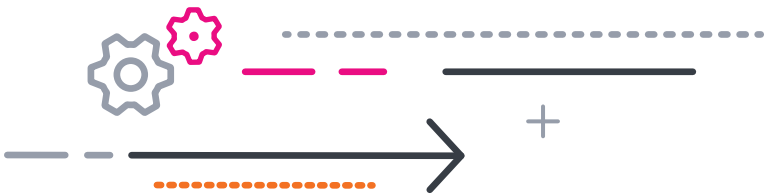
Must-Haves for Managing Multicloud Complexity

A guide for CIOs, CTOs and CISOs on their cloud journey

splunk>
turn data into doing™



The security, IT and DevOps teams at too many organizations today find themselves in a bind: They've adopted multicloud or hybrid cloud, but the supporting systems that ensure their technology environments help them reach their organizational goals haven't kept pace. How did they get to this point, and what can they do now?

Virtually all organizations are already operating in a multicloud or hybrid cloud environment. According to a survey by IDC, 93% of organizations rely on multiple clouds. The decision may have come from a desire to save costs and avoid vendor lock-in, increase resilience, or maybe organizations found themselves with multiple clouds because of the compounding decisions of various teams. The reality is that very few organizations first ask themselves, "How can we secure and monitor our technology?" before making these strategic technology decisions.

Yet once they make the decision to go multicloud or hybrid cloud, security, IT and DevOps teams in these organizations are finding these environments come with their own challenges. Just keeping track of all the cloud services in an organization is difficult since spinning up new cloud infrastructure can be as easy as making a purchase online. In tandem, complexity grows as operations span across a distributed landscape. Security becomes more challenging with an ever-growing attack surface: Security teams must defend against new threats while managing cloud services and tools that are different from one cloud provider to the next. In addition, the potential for redundant costs increases as teams across an organization employ their own tools, sometimes doubling up on capabilities. Failure to manage the complexity due to poor visibility and a lack of control leads to missed opportunities and potentially costly mishaps.

At the same time, security, IT and DevOps teams in these organizations are realizing that their previous approaches to monitoring and troubleshooting are not sufficient for the new, more complex cloud landscape. Research indicates that just 11% of decision-makers are satisfied with their monitoring tools. Legacy technology was designed for on-premises infrastructure and monolithic applications. In that world, batch processing and getting updates every few minutes was often good enough. But in a container-based, cloud-native environment, the short-lived nature of spinning up and down services means that batch processing won't work. Yet tools purpose-built just for the cloud-native world may not be good enough either, as the vast majority of organizations find their systems distributed across old and new generations, and need visibility and the ability to take action across environments. And what about the native tools from the cloud service providers? While they have made solid advancements, they are designed with the primary purpose of visibility into their own services.

For organizations that moved to multicloud and hybrid cloud and are finding that they need a change in how they manage across their environments, they must put in place a data backbone to ensure success. A data backbone for the modern technology landscape requires tools that provide observability for IT and DevOps and an end-to-end view for security professionals that empowers them to investigate, monitor, analyze and act.

Organizations must move beyond traditional monitoring approaches to observability. Monitoring and observability are complementary, but while monitoring shows whether the system works, observability lets organizations ask why it's not working. Put another way, monitoring will alert on predictable failures, while observability provides a view into all possible permutations of full and partial failure. It is critical for organizations to make their systems observable so they have visibility across the multicloud and hybrid cloud landscape. Within security, organizations also need visibility and control to manage the complexity of modern infrastructure. A single view of all systems to normalize and manage data across hybrid infrastructure helps security analysts to centralize findings, prioritize alerts and streamline investigations.

3 Must-Haves for Multicloud and Hybrid Cloud Success

Every security, IT and DevOps team requires the following capabilities to power their data backbone:

1. **Analysis of any data from any source, at any scale:** Teams must be able to leverage all data across clouds and on-premises to proactively detect, alert and direct investigations. As cloud thought leader David Linthicum put it, "The reality is that you won't be successful without a sound layer of abstraction that's able to bring operational simplicity and observability."
2. **Real-time insights:** Organizations cannot wait minutes to see if they are having infrastructure issues, given the short-lived nature of containerized operations and functions as a service. Only a scalable streaming architecture can ingest, analyze and alert quickly enough to identify and investigate issues and keep them from affecting customers in a big way.
3. **Analytics that empower teams to act:** Since multicloud and hybrid cloud strategy does not sit with just one team, organizations need the ability to analyze data within and across teams to make decisions and take action quickly. In particular, IT, DevOps and security teams have a critical role in driving and securing cloud transformation and must be able to analyze and act, leveraging the most up-to-date data.

With these three capabilities organizations are well on their way to successfully securing, operating and innovating in multicloud and hybrid cloud environments.

Secure

Recent attacks point to the importance of seeing all data across clouds and on-premises infrastructure, as well as the spaces between these environments, as data flows from one service to another. Median global dwell time for security threats is 56 days, which is more than enough time for hackers to do significant damage. The MITRE Cloud ATT&CK Matrix documents a growing number of tactics and techniques that cyber criminals use against enterprise cloud-based services.

With this in mind, it's critical to establish the first capability mentioned above within security and be able to take in any data from any source and at scale. Taking in all data — and analyzing and prioritizing it properly — eliminates blind spots in distributed ecosystems that can create security vulnerabilities and hinder investigation and resolution. With end-to-end visibility, organizations are able to monitor for threats in one place, simplifying and strengthening their security posture.

> Taking in all data eliminates blind spots in distributed ecosystems.

Organizations also need insights from this data instantly, with the ability to rapidly investigate across their entire tech stack. Fast investigation can lead to quick response times, minimizing impact from security threats. But real-time insights are not enough considering that today's security teams are often understaffed and overwhelmed by alert volumes. An attribution-based approach to alerting, or risk-based alerting, helps radically reduce alert volumes, giving analysts back hours each week to focus on real threats. Moreover, automation and orchestration are critical security capabilities that help analysts detect, investigate and respond to alerts faster. For example, security teams can leverage automated playbooks to triage SIEM alerts, block suspicious activity or even remediate an entire security incident at machine speed. With these tools, security teams can quickly improve response time and focus on what's most important.

An example of the type of results organizations see with the implementation of a data-driven multicloud and hybrid cloud security strategy comes from a large European multinational manufacturer. This company faced significant blind spots across their complex environment. They were able to implement Splunk as a single security platform globally for 350 security operations center (SOC) use cases, and after 18 months they saw a 40x increase in assets monitored and an eight-fold increase in data analyzed per day. They also saw significant increases in automation, with automated responses handling 80% of level-one alerts and 50% of level-two alerts, saving countless hours for the 1,000 unique active users leveraging the platform each month. Furthermore, through a data-driven culture, the Cloud Security Operations department reduced non-compliance of AWS cloud assets against their corporate standards and policies by more than 50%.

> …after 18 months they saw a 40x increase in assets monitored and an eight-fold increase in data analyzed per day.

Operate

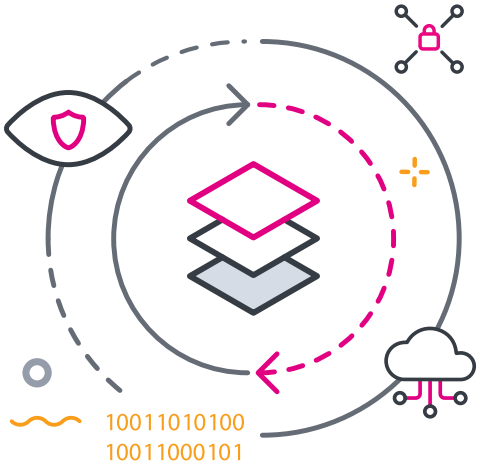
The multicloud and hybrid cloud stack makes it difficult to see across the entire IT landscape. Data trapped in silos means that it takes longer to detect and resolve issues. In addition, cloud-native technologies — such as containers and serverless functions — often only live for seconds or minutes, meaning organizations need to be able to monitor and take action in real time. These challenges are unfolding with the backdrop of ever-increasing customer and employee expectations for a flawless digital experience every time, without slowdowns or other performance issues.

> To tackle these challenges, organizations must move toward making all of their systems observable.

To tackle these challenges, organizations must move toward making all of their systems observable. They need visibility and control across the entire IT landscape, leveraging all data across clouds and on-premises to proactively detect, alert and direct investigations and reduce performance issues. Visibility also creates new opportunities for optimization and cost reduction, such as identifying resources that are overprovisioned. Additionally, cloud-native technologies require real-time monitoring and investigation that traditional monitoring tools cannot deliver. Finally, with all the event noise facing ITOps and DevOps teams, built-in AI/ML-driven analytics can help speed up investigations, streamline workflows and predict future performance degradation and outages.

The Japanese credit card payment and marketing services provider Vesca experienced a number of these operational benefits by updating its technologies during the COVID-19 pandemic. Vesca saw large growth in its business from increased demand for e-commerce and cashless payments, with the number of monthly credit card payment transactions exceeding 10 million. Plus, it could take two or three people a whole day just to tackle a single system failure. Despite the additional business volume, the company was able to deploy Splunk to create a stress-free experience for monitoring its cloud architecture, even with a limited staff. Vesca experienced a 99% decrease in incident response workload after implementing Splunk, and now Vesca is able to automatically detect problems in just minutes versus an entire day.

> Vesca experienced a 99% decrease in incident response workload after implementing Splunk.



Innovate

It can be challenging to find the right balance between giving developers and other teams the freedom to choose their own cloud services and imposing rigid guidelines to avoid shadow IT. Organizations often struggle to track all of the cloud services they are paying for and need to monitor and secure. In addition, lack of transparency into infrastructure creates headaches for DevOps teams that struggle to pinpoint the cause of issues.

While multicloud is often thought of as a play to optimize costs or increase resilience, when done right, a multicloud cloud strategy encourages innovation for organizations. Multicloud spurs experimentation through choice, flexibility and dynamism. Developer, IT and architect teams can choose the services that are uniquely fit for the problem at hand, instead of being constrained by a limited set of capabilities. Multicloud empowers organizations to find the best approaches to any problem and can ultimately bolster the bottom line. Organizations no longer have to just imagine an environment of hand-picked, best-of-breed tools powering their business outcomes. They can use and build solutions composed of the best options for the most effective user experience and business outcomes.

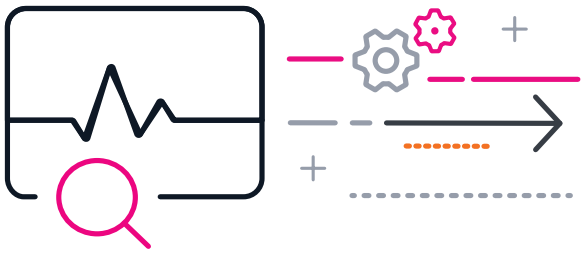
> Multicloud empowers organizations to find the best approaches to any problem and can ultimately bolster the bottom line.

With observability, this vision can become a reality. Leaders are able to maintain transparency and control over their environments however developers use them. In other words, there is no more shadow IT, since organizations have full visibility into all of their cloud services. By analyzing all data from any source in real time, organizations are able to discover, monitor and troubleshoot all of an organization's cloud services and democratize that information across the organization — to ITOps, DevOps, security, lines of business and beyond.

Leveraging all their data also helps teams ensure infrastructure is running correctly across the full tech stack and frontend to backend. Developers are able to reduce performance issues and make certain that infrastructure scales with the needs of the business so they can spend more time innovating for customers.

> Splunk helps Nasdaq to bridge the gap between its cloud and on-premises ecosystems and free up time for teams building new products for customers.

Nasdaq is a prime example of needing to innovate in a heterogeneous environment. The company relies on Splunk to monitor and troubleshoot its infrastructure, applications and operating systems across its hybrid cloud stack. This enables Nasdaq to do what it does best — build applications specific to capital markets, trading and market data. With Splunk making it possible to investigate any data from any source, it helps Nasdaq to bridge the gap between its cloud and on-premises ecosystems and free up time for teams building new products for customers. Hear more about Nasdaq's experience from its CIO/CTO here.



A Data Backbone for the New Technology Landscape

Confronted by the challenges and opportunities of a multicloud and hybrid cloud environment, organizations need a single, unified solution to centralize all their data, provide real-time insights and promote action based on analytics.

Splunk is the data backbone for the new technology landscape, accelerating cloud-driven transformation by powering comprehensive data strategies for IT, DevOps and security teams, so they can secure, operate and innovate faster across multicloud and hybrid cloud environments.

With the powerful combination of the leading data platform and purpose-built solutions, Splunk helps organizations overcome complexity and realize the power of cloud transformation: becoming more agile, optimizing costs, securing what matters and reducing downtime.

Ninety-one of the Fortune 100 use Splunk, so Splunk is likely already used at your organization. Talk to your team about how to use Splunk's platform to cultivate multicloud and hybrid cloud success.

Learn More.

Visit splunk.com for more on accelerating your cloud transformation across your multicloud and/or hybrid environment with the industry's leading data platform and solutions.

21-18311-3 Must-Haves for Managing Multicloud Complexity-LS-114

splunk> turn data into doing™