How to Get Your Cloud Migration Strategy Right

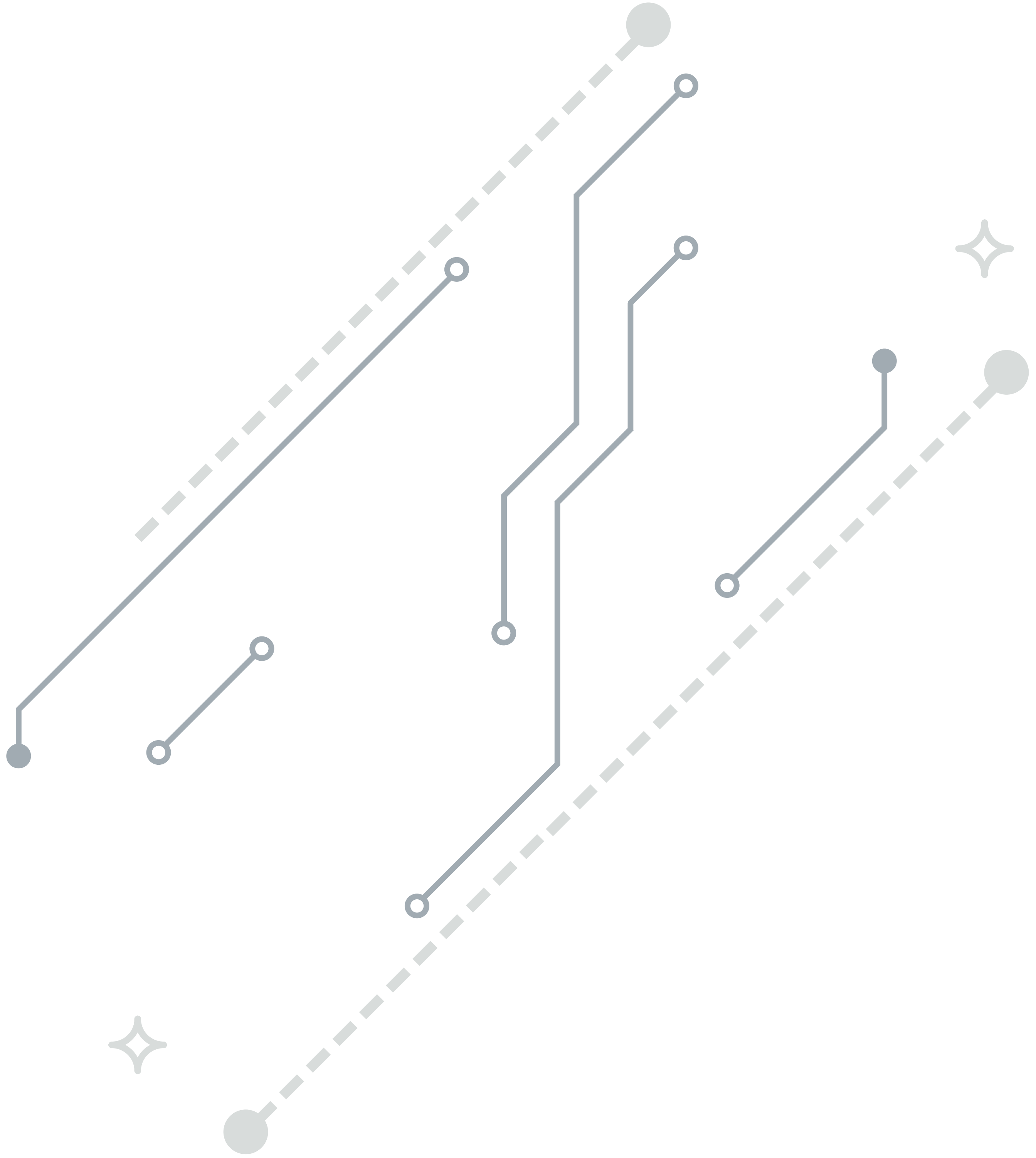
Tips for gaining full visibility for operations, security and cost management — before, during and after migration

splunk>
turn data into doing™

Gain Full Visibility

In Brief

- **When migrating workloads to the cloud,** it's critical to monitor performance across hybrid architectures with tools that collect and correlate data from every location.
- **Don't wait to add end-to-end monitoring services until migration.** Instead, secure a solution to establish a pre-migration baseline, mid-migration insights and post-migration success.
- **Only end-to-end monitoring solutions** that easily collect public cloud provider log files can pinpoint vulnerabilities, threats and breaches.
- **Cost management tools** offer current and historical instance usage and show unused resources. But it's critical to have full infrastructure economics for strong resource forecasts and intelligent migration decisions.



The Landscape Is Changing

Every day, industry leaders are competing with digital upstarts that develop their business exclusively in the cloud.

To fight this battle, companies are digitizing every area of their operations, looking for agility and insights from data and analytics. This transformational effort includes migrating workloads to Amazon Web Services, Microsoft Azure, and Google Cloud Platform, which may not have been historically deployed as cloud-ready applications.

But digital business infrastructure has become more complex — spanning mainframe, client-server, virtualized, serverless and hybrid cloud platforms that include containers and microservices. Yet the core responsibilities of IT to monitor and measure the infrastructure haven't changed. How does one achieve infrastructure visibility and insights into workloads when performance data spans diverse environments?

And the challenges of navigating the cloud strategy aren't felt by IT alone. Security must ensure the posture of an infrastructure they no longer directly control and IT business partners must demonstrate the ROI of moving to "renting" instead of "owning" infrastructure.

More than ever, it's critical to monitor performance across hybrid architectures with tools that collect and correlate data from every location. Multiple, fragmented monitoring solutions don't provide the visibility and intelligence to meet business, security and IT goals.

An IT Operations Perspective

Making your migration successful — before, during and after

As companies migrate to the cloud, end-to-end operational visibility is essential before, during and after the switchover to maintain insight into performance and address fears related to losing infrastructure control. It also eliminates finger pointing when KPIs are missed and when IT's reputation is on the line.

And what does operational visibility look like in a hybrid cloud environment? It's an end-to-end view of infrastructure performance across application workloads and microservices, wherever they reside. It provides the intelligence needed to monitor and measure KPIs to ensure a compelling user experience when infrastructure spans public and private domains.

BEFORE a cloud migration, it's important to measure the baseline user experience and performance, as well as define acceptable post-migration levels. Degradation in one performance area may be tolerated if it's balanced or offset by gains in another. To accurately validate a migration's success, the same monitoring tool should be used throughout the migration process.

DURING a cloud migration, established performance metrics should be closely monitored. Variation from the baseline is an early indicator of trouble. A monitoring solution's dashboard and alerts will quickly identify these issues well before production, and save time and resources. A performance issue is better identified during a migration when it's easier to pause and make corrections.

AFTER a cloud migration, the same monitoring solution should be used to measure acceptable metrics and success. And continued use of the solution and dashboards, well after the switchover, is essential to ensure compelling customer journeys that cross on-premises and public cloud workloads.

A Security Perspective

Getting the complete picture to protect your organization — and your customers

To maintain security in a hybrid cloud environment, organizations need an end-to-end view of user identity and behavior at every application and database access point. This view shows unauthorized access, threat and attack locations and privilege changes. It also provides critical knowledge as entry points are spread more broadly across platforms and geographies.

When migrating to the cloud, security and IT teams are still responsible for the full protection of corporate data and customer information. And finger pointing and breach disputes aren’t considered acceptable by business leaders. Technology teams must have a full view of security posture across hybrid architectures, respond quickly to vulnerabilities and threats, and produce timely audits.

That said, adding workloads to a public cloud does increase the complexity of the security landscape. It extends the points of entry for hackers and adds cloud provider staff to the list of potential threats. So for comprehensive user activity monitoring across hybrid cloud architectures, it’s key to have easy access to log files and end-to-end tools that collect, correlate and analyze suspicious behavior.

Identity and access monitoring
Log files and monitoring tools provide ample visibility and analysis into user activity. They track the identity of users who submit, modify and delete data, and the time when that event occurs. They also reveal unauthorized access attempts, simultaneous logins from disparate locations and changes to access privileges. They can even help spot inadvertent information changes.

Dashboards within cloud monitoring tools can help visualize user identity and access events, and create a foundation to analyze trends. Alerts and reports allow seamless transition from a reactive to proactive response. Also, some tools offer predictive analytics that provide security intelligence to obtain a comprehensive view of the cloud infrastructure and security posture. And many monitoring tools can help establish audit procedures and conduct compliance checks to ensure adherence to internal and industry standards. With audit trails, IT and security teams can rapidly troubleshoot threats before they become a cybersecurity breach.

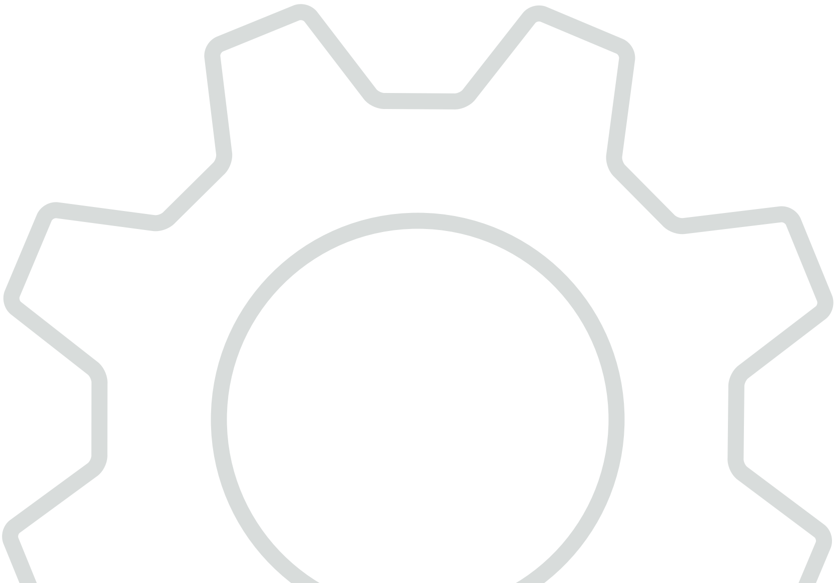
An Operations Perspective

Predict and manage costs with analytics

Migration to the cloud can offer huge cost savings by reducing server ownership and management. But if cost projections are incorrect, the entire cloud business case can be jeopardized. ROI can decline and break-even dates can lengthen — the blame placed on IT for inaccurate projections. True spend can vary substantially from even the best crafted budget.

Strong visibility and projections of cloud provider costs can address this concern. When applied to existing cloud workloads, monitoring tools help improve forecasts for the next set of migrated apps. Through usage and cost analysis, they reveal when workloads should be moved to the cloud or left on-premises until cost structures change.

Machine learning to cut costs
Cloud monitoring analytics can optimize costs by signaling users to buy instances in advance at lower prices. By applying machine learning algorithms to the consumption data of existing workloads, IT can more accurately predict compute and adjust predictions based on expected spikes in demand. This yields better use of company assets and increases margins. Flawed forecasts, on the other hand, can place IT's reputation at risk and drive business teams to bypass recommendations and set their own purchase patterns without visibility provided by monitoring tools.



The More Things Change, the More Things Stay the Same

It's frustrating not knowing the source of an infrastructure performance problem or security threat, especially at the critical point of workload migration. Multiple, fragmented monitoring solutions add to this issue, providing a fragmented view of an already stratified infrastructure.

But a single monitoring solution that provides dashboards to multiple audiences from the same data can unify teams and make the transition to the cloud as seamless as possible.

When managing a hybrid environment, the goals of IT, security and business teams will remain constant. For example:

- The KPIs IT will need to monitor the scale up/down of changing instances and workloads are the same for monitoring on-premises workloads — and IT will need to connect that data with application metrics for holistic monitoring.
- Security will need a complete picture of the entire infrastructure, including all cloud nodes, transactions and users to ensure the security posture, and protect against potential threats.
- Business teams will need to know what has been deployed in the cloud, the usage, and if any devices are unpaired or orphaned in order to mitigate costs and demonstrate ROI. Having all three groups drawing analysis from one source prevents finger-pointing and eliminates silos.

More than ever, it's critical to monitor performance across hybrid architectures with tools that collect and correlate data from every location. A single end-to-end monitoring tool that traverses a hybrid cloud environment is beneficial to three separate teams — IT, security and expense management. But having all three teams unified on the same data is even more beneficial to the entire business.

Migrate to the cloud without losing visibility

Learn More