Fast Track Your **Multicloud Monitoring Initiative**

splunk> turn data into doing™

The Rise **of Multicloud**

Cloud migrations are on the rise — so much so that **Gartner predicts 80% of enterprises** will have migrated away entirely from on-premises infrastructure by 2025. The latest development in cloud computing is the rise of multicloud, a strategy where an organization uses at least two cloud services within a single architecture — in other words, different cloud stacks for different tasks, such as Google Cloud Platform for internal apps and Amazon Web Services (AWS) for customer-facing apps. This type of approach has become so popular that more than **80% of companies use it today.**

There are different kinds of cloud solutions that can make up a multicloud environment. Public cloud services include AWS, Microsoft Azure, Google Cloud Platform and other cloud computing services offered by third-party providers. Private clouds, on the other hand, limit access to specific organizations. The services and infrastructure are maintained on a private network, providing increased security and control compared to public clouds.

Different Stacks **for Different Tasks**

Why Organizations Use Multiple Public Clouds

AWS for Development
Microservices
Containers
EC2, VMs, Storage

GCP for Internal Services
G Suite, Workday, Salesforce

Azure for Lift and Shift
Reduces costs
Disaster recovery

Understanding **Multicloud Environments**

It's also worth defining "hybrid cloud" and "multicloud." A hybrid cloud solution means an organization uses a mix of on-premises, public cloud and private cloud infrastructure, while multicloud refers to the way organizations use multiple cloud providers for more than one cloud deployment of the same type — for instance, if they use public clouds from two different vendors. Different teams have different needs, so they'll usually choose whichever cloud vendor best suits their specific set of criteria.

What's the Difference?

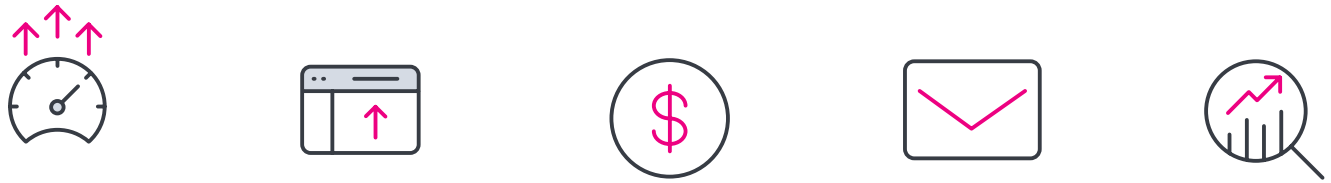
Multicloud	Hybrid cloud
More than one cloud deployment of the same (public or private) sourced from different vendors	Mix of services (on-prem, private, public, third-party) with integration or orchestration between them
Example: two public clouds, AWS+Azure	**Example:** a public cloud AND an on-prem customer-maintained datacenter infrastructure

Why Are Companies Taking a Multicloud Approach?

Performance optimization: If a primary cloud is taken down or experiences performance issues, a passive cloud can serve as a fallback solution. This strategy ultimately reduces downtime or eliminates it altogether, until the primary cloud gets back online.

Cost savings: Combining improved reliability and optimized performance means cost savings for businesses. Downtime at a bank may result in lost revenue, while downtime at a hospital may result in lost revenue and endangered lives. Whatever the case may be, keeping networks up and running is crucial for every organization's continued success.

Flexibility: A multicloud approach helps avoid vendor lock-in, where organizations are dependent on a particular cloud provider's infrastructure and services, potentially facing substantial costs and constraints if they switch vendors. Using a mix of vendors also lets organizations optimize performance by choosing a combination of services that meets their specific needs.
A particular company may choose to use Microsoft tools for one use case, and Google or AWS for others (e.g., infrastructure and development).



Key Challenges in **Multicloud Environments**

While a multicloud strategy offers many benefits, the challenges are not insignificant. The same features that offer increased flexibility and reliability also create additional security risks and IT challenges.

All the challenges IT teams face in cloud computing are amplified in multicloud environments, making it more difficult for teams to identify, investigate and resolve critical issues in the cloud; more services means more complexity, and siloed systems make holistic monitoring much more difficult.

On the security side, recent studies show a link between the number of cloud services used and the likelihood of a **2019 study by Nominet** found that 52% of multicloud environments have been breached within the past year, in comparison with 24% of hybrid-cloud organizations and 24% of single-cloud users. Multicloud environments are also more likely to suffer multiple breaches: 69% of such organizations report 11 to 30 breaches, in contrast with 19% of single-cloud organizations and 13% of hybrid-cloud users.

The challenges posed by multicloud environments impact IT and security teams in different ways:

Multiple Systems Create Silos: A multicloud approach may improve security and system reliability because services are distributed across multiple cloud solutions. But it may also pose risks by making it that more difficult for organizations to have visibility across all their hosts and services.

Using different cloud solutions, each with its own native tools for monitoring and security, means that IT teams can't efficiently see across the whole stack to tell if service degradation or downtime is due to a particular service, or if the system is working as intended.

Traditional cybersecurity fundamentals aren't necessarily applicable to multicloud environments. An organization could use multiple solutions to monitor its cloud services, but this methodology slows down teams and comes at a cost, especially when time-sensitive problems occur.

Increased Mean-Time-to-Resolution (MTTR): Wrangling information about an outage or breach out of a multicloud system can be a headache for IT and security teams and cost the organization time, money and customer satisfaction and trust.

Reduced visibility across the stack means that teams spend much more time trying to figure out where and why outages occur, having to transition between multiple monitoring systems to correlate and analyze event data to gain a complete understanding of the issue. Every minute counts in a service outage or malicious attack and the additional complexity of a multicloud system has a direct impact on the bottom line.

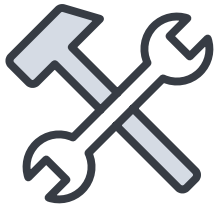
Data Governance, Compliance and Infrastructure Vulnerability: Plus, the lack of visibility across multiple stacks makes it harder to meet compliance mandates and fend off hackers, who have an easier time finding and exploiting vulnerabilities within the organization's distributed infrastructure. Essentially, each additional cloud service increases the number of access points into a network.

Visibility issues also create data governance and compliance problems. Multiple clouds can offer greater flexibility, but also create regulatory challenges. For example, an organization might accidentally run an application in an unapproved environment and violate regulations under the General Data Protection Regulation (GDPR). Violating these guidelines and others can lead to substantial fines.

Monitoring with Different **Native Cloud Tools Lead to:**

- **Siloed Views**
- **Siloed Teams**
- **Siloed Data**

Teams have a hard time identifying, investigating and resolving critical issues in the cloud.

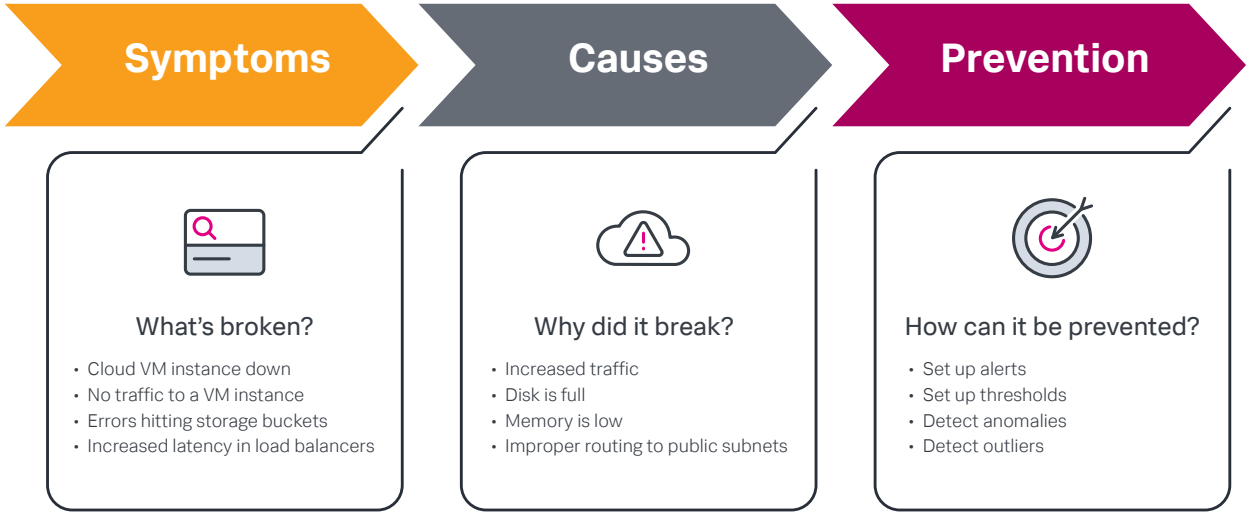
Lack of visibility  Can't see if service degradation or downtime is due to cloud services	**Complex toolset**  Using multiple cloud services make it hard to have one unified monitoring strategy
Poor MTTR  Too much time figuring out where and why outages occur	**Scale difficulties**  Hard to gather data across multi-region, multi-account and multicloud environments

How to Tackle **Multicloud Monitoring**

So how can organizations overcome these challenges? As cloud infrastructures expand in scope and complexity, it becomes more important for businesses to have monitoring solutions and strategies that address these security and IT challenges.

The good news is that it's certainly possible for organizations to reap the benefits of a multicloud approach while mitigating the accompanying risks. As modern IT infrastructures grow increasingly complex, having a centralized method for monitoring and troubleshooting across the entire multicloud environment is crucial. Without the right tools, today's enterprises will find it more challenging to get the data they need to properly handle outages and incidents. Organizations that invest in modern IT tools can create positive customer experiences and ultimately maximize innovation and revenue.

Path to Easing Monitoring Pains



The first step is to find a consolidated IT infrastructure monitoring solution that replaces multitudes of monitoring and troubleshooting tools. Monitoring with one tool and troubleshooting with another can be needlessly complex, slowing down teams even when critical issues arise, but simplifying the toolset allows for both functions within the same solution. Next, getting data in needs to be seamless. Having guided data onboarding is key here — the right solution will need to make it easy to collect data from multiple cloud vendors and bring it all together into a single view. This empowers organizations to better keep track of the operations, security and costs of all their different cloud environments.

Finally, a solution that unifies monitoring across infrastructure, apps and services, and uses artificial intelligence (AI) and machine learning capabilities can help organizations predict and prevent cloud outages before they occur. For multicloud environments in particular, organizations need a solution that simplifies and hosts data collections from multiple clouds, gives an aggregated view of the environment by grouping disparate cloud services and lets teams track overall cloud usage across all environments.

Learn How.

Monitoring multicloud environments can be a challenge, but it doesn't take an arsenal of tools for businesses to keep up with what's happening within their cloud infrastructures.

Simplify your toolset by contacting sales@splunk.com.

2020-IT-splunk-multicloud monitoring-EB-114

splunk> turn data into doing™