Network, Meet Cloud; Cloud, Meet Network

The widely believed notion that the network and the cloud are two different and distinct entities is not true. While it may have been so 10 to 15 years ago that the network was an on-prem architecture that operated independently and required different solutions or protections separate from the cloud, that is no longer the case.

While many organizations have embraced the cloud as part and parcel of their network infrastructure, some companies are still evolving. And it is easy to see why. On-prem architecture ensures that your team has full control over your network, right down to the wire. With appliances, you essentially have one built-in inspection point, you can buy routers and firewalls and then segment everything behind the scene. With the cloud all of this is gone; you lose some of these controls in that your network is not neatly contained within a physical infrastructure. You spin up your resources wherever you want – in other regions, other countries – and in doing so, the choke point you once relied on in the on-prem environment, is now multiplied across many different access points.

There is comfort in having the control provided with managing an on-prem-only network. But this approach is no longer tenable. As organizations grow, dropping in appliances at every site or datacenter is expensive and often requires additional resources and manpower to set up and deploy.

Cloud services offer the ability to scale resources up or down based on demand. This flexibility is critical for handling varying workloads and ensuring network resources are

efficiently utilized and security measures are properly deployed. AWS, Azure and other cloud environments all have great ways to protect, but visibility becomes an issue. You lose the control to dive into packets or you pay a premium to have the ability to do this.

Organizations must rethink ways to jointly achieve both visibility and security for networks that are not one-size-fits-all. A comprehensive security strategy that encompasses both on-premises, multi-cloud and hybrid environments. This strategy should include regular risk assessments, security policy enforcement, continuous monitoring and threat detection, and incident response mechanisms. Collaboration between CloudOps and SecOps teams to ensure a holistic security approach is critical, along with implementing security solutions that are designed for multi-cloud environments.

Cloud-native security solutions that combine network metadata with context from third parties can provide a better understanding of what is happening on the network and in a way that teams can visualize the data and know which actions to take.

It’s important to note that the perceived separation between network and cloud can vary widely from one organization to another and may evolve over time as technology and business needs change. Many companies are gradually adopting a more integrated approach, where network and cloud resources are managed holistically to maximize efficiency, scalability, and agility while meeting specific business requirements.

Advertisement. Scroll to continue reading.
https://www.securityweek.com/network-meet-cloud-cloud-meet-network/