Securing the Clouds

Safeguarding your network in a multicloud world

InterCloud

www.intercloud.com

Securing the Clouds

To deliver the true value of the cloud, enterprises must consider new ways of safeguarding their network in the multicloud era.

Executive summary

The rapid adoption of multicloud strategies by enterprises has unlocked agility, scalability, and cost efficiencies. However, these benefits come with significant security challenges that organizations must address. According to recent research, 38% of senior executives surveyed are expecting cloud-based security threats to significantly affect their organization in 2023 as compared to 2022*.

Traditional network approaches often struggle to meet the complexity of multicloud security, compounded by growing security threats and compliance concerns. In the same survey, 31% of senior executives state that they expect attacks against cloud management interfaces to increase significantly.

So, what are leading enterprises doing to embrace multicloud infrastructures securely? This InterCloud white paper identifies critical issues, discusses current solutions, and explains why a centralized approach to cloud connectivity management can eliminate the complexity in securing your cloud.

*PwC | Digital Trust Insights survey | February 2023
Gartner | Is the Cloud Secure? | October 10th, 2019, | Kasey Panetta

The multicloud security challenge

Enterprises are embracing multicloud strategies to unlock agility, scalability, and cost efficiencies. However, alongside these benefits, multicloud environments present significant security challenges that enterprises cannot afford to overlook.

Network visibility and control

The lack of network visibility and control in multicloud environments presents a significant problem for organizations with recent Gartner research attributing 99% of cloud security failures to customer negligence. In these cases, it is the user, not the cloud provider, who fails to effectively manage the necessary controls to safeguard organizational data.

The absence of centralized visibility hinders security teams from efficiently detecting and responding to threats. Obtaining a comprehensive view of the network becomes challenging with assets and workloads dispersed across multiple cloud service providers (CSPs). This fragmented visibility severely impairs the timely identification of anomalies or malicious activities, consequently leaving organizations susceptible to potential cyber attacks.

Furthermore, the lack of centralized control complicates the enforcement of consistent security policies and configurations across diverse cloud environments. This absence of control raises the risk of misconfigurations that could inadvertently expose critical resources or result in compliance violations.

Data protection and compliance

Maintaining data privacy and ensuring compliance with regulations in a multicloud environment presents a complex and pressing task for organizations.

The intricate nature of data flowing across global enterprise networks, to multiple clouds and across diverse geographic regions, each with its own compliance requirements, demands meticulous diligence. Organizations must undertake necessary measures to ensure that sensitive data remains adequately protected throughout its journey across the vast multicloud landscape.

One of the primary obstacles to effective data protection in a multicloud setup is the decentralized nature of such deployments. Establishing consistent data protection measures becomes exceptionally challenging due to the absence of a unified security framework across various cloud environments.

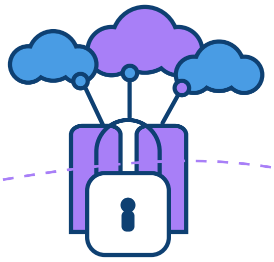
Each cloud service provider typically possesses its unique set of security controls, encryption mechanisms, and compliance standards, thereby necessitating organizations to navigate and harmonize these diverse requirements.

Identity and access management (IAM)

Fragmented identity management arises from each cloud provider having its own IAM system and repositories. This lack of a unified approach hampers enforcing consistent access controls, efficient user provisioning and deprovisioning, and maintaining a centralized view of user identities.

Different cloud providers offering diverse authorization models further complicate IAM in multicloud setups. Implementing consistent access control policies across multiple clouds becomes challenging due to varying permissions, policies, and access requirements. Coordinating and maintaining a standardized authorization framework becomes intricate, leaving organizations vulnerable to security breaches and compliance risks.

Seamlessly integrating IAM systems across multiple cloud platforms presents another major hurdle. Incompatible APIs, protocols, and identity management standards hinder smooth integration, limiting visibility into access controls and increasing complexity resulting in operational overhead and reduced efficiency.



Security integration and interoperability

Integrating security controls and tools across multiple cloud providers presents a significant challenge with each provider offering its own security solutions, leading to difficulties in establishing a unified security architecture. Inconsistent policies and lack of coordination between providers create security gaps, leaving organizations vulnerable to malicious attacks. This fragmented approach not only weakens security but also increases complexity in managing and monitoring across clouds.

The complexity and diversity of cloud environments exacerbate the challenge. Integrating unique security offerings becomes daunting, hindered by tool incompatibilities and the absence of standardized protocols for information exchange. This hampers effective coordination and threat intelligence sharing.

Ineffective security integration and interoperability can have severe consequences. Data breaches, unauthorized access, and other threats can occur due to security gaps. Limited visibility and control hinder prompt incident detection and response. Compliance with regulations and data protection standards may also be compromised, leading to legal and financial risks. Addressing these challenges is crucial for robust protection of sensitive data and systems in multicloud environments.

Challenges and limitations of traditional network security approaches

Despite the growing popularity of multicloud architectures, traditional approaches to network security encounter various challenges and limitations that hinder organizations from fully leveraging the benefits of the multicloud era.

Lack of neutrality and flexibility

Many traditional approaches to network security are tied to specific cloud providers or suffer from a lack interoperability between different clouds. This lack of neutrality restricts enterprises from reaping the benefits of adopting a multicloud strategy which is why organizations need cloud-agnostic solutions that enable them to choose and integrate multiple cloud providers seamlessly, with a consistent security posture.

Inability to meet varying connectivity requirements

Enterprises often face diverse connectivity requirements when adopting multicloud architectures. Traditional approaches struggle to accommodate the different networking protocols, bandwidth options, and performance levels required by various cloud providers. Organizations need network security solutions that can adapt with them as their business shifts, ensuring optimal performance and reliability across their multicloud environment.

Complexity and lack of certainty

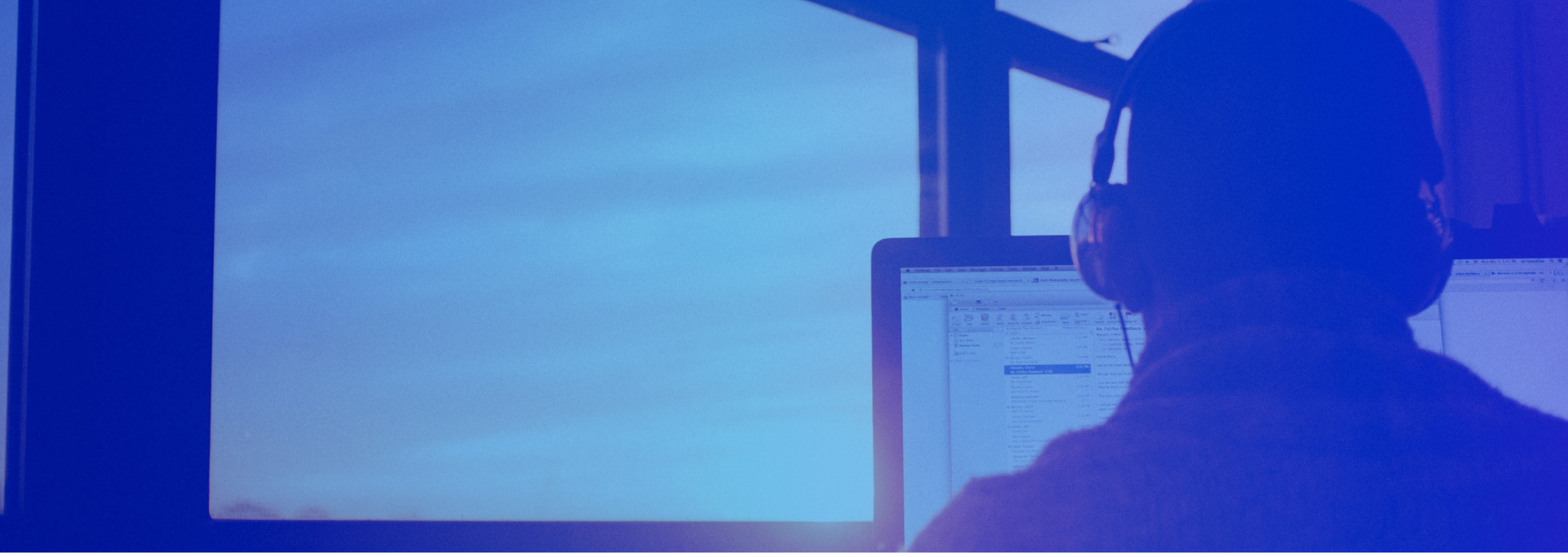
Managing security in a multicloud environment can be complex and challenging. Traditional approaches lack the simplicity and certainty enterprises seek. Enterprises require a centralized and comprehensive connectivity solution that simplifies management, and need their network provider to ensure existing security postures can be easily integrated as they connect to different clouds, from different locations.

Growing network security threats

The evolution of network security threats poses a significant concern in the multicloud era. Enterprises face an increasing number of sophisticated cyber attacks, ranging from data breaches to ransomware and DDoS attacks. Traditional approaches may struggle to keep pace with emerging threats and lack the necessary defenses to safeguard multicloud environments effectively. Enterprises need security assurance at the network level that offers real-time threat detection, proactive risk mitigation, and continuous monitoring to protect their critical assets.

Compliance and sovereignty concerns

Meeting compliance requirements and ensuring data sovereignty are paramount for enterprises operating in the multicloud era. Traditional approaches often lack the necessary capabilities to address complex regulatory frameworks and regional data privacy laws. Enterprises need a network infrastructure that enables them to maintain compliance, manage data residency and transit, and adhere to the regulations applicable to their specific geographic locations.



The benefits of a centralized managed connectivity approach

An end-to-end approach for cloud connectivity addresses the challenges of multicloud security comprehensively – providing consistency, simplified management, scalability, and enhanced visibility, empowering organizations to effectively secure their multicloud environments while maintaining control and agility in their operations:

Consistency and control

A centralized platform provides a unified view and control over security policies, enabling consistent enforcement of measures across multiple cloud platforms. This ensures that security practices remain aligned with organizational policies and regulatory requirements.

Simplified management

Managing security policies becomes more streamlined and efficient with an end to-end-cloud connectivity partner. It reduces the complexity of managing multiple security systems and enables policy changes to be implemented consistently across the entire multicloud environment.

Scalability and flexibility

A centralized, software-defined approach allows organizations to scale their cloud infrastructure and security operations seamlessly. As the multicloud environment expands or changes, a centralized platform for network connectivity can adapt to accommodate new cloud providers and security requirements without significant disruptions.

Enhanced visibility

With a centralized cloud connectivity platform, organizations gain better visibility into security events, threats, and compliance posture across the multicloud environment. This increased visibility enables proactive threat detection and rapid response to potential security incidents.

The InterCloud advantage:

InterCloud's end-to-end global connectivity platform eliminates the complexity in securing cloud connectivity, giving businesses full control over the security, sovereignty, and performance of their critical data traffic with complete peace of mind.

InterCloud's platform, along with its end-to-end cloud connectivity services deliver:

Secure and reliable data exchange across multiple cloud

InterCloud's global private backbone eliminates the need for data to traverse over the public internet. This feature ensures enhanced resilience and security, safeguarding your valuable information.

By leveraging advanced encryption protocols, secure tunnels, and traffic filtering mechanisms, InterCloud ensures secure and reliable data exchange, and confidentiality of customer traffic between multiple clouds – guaranteed by SLAs. Additionally, InterCloud offers robust security measures to protect data from unauthorized access or breaches, ensuring customers maintain control over their data even in distributed cloud environments.

Integration of security across services

InterCloud enables enterprises to adopt a centralized and standardized approach to network security management. Organizations can enforce consistent security policies, access controls, and threat detection mechanisms across different cloud platforms. Through its centralized platform, InterCloud provides customers with complete control and visibility over their network, allowing them to adopt enterprise security policies and minimize threats across multiple cloud environments.

Simplified multicloud connectivity

With InterCloud, organizations can connect to multiple clouds via one platform with connectors to interface all CSPs that supports business continuity. This consolidated approach simplifies network architecture, reduces complexity, and improves overall network performance. InterCloud also offers a wide range of connectivity options, including private connectivity, service hubs, and managed peering. This flexibility allows customers to tailor their connectivity solutions to meet specific requirements.

Advanced threat detection and mitigation

InterCloud's solution is designed with strong security measures to protect data from unauthorized access or breaches and continues to develop with a Zero Trust approach. It's agnostic multicloud platform leverages advanced threat detection and mitigation techniques. By analyzing network traffic, InterCloud distinguishes between legitimate and malicious activities – filtering good / bad traffic before it reaches the customer – reducing the risk of cybersecurity breaches and unauthorized access to sensitive data.

Increased visibility and control

InterCloud enhances visibility and control over multicloud environments through APIs and telemetry. Organizations gain real-time insights into network traffic, security events, and compliance posture. This enables efficient management of security policies, access controls, and compliance requirements across different deployment locations and capacity additions for applications and services. InterCloud also ensures stringent service level agreements (SLAs) for service availability, network performance, and repair time, demonstrating their commitment to delivering high-quality services for business-critical applications.

Managed end-to-end service:

InterCloud provides a comprehensive managed services solution, offering end-to-end management of network connectivity from site to cloud. This means that customers can have peace of mind, knowing that InterCloud's expert team will handle the intricacies of network management and continuously monitor, track, and update as security threats evolve. The ability to manage network connectivity comprehensively ensures that customers can focus on their core business while relying on InterCloud's expertise for a secure and efficient cloud connection.

Summary

In today's cloud environment, applications can be hosted anywhere, and network data flows can traverse multiple boundaries, including those of cloud service providers and enterprise networks. To effectively control, secure, and manage data across these boundary-crossing networks, enterprises require a new type of connectivity solution – a centralized architecture with software-defined capabilities. This solution must seamlessly connect disparate resources while maintaining control, visibility, and security over network connections.

One of the key advantages of a centralized platform is enhanced visibility, enabling rapid response to threats and security concerns as they arise. Organizations can gain a comprehensive view of their multicloud traffic, can quickly respond flag anomalies or malicious activities, and take immediate action to mitigate risks. This level of visibility is crucial in today's threat landscape. By adopting a centralized cloud connectivity platform, organizations can enforce unified security policies across multiple cloud providers, ensuring consistent protection and compliance with regulations. Streamlined management processes enable efficient policy changes and reduce complexity. The platform's scalability and flexibility allow organizations to adapt to changing cloud environments without disruptions.

InterCloud's centralized managed cloud connectivity platform offers a robust solution to address multicloud security challenges. It ensures secure and reliable data exchange across multiple clouds, integrates security across services, simplifies multicloud connectivity, and provides advanced threat detection and mitigation capabilities. Additionally, InterCloud enhances visibility and control over multicloud environments, empowering organizations to effectively secure their critical assets.

In the era of multicloud adoption, a centralized cloud connectivity platform like InterCloud is not a luxury; it is a necessity. Organizations that embrace this approach will gain a competitive edge, ensuring the protection of their sensitive data and systems while leveraging the benefits of multicloud strategies. Stay ahead of the curve and safeguard your network in the multicloud world with InterCloud organization – making global connectivity a driver for business performance.

InterCloud

About InterCloud

InterCloud's end-to-end global connectivity platform eliminates the complexity in deploying the cloud, giving businesses full control over the security, sovereignty, and performance of their critical data traffic with complete peace of mind.

Working with organisations to help them transform global connectivity, reduce network complexity, and accelerate growth and innovation, InterCloud is a trusted advisor to some of the world's leading brands when it comes to leveraging the cloud for future success.

With offices across Europe, the company's platform is underpinned by its team of cloud experts who guide customers to implement effective strategies to leverage the power of the cloud across their organization – making global connectivity a driver for business performance.

www.intercloud.com