

Securing the Chaos – Harnessing Dispersed Multi- Cloud, Hybrid Environments

The move to the cloud started years ago but adoption, especially at the enterprise level, suddenly exploded in the last three to four years. The ability with the cloud to pivot quickly to support the needs of remote workers and reach customers and partners wherever they are with what they need, has kept organizations moving forward amid unprecedented disruptions.

The cloud has become a growth and innovation engine, with most organizations optimizing outcomes by embracing multi-cloud strategies. The *Flexera 2023 State of the Cloud Report* found that 87% of organizations have a multi-cloud strategy and even in the face of economic uncertainty, 45% of organizations plan to increase their usage and spending and 45% plan to stay the same as planned.

There are several reasons why organizations are choosing multi-cloud, including:

- **Business resilience:** Diversity has been a tenet of network infrastructure design for decades and has served us well. When so much of business operations and innovation relies on the cloud, using the same approach to mitigate risk in the cloud makes good business sense. No cloud service provider (CSP) is perfect; they all experience outages. So, best practice for enterprises is to spread the risk across multiple infrastructures.
- **Best of breed capabilities:** Different clouds have different strengths in different areas. Development

teams may find one application is better suited to be built in one cloud than another. And SaaS is driving many organizations to use numerous providers to address a specific IT or business need. In fact, 81% of organizations are using six or more SaaS-based applications for communications and collaboration alone according to *Enterprise Strategy Groups' Research Report, Unified Communication and Collaboration Integrations for Modern Business Workflows, February 2023*.

- **Speed to market:** Building applications on-premises is a heavy lift these days with the need to order hardware and add power and bandwidth. Even virtual machines are still typically built on-demand and require capacity planning. So, when organizations need to accelerate service delivery, the cloud is a huge enabler to speed time to market. Developers can spin up new cloud instances in minutes and get the services they need already built-in, like managed databases and managed authentication providers. Application owners can innovate and help drive strategic business initiatives quickly with a simple, convenient package.

Complexity breeds chaos

Business resilience, best of breed capabilities, and speed to market are all important reasons for a multi-cloud strategy. But the result is complexity that gets thrown on the backs of the security operations center (SOC) and operations teams responsible for securing and managing these environments. And that's the price we pay for this chaos. What's more, there are good reasons why many organizations will continue to maintain on-premises and legacy infrastructure. Particularly for organizations in highly regulated sectors, a certain portion of data will always stay on-premises. The complexity resulting from these dispersed environments and diverse tools that make up today's Atomized Networks impacts visibility and control

and, ultimately, security effectiveness.

As I've discussed before, individual CSPs can provide good visibility mechanisms for their specific cloud environments, but they don't provide a unified view across clouds or the rest of the infrastructure. So, teams move between multiple panes of glass and multiple environments to try to piece together a picture of what is going on.

Complexity carries over to the control side of things. How security and detection are defined varies from cloud to cloud and is different still from on-prem environments and what the SOC is used to. Different teams use different cloud tools alongside their traditional tools with each tool speaking a different language and offering different capabilities. This fragmentation eliminates the possibility of automation and simplicity, which makes it impossible for teams to collectively know what's happening and how to respond in a comprehensive manner across dispersed environments in anything close to real time.

In this chaotic environment, detection, investigation, and response suffer, and the net effect is that security effectiveness takes a major hit. Perhaps this helps explain why the latest FBI Internet Crime Report released by the Internet Crime Complaint Center (IC3) finds that the total financial losses from cybercrime in 2022 jumped to \$10.3 billion from \$6.9 billion in 2021. Loss of visibility and control translates into more gaps where attackers can hide and inflict more harm.

Necessity is the mother of invention

The good news is the security industry has been through this cycle before. Any time technology evolves, people identify a problem and then new approaches are introduced to address the problem. As networks have become atomized, SOC and operations teams are expected to secure and manage what used to be and

what's new with a patchwork of tools, which is detrimental to their effectiveness. And when something is detrimental to an organization's security team, that's a very dangerous place to be.

What's needed is a new approach that is architected for diverse environments. When every environment is treated the same, teams get consistent visibility, a unified view, and one common language to describe what's happening for real-time detection, investigation, and response across dispersed multi-cloud and hybrid environments. It's the only way to secure the chaos – a chaos that's critical to business success moving forward.

Securing the Chaos – Harnessing Dispersed Multi-Cloud, Hybrid Environments