KOVRR
Cyber Decisions. Financially Quantified.

www.kovrr.com

What Keeps a CISO Up at Night? Managing Multi-Cloud Environments

MAY 2022

With businesses making the shift from on-premise to cloud computing environments, chief information security officers (CISOs) have had to adapt their security strategies to align with new technologies, new processes and ensure IT employees have the skills to keep their organizations secure in this new era.

But it's typically not just a matter of switching from one on-premise data center to one cloud service provider. CISOs also have to deal with the reality that enterprises often use multiple cloud providers like Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP) together.

In fact, 89% of those involved with cloud usage at their organizations say they have a multi-cloud strategy, and 80% use a hybrid cloud model (with both public cloud and private cloud adoption), according to a global survey by Flexera, an IT management software provider.

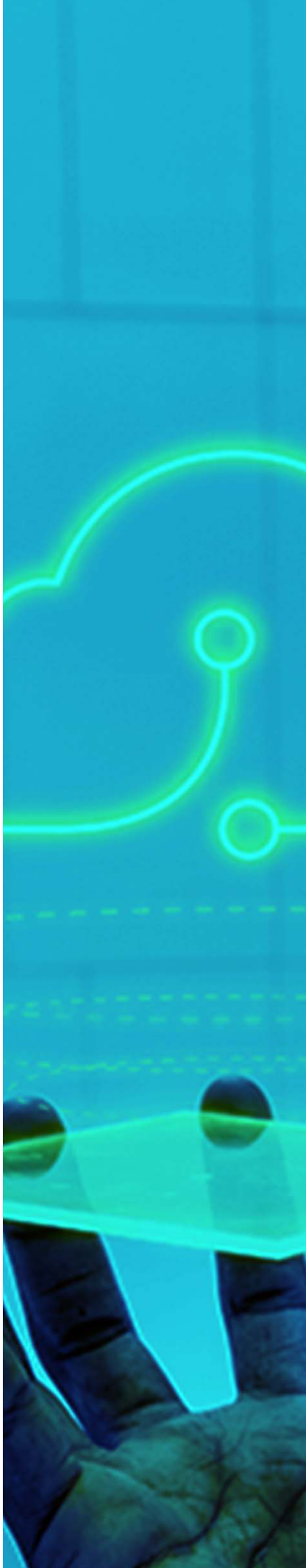
This multi-cloud approach can provide benefits, with companies going this route to increase flexibility and reduce the risk of being locked in with one cloud vendor, explains Gartner. "The decision may be driven by a variety of factors, including availability, performance, data sovereignty, regulatory requirements and labor costs," Gartner adds.

And in some sense, multi-cloud environments can strengthen cybersecurity, such as warding off shadow IT. "This problem (shadow IT) tends to arise when IT policies fail to fully meet the needs of an organization, which is where a multi-cloud environment can be effective: It allows users to benefit from chosen cloud technologies while complying with security standards," explains Citrix.

Plus, multi-cloud models can reduce the risk of downtime stemming from distributed denial of service (DDoS) attacks, adds Citrix.

That said, multi-cloud environments do require several shifts that CISOs need to stay on top of so that they can reduce the risks of storing data, managing applications and maintaining infrastructure with multiple cloud platforms.

In this series on "what keeps a CISO up at night," we're examining some of the top issues that CISOs and other IT leaders face. Here, we'll take a closer look at the challenges of multi-cloud management.



Gaining Full Visibility

When businesses use multiple cloud providers, CISOs and other key leaders might struggle to gain full visibility into everything that occurs within these cloud environments.

Only 21% of cybersecurity professionals think they have a centralized view into their "organization's security posture and policy compliance across all cloud accounts," finds a survey by Tripwire (a cybersecurity company) and Dimensional Research.

One solution is to centralize who has control over your cloud environments so qualified team members can gain the visibility and oversight your enterprise needs.

"Rather than leaving individual project teams responsible for determining their own route to compliance, a central security team provides the framework and services necessary to help all teams maintain compliance using a consistent suite of centrally managed security tools and services," advises consultancy Booz Allen Hamilton.

Organizations can also turn to cloud security solutions that scan for threats across cloud environments, giving you greater visibility and capabilities to handle threats. For example, cloud security platform Wiz explains that it "continuously analyzes your entire security stack to discover the toxic combinations that represent real risk. Cloud controls take the work out of manually analyzing siloed policies to deliver a prioritized list of the alerts that actually matter."

Handling Provisioning

Another concern that CISOs have to navigate with multi-cloud environments is how they go about provisioning these platforms. Even if cloud environments provide some security advantages, plenty of risks still exist. You need a holistic strategy to make sure IT/cybersecurity staff can establish the proper controls and permissions across multiple cloud services.

"Cloud computing offers tremendous potential benefits in agility, resiliency, economy as well as security. However, the security benefits only appear if you understand and adopt cloud-native models and adjust your architectures and controls to align with the features and capabilities of cloud platforms," notes the Cloud Security Alliance.

A key part of securely provisioning multi-cloud environments is making sure that access controls remain up-to-date and relevant, considering that 98% of U.S. companies have experienced a cloud data breach over an 18-month period, with 83% saying that at least one of those breaches related to access, according to a survey by Ermetic (a cloud infrastructure security company), conducted by IDC.

Navigating Procurement

The shift to multi-cloud environments has also meant that procurement needs have changed. CISOs need to work with other leaders such as CFOs to review areas such as the costs of various cloud platforms weighed against any perceived risk differences. Those who have yet to move forward with multi-cloud deployment or who want to add an additional cloud solution generally face more complex procurement processes than if they were to only use one cloud platform.

As alluded to, CISOs also need to consider procuring new cybersecurity solutions to detect threats (e.g., Wiz, Orca) across multiple cloud environments.

Plus, when procuring new vendors — whether that's for invoicing software, HR systems, CRM platforms, etc. — companies also need to consider those vendors' data management and cybersecurity practices. Some of those vendors could be using multi-cloud environments too, which might affect your procurement choices and risk evaluation processes.

Understanding the Financial Impact of Multi-Cloud Environments

While managing multi-cloud environments can be hard, understanding what that exposure means for your financial risk can be easy. Instead of guessing what your financial losses would be if you suffer a cloud data breach, for example, you can use Kovrr's Quantum cyber risk quantification platform to model the financial impact of hundreds of thousands of cyber events, including attacks and failures impacting the organizations' cloud environment.

By gaining clarity on your financial exposure, you can then prioritize what cybersecurity measures to take. For example, if you see that controlling the use of administrative privileges can reduce how much money you'd lose due to a cyber event, perhaps more so than if you implemented a cybersecurity awareness and training program, then you might first put more emphasis on securing your controls across different cloud environments.

Even if CISOs understand the technical aspects of cyber risk amidst multi-cloud environments, other executives might not. But if you use Kovrr's financial quantification platform to communicate what cyber risk means in dollar amounts, that can make it easier to get buy-in for your cybersecurity strategies.

> **Want to see how Kovrr can help your company financially quantify cyber risk? Book a demo with our experts today.**

KOVRR
Cyber Decisions. Financially Quantified.

The Author

Shalom Bublil

Chief Product Officer

About Kovrr

Kovrr's cyber risk modeling platform delivers global (re)insurers and enterprises transparent data-driven insights into their cyber risk exposures. The Kovrr platform is designed to help chief risk officers, chief information security officers, underwriters, exposure managers, risk professionals and catastrophe modelers understand, financially quantify and manage cyber risk by utilizing AI-powered risk models.

To learn more please contact the Kovrr team: contact@kovrr.com