



PLURALSIGHT

# A leader's complete guide

to cloud migration



Updating legacy processes and systems has become a more immediate challenge than ever before, a necessity for laying the groundwork for future innovation. Companies are investing more heavily in areas that will allow them to take full advantage of new technologies and processes in 2021 and beyond. And cloud migration is one of the top priorities for CIOs.

While more than half of all organizations have accelerated their migration to the cloud since the early days of the COVID-19 crisis, many are finding that it isn't all they dreamed it would be. A recent McKinsey study reports that **80%** of CIOs have not reached the level of agility and business benefits they were aiming for. Additionally, many organizations that transitioned the majority of workloads to the cloud are still within the same range of agility as their counterparts that are transitioning slower.

To remain competitive, tech leaders need to continue to mature their company's cloud strategies, ensuring that they have the right organizational design, skill development and processes in place to realize value. This is your complete guide to doing just that.

## What we'll cover

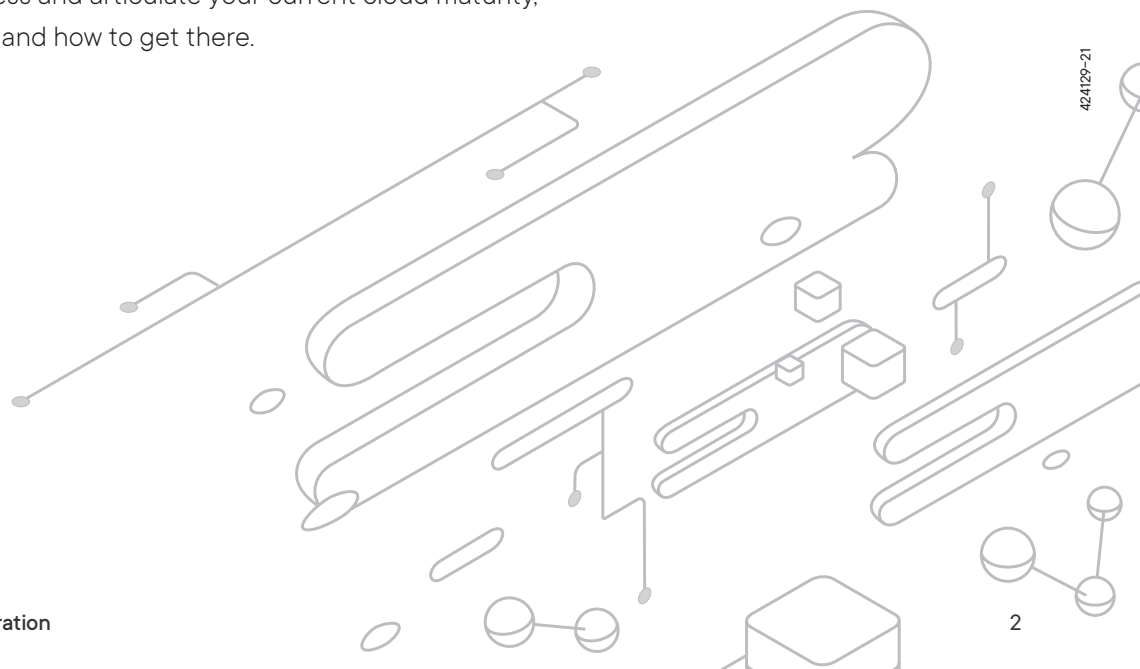
**Section 1:** Assessing your cloud maturity

**Section 2:** Cloud migration: Everything from nuts & bolts to earning buy-in

**Section 3:** Philosophies for a multi-cloud strategy

**Section 4:** Cloud security: Focus on what matters most

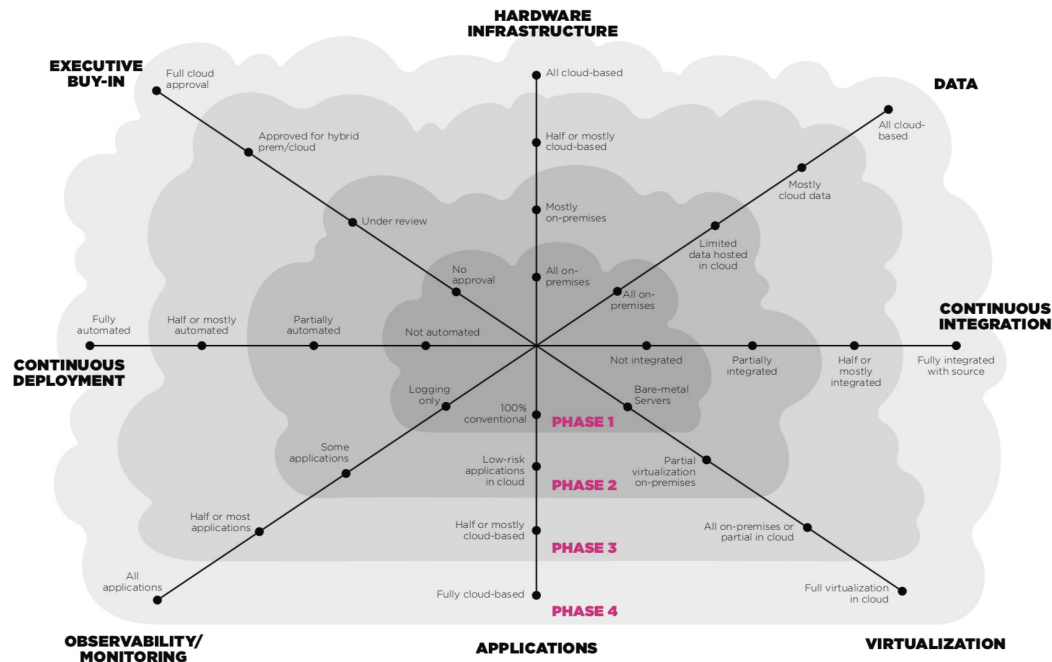
Use this opportunity to assess and articulate your current cloud maturity, your ultimate cloud targets and how to get there.



## SECTION 1:

# Assessing your cloud maturity

We've compiled a shortlist of critical factors to help you assess your organization's current cloud maturity—as well as where you want to go. Though all of the factors operate on a scale, you don't need to go to the end of the scale for each item to consider your cloud “mature.” Every organization is different. Successful cloud-native organizations land at different parts of each vector.



To map where your cloud maturity is—and where it needs to be—ask yourself these questions:

- ☐ **Executive buy-in:** Is management reviewing (or interested in reviewing) proposals for cloud offerings? What level of commitment have they already given for migrating to the cloud?
- ☐ **Hardware infrastructure:** Does it live on-site in a data center, entirely in the cloud or is it a hybrid approach?
- ☐ **Data:** Is your data on-premises with servers, all in the cloud or a mix?
- ☐ **Continuous deployment:** Are new software launches deployed automatically, manually or somewhere in between?
- ☐ **Continuous integration:** Is new code introduced manually, through automation or a mix?
- ☐ **Observability and monitoring:** How and where is your organization's logging system behavior, including aggregation, storage and quality control?
- ☐ **Applications:** Are they hosted on a traditional web server, hosted in a cloud service or both?
- ☐ **Virtualization:** Are you using conventional bare-metal machines, all virtual or both?

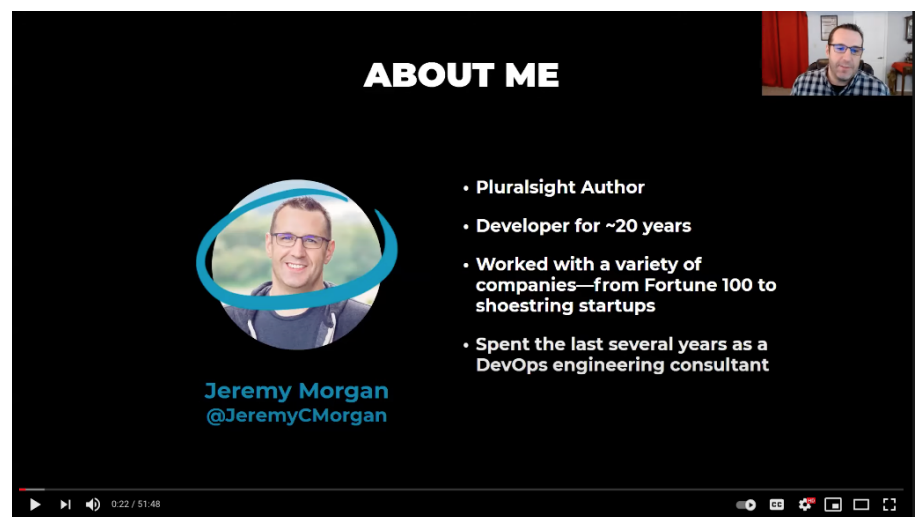
It's also helpful to assess the standards at the industry level. What are others in your industry doing? Do any regulatory considerations impact how your data is stored? How large is your organization, and how fast are you growing compared to the industry? Answering questions like these can help you narrow your focus and start building a plan.

Remember: without a concrete plan, cloud transformations can be very problematic. Taking things one step at a time and methodically working through the process will reduce risk and pain points.

## See the cloud maturity matrix in action

### WATCH IT »

Want a guided experience when evaluating your cloud maturity? Pluralsight author Jeremy Morgan walks you through the process of assessing your cloud maturity, including how to identify which phase of cloud maturity your org resides in, how to break down the cloud migration process and how to reach your organization's cloud goals.



## SECTION 2:

# Cloud migration: Everything from nuts and bolts to earning buy-in

## CLOUD MIGRATION IN ACTION

You've chosen to adopt the cloud. Now comes the hard part—actually using it. You don't have the luxury of starting fresh, though. You've got decades of software and processes already in place, but you're not alone. Most anyone adopting public cloud is coming to grips with how to get their existing investments into the cloud. To be successful in this, you need to know what you need to move, how to move it and why.

### WHY YOU'RE MIGRATING

We don't need to sell you the reasons why cloud can streamline and bolster your company. You likely already know them, and you're bought in. But you'll need to communicate them to earn buy-in from executives and other stakeholders in your organization. Remember: your non-technical stakeholders don't need to get in the weeds. Your technical stakeholders know how it works (and how it could possibly delay value-added work).

Rather than diving into the technical details, focus on the value cloud migration will bring to the organization. Get a clear understanding of the real “why” behind the migration—the outcomes that the cloud enables for your organization. Articulating these reasons improves understanding and buy-in from the rest of the organization, including the technical stakeholders.

### Pro tip

Here's your litmus test: The biggest reasons for migrating to the cloud shouldn't even use the word “cloud” in them. The “why” is that your organization can ship value more often.

Customers receive results more effectively, and in return, the company becomes more resilient. You are improving cost transparency, enabling more effective data-driven decisions. The organization will access innovations and create new, engaging ways to acquire and retain customers.

Cloud migration success—particular to your organization—needs measurements in understandable terms rather than tech-centric ones. No one outside of tech cares how much of the workload is in the cloud or migrated. Non-tech people want to know the “so what”—what has changed for them, and how is it better?

Framing success in an easy-to-understand language requires conscious effort; it is relatively simple because cloud migration is a tech initiative that genuinely is about business value.




## WHAT YOU'RE MIGRATING

Now, non-technical stakeholders may not need to understand the minutiae of cloud migration, but you and your teams certainly do. It's easy enough to assume (mistakenly) that migrating your virtual machines to the cloud is all you need to do—the organization-wide equivalent of shifting all your hard drive files to Dropbox. There are many more facets to consider to make the migration both functional and complete.

The specifics of your migration will depend on your organization's particular collection of programs, data and goals. Still, these are some broader buckets to consider before jumping feet-first into the migration.

- **TECHNOLOGIES.** You can either look at your technologies from the top down or the bottom up. Top-down, you're taking a broader view of the systems and applications you're migrating. Of course, these things consist of many dozens of individual components. A bottom-up inventory enables you to see all the pieces you'll be migrating to the cloud. Compute components are relatively portable, and many clouds offer some VM or container migration tools.
- **STORAGE.** You'll be migrating file shares, archival storage and other storage systems, along with all the retention policies. These are often trickier to migrate than technologies, simply given the sheer volume of information. Beyond quantity, though, you need to consider the storage you need (e.g., object storage, file storage or block storage), what kind of performance you need—and what makes financial sense for your organization.





- **DATABASES AND DATA WAREHOUSES.** Migration of these two includes your analytics and reporting infrastructure—and all this stuff is not easy to migrate. Different systems depend on those databases, so moving the databases requires moving the systems. Many public clouds recognize these difficulties and offer some form of database migration tooling, including ways to physically ship your data to the cloud.

- **LINE OF BUSINESS SYSTEMS.** Often, you can migrate these systems in one fell swoop, but you also have to do so without incurring downtime or data loss. You also have to be sure to remember to migrate the middleware too, which is often easy to overlook.

- **NETWORKING ASSETS AND CONFIGURATIONS.** When migrating your firewalls, VPNs and load balancers, you do not want to duplicate your on-premises setup; this is your chance to simplify matters with a more cloud-native approach to network and security.

- **IDENTITY MANAGEMENT SYSTEMS AND OTHER SECURITY SERVICES.** The way your organization handles identity and security on-premises can evolve to operate in new ways in the cloud. This is another chance to modernize while you migrate.

- **MANAGEMENT SERVICES.** Some on-premises vendors extend their tools to help you manage in the cloud and ease the transition. You can take advantage of that or you can take this chance to refresh your management tools and systems to a more cloud-native approach. These include but are not limited to:

1. Configuration management
2. Provisioning tools
3. Log collection
4. Patching systems
5. Ticketing systems

- **COMPONENTS FOR DEVELOPERS.** These are your source control systems, your artifact repositories, your sandboxes. Migrating many of these components is straightforward enough, though you are likely to be handling a ton of data.

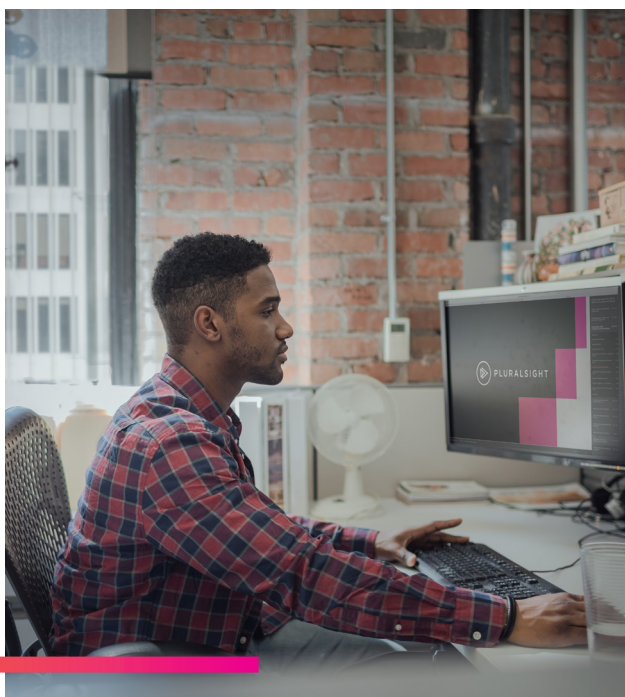




It's also easy to only think about the technology that you're migrating to the cloud. But, don't forget. Your processes have to migrate as well. Sure, some principles work across the board, but to apply the same processes to both on-premises and cloud setups is a recipe for failure.

### Here are some processes you'll need to refresh as part of your cloud migration.

- **CHANGE REQUEST PROCESSES.** By adapting to the cloud, you're embracing a style of more continuous delivery. How you initiate, approve and roll out changes will not remain the same. A well-designed automation pipeline can help protect you from bad code reaching production and maintain a constant shipping value.
- **INCIDENT RESPONSE.** What happens once you're in a distributed cloud environment and you don't own and can't access anything below the service? You will likely have different people responding to alerts, which means providing production access to a whole new set of people. The tools you use to triage problems, notify customers and restore service may well need to change, too.
- **CONFIGURATION MANAGEMENT.** How will you set up, audit and manage this growing pool of cloud assets? It's too much for people to configure manually. Plus, in the cloud, services are more transient. Automation is key to managing your technologies and processes.



Speaking of fundamental alterations: A cloud migration means you will transition from an arms-length relationship between IT and the company to a more collaborative partnership. The cloud generally changes the old transactional relationship between tech and non-technical stakeholders because effective cloud computing removes the technical limitations to delivery and enables accurate and complete cost transparency. The entire organization has fewer technical hurdles in its way, so it spends more time on problem identification, experimentation and analyzing feedback to iterate the next improvement.





## How you're migrating

Once you have buy-in and a game plan for what you'll be migrating, you're ready to start migrating. Here are eight considerations to help you through the process:

❑ **GET OUTSIDE HELP.** We get it. Technical people, whether in IT or engineering, are creative problem solvers. Once you decide to migrate to the cloud, the process can become an enticing challenge. It's also a beast of an undertaking. So we recommend, first and foremost, that you get help from outside experts who have succeeded in guiding companies through the transition. You likely have an incredibly talented team in-house, but their skills are better focused on their areas of expertise. Of course, they are taking part in the migration, but they don't need to learn everything from the ground up. You want partnership and knowledge transfer from people who have done this rodeo before.

❑ **BUILD OUT THE SHARED INFRASTRUCTURE.** Using the public cloud correctly permits self-service provisioning and enables teams to move more quickly to deliver value—which is great. But there's a hitchhiking risk that people may veer from the standards that control cost, protect data and improve manageability. Before setting a team loose in the cloud, it's helpful to lay a foundation for them to use.

### Pro tip

- Consider account structure.
- Will each team get an account, provisioned and managed by a central IT team?
- Will all team members use one account and share a standard configuration, or will everyone get an account that they can configure as they see fit?


Other shared infrastructure components to resolve up front include identity management (i.e., setting up a single source directory that each team can use to authenticate and authorize themselves and their customers) and creating a persistent connection between your corporate network and the public cloud.

❑ **LEVERAGE APPROPRIATE TECHNIQUES.** There are many techniques you may use to migrate your workload, and you'll use several or all of these approaches during the migration.

**Lift-and-shift** means that you migrate something to the cloud as-is. You pick up a virtual machine and run it in the cloud without any changes. You might use lift-and-shift on workloads nearing the end of their lives, from which you just need some incremental benefits from running in the cloud. Alternatively, this method comes into play when you're doing a complete data center exit and want to get your assets to the cloud as fast as you can.

**Lift-and-optimize** is a step further than lift-and-shift. The application itself does not change, but you might swap out a proprietary server for an open-source one or containerize the workload to run on a denser and cheaper host in the cloud. Lift-and-optimize often brings more benefit than lift-and-shift incrementally, but still without paying down any tech debt for the workload.

**Move-and-improve** involves changing the workload. Essentially, you start with a lift-and-shift or lift-and-optimize, but with the intent to invest in changes to the application once there to make it more cloud-native.



**Improve-and-move** can get you to the same place as move-and-improve, but you'll make the changes to the application before you migrate. If feasible, this technique is preferable because the changes are in place from the start, rather than getting bumped down the line.

**Rebuild-and-replace** is probably the one you'll use least often, yet it's the one likely to yield the most significant benefits. By rebuilding an app for the cloud, you can take advantage of elastic scale and cloud-managed services and make your workload easier to change. Consider applying this approach to the critical systems that need to evolve for your business to succeed.

**Retire-and-replace** the apps and systems that are particularly outdated or ill-suited for the cloud. It can be challenging to let go of a bespoke system, but look into whether a SaaS product is designed for the cloud that will suit your needs almost as well—or even better—without the complications of migrating the old stuff. In other words, use the migration effort to do a bit of housekeeping on your app portfolio.

There are benefits and risks to each approach, and you and your team will have to develop your decision matrix to determine which one to use for a given workload.

□ **DECIDE WHICH CLOUD SERVICES TO USE.** This is an extension of the previous section. It boils down to this: What software investments are you going to preserve, and which ones will you swap out for cloud-native?

These decisions have cost, maintenance and delivery implications, and they ask you to consider busting out of the way-things-always-have-been mentality. You may not still need a dedicated app server on a virtual machine if the native app service offered in the cloud works well. You can still self-manage your software if portability is a top priority, but otherwise, it may behoove you to embrace managed services. These are examples of undifferentiated areas where you can offload your effort to the cloud and witness a significant reduction in the total cost of ownership.

One further consideration here: Your tech team will be transitioning from a relatively constrained on-premises option set to a dizzying array of cloud options.

### Pro tip

You may want to intentionally limit some of these cloud choices for your team up-front. Decide what offerings you want to use for your portfolio—narrow down the possibilities to allow input from your team. They will see considerations you don't, but it's primarily up to you to choose the right managed services for your team.

❑ **REALIZE VALUE BY MIGRATING VERTICALLY.** Your team's priority may well be the migrant infrastructure layers, compute, storage, networking apps moving up the stack. That's because teams own those layers. But to ensure you realize value, migrate applications and systems, not layers—vertically, not horizontally. Migrating a single horizontal layer brings your organization no value; if the budget runs out, you have nothing usable. But if you migrate an entire app, which cuts through those layers, you've realized some value post-migration.

❑ **EVOLVE YOUR PROCESSES AT THE SAME TIME.** We introduced the concept earlier of migrating your processes along with your tech. It's worth reiterating here. If you apply current on-premises processes to the cloud, your adoption will probably fail (or at least fall short of its potential). Migrating to the cloud requires rethinking how you budget, provision and approve changes. Preserve the spirit of what your core processes intend, but reimagine them for the cloud.

❑ **DOUBLE YOUR INVESTMENT IN AUTOMATION.** To trust all these new processes for the cloud, you'll want repeatability and audit-ability. That means automation

everywhere. Scaling environments based on spikes and usage? Automation. Scanning all your deployed cloud services to look for non-compliance? Automation. Deploying code to production? You get the idea.

### Pro-tip

Done right, automation in the cloud provides a much more secure environment than you'd otherwise achieve. It's the most effective way to scale your teams, and as a plus, you'll end up with a better audit trail.

❑ **INVEST IN UPSKILLING.** Skill development is necessary for adopting a new paradigm that will impact your whole organization. Up front, you'll have training for developers, architects, operators, project managers, product managers, business analysts and systems owners. You cannot assume that self-paced learning is enough. Dedicate work hours to developing new skills. And do so on an ongoing basis—the cloud is the fastest-changing IT investment you'll ever make, so your team members will need to improve and update their skills and knowledge continuously.

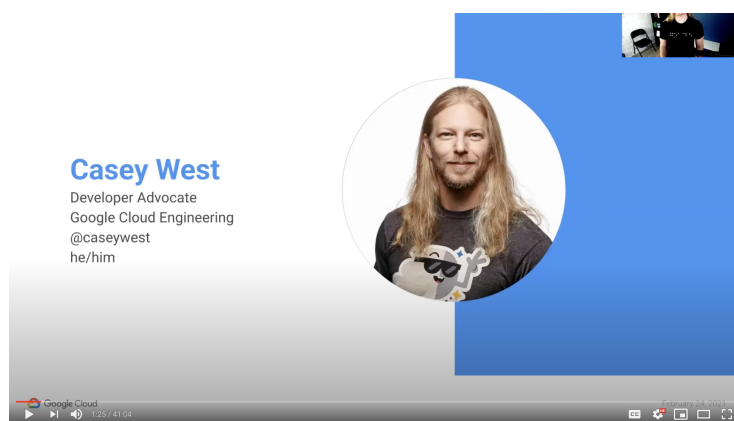
## Expert guidance through the four phases of cloud migration

### Pro tip

The cloud migration journey is a four-phase process: assess, plan, deploy and optimize, but it's rarely linear in practice. These phases are happening in parallel for different workloads.

Cloud expert and lead for Enterprise Developer Advocacy at Google Cloud, Casey West, walks tech leaders through these phases of cloud migration in real time.

**WATCH IT »**





## SECTION 3:

# Philosophies for a multi-cloud strategy

Odds are, you're tackling a cloud migration because it will benefit your organization. It's only a matter of time before every forward-thinking company's infrastructure and services are in the cloud, so knowing how to build a successful hybrid, multi-cloud strategy is essential. Here are four strategic approaches to help you navigate the multi-faceted waters of cloud—plus, a big bucket of resources from the pros.

❑ **SOLVE DATA SILOS WHEN THEY ARISE.** Regardless of what storage choices you make, it's essential to keep an eye out for data silos in your organization. They come in many forms and will hamper the productivity of your organization.

Typical forms of data silos include standalone relational databases, block storage such as persistent disks and data warehouses holding semi-structured data.

### Pro tip

If you have the same data stored in multiple locations, you have no single source of truth. Updating one storage location more frequently than another also leads to problems.

There are two approaches to solving data silos: integration and data lakes.

- **Integration:** If you want to let your silos exist, you can connect up the disparate data sources using extract transform load (ETL) pipelines; this allows you to bring essential bits of data together for visualization or analytics.
- **Data lakes:** Azure, AWS and other cloud providers have their own data lake solutions you can use. They hold raw data in all formats—structured, unstructured and semi-structured data—and they're built around blob storage such as S3 buckets, Azure blob storage or Google cloud storage buckets. Data lakes allow you to have a single source of truth and are great if you're going with a cloud-first approach where you're planning to do a one-off migration to the cloud.



❑ **AVOID VENDOR LOCK-IN.** Along with all the considerations of how a company can serve your organization in the cloud, it's beneficial to consider flexibility with the service without vendor lock-in.

Here are two rules of thumb for avoiding vendor lock-in on the cloud:

- **Avoid past offerings or platform-as-a-service offerings for compute.** Hosted applications will offer you automatic load balancing, version management, traffic splitting and more—which is incredibly convenient—but if you want to move your app to another platform, it may involve a full record. Instead, set up your application using Kubernetes containers; this will make your applications more portable.
- **Avoid platform-specific solutions for ML and AI applications.** Use generic data formats and RDBMS engines where possible.

❑ **BE A SATISFICER, NOT A MAXIMIZER.** Generally speaking, we can be one of two types of decision-makers: maximizers or satisficers.

Maximizers try to squeeze every last drop of value out of a decision. The process may take a great deal of time and effort, but maximizers want to leave nothing of value on the table.

On the other hand, satisficers identify a smaller number of desired outcomes and then choose a solution that satisfactorily meets those requirements. Their process tends to be quicker and requires less effort; they may leave excess value on the table, but they achieve what is most important.

### Pro tip

You might think that maximizing the outcomes of your decisions is the way to go. But studies show that satisficers tend to be happier and more successful in business. Think of it this way: In a tech-driven field, it's typically better to choose a direction and iterate along the way. A maximizer approach risks halting all forward momentum until the best decision is reached. However, the satisficer approach keeps progressing forward, valuing the most significant returns over excess or extraneous value.

We know there are multitudes of choices out there for every step of the cloud migration process—exponentially more when you're constructing multi-cloud strategies. Whatever your use case, there will be only minor differences between the big flagship products, and each will have its areas of strength. Trying to squeeze out every last drop of performance optimization will likely lead to platform-specific changes, which can create vendor lock-in.





## ❑ **KEEP YOUR EAR TO THE GROUND.**

Cloud-based systems are inherently distributed and replicated horizontally. Scale systems such as these are more complex and need more coordination and integration. Each point of coordination and integration is a potential point of failure, which is why it's so important to be conscious of the small things.

We'll get into more details on cloud security in the next section. But on a higher level, tech leaders need to keep their ears to the ground as a strategy for protecting the organization.

Talk to analysts, their support team and engineers often. Look for patterns to emerge in their stories. A one-off event for a particular developer may be part of a more significant ripple visible only from the big-picture plane. Even if we're not talking security threats, you'll want to stay vigilant for cracks in the structure and process that, over time, will lead to lost efficiency and productivity.

### **Pro tip**

When it comes to building a successful multi-cloud strategy, progress isn't always linear. You may need to experiment for a while before you figure out an excellent system for your organization's needs. Developers iterate your product, but as a leader, the entire company's operation is your product. Listening to team members' experiences from the start will help you identify the spots where processes are sticking—and how you can improve them.

## WATCH AND LEARN:

# Building your multi-cloud strategy

What better way to dig into the skills and strategies of constructing a multi-cloud strategy than by hearing it straight from the experts themselves?

### WATCH IT »

Pluralsight author and cloud architect Ryan Lewis explains the five things you need to do to prepare your company for the multi-cloud. He dives into various multi-cloud tools worth using while choosing the right cloud vendor(s) for your company and the future look of multi-cloud.

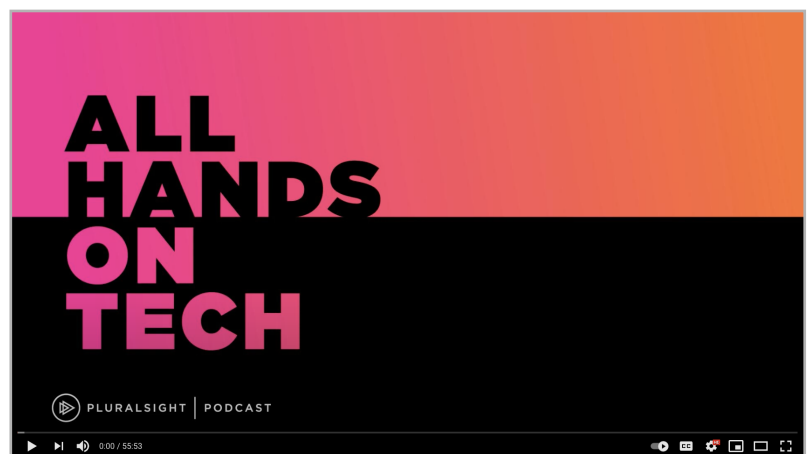


### « WATCH IT

Janani Ravi, the co-founder of Loonycorn and a Pluralsight author, discusses technological design patterns that matter in a hybrid, multi-cloud and ML/AI-permeated world. She also addresses questions to ask when building and implementing a cloud strategy and what the answers should look like.

### WATCH IT »

And again, Janani Ravi joins David Tucker and Casey West to talk about specific tools and strategies impacting cloud architecture, management and security and provides actionable insight to help technologists and leaders strengthen their organization's cloud muscle.



# Cloud security: Focus on what matters most

It's relatively commonsensical that transitioning an entire operation from an on-premises setup to the cloud opens vulnerabilities. It's why many security and DevOps teams put up anything from hesitation to resistance when you discuss any change, period, let alone such a significant undertaking. And we can't fault them. New deployments introduce change and the potential for code to break and things to go down. The InfoSec team's top priority is the security of the business, and cloud migration poses a potential threat.

We cannot argue that the potential for security breaches is nonexistent. But you can take steps to improve and ensure security throughout and after the migration. As the saying goes, knowledge is power, and focusing on these six foundations of security will help DevOps and InfoSec buy into the process. Security is a path, not a destination, and these buckets will help you continually focus energy and resources on what matters most for keeping your company's information secure.

❑ **IDENTITY.** A key place to start (albeit difficult) is establishing a centralized identity source for users and authenticating them. Role-based access control should be administered to groups to avoid one-off permissions. And of course, a common identity threat stems from password security. Multi-factor identification makes much sense for securing multi-cloud systems.

Also, developing strict security management bolsters privileged accounts.

## Pro tip

Think of your cloud administrators for Azure, Salesforce or an active directory. Pairing multi-factor identification with a time limit within the account, and keeping a log of entries and activity, are reasonable steps to add for these accounts.

❑ **DATA.** Identity is used to access data. When it comes to data security, it's more important to protect the data than the data store. Think of it this way: A malicious actor is more likely to hack into your system than walk into your data center to steal a physical hard drive. To that end, you need to encrypt data when it's at rest, in transit and even in memory. Many clouds already come with this level of encryption, which handles many of your data security issues.

However, once that data is accessed on a desktop, it becomes harder to ensure it's secure. Simplifying data classifications will help.

## Pro tip

As a rule of thumb, we recommend aiming for fewer than three to five different levels of classification and perhaps another one or two for client-facing classifications.

❑ **INFRASTRUCTURE.** A common best practice for infrastructure security is to layer your defense. But just like with data classification, keep it within reason. Your team will spend less time troubleshooting if something breaks if the security layering is precise and not overcomplicated. From a user perspective, the North Star here is to make security as easy as possible.

## Pro tip

Consider developing infrastructure templates so that security is already baked in when someone deploys an app. Burdensome security measures mean that users will try to circumvent them—and that's when breaches happen.

❑ **AUTOMATION.** We've stressed how automation will be critical to a successful migration. It also requires a great deal of caution. A small mistake on one server could bring down a whole company. The safest and often the most beneficial places to integrate automation are policy and compliance. You can bake security into pipeline updates before they deploy.

Regardless of how much you choose to automate, place some sanity checks and manual gates in the process.

### Pro tip

Getting human eyes on deployment will help you catch serious errors that automation may overlook. Always answer the question, "Is this the action we want to take?"

❑ **COLLABORATION.** Given the current state of multi-cloud security, you'll want to seek to collaborate across teams. If you get DevOps and security into the same room right at the start, you can set clear goals that guide the entire migration process.

❑ **ANALYTICS.** Clouds are chatty, and in a multi-cloud environment, it's easy to get log exhaustion. Aim to standardize on a platform to ingest and analyze your logs. Of course, each cloud has its log, but a third-party platform is the best way to go when dealing with multiple clouds. It's also not a bad idea to farm out the analysis to a company specializing in finding threats and understanding the activity across all your clouds.

Maintaining a strong security posture is a multi-cloud architecture necessity.

### Pro tip

Align your DevOps, InfoSec and development teams around these core principles to pave the pathway to a more secure organization.



## Expert insight on securing your cloud operations

### « WATCH IT

Pluralsight author and cloud thought leader Kevin L. Jackson shares steps for securing your cloud operations.

# What you need to be successful

Let's end by looking forward. Migrating to the cloud, and establishing your particular cutting-edge processes, is a big step—but it is just the first step. Living in the cloud requires you, your team and your organization to remain active and vigilant in growing, learning and applying advanced skills.

Of course, you'll be experienced after you complete your first migration. But multi-cloud strategies will require you to get to know other players in the game. Cloud security will always need to stay ten steps ahead of your adversaries. And complacency cannot even factor into a successful cloud strategy. Your subsequent assessments may be less drastic than your initial one when you shifted from on-premises to the cloud, but you should constantly evaluate what your team can do better and how you can achieve it.

## WORDS OF WISDOM

*"Perhaps the greatest opportunities (as well as the greatest threats) in our cloud today arise from the speed at which new technologies emerge, explode in popularity and then fizzle. For example, in 2017, data professionals were stampeding into TensorFlow and out of scikit-learn; two years later, the stampede was headed the other way, into PyTorch from TensorFlow. In a strange way, the dominance of the big cloud platforms has made cloud computing somewhat more stable than other 'hot' areas in tech today. But the fact remains that we have to focus way more effort today than even ten years ago on staying current and learning new cloud technologies.*



*To apply the words of famous economist Tyler Cowen to the current cloud boom: Average is over. Cloud is moving fast, so the more you can gain diversified expertise in as many of the big platforms as possible, the more set you'll be for the future."*

**—Janani Ravi, cloud expert**