How to secure multicloud

The promise of cost savings, flexibility, and agility is making it easier for more organizations to embrace a multicloud strategy. But multiclouds can mean multiple risks if not secured correctly from build to runtime.

LACEWORK

Multicloud is gaining steam, but it brings with it a new set of security challenges. This book will help you understand the value of multicloud, how to secure it effectively, and what to look for in a cloud security platform to enable innovation with speed and safety.

> “88% report security of their cloud environment will continue to become even more important next year.”
>
> CLEARPATH STRATEGIES & LACEWORK CLOUD SECURITY STUDY, NOVEMBER 2021

Multicloud explained

Multicloud means more than one cloud. The concept may be simple, but securing it safely can be tricky. And so can understanding the difference between multiple secure clouds and a multicloud environment. The two are related but not equivalent. Multicloud consolidates all clouds, public and private, into one secure environment for cost-savings, reliability, and better performance. Multicloud requires a single secure enterprise network that spans the data center (physical or software defined) and all the independent clouds an organization owns or subscribes to.

Amazon Web Services (AWS), Google Cloud, and Microsoft Azure remain the top three public cloud providers, while private clouds are those that are exclusive to an organization or hosted privately. For public and private alike, cloud-first policies and cloud migration are top of mind for IT leaders as they look to capitalize on expanded usage of containers, Kubernetes, and cloud services like Office 365, Google Workspace, Workday, Salesforce and more.

According to the State of Cloud report, **92% of enterprises have a multicloud strategy, and on average utilize 2.6 public and 2.7 private clouds.** More and more organizations are bringing public and private cloud services into one overall cloud deployment to more effectively run their business.

Multicloud moves mainstream

Adoption goes sky high

According to Gartner, 76% of organizations adopted, or planned to adopt, multicloud environments by the end of 2021. This uptick is driven in large part by the flexibility it provides organizations who prefer to spread services for better performance and distribution of risk.

From darkness to clarity

When data hides in cloud silos, it's hard to know what security risk poses the biggest threat. Organizations need complete visibility to keep cloud accounts and workloads safe from zero-day threats, vulnerabilities, and misconfigurations. With all clouds i n one environment, CISOs can confidently shine a light on evolutionary threats, identify critical risks that need action, and mount a coordinated response.

Organizations rely on 7 different infrastructure monitoring solutions, on average, to manage multicloud environments, and 57% say this makes it difficult to optimize infrastructure performance and resource consumption.

INDEPENDENT GLOBAL SURVEY OF 1,300, CIOS AND SENIOR IT PRACTITIONERS, 2021

Freedom to enable

Organizations now have more choices. With multicloud, DevOps, HR, marketing, sales, and others have more control over the SaaS or cloud services they wish to select to meet their immediate business needs. IT leaders can now easily add another cloud or bring a new service vendor into a secure environment at any time. Multicloud allows security to be seen as an enabler, not a blocker, for the business

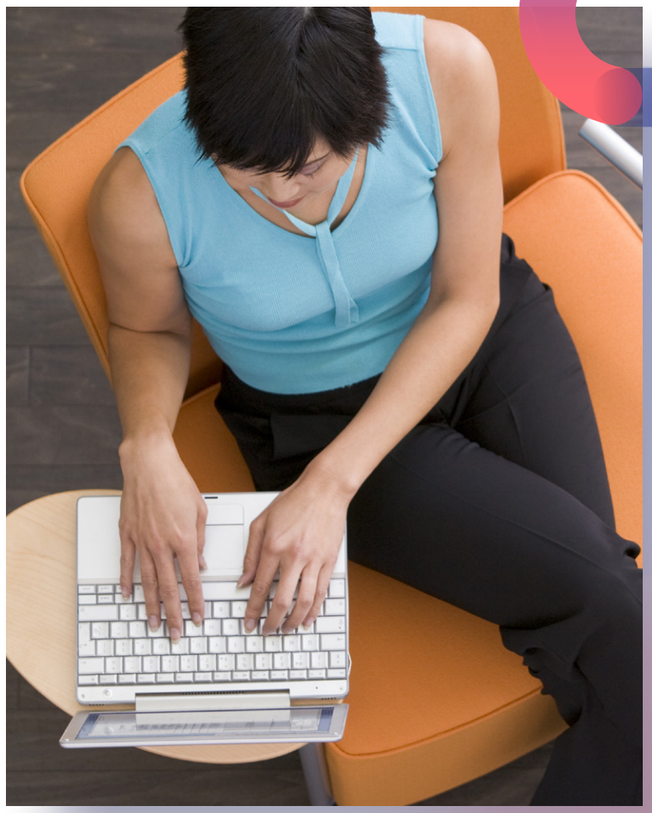
Redundancy adds reliability

In addition to avoiding vendor lock-in, the distributed approach of multicloud eliminates a single point of failure and adds a layer of redundancy. It can make it more challenging for hackers to disrupt all of an organization's services if all their eggs are not in one cloud basket. If one cloud goes down, an organization can minimize total disruptions and downtime more easily with a multicloud strategy.

Cloud cost savings

Securing a multicloud environment can translate into serious savings for security and IT leaders who are resource stretched and budget constrained. Spending hours matching and aggregating data from different clouds or mining data takes time and resources that CISOs often don't have, especially with the rise in zero-day threats and ransomware in the cloud.

LACEWORK



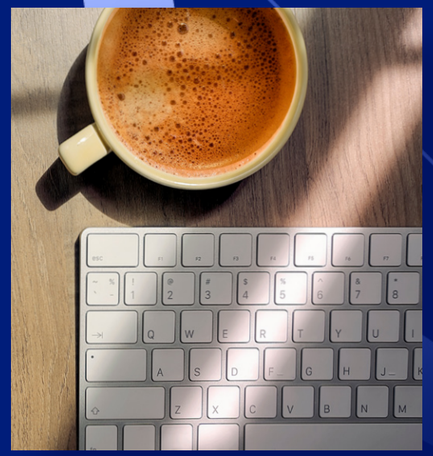
What to look for in a multicloud security platform

Many organizations still believe that cloud providers are required – or should be required – to have security measures in place. Rest assured, these providers do have security measures in place, but their responsibility and scope are limited. The cloud provider is generally only held accountable for the security of the clouds, not the activities that occur in the cloud *environment*.

If you're challenged by changing cloud configurations, compliance mandates, and pressure to secure numerous cloud and containerized environments, you need to invest in a data-driven platform approach that automates analysis and decision-making.

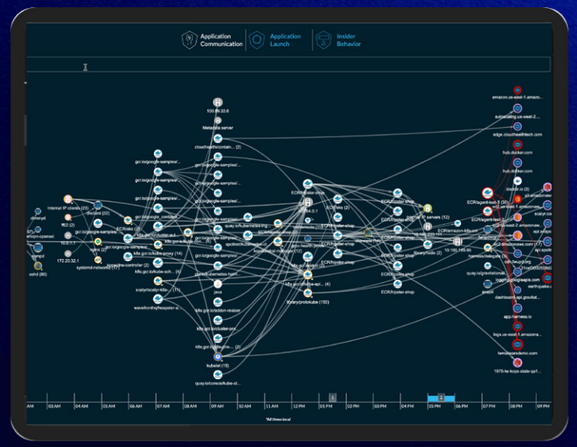
An organization can inadvertently make a mistake at the console level of a cloud environment. Simple mistakes, like leaving an S3 bucket open to the public, can invite hackers to easily exploit the misconfiguration, leading to breaches and data loss. Look for a solution that will collect the right information, at the right time, for the best visibility into your multicloud environment.

Nine must-haves for multicloud security



1. **Utilize** a layered agent-based and agentless approach to effectively gather the right information and understand what's happening in your cloud accounts and on your cloud compute systems — with continuous activity monitoring
2. **Support** inventory of resources and check configurations against cloud best practices, like CIS Benchmarks
3. **Assess** risk within the context of your organization without reliance on manual rule-writing engines
4. **Monitor** ongoing activity on all cloud platforms, across both the control plane and workload levels, to identify vulnerabilities in hosts and containers
5. **Automate** detection with analysis that correlates data and behavior to assess security posture
6. **Reduce** alert noise from hundreds or even thousands to a handful of high fidelity alerts per day
7. **Speed** decision-making with context-rich visualizations and alerts for faster investigation, triage, and remediation
8. **Simplify** operations and maintenance with a platform that acts as an extension of your team
9. **Integrate** easily with existing workflows and systems like messaging, incident response, and security information and event management (SIEM) solutions

LACEWORK



Ready to chat?

Request a demo

Lacework delivers security and compliance for the cloud generation. The Polygraph® Data Platform is cloud-native and offered as-a-Service, delivering build-time to run-time threat detection, behavioral anomaly detection, and cloud compliance across multi-cloud environments, workloads, containers, and Kubernetes. Trusted by enterprise customers worldwide, Lacework significantly drives down costs and risk, while removing the burden of unnecessary toil, rule writing, and inaccurate alerts. Lacework is based in San Jose, California, and backed by Sutter Hill Ventures, Liberty Global Ventures, Spike Ventures, the Webb Investment Network (WIN), and AME Cloud Ventures.

`Get started at www.lacework.com`

LACEWORK®

1 State of Cloud Security Report, 2021 (92%)

2 Clearpath Strategies & Lacework Cloud Security Study, 2021 (88%)

3 Gartner Hype Cycle for Cloud Computing, 2021 (76% stat)

4 Research Shows the Move to Modern Multicloud Environments Has Broken Traditional Approaches to Infrastructure Monitoring (acrofan.com)