Fast Track Your **Multicloud Monitoring Initiative**

splunk>

turn data into doing®

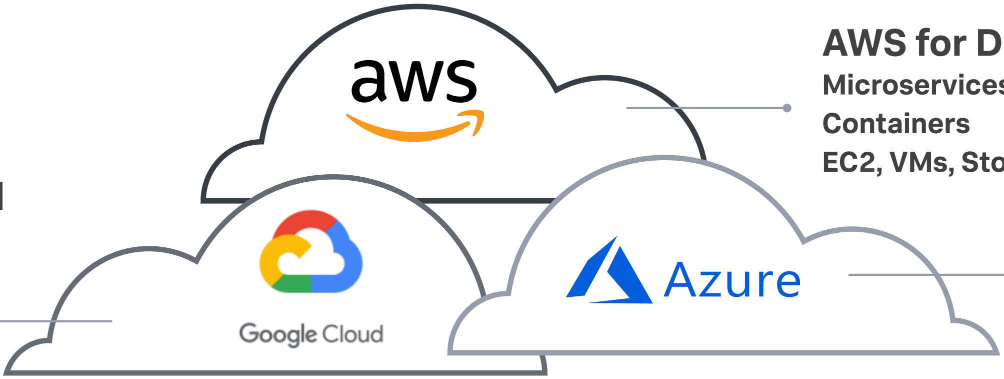
The rise **of multicloud**

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 and it's fast becoming the norm in the pubic sector as well.

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
Workloads can be delegated to cloud platforms without interoperability between providers	Workloads distributed across multiple cloud and on-premises environments — highly portable and interchangable environment
Example: two public clouds, AWS+Azure	**Example:** a public cloud AND an on-prem customer-maintained datacenter infrastructure

Why are organizations taking a multicloud approach?

Resiliency: 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.

Efficiency: Combining improved reliability and optimized performance means cost savings for businesses, and better citizen services and protections for the public sector. 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).

Improved reliability

Performance optimization

Cost savings

Avoid vendor lock-in

Scalability

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, in 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 much more difficult for organizations to have end-to-end visibility across all their hosts and services. Public cloud adoption increases an organization's attack surface with more services to secure and monitor.

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/citizen satisfaction and trust.

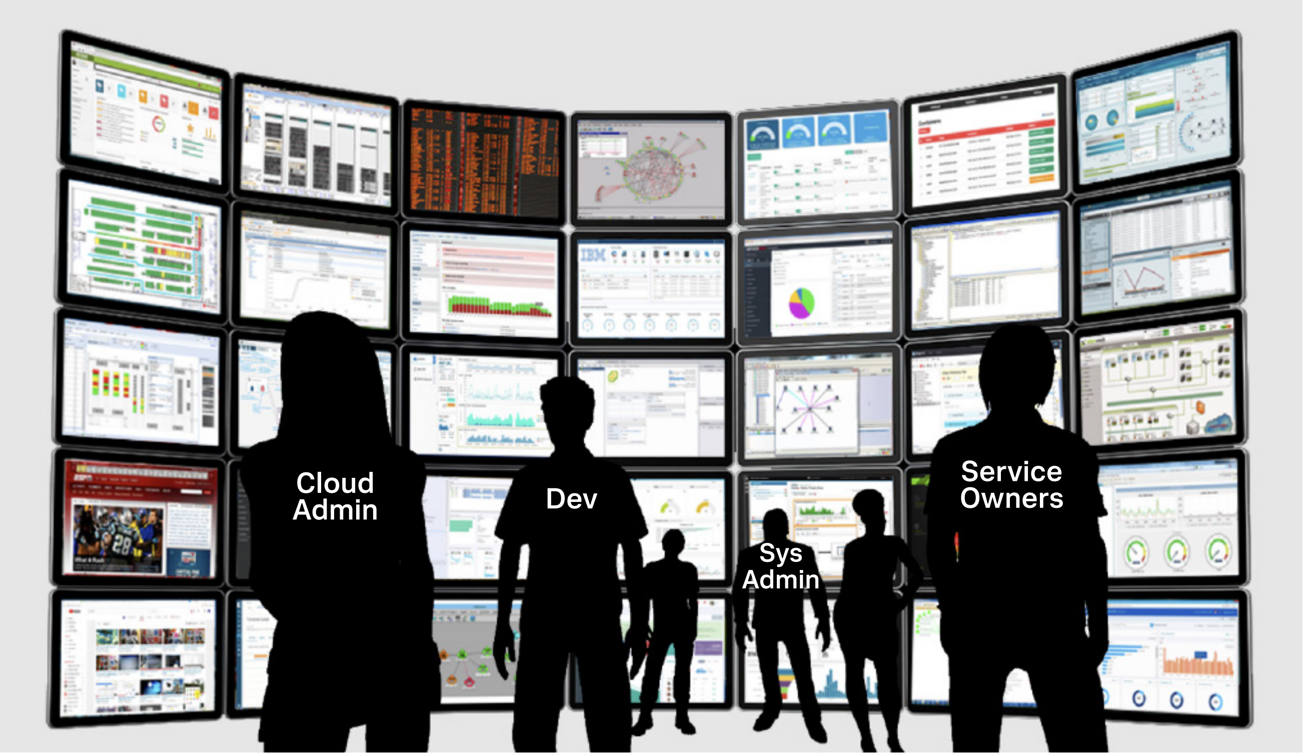
Reduced visibility across the stack means that teams spend much more time trying to figure out where and why outages occur, having to transition between multiple monitoring systems to correlate and analyze event data to gain a complete understanding of the issue. Every minute counts in a service outage 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: 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 leads 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 makes it hard to have one unified monitoring strategy

Poor MTTR

Too much time figuring out where and why outages occur

Scale difficulties

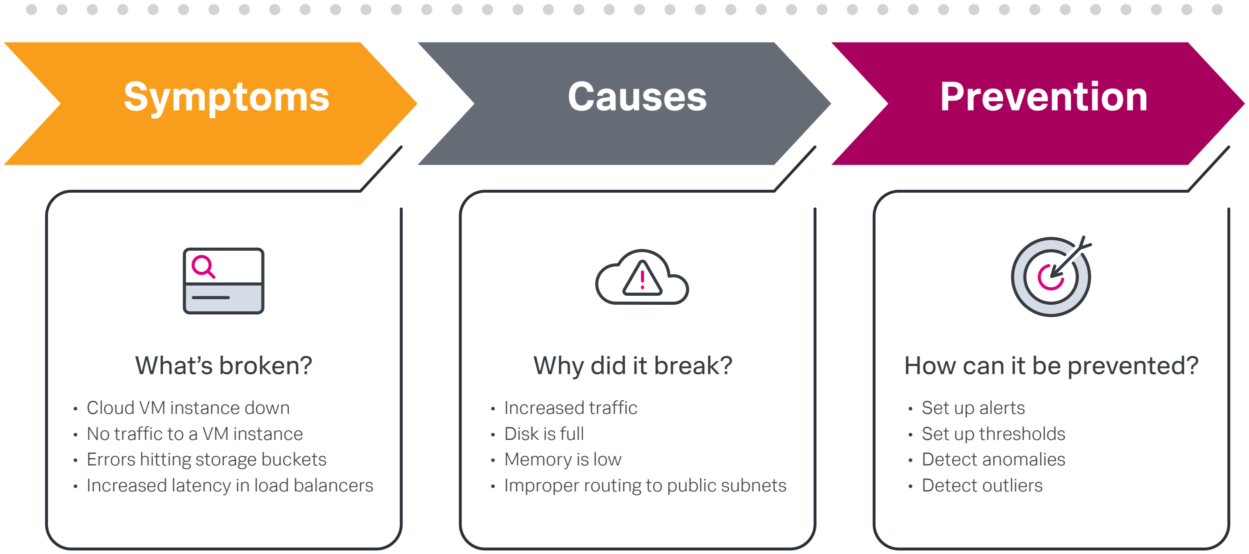
Hard to gather data across multi-region, multi-account and multicloud environments

How to tackle **hybrid/multicloud monitoring**

So how can organizations overcome these challenges? As cloud infrastructures expand in scope and complexity, it becomes crucial for businesses and government agencies to have comprehensive monitoring solutions and strategies that address multicloud needs and challenges.

As modern IT infrastructures grow increasingly complex and IT leaders democratize data access for their distributed teams to release better applications faster, having a centralized method for monitoring and troubleshooting across multicloud environments has become essential. Without the right solution, today's enterprise will find it more challenging to observe and use the data required to properly prevent and manage outages and incidents. Organizations that invest in modern IT and DevOps tools can create positive customer/citizen experiences and ultimately maximize innovation and revenue.

Path to Easing Monitoring Pains



Symptoms

What's broken?

- Cloud VM instance down
- No traffic to a VM instance
- Errors hitting storage buckets
- Increased latency in load balancers

Causes

Why did it break?

- Increased traffic
- Disk is full
- Memory is low
- Improper routing to public subnets

Prevention

How can it be prevented?

- Set up alerts
- Set up thresholds
- Detect anomalies
- Detect outliers

Splunk infrastructure **monitoring and troubleshooting**

Cloud tools often come with their own monitoring and troubleshooting tools and services. But transforming enterprises require a solution that works across multiple clouds and services in real time to provide one comprehensive view across the technology stack and platform from which to direct and take action. Monitoring with one tool and troubleshooting with another can be needlessly complex, slowing down teams even when critical issues arise.

This is where Splunk for infrastructure monitoring and troubleshooting comes in. Splunk offers a consolidated infrastructure monitoring solution that extends on your data platform when building new use cases. Finding both functions within the same solution can vastly simplify processes and ease resource strain. It also reduces friction in sourcing data by enabling its collection from multiple cloud vendors and optimizing the value of this data. This empowers organizations to better keep track of the operations, security and costs of all their different cloud environments in real time.

Splunk does this through friction-free monitoring out-of-the-box for the entire cloud stack that offers visibility and directs on problems by leveraging all data from any source, at any scale. Accurately detect and alert in seconds with real-time, AI-driven analytics that predict and prevent issues. Get a better understanding of the IT health that's impacting business performance and improve service reliability. Match the growth of the organization across any stage of their cloud journey with flexibility and scale, while future-proofing their IT investments made.

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.

Test out Splunk's infrastructure investigation and monitoring capabilities. Sign up for a free trial of Splunk Infrastructure Monitoring.

Or contact sales@splunk.com to learn how you can quickly and effectively fast track your multicloud initiatives.

splunk>
turn data into doing