of organizations to enhance security against known and novel attacks.[21] As federated security has matured, organizations are increasingly focused on web services,[22] security-as-a-service for a cloud federation,[23] multicloud environment,[24] blockchain-enabled frameworks, and network ecosystems[25] (figure 5).

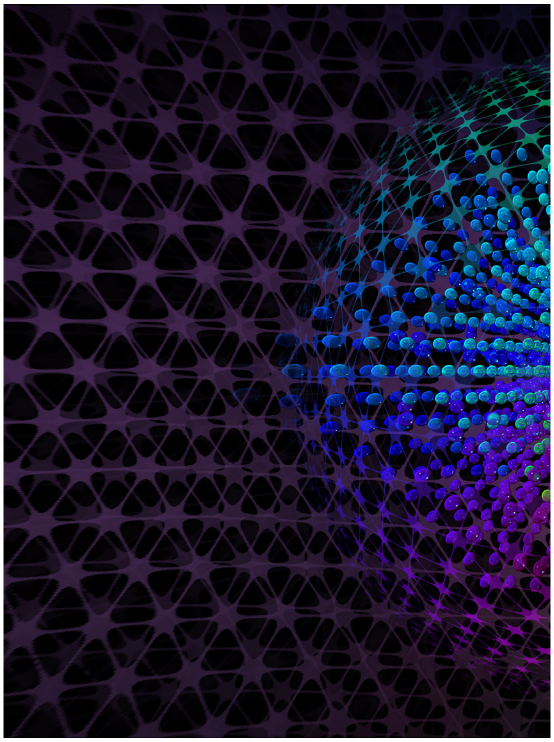


FIGURE 5

Federated security for the future of work, workforce, and workplace

NEW CHALLENGE	WHERE WE WERE	WHERE WE'RE GOING	WHY ARE WE GOING THERE
IT SECURITY			
• A heterogeneous IT infrastructure requires a heterogeneous security model.	• Implement federated security to secure infrastructure across application, network, and system layers as well as the C2 security center.	• Manage federated computing down to the end-point level across tiers/devices (cloud, edge, mobile, IoT).	• Increase situational awareness, better manage access-point attacks, and enable more dynamic threat intelligence and remediation.
ACCESS MANAGEMENT			
• Trusted access is increasingly important in a remote world.	• Implement role-based access controls, centralized security management, and identity access management.	• Use embedded zero-anonymity security features, multifactor authentication (MFA), privileged access management (PAM). Consider a trusted internet connection policy.	• Enhance governance of network access.
PERIMETER SECURITY			
• Perimeter security becomes ineffective when the office perimeter is no longer relevant.	• Perimeter security for the physically protected data center needs to consider access points for those that need remote access, where possible, and virtual alternatives that will require new security models.	• Look to replace perimeter-level security with device-level security; virtualize services and desktops, and remote IoT devices; and secure every component, including object repositories, network segmentation, and web services.	• Manage security across a shifting threat surface area.
INFORMATION SHARING			
• Security information–sharing and collaboration becomes increasingly challenging across distributed teams and multiple cloud solutions.	• Implement IM solutions across the federated network.	• Shift away from single-vendor IM solutions to integrated, federated IM solutions to fully leverage the cloud providers' technology.	• Enhance security system interoperability, collaboration, and information-sharing. Avoid vendor lock-in.

Source: Deloitte analysis.

These trends will likely continue to develop, in addition to several new ones introduced by remote working orders, triggering new work infrastructure related to trusted network access, perimeter-based security, federated instant messaging (IM), and federated computing down to the end-point level.

- **Heterogeneous security for heterogenous IT infrastructure:** As organizations look to secure a multitiered architecture encompassing the cloud, the edge, mobile, and IoT, they have to secure each architecture tier against threats specific to that tier. In fact, managing heterogeneous infrastructure requires a heterogeneous security model that is federated across the technology providers for the different tiers.[26] At the end-point level, organizations should combine infrastructure monitoring and remediation with DevSecOps, coupled with AI for predictive and automated threat management, monitoring, and resolution, all at the desktop/mobile device level. In a federated security model, organizations are able to reach every infrastructure tier, device, or process and close security gaps with network segmentation. With COVID-19, the attack surface is now larger as the work infrastructure network is more dispersed or distributed, increasing the importance of proactive dense monitoring across all devices that **extends beyond "threat detection" to "threat remediation."**

- **Trusted access in a remote world:** One industry study found that 33% of enterprise security attacks on cloud infrastructure are due to a lack of proper governance and security parameters related to role-based access control.[27] Identity access is one of the top vulnerabilities—33% of respondents to a Sophos study reported that identity access management roles were impacted by cloud security breaches and top threats (including malware, ransomware, and cryptojacking incidents).[28] Centralized security management is a timeless concept for managing security across distributed resources.[29] Identity management focused on access privileges remains a cornerstone of securing the network, particularly as the new remote-working conditions have increased the remote network attack surface area. As perimeters vanish, a zero trust approach to cybersecurity can help organizations preserve the integrity and security of their data and assets outside of the perimeter across a range of devices.[30] The approach shifts from network-based control to identity-based principles with access controls and identity management as a key focus. With zero trust, organizations take a "never trust and always verify" approach to improve their cyber posture across individuals and devices. The US Department of Defense, for example, has *embedded zero-anonymity security features* built onto its federated cloud infrastructure. This empowers administrators to monitor, track, and control all software, hardware, and user access to their respective clouds in real time.[31] In response to the pandemic, the Cybersecurity and Infrastructure Security Agency announced an interim *Trusted Internet Connection Policy* to deal specifically with telework.[32] Organizations are taking a "never trust, always verify, enforce least privilege" approach to securing privileged identities.[33] Cosmo Films, a manufacturing company, has completely transformed its infrastructure from a centralized plant/office unit to a decentralization model with access layers: "We have access layers allotted based on user needs and have given availability and accessibility of our data lake and critical information to users pan-India without any geographical or time-zone challenges," says Jagdip Kumar, the organization's chief information officer.[34]

Security now needs to factor in access points for those that need remote access, where possible, and virtual alternatives—all these will likely require new security models.

- **Perimeter security of the office:** COVID-19's impact on work location (now home) has made traditional perimeter security models obsolete. The physically protected office no longer has people working inside the perimeter. So, security now needs to factor in access points for those that need remote access, where possible, and virtual alternatives—all these will likely require new security models. Organizations should replace perimeter-level security with device-level security, virtual services, virtual desktops, and remote IoT devices, and secure every component, including object repositories and web services.[35]

- **Integrated/federated IM solutions:** An emerging trend in federated security is the shift away from single-vendor IM solutions to integrated, federated IM solutions to fully leverage the cloud providers' technology and avoid vendor lock-in. Amazon Web Services and Google Cloud Protocol (GCP) can now be integrated with Microsoft Active Directory, making security management across multicloud infrastructure easier.[36] Organizations, for example, can use GCP's federated integration to integrate with a home Active Directory solution, which enables them to streamline virtualized security communications for faster threat detection and remediation. This shift in how people are collaborating across security is being seen at a much larger scale now across all broader DevOps practices across all of the organization.

DevOps in a distributed world and altered ways of working

MANY COMPANIES SUCCEED with small cloud migrations, but when it comes to scaling the cloud, they stumble over organizational and process bottlenecks.[37] This is where DevOps can streamline processes. DevOps encourages great communication and collaboration (in other words, teamwork) to foster better-quality software more quickly with more reliability. DevOps is a culture shift. Another study found that DevOps plus cloud is a multiplier that improves performance by as much as 81%.[38] It's no surprise then that an industry analyst firm showed double-digit DevOps tools growth in 2019, with worldwide revenue reaching US$8.5 billion.[39]

The easiest part of DevOps is the technology—automated scripts, continuous integration and delivery, and automated provisioning. Where organizations tend to struggle is transforming existing processes and structures to support automation and drive a culture change across a range of operations. These can be done via change management, deployment, user acceptance testing, security, compliance, and ongoing product strategy.

What's changed with COVID-19 is that when people and teams are working remotely across nonstandardized infrastructure, processes should change. This is a unique opportunity to build greenfield processes and infrastructure given that pressing organizational needs are outweighing some of the usual barriers. In the postpandemic world, when organizations recover, decisions made now should enable companies to rationalize, standardize, and create more repeatable processes. DevOps strategies should evolve to bring in new, flexible communication and collaboration techniques that factor increasingly fragmented, remote, and heterogeneous work environments (figure 6).

FIGURE 6

DevOps strategies can enable new ways of working

NEW CHALLENGE →	WHERE WE WERE →	WHERE WE'RE GOING →	BENEFITS
OPERATIONS			
• Rapidly shifting business strategies require fast reaction time and resilient solutions.	• Follow a shift-and-adopt strategy for incremental cloud replatforming.	• Double down on agile to align business and technology operations and maintain flexibility needed during times of uncertainty.	• Enable teams to react and respond instantaneously to focus on tactical work that provides immediate value.
COLLABORATION			
• Remote work requires more collaborative ways of working.	• Embrace communication and collaboration tools for virtual, distributed teams.	• Use ChatOps across project teams, departments, and organizations.	• Enable real-time knowledge-sharing, facilitate knowledge management, and generate collective intelligence.
AUTOMATION			
• Flexible, dynamic infrastructure requires minimizing manual human intervention.	• Adopt DevOps tools for automated provisioning.	• Move toward hyper-automation by incorporating cloud AI and ML services.	• Create automated and repeatable processes.
TEAMS			
• Traditional supply chains have been irrevocably disrupted.	• Implement a cloud center of excellence team.	• Reimagine traditional roles and embrace an IT-as-a-service operating model with the architect elevated in the business.	• Achieve shared goals and objectives as well as greater alignment across full-stack product teams.
PROCESSES			
• DevOps continues to shift left toward end-to-end DevOps.	• Shift left to incorporate DevSecOps into your DevOps strategy.	• Continue to shift left to operations, governance, and customer support.	• Standardized and consistent build and development environment; enhanced governance and customer experience.

Source: Deloitte analysis.

We expect an increased focus on agile release cycles, virtual collaboration tools, hyperautomation, and continuous improvement across the entire product life cycle as organizations continue to shift left toward end-to-end DevOps.

- **Doubling down on agile for increased responsiveness:** A shift-and-adopt strategy is the standard for incremental cloud replatforming to cost-effectively enable elastic workflows that scale as needed, saving up-front cost and allowing the cloud environment to grow with need.[40] As organizations accelerate their cloud programs—as is the case now—a lift-and-shift approach can work to consolidate data centers or avoid the cost of an infrastructure refresh. Cloud modernization programs can embrace DevOps to align IT development and business operations and to achieve greater delivery agility while maintaining flexibility during times of uncertainty.

  Continuous build and continuous deployment automation tools are the key features of DevOps currently, supported by test automation tools.[41] They are the baseline organizations should consider for an agile cloud migration that delivers speed to market and flexibility during uncertain times, such as now. During such times, organizations should be able to **react and respond instantaneously**. With COVID-19, there is less appetite for large strategic innovation initiatives and more focus on tactical work that provides **immediate value** and solves today's pain points, now.

> **With COVID-19, there is less appetite for large strategic innovation initiatives and more focus on tactical work that provides immediate value and solves today's pain points, now.**

- **The rise of ChatOps:** A remote working environment has fed the adoption of **project team-focused, cross-departmental, and cross-organizational** communication and cooperation tools. Project teams are using Slack, Microsoft Teams, and other internal communication platforms focused on team collaboration for interactive and instantaneous conversations. These support work across virtual teams, a trend accelerated by COVID-19. For example, Microsoft Teams clocked 4.1 billion meeting minutes per day in April compared to 900 million in mid-March.[42] Its daily active user base more than doubled to 75 million from 32 million.[43] Similarly, during the first quarter of FY20, Slack added 90,000 net new organizations, of which 12,000 were paid customers (28% increase year over year).[44]

  Especially when working remotely, collaboration tools are of immense value at the project level because teams can communicate in real time, develop a centralized knowledge base, and create a consolidated, instant access network that's accessible anywhere and anytime. If the full-collaboration potential can be unlocked, teams can free up meeting time and move toward more efficient collaboration methods. Project teams can set up channels (define) to reach beyond the group to experts outside of the team to gain warm responses and crowdsource intelligence and push thematic updates into filtered channels and access them on demand. To enable collaboration across technology and business, social business collaboration tools,[45] are gaining attention as they allow for real-time engagement with business stakeholders throughout the development process. These tools are especially important as business and technology strategies shift rapidly in response to COVID-19. Last but not least, cross-organization collaboration tools can support remote data center management by connecting stakeholders across organizations for more seamless communication between IT teams and their vendors, and partners and clients.

- **Hyperautomation: Automated provisioning** is a key DevOps capability that delivers computing capacity on demand without manual intervention, providing the foundation for flexible infrastructure and dynamic resource allocation. This can help get rid of the "toil"[46] (any work that is directly tied to running a service that is manual, repetitive, and automatable, and where there's no enduring value), which is a major roadblock to success. IT automation is core to any DevOps strategy, given the goal is to create automated and repeatable processes. But in a post-COVID-19 world, automation will likely be more important than ever because of the need for continuous learning and improvement. COVID-19 is pushing the need to streamline processes and make them less human dependent, urging organizations to explore next-level value from **cloud AI and machine learning services**. Additionally, for new initiatives, think about cloud-native applications for new infrastructure, which further automates and streamlines IT and development operations with automated provisioning and zero-downtime deployment, and microservices architectures that manage risk and volatility more easily.[47]

- **Reimagining traditional roles:** Cloud has also forced many organizations to reimagine tried-and-true roles, moving away from silo-based domain teams building servers and networks as a single focus and driving toward the creation of a full-stack cloud "platform" team delivering cloud services that developers can use to deliver to their customers in a secure and compliant manner. There is a fundamental mindset shift from an IT command-and-control center model to **a customer-centric IT-as-a-service model** where IT is supporting a **customer-centric, product-focused operating model**. This marks a shift from centralized operations support to embedded operations capabilities. These capabilities shift the product team to a very different full-stack team model with shared goals and objectives around a product for greater alignment. Antony Edwards, chief operating officer, Eggplant Software, speaks to this DevOps evolution, stating, "The combination of customer-centric development, microservices, and automated DevOps pipelines pushes the role of developer further away from a coding focus and more toward product design. This evolution mirrors how CAD tools moved architecture from materials engineering to design."[48] In a Flexera study, 73% of enterprises report having a central cloud team or cloud center of excellence[49] versed in cloud, microservices, and API technologies.

  In addition to the creation of platform teams, the architect is being elevated within the organization to solve multidimensional business challenges given the prevalence of interconnected technologies and devices.[50] With COVID-19, manufacturing/consumer packaged goods, health care, education, travel and hospitality as well as state and local governments are seeing the destruction of traditional supply chains. This can provide a unique opportunity for architects to work with the business to build new solutions that enable organizational agility for next-generation supply chains.

- **End-to-end DevOps on the horizon:** Organizations continue to push forward with a "shift left" DevOps strategy, shifting beyond infrastructure and successfully using DevOps to achieve consistent build and automated testing, despite different environments. Organizations that are further in their journey have embraced DevSecOps for integrated security across development operations—integrating security into the development design process. “Essentially, security becomes a design constraint. The shift-left paradigm … requires security to be built into software instead of being bolted on,” says Shannon Lietz, leader and director of DevSecOps, Intuit. “Shifting left requires everyone knows how to collaborate and understand enough of the context to ensure the safety of software,” she continues.[51] Telstra, an Australian telecom company, cited a 20–30% improvement in secure coding skills among its developers.[52] Alana Brown, senior director, Puppet, and the creator of the annual *State of DevOps* report, states, “I think there’s a big misconception that DevSecOps is just about shifting some security tests to the left. That’s not it. This is about fundamentally changing how all of these teams work together and how they collaborate … collaboration really is key, and it really does lead to better outcomes.”[53]

Organizations that are further in their journey have embraced DevSecOps for integrated security across development operations—integrating security into the development design process.

The next frontier is how to move operations, governance, and customer support to the left. Companies, such as Concourse Labs that recently received US$15 million in series A funding and offers automated cloud compliance, are emerging to address these areas. The platform uses a system of record (including enterprise policy, identity, and cloud usage histories) to generate baselines and predictions and enable automatic detection of anomalous behavior as well as test application releases with proposed remediation guidelines.[54]

Conclusion: The next frontier is upon us

COVID-19 HAS AFFECTED work, workforce, and workplace in dramatic ways and forced organizations to think about their future infrastructure needs and accelerate their movement to the cloud that can better handle constantly shifting business and workforce needs. Multicloud solutions and hybrid cloud technology strategies are the norm for those already in the cloud and will likely continue to see increased adoption as they enable business flexibility.

> The next frontier of managing cloud complexity will likely be developing multicloud solutions that use the right combination of tools, software, and technology to manage cloud services and enable business applications—everything from orchestrating data from virtual data centers to implementing AIOps.

The next frontier of managing cloud complexity will likely be developing *multicloud solutions* that use the right combination of tools, software, and technology to manage cloud services and enable business applications—everything from orchestrating data from virtual data centers to implementing AIOps. These heterogeneous IT infrastructures are seeing shifts in consumption that make cloud—given its flexibility—a favorable solution. At the same time, it creates new access points and a large surface area for cyberattacks. Changes to location have made the perimeter-in-perimeter security obsolete, necessitating a shift to federated security models that can better manage security across infrastructure tiers and devices.

Finally, ways of working have been altered in profound ways, prompting organizations to double down on DevOps best practices that increase collaboration and introduce new approaches for a distributed world. Organizations can look to double down on agile development, embrace ChatOps for virtual collaboration, automate DevOps processes that continue to shift left, and step into new roles to support an IT-as-a-service operating model. This combination of multicloud solutions, federated security, and distributed DevOps can help create a future of cloud-enabled work infrastructure needed to make virtual business infrastructure work.

Endnotes

1. LogicMonitor, “Cloud 2025: The future of workloads in a cloud-first, post-COVID-19 world,” June 22, 2020.
2. Angus Loten, “Cloud spending hits record amid economic fallout from Covid-19,” *Wall Street Journal*, August 3, 2020.
3. Jared Spataro, “2 years of digital transformation in 2 months,” Microsoft, April 30, 2020.
4. Joao-Pierre S. Ruth, “Next steps for cloud infrastructure beyond the pandemic,” InformationWeek, April 29, 2020.
5. John Hagel III, Sheryl Jacobson, and John Seely Brown, *New architectures of resilience: Are you heading for a restart or a new start?*, Deloitte Insights, June 3, 2020.
6. Suchitra Nair, “Cloud outsourcing in financial services and COVID-19,” Deloitte, May 6, 2020.
7. Katherine Noyes, “COVID-19: How CIOs can lead the way,” *Deloitte CIO Journal* on the *Wall Street Journal*, April 1, 2020.
8. Deloitte, “Cloud Complexity Management survey results,” accessed July 30, 2020.
   This is of particular importance to resolve, given almost half of C-suite executives cited cloud complexity (47%) as the factor that will have the most negative impact on cloud computing’s ROI over the next five years.
9. Nutanix, *Enterprise Cloud Index 2019 Edition: Application requirements to drive hybrid cloud growth*, accessed July 30, 2020.
10. David Linthicum, “Multicloud is not really about clouds anymore,” InfoWorld, July 24, 2020.
11. Flexera, *Flexera 2020 state of the cloud report*, 2020.
12. Eric Knorr, “The 2020 IDG Cloud Computing Survey,” InfoWorld, June 8, 2020.
13. Deloitte, “Cloud computing case studies,” accessed July 30, 2020.
14. Antonio Gulli, “Supply chain resiliency begins in the cloud,” *Forbes*, July 28, 2020.
15. Aaron Tilley, “Another Covid-19 problem for companies: All this working from home isn’t cheap,” *Wall Street Journal*, July 27, 2020.
16. David Linthicum, “CloudOps is different than traditional ITOps,” Deloitte on Cloud Blog, August 28, 2018.
17. Johnny Baltisberger, “Voices in innovation—David Linthicum speaks about AIOps,” Gigaom, June 16, 2020.
18. Paul Bevan, “Another AIOps vendor gets snapped up—Following on from Virtual Instruments deal to buy Metricly, Resolve have now acquired Fixstream,” Bloor, August 23, 2019.
19. Patricia Brown, “Federated cloud strategies: What CIOs need to know,” *CIO*, November 11, 2011.
20. Weiliang Luo et al., “Federated cloud security architecture for secure and agile clouds,” *High Performance Cloud Auditing and Applications* (Springer, 2013), pp. 169–88.
21. Department of Homeland Security, “Federated security,” accessed July 30, 2020.
22. Microsoft, “Federation,” accessed July 30, 2020.
23. Áine MacDermott et al., “Security as a service for a cloud federation,” presented at the 15th Post Graduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting at Liverpool, June 2014.

24. Pramod S. Pawar et al., “Security-as-a-service in multicloud and federated cloud environments,” *IFIP Advances in Information and Communication Technology* (Springer, 2015), pp. 251–61.

25. Olumide Malomo, Danda Rawat, and Moses Garuba, “Security through block vault in a blockchain enabled federated cloud framework,” *Applied Network Science* 5, (2020).

26. Yuri Demchenko et al., “Federated access control in heterogeneous intercloud Environment: Basic models and architecture patterns,” paper presented at IEEE Third International Workshop on Cloud Computing Interclouds, Multiclouds, Federations, and Interoperability at the Proc IEEE International Conference on Cloud Engineering, March 11, 2014.

27. Bill Doerrfeld, “3 key issues with hybrid cloud transformation,” DevOps.com, July 28, 2020.

28. Sophos, *The state of cloud security 2020*, July 2020.

29. David Linthicum, “3 post-pandemic cloud architecture trends,” InfoWorld, May 1, 2020.

30. Deloitte, “Zero trust cybersecurity: Never trust, always verify,” July 30, 2020.

31. BAE Systems, “Federated secure cloud,” accessed July 30, 2020.

32. Libby Bacon, Sean Morris, and Nicole Overley, *COVID-19 and the virtualization of government: Responding, recovering, and preparing to thrive in the future of work*, Deloitte Insights, April 28, 2020.

33. Louis Columbus, “Protecting privileged identities in a post-COVID-19 world,” *Forbes*, May 10, 2020.

34. Nikhar Aggarwal, “Charting out your multi-cloud strategy,” *The Economic Times CIO*, March 18, 2020.

35. Marek Hatala, Ty Mey Eap, and A. Shah, “Federated security: Lightweight security infrastructure for object repositories and web services,” paper presented at the Next Generation Web Services Practices international conference, September 2005.

36. Yegor Tokmakov and Sebastian Doell, “How to use G Suite as an external identity provider for AWS SSO,” AWS Security Blog, July 6, 2020.

37. Mike Kavis, “Architecting the cloud: Doing cloud correctly requires a cloud enabled workforce,” Deloitte, June 2019.

38. Freeform Dynamics and CA Technologies, *DevOps and cloud computing*, October 2017.

39. Jim Mercer and Mary Johnston Turner, “Worldwide DevOps software tools forecast, 2020–2024,” International Data Corporation, July 2020.

40. Narendar Nallamala, “The best cloud migration approach: Lift-and-shift, replatform, or refactor?,” *DZone*, January 30, 2019.

41. David Norfolk and Daniel Howard, “DevOps,” Bloor Research, July 10, 2020.

42. Jennifer Langston, “Growing Azure’s capacity to help customers, Microsoft during the COVID-19 pandemic,” Microsoft, June 16, 2020.

43. Tom Warren, “Microsoft Teams jumps 70 percent to 75 million daily active users,” The Verge, April 29, 2020.

44. Isabelle Kirkwood, “Slack reports record customer growth as global workforces go remote,” Betakit, June 5, 2020.

45. Norfolk and Howard, “DevOps.”

46. Google, “Table of contents,” accessed July 30, 2020.

47. Shanker V. Selvadurai, “Cloud native thrives in the COVID-19 era,” *Economic Times*, June 5, 2020.

48. Ericka Chickowski, “The top 5 DevOps trends: What being mainstream means to your team,” TechBeacon, accessed August 27, 2020.

49. Flexera, *Flexera 2020 state of the cloud report*.

50. Deloitte, “Tech Trends 2020,” 2020.

51. Jason Bloomberg, “Can DevOps really shift everything ‘to the left’?,” *Forbes*, June 8, 2018.

52. Chickowski, “The top 5 DevOps trends.”

53. Architecting the Cloud podcast series, “Struggling with DevOps? Remove silos and embrace change,” Deloitte, accessed August 27, 2020.

54. PR Newswire, “Concourse Labs raises $15.2 million in series A funding led by ForgePoint Capital to accelerate enterprise digital transformation by automating cloud governance,” June 9, 2020.

Acknowledgments

The authors would like to thank **Jay Parekh** for his research and analysis contributions to this article as well as **Adrienne Smathers** for the support.

About the authors

David Linthicum | dlinthicum@deloitte.com

As the chief cloud strategy officer for Deloitte Consulting LLP, David Linthicum is responsible for building innovative technologies that help clients operate more efficiently while delivering strategies that enable them to disrupt their markets. He is widely respected as a visionary in cloud computing and was recently named the No. 1 cloud influencer in a report by Apollo Research. He is the author of more than 13 books and 5,000 articles.

Mike Kavis | mkavis@deloitte.com

Mike Kavis is the chief cloud architect in Deloitte Consulting LLP's Cloud practice, responsible for helping clients implement cloud strategy and architecture to drive digital transformation. Beyond his technology experience, Kavis brings an insightful understanding of how to address the organizational change, process improvement, and talent management challenges associated with digital transformation. He brings more than 30 years of experience in software development and architecture to his role.

Myke Miller | mykemiller@deloitte.com

Myke Miller is the dean of Deloitte Consulting LLC's Cloud Institute, where he draws on more than 20 years of experience to deliver curated and collaborative learning experiences focused on key cloud roles. As managing director for Deloitte's Cloud Engineering Group, he helps clients transform legacy infrastructure into innovative and secure platforms for business growth. He specializes in the energy and resources industry and the power and utilities sector.

Diana Kearns-Manolatos | dkearnsmanolatos@deloitte.com

Diana Kearns-Manolatos is a senior manager in Deloitte's Center for Integrated Research where she analyzes market shifts and emerging trends across industries. Her research focuses on cloud and the future of workforce. Additionally, Manolatos draws on almost 15 years of award-winning marketing communications expertise to align insights with business strategy. She speaks on technology and women in leadership and holds bachelor's and master's degrees from Fordham University.

Contact us

Our insights can help you take advantage of change. If you're looking for fresh ideas to address your challenges, we should talk.

Industry leadership

David Linthicum
Managing director | Chief cloud strategy officer | Deloitte Consulting LLP
+1 703 216 6676 | linthicum@deloitte.com

Mike Kavis
Managing director | Chief cloud architect | Deloitte Consulting LLP
+1 813 619 4606 | mkavis@deloitte.com

Myke Miller
Managing director | Cloud Engineering | Dean of Deloitte's Cloud Institute
+1 612 599 4267 | mykemiller@deloitte.com

Deloitte Center for Integrated Research

Diana M. Kearns-Manolatos
Senior manager and subject matter specialist | Deloitte Services LP
+1 212 436 3301 | dkearnsmanolatos@deloitte.com

Deloitte.
Insights

Sign up for Deloitte Insights updates at www.deloitte.com/insights.

Follow @DeloitteInsight

Deloitte Insights contributors
Editorial: Kavita Saini, Aparna Prusty, Rupesh Bhat, and Nairita Gangopadhyay
Creative: Stela Murat and Sanaa Saifi
Promotion: Alexandra Kawecki
Cover artwork: Jean-Francois Podevin

About Deloitte Insights

Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte Insights is an imprint of Deloitte Development LLC.

About this publication

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.