The Reality of Securing Today's Enterprise Hybrid Clouds

FROST & SULLIVAN

Powering clients to a future shaped by growth

Introduction

In the third in a series of Virtual Think Tanks for DXC Technology and VMware, Frost & Sullivan Industry Director Toph Whitmore spoke with industry IT security experts with experience leading secure cloud transformations in their organizations. The group discussed best practice strategies, roadmaps, and use case examples for securing enterprise work spanning on-prem and cloud environments. Panelists included Chris Russell-Miller, CISO and Head of IT & Cyber Risk with BNP Paribas Personal Finance; Satya Pradhan, Senior Director of IT for General Dynamics Information Technology (GDIT); Sundeep Kumar, VP of Global Technology for Wells Fargo; and Peter Scott, Global Director of Security for DXC Technology.

Hybrid cloud security for CISOs: navigating a complicated patchwork of less-than-perfect solutions

Pundits often note that everyone is moving to the cloud. In reality, enterprises are already in the cloud, embracing cloud-first strategies to enable hybrid working environments and set their organizations up for scalable growth. Cloud has become a business decision, a mandate, and a strategy, and as recent Frost & Sullivan research noted,[1] organizations are pursuing hybrid- and multi-cloud strategies to support the work of their employees.

However, such broad and comprehensive enterprise digital transformation introduces new business risks. The to-be-managed enabling technology fabric now extends into the cloud and widens to encompass work-from-anywhere connectivity. IT leaders must balance organizational cloud aspiration with operational realities, a dichotomy that complicates security delivery, efficacy, and management. Securing hybrid- and multi-cloud environments can require IT leaders to integrate solutions to mitigate risk. And then they must ensure nothing falls through the cracks of a diverse, disparate infrastructure landscape.

1 The State of the Cloud 2021, 2021 Frost & Sullivan Global Cloud Survey, December 2021

The hybrid- and multi-cloud security market could be described as splintered. Though cloud service providers offer a host of management and security tools, protecting cloud instances across multiple vendors can complicate security administration. Every Zero Trust solution developer claims to support multi-cloud customer environments, yet few (read: only the largest) can provide a security platform comprehensive enough to accommodate the broad security needs of hybrid- and multi-cloud work. And even then, most enterprise IT leaders are left to wade through a morass of competing vendor claims to ensure secure working environments for their employees and secure data, resources, and assets for their organizations. Complicating matters further, many enterprise IT leaders operate under strict industry regulatory oversight that may dictate separate administration for different cloud deployments.

These complexities lead to a rather commonsense conclusion: CISOs will find value in seeking the counsel of trusted partners when they embark on a hybrid- or multi-cloud security journey.

Hybrid cloud security in the real world: new opportunities, new platforms, new risks

As this Virtual Think Thank session's panelists attested, no one-size-fits-all approach exists for securing hybrid- and multi-cloud enterprise environments. Each panelist detailed their own unique experiences securing disparate, dispersed, and diverse infrastructure. Some key takeaways:

- "Everything-all-at-once" cloud migration initiatives are bound to fail.
- Securing hybrid- and multi-cloud environments can complicate regulatory compliance.
- Third-party risk increases in hybrid- and multi-cloud environments.
- Data in motion between clouds is difficult (though imperative) to secure.
- Cloud misconfiguration is a tangible risk in hybrid environments.
- Collaboration with partners can facilitate integrating security into phased cloud migration.

"Everything-all-at-once" cloud migration initiatives are bound to fail.

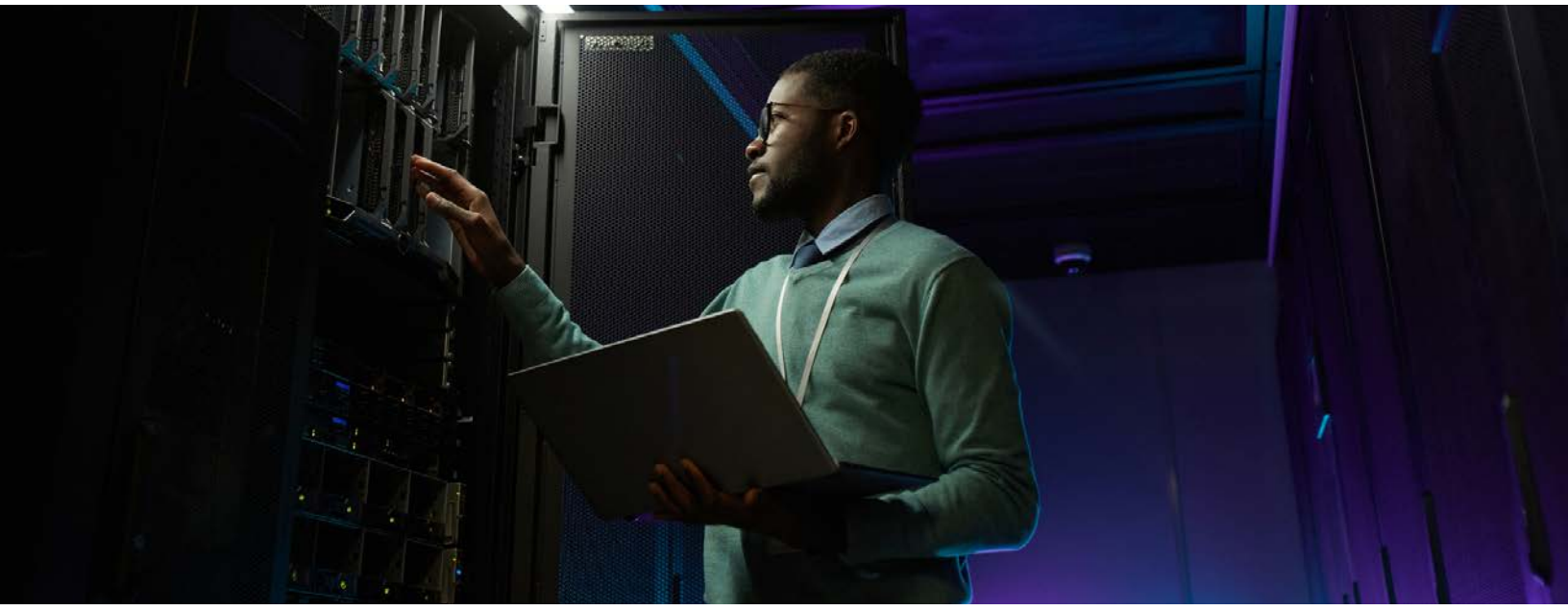
"Going full public cloud" may not be efficient for all workloads and applications. Accelerated cloud migration—the everything-all-at-once strategy—may seem constructively disruptive, but is rarely if ever practical. A common pitfall is overlooking the complexity of migrating legacy applications to the cloud.

It's good to aspire to the cloud. It's realistic to accept that moving all workloads to the cloud can't be done efficiently.

"Lifting and shifting doesn't work," noted **BNP Paribas' Russell-Miller**. "You have to substantially refactor the applications to make them cloud-aware, and in some cases, replace the application entirely. So we've taken an opportunity to get rid of some of our AS/400-type stuff. And replace it with [an] application that is cloud-ready."

Added **GDIT's Pradhan**, "Anything that worked on-prem will not work on cloud. And everything that works on cloud will not [necessarily] work on-prem…We had to start looking at security through a different lens, where we started looking at what are the different components? What works on-prem? What works on cloud? And it's pretty complex."

DXC's Scott offered a service-partner perspective: "We tend to talk about cloud-right, rather than cloud-first—so, putting the right applications in at the right time. To really get the benefit of the cloud, it's not a lift and shift. It's about taking advantage of what the cloud offers, rather than just treating it like a hosting platform."



Securing hybrid- and multi-cloud environments can complicate regulatory compliance.

Kumar from Wells Fargo advised CISOs to pay close attention to regulatory requirements during cloud migration.

"We have to make sure that whenever we are going towards the cloud, we take everything into account…data security, as well as compliance," said **Kumar**. "We are in practically every single jurisdiction. And we have to keep up with GDPR…Our aspirations are to go full public cloud. We have been working towards this. Yet, we might never reach full. We will probably have a mixture of private and public cloud and some on-prem."

Pradhan concurred. "It is very easy to fall out of compliance when you have a different mix of environments," said the **GDIT Senior Director of IT**, "because the governance standpoint that you had on-prem for your standards policies and the controls will not work on cloud."

For **Russell-Miller**, financial services-industry regulations limit where BNP Paribas can host its corporate applications, forcing the company to divide resources between clouds. In some cases, even administration must be distinctly separated for public- and private-cloud apps.

"There are lots of [our] SaaS products—Salesforce, ServiceNow—that are public cloud only," explained the **BNP Paribas CISO**. "So we are now in the process of trying to create a merged-up together, public/private cloud experience. For example, anything that's to do with traditional banking applications, the regulations do not allow it to go in public cloud, but it can go in private cloud. But a huge amount of our customer relationship management, our service portal, asset management, buildings management, vehicle-leasing solutions are all from third parties, [and] they're all public cloud. And the two [platforms] have got to work together."

Third-party risk increases in hybrid- and multi-cloud environments.

"It's pretty hard for a threat actor to break through my front door," said **Russell-Miller**. "I've got a lot of big locks on [it]. But [threat actors] can very easily come through a third-party digitally-connected supplier who is weak."

Russell-Miller's observation highlights a key challenge for CISOs looking to secure hybrid- and multi-cloud environments: it's difficult enough to integrate third-party connectivity into enterprise workflows. Adding support

for (and third-party access to) hybrid- and multi-cloud environments only complicates security for such integrations. That's especially troubling when supply chain partners, in **Russell-Miller's** words, "migrate to cloud in a potentially less-due-diligent way," something that can "open us up…to their weaknesses."

Data in motion between clouds is difficult (but imperative) to secure.

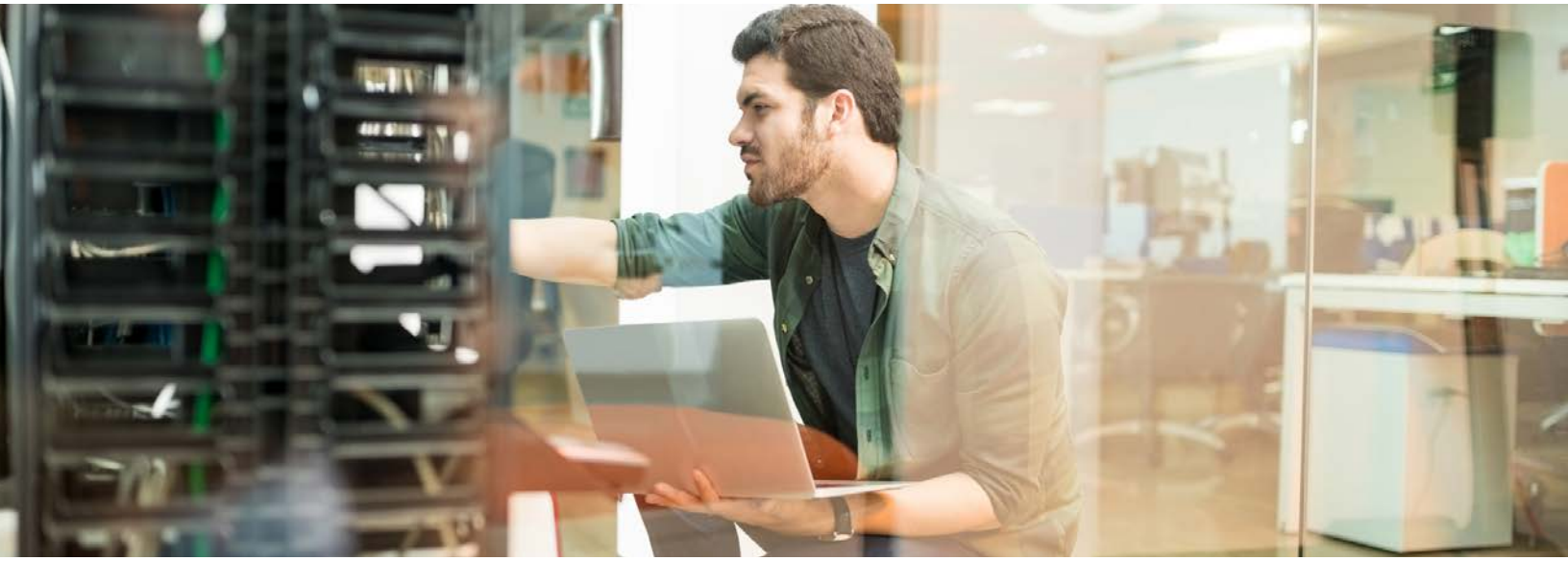
GDIT's Pradhan advised CISOs to recognize the risk of, and subsequently address "insecure cloud data transmission."

"[You have to] ensure that security gaps do not develop because of the 'hops' that you have," explained **Pradhan**. "You have something on-prem, you have something on Cloud A, and you have something on Cloud B. You have heavy data transmission going on between the three platforms…When you're transferring the data, there is a very good chance of cyberattacks. [You] have to make sure [you] have all the security modules and other cryptographic tools to make sure you're encoding all the data that you're transferring."

Cloud misconfiguration is a tangible risk in hybrid environments.

Credit skillset mismatch, cloud configuration administration complexity, or simple oversight: cloud security misconfiguration is a huge new risk, one that grows with each new enterprise cloud platform integration.

"I've yet to find the cloud data breach of any significance that was down to a technology failure," said **BNP Paribas' Russell-Miller**. "The majority of them have been due to misconfiguration, poor configuration, badly-thought-out configuration, or human error. The actual technology is pretty secure, but [the risk is] whether you've implemented it correctly. And this is where the traditional infrastructure engineering services just don't quite get it. Whereas before, if you had a slightly vulnerable server, it didn't matter. It was behind a rock-solid firewall. Now it's presented to all in sundry to have a go at. So, everything has to be as good as everything else. So we can't have risk acceptance on an unpatched server anymore, it's not allowed. We have to have total 100% compliance."



DXC's Scott also noted the challenge of ensuring strong cloud security posture management in a complex, cloud-migrated enterprise environment.

"The cloud fabric itself is very well engineered, very well secured," said **Scott**. "The mistakes that [IT leaders] make will be how [they] configure it and use it. And it's that transition from old ways of working to new ways of working [that are difficult]. And every customer we talk to, they struggle with that extra complexity. We're ending up with more complexity, more things to look after. And we know that's the enemy of security."

Collaboration with partners can facilitate integrating security into phased cloud migration.

To facilitate its journey to secure cloud adoption, GDIT established (and continues to follow) a phased "move-to-cloud (M2C)" migration framework.

"[M2C] provides a logical approach to identifying and managing all necessary activities across the necessary security planning [and] development implementation of phases of the cloud migration," explained **GDIT's Pradhan**. "We wanted this framework to be [a] repeatable, cost-effective migration methodology that supports cloud security, agile IT management, governance operations technology, the human capital, and culture to accelerate the pace of [our] move to a cloud platform. So we partnered...We made it possible through our strategic alliances with both the cloud service providers and next-generation technology providers to optimize this journey."

Pradhan and **the GDIT team** broke down their framework into three phases to evaluate workloads for secure cloud migration:

1. Discovery and access: "Discovery and assessment of the whole thing."
2. Plan and migration: "Rapidly, iteratively plan, prepare, and move workloads."
3. Operate and optimize: "Monitor and sustain and ensure the optimal workload performance."

> As part of each workload cloud journey, GDIT determines scope and cloud target, asking, "Is it a multi-cloud project or is it something that meets a hybrid-cloud approach?"

The reality of hybrid security? It's a journey, not a destination.

Doing cloud right means being cloud smart. As the panelists' unique experiences illustrate, putting hybrid cloud security into practice is an ongoing journey, not a destination. Enterprise CISOs who rush to the cloud with an everything-all-at-once approach are destined to fail. In contrast, those that seek out expert counsel and prioritize discovery, migration, and ongoing optimization for individual workload migrations will find greater success in securing disparate cloud and on-premise infrastructure.

"The cloud is different," noted **DXC Global Director of Security Peter Scott**. "You secure it in a different way. The old ways of securing on-premise infrastructure don't really apply in the same way."

Concluded **Scott**, "You can do amazing things with the cloud and that's why we're all interested in it, but you've got to deal with all of that reality…My advice is, try and plot a path that simplifies and converges, because if you're not careful, everything just gets more and more complex, more and more security to [apply], more and more things to deal with. With security…you need to make sure that you are executing [the basics] brilliantly. There's no magic source for doing that, but [then] that's the challenge in front of us all."

FROST & SULLIVAN

Growth is a journey. We are your guide.

For over six decades, Frost & Sullivan has provided actionable insights to corporations, governments and investors, resulting in a stream of innovative growth opportunities that allow them to maximize their economic potential, navigate emerging Mega Trends and shape a future based on sustainable growth.

Contact us: Start the discussion