ConductorOne

Overcoming Common Multicloud Security Challenges

Businesses are increasingly shifting their cloud strategy to align with a multicloud approach. This means that their infrastructure is split across different cloud platforms but still works together with the help of events, APIs, and cloud-agnostic tools for infrastructure as code (IaC), secrets management, and orchestration, among other things.
On the one hand, adopting a multicloud approach helps businesses get the most out of the offerings from different cloud platforms. On the other hand, it also introduces various security and management challenges that must be handled for a successful multicloud posture. This article introduces some of those security challenges and how you can use multicloud best practices to address them head-on.

Multicloud Security Challenges

Multicloud environments empower developers and engineers to use a broader range of resources. At the same time, they also bring challenges from the individual cloud platforms and create new ones specific to the multicloud setup. Many challenges relate to identities, access control, security, governance, and so on. The following sections highlight some of the most prominent challenges.

Data Protection and Privacy

Data protection is a foremost concern for businesses in light of the growing regularity of data breaches. With a multicloud setup, there will undoubtedly be some cross-cloud data movement. The data must be encrypted in transit and at rest to ensure data security across clouds. You need strict access controls on data to comply with any data protection regulations.

Moreover, many businesses, such as banking institutions, NBFCs, trading platforms, news organizations, and government departments, might have data residency and sovereignty requirements. Some of the common examples of such regulations are the GDPR, the CCPA, and HIPAA. You must ensure that your multicloud strategy has proper tooling to coordinate and monitor any potential breach of these requirements.

Identity and Access Management (IAM)

Although the conceptual foundations for identity and access management (IAM) are more or less the same across cloud platforms, there are slight differences in implementations. Though the differences are minimal, it's still difficult to translate one cloud platform's policies to another or have uniform policies, especially if you must also integrate with on-premise systems. To solve this problem, you can use distributed multicloud identity management (DMIM) and customer identity and access management (CIAM). DMIM allows you to manage identity for internal applications and components, while CIAM lets you manage identity consistently for customer-facing applications. Both DMIM and CIAM abstract away vendor-specific implementation of identity using standards like OIDC and SAML, allowing you to work with various cloud vendors and tools.

Network Security and Segmentation

Every major cloud platform provides several layers of network security based on similar concepts in networking, such as VPCs, subnets, NACLs, and security groups. However, networking gets trickier when you create network segments and microsegments using these layers in a multicloud setup to create a distributed network infrastructure. For instance, two common problems when integrating multiple clouds are overlapping CIDR blocks and conflicting private IPs.

The same is true for network security. Although network security tools are similar, they are implemented quite differently, and they create a lot of new problems when they're merged and expected to work together seamlessly. Examples of such tools are AWS Shield, Azure DDoS Protection, Azure Firewall, and AWS WAF.

Compliance and Regulatory Requirements

Compliance and regulatory requirements have taken center stage in recent years, given the breaches involving the most sensitive data, including medical data, government cables, credit card numbers, and more. In March 2023, a data breach at PharMerica impacted over 5.8 million customers. The data included sensitive identity- and health-related information. Such repeated incidents have driven governments to put in place stringent compliance and regulatory requirements. Breaching these could result in huge fines and legal action, with an offending company possibly ending up bankrupt.

Some of the widely recognized compliance and regulatory certifications include PCI DSS, HIPAA, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171. A business must ensure that all the cloud platforms in its multicloud environment have the required compliance readiness for these certifications.

Cloud Provider Heterogeneity

Different cloud providers have heterogeneous security capabilities, features, and configurations. Managing infrastructure, access, and networking across heterogeneous services and cloud providers requires multicloud expertise. Despite the heterogeneity, maintaining a consistent security posture in your multicloud setup is a must.

Cloud provider heterogeneity also refers to the differences in types of infrastructure resources and PaaS offerings. For instance, not all cloud platforms would support similar processors, disk IOPS, RAM speeds, etc. This can lead to confusion about the availability of such resources, cost control, and infrastructure management.

Interoperability and Integration

To have interoperability between cloud platforms, you must ensure secure communication with the help of various tools and techniques, such as site-to-site VPNs, secure endpoints, direct connections, and secure data transfer and sharing options.

On top of cloud interoperability, you can also have application-level interoperability, which is another way of saying that you have service-level integration between cloud platforms. For instance, you'd integrate services across cloud platforms—such as Azure Kubernetes Service (AKS), Google Kubernetes Engine (GKE), and Amazon Elastic Kubernetes Service (Amazon EKS)—that are based on the same underlying technologies, such as Kubernetes. Another example would be having a disaster recovery and backup plan for your databases by enabling cross-cloud replication and hot standbys.

Incident Response and Forensics

Managing incident response is challenging in a multicloud approach because all cloud platforms have their own separate security logging, observability, and alerting mechanisms. For the same reasons, conducting forensic investigations into suspicious activity is also very difficult. To collect and respond to observability data, you need centralized logging and monitoring to fetch data from all your cloud environments.

A centralized logging and observability tool will give you complete visibility into your infrastructure. That tool must provide you with an integration and an aggregation layer to provide a consolidated view of audit logs and trails from all your infrastructure across cloud platforms and on-premise infrastructure. With a singular view of all your logs, traces, and other observability data, monitoring and investigating incidents will become far easier.

Vendor Lock-In and Dependency

In a wholly cloud-based setup, cloud services are the foundation of the infrastructure that runs all applications, services, databases, and the rest of your business. If you're using multiple cloud providers and build your security posture around any of their premium features, you may end up locked in to a cloud provider's unique and proprietary service offering.

Some of the services, especially those based on open source or open core projects, allow you to port from one cloud provider to another, but that's not true for many services. Therefore, one of the main challenges involves ensuring that such cases are avoided. Or, if you're still getting locked in, the reasons to do so must be clear and concise.

Multicloud Security Best Practices

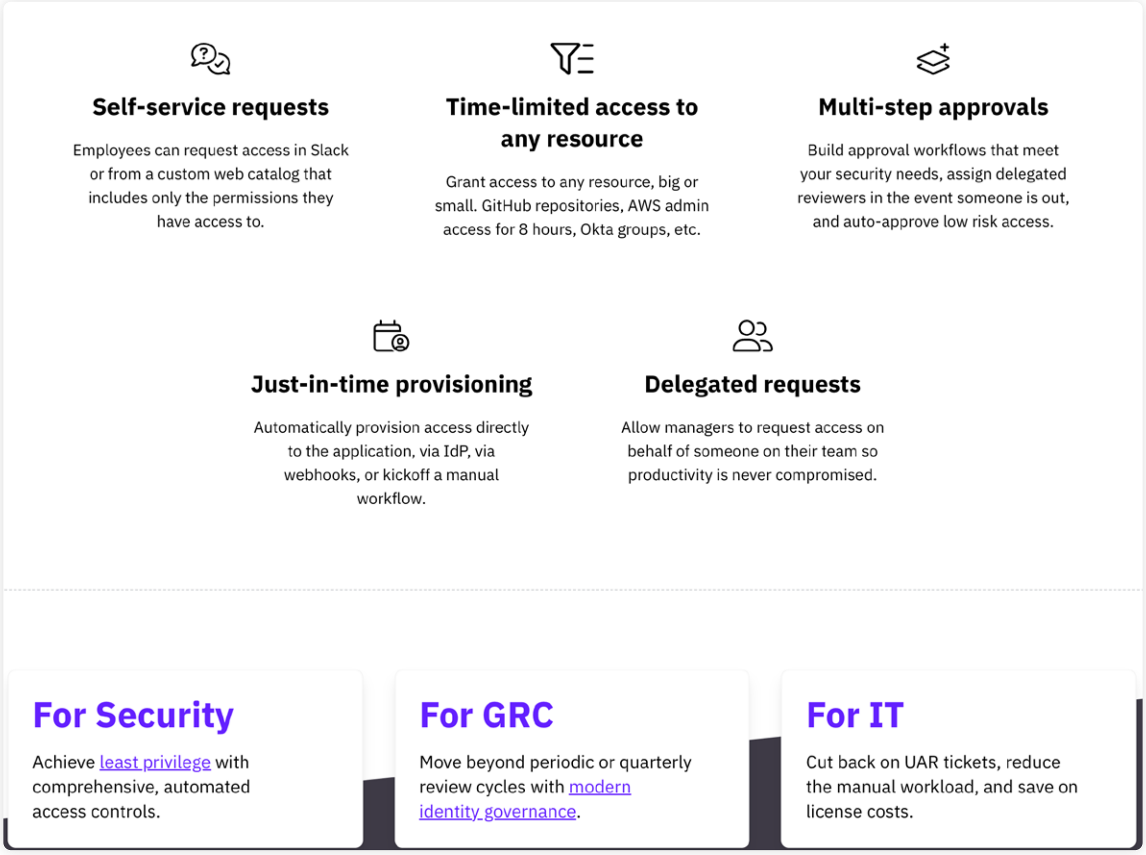
Now that you've seen some of the challenges of a multicloud setup, let's look at some of the security best practices that can help mitigate or eliminate some of the security and privacy risks.

Consistent Security Policies

Consistently defined security policies are essential for a robust multicloud security framework. Though every cloud provider will have its specifications for security management, data classification, encryption standards, and lifecycle management, you'll need to find a way to align and manage them effectively. A good test of consistency in security policies is to identify how reusable and transferable policies are between different cloud platforms. Can they be reused across cloud platforms with minor syntax and nomenclature changes? This level of consistency strengthens your security posture and saves you from redoing work when moving resources and workloads from one cloud platform to another. ConductorOne provides this consistency with several integrations across cloud platforms and tools. For instance, if you have your infrastructure split across AWS and Google Cloud, you can run user access reviews (UARs) and enforce just-in-time (JIT) access requests consistently across both cloud platforms.

Centralized and Robust Identity and Access Management (IAM)

IAM is one of the most important facets of cloud engineering. It's easy to get wrong, especially in a multicloud and hybrid environment. A good IAM solution should be centralized and able to manage identities, roles, groups, and permissions across multiple cloud platforms. Adding SSO and MFA on top of that will provide enhanced security. To ensure your multicloud approach is a success, you'll need a robust identity and access management solution that enables self-service cloud access across cloud platforms, just-in-time zero-touch provisioning, automated access reviews, and privileged access management. ConductorOne supports all these features out of the box. It also provides solutions and playbooks for established IAM patterns, such as enabling least privilege access and identity governance. You can do all of this with ConductorOne's out-of-the-box integrations. For instance, the Google Cloud Platform (GCP) integration works as a separate Google Cloud project where you assign ConductorOne permissions to APIs like the Identity and Access Management (IAM) API, the Cloud Resource Manager API, the Cloud Asset API, and the Admin SDK API, which let you manage identity in an automated fashion. The AWS integration in ConductorOne works the same way but with AWS-specific workflows for setting up the integration. Once you've set up the integration, the experience of automating UARs and JIT access requests is consistent, which emphasizes the value of a tool like ConductorOne. There are many other integrations across identity management, security, infrastructure, and DevOps that you can utilize to solve multicloud identity and security challenges in a consistent and coherent manner. You can check all of these integrations out in the integrations library.



Self-service requests

Employees can request access in Slack or from a custom web catalog that includes only the permissions they have access to.

Time-limited access to any resource

Grant access to any resource, big or small. GitHub repositories, AWS admin access for 8 hours, Okta groups, etc.

Multi-step approvals

Build approval workflows that meet your security needs, assign delegated reviewers in the event someone is out, and auto-approve low risk access.

Just-in-time provisioning

Automatically provision access directly to the application, via IdP, via webhooks, or kickoff a manual workflow.

Delegated requests

Allow managers to request access on behalf of someone on their team so productivity is never compromised.

For Security

Achieve least privilege with comprehensive, automated access controls.

For GRC

Move beyond periodic or quarterly review cycles with modern identity governance.

For IT

Cut back on UAR tickets, reduce the manual workload, and save on license costs.

Image courtesy of ConductorOne

Encryption and Key Management

Regarding cross-cloud communication, data encryption at rest and in transit is crucial. It's essential to have consistent encryption standards, key management practices, key lifecycle policies, and key backup strategies across cloud platforms.

An excellent way to ensure consistency is by using dedicated key management services or hardware security modules (HSMs). These services usually have the same features across cloud platforms. Some features include symmetric and asymmetric encryption, FIPS 140-2 Level 2 certification, encryption modes, and key sizes.

Network Security and Segmentation

Enforcing a network security standard across a multicloud setup involves mapping cloud services with similar offerings and finding ways to integrate them wherever required. Implementing network segmentation and enforcing firewall rules are two other important aspects of controlling the inflow and outflow of traffic.

Having VPCs and VNets designed to be consistent across platforms is crucial for cross-cloud communication. For instance, you must ensure your VPC CIDR ranges don't overlap and that your gateway endpoints are correctly configured.

Logging, Monitoring, and Auditing

To ensure full visibility into your multicloud setup, you'll need to implement a comprehensive logging, monitoring, and observability solution that captures and analyzes audit logs, database logs, flow logs, API logs, and other security-related logs from all cloud platforms.

You'll need to utilize security information and event management (SIEM) tools to centralize monitoring and threat detection. These tools can use the same rules to detect and block attacks across all the cloud platforms in your multicloud environment.

Regular Security Assessments

As a best practice, you must strengthen security by conducting audits and assessments to identify security vulnerabilities, violations, and threats. This involves network testing your infrastructure for leakages as well as penetration testing by simulating security attacks. Some of these tests include using tools like a reachability analyzer and a network access analyzer. You can also write custom tests designed for these audits and assessments.

If successful, these assessments will result in you identifying gaps in your cloud security framework. To ensure continuous protection against vulnerabilities and attacks, you can implement vulnerability management programs that enable you to detect, categorize, fix, and prevent the highest-priority issues.

Cloud Security Training and Awareness

Cloud security is still an evolving subject. Many engineers who interact with cloud platforms for data, AI, ML, application development, and other use cases aren't fully aware of many of the security risks in a cloud-based setup. The key is to have a security baseline framework that everyone interacting with the cloud should be aware of and be trained on.

You can conduct regular security training and awareness programs to enable this, mainly focusing on best practices in multicloud environments. You also need to foster a culture of responsible cloud usage regarding security, like you do regarding cloud cost.

Third-Party Security Tools and Services

As mentioned at the beginning of the article, multicloud setups are becoming more prevalent by the day. Hence, there's a healthy third-party security tooling landscape that you can use to centralize, simplify, and secure your environment.

For instance, you can implement a cloud access security broker (CASB) for enforcing policies around data security and compliance. You can also use some of the cross-cloud backup and data loss prevention solutions.

Conclusion

This article introduced some common challenges and best practices for security when working with a multicloud environment. It also took you through some of the tools, technologies, and frameworks you can use to improve your organization's security posture.

ConductorOne, with its self-service access, just-in-time zero-touch provisioning, and access review features, makes a great addition to your multicloud setup. It's built to solve the inherent problems in such environments, such as mismanaged identities, overpermissioned users, orphaned accounts, and discretionary access. Try it out to solve these issues in your multicloud setup today!