Sponsored by
TATA COMMUNICATIONS

IDC IN CONVERSATION

September 2021

That Moment of Truth for Your Digital-First Enterprise

The moment of truth — that moment when everything falls into place, and the customer is delighted — is something most financial institutions aspire to, but few succeed in finding. The need to cater to demanding, work-from-anywhere consumers (or employees for that matter) has only added on to the need of continuously re-assessing the core infrastructure, operations, cyber risks and processes.

When asked the question, “What really are the inhibitors or limitations in achieving this epiphany or continuous moments-of-truth?”, several banking and insurance CxOs had a shortlist, namely;

- Enabling a large, remote, workforce with secure access to critical systems, databases, applications — via public networks and virtual private networks (VPNs).
- Identifying, engaging, and onboarding customers through an any channel, at any time, whilst creating a seamless, personalised experience.
- Creating a dynamic and scalable application programming interface (API) orchestration layer to leverage third-party services such as 360-degree customer views, data analytics, contact-centre solutions, omni-channel experiences and assisted selling/servicing via third parties.
- Enabling a secure and trusted ecosystem that allows digital interactions for save-borrow-pay between banks, partners, and consumers.

In response to these challenges, forward-thinking institutions have started to build a scalable and future-proof network infrastructure, one that is cloud-first, internet-enabled and highly optimised — and also very secure.

Early success stories in building such a scalable network infrastructure are nudging other enterprises to act. Standard Chartered Bank’s CIO, Michael Gorriz, disclosed to IDC on how he is moving the bank’s infrastructure, critical workloads, customer journeys, and even internal (employee) facing systems and microservices to a hybrid cloud environment, while securing the bank against cyber attacks*.

Similarly, IDC client Bank Danamon Indonesia, fully owned by MUFG, has successfully enabled thousands of its employees with the necessary toolsets and connectivity so that they can continue to onboard new retail and corporate banking customers, service existing accounts, and create a micro-services orchestration layer that caters to both internal users and customers*.

The most common question, however, for organisations planning to go down this route is, how and where do we begin, especially given what we already have in place?

Cyrus Daruwala
Managing Director
Financial Services
& FinTech, IDC

Andrew Yeong
Vice President
Customer Success Group
Tata Communications

*Source: IDC

IDC recognizes the need for a blueprint to establish key best practices and help identify markers for teams that manage the heavy lifting in these domains. IDC tied up with **Tata Communications**, a global major in technology and network services, to create this blueprint to help simplify the priorities and the processes in enabling a seamless secure digital ecosystem for internal and external customers across enterprises in the financial services industry (FSI). We hope this alleviates some challenges, identifies inhibitors, and outlines a step-by-step approach to arriving at a custom plan for multiple epiphanies across the value chain.

Cyrus Daruwala, Managing Director, Financial Services & FinTech practice at IDC Asia/Pacific, discusses the blueprint for a scalable and future-proof network infrastructure (the toolsets, the roadmap, the "how to" components) in engineering multiple moments of truth with **Andrew Yeong**, Vice President, Customer Success Group at Tata Communications.

Cyrus: Seamless cloud-to-cloud connectivity for applications and data migration seems to be the greatest single challenge cited by larger (legacy-riddled) FSIs IDC spoke with. How can these firms deal with the issue? How should they evaluate the requirements of running an application on different cloud instance?

Andrew: Good question, Cyrus. We have heard this from multiple clients — across developed economies and emerging markets. This is quite high on the list of every IT practitioner, and rightfully so.

A major step to cloud migration involves moving data to the cloud. This can be achieved by moving data bit by bit through a network that is fit for this purpose. This approach allows the business to ensure that current systems remain operational through the migration and are available while production-testing the cloud setup. We offer multiple methods to move data to the cloud:

- **Private networks like multiprotocol label switching (MPLS) VPNs or Ethernet to access clouds.** Ideally, this should be a unified platform supporting multiple technologies, available globally, and integrated with as many of the world's cloud players as possible so that it offers high performance and secure connectivity across your business network. We have our own home-bred IZO Private Connect that enables secure access to enterprises globally to Amazon Web Services, Microsoft Azure, Google Cloud, IBM Cloud, Oracle Cloud, Salesforce, Alibaba Cloud, and SAP Cloud Platform.
- **Software-based application wide-area network (WAN) in the clouds.** This is the use of software-only networking solution with application-specific performance, security, reliability, and agility across any set of networks and clouds. This gives businesses control over their networks without the need to build or manage the underlying infrastructure. For instance, the NetFoundry platform enables administrators to instantly spin up software-only, zero-trust, micro-segmented networks called AppWANs at scale using a web orchestration console and APIs. These AppWANs allow organisations to establish on-demand tunnels to the CSPs for data transfer. The software-based AppWAN can also optimise performance at the edge, thereby enhancing user experience significantly.
- **Setting up virtual router or SD-WAN in close proximity to cloud.** For organisations that deploy SD-WAN as a managed service, their managed service providers could deploy SD-WAN as virtual network functions next to the major cloud locations. For example, IZO Network Edge allows IZO SDWAN to be loaded to a virtual machine that sits next to clouds, extending the organization's WAN into the CSP's, and enabling multicloud connectivity.

Cyrus: A key concern for most financial institutions (FIs) when moving to the cloud is security. Can you help us understand the heightened need for cloud security, including secure access, secure passage, and data storage?

Andrew: Globally, enterprises are looking to move applications to the cloud. Access optimisation, changes in the security perimeter, and enabling a performance network layer are the key imperatives for CIOs everywhere. Data breaches can cost companies millions of dollars, not to mention the loss of credibility and reputation. Violations can come in various forms:

- Compromised privileged account passwords
- Viruses and Trojans from a user's bring-your-own-device (BYOD) machine
- Weak access credentials
- Protocol vulnerabilities and misconfigurations
- Unpatched devices and operating systems

On the secure access front, the traditional VPN gateway approach, which has worked well for a long time, has now come under pressure from the need for maximum flexibility and security. For example, a hardware-based gateway is limited by physical capacity, and perimeter-based security is now unable to cope with the increasing complexity of security attacks.

We, therefore, recommend the use of a multi-layer zero-trust access model, which would look at other attributes like identity, device security, and access location to ensure that only the required applications are granted access to the users.

Cyrus: Maintaining consistent security controls and policies across these networks and cloud instances, while not limiting access at the same time, seems to be the follow-on challenge. Centralised firewalls may be the answer. What are your views on deploying these?

Andrew: We have always been bullish about secure network transformation and have been working with all our customers on creating secure environments for not only lift and shift but also compute and storage. We are seeing several issues with security especially during movement and with gaps-riddled BYOD. Once apps and users move out of the protected office perimeter, anyone with credentials to the applications can freely access them from the home network.

Since the introduction of SD-WAN, much work has gone into plugging these security holes. Most vendors today offer next-generation firewall (NGFW) and unified threat management (UTM) features on the SD-WAN device to control user access to applications. These features work to safeguard user access in the office, but leave gaps when users move the access application to their home or other non-office settings.

We recommend organisations combine on-premises security with managed cloud-based security like virtual UTM, secure web gateways (SWGs), and cloud access security broker (CASB) services.

Enterprises should look to combine network management through SD-WAN, and network security (like zero-trust network access [ZTNA], SWG, firewall as a service [FWaaS] and CASB) into a converged architecture and delivered from the cloud, enabling distributed security. One that enables consistent enforcement and is easier to manage and apply as enterprises expand their branches, remote users and network footprints.

Very often, service providers can leverage their ecosystem partners to allow close service edges to enforce security measures and ensure a consistent security posture across the organisation.

Cyrus: Let's assume we have achieved all of the above here-and-now; let's look ahead to discuss a future-proof network for an ever-evolving workplace. Is there a blueprint or a framework that FIs can follow? I envision one that enables an institution to change network policies on the fly, perhaps with a self-service portal.

Andrew: Absolutely. The promise of SD-WAN has always been enhanced visibility and improved utility. Many organisations decide that a do-it-yourself (DIY) approach is more suited to them. But a DIY approach has several challenges:

- Takes a longer time to realize value
- Challenges in evaluating features
- Hard to run a comprehensive vendor selection
- Complexity in deployment planning, e.g., in data centres, monitoring, or backups
- Ability to correctly implement and enforce security controls across cloud, network, and users
- L1, L2, and L3 support resources to manage and monitor
- Data centre space, compute, and storage is expensive
- Managing different service level agreements (SLAs)
- Complex, in-house skillsets required to operate and manage the new environment, in addition to the constant updates and other fixes that need to be managed, i.e.,
  - Patch management
  - Bugs and new feature releases
  - Interacting with vendor for fixes

> “A more astute approach would be to partner with a managed service provider for an end-to-end digital enablement services that includes SD-WAN with required security controls as a critical enabler and build a bespoke model for deployment and operations.”

A more astute approach would be to

- partner with a managed service provider for an end-to-end digital enablement services that includes SD-WAN with required security controls as a critical enabler; and
- build a bespoke model for deployment and operations. The ideal service provider should be able to create a bespoke routing policy, in real time, to respond quickly to business requirements.

Tata Communications' IZO SDWAN offers a real-time self-service portal that shifts control back to the organisations, enabling a swift change in application policy, managing application definitions, and accessing analytic reports. The underlying network, Ethernet, for instance, would also allow the use of a self-service portal to change bandwidth on the fly. And being a managed security service provider ourselves, we factor the requisite security of networks in the design itself.

Cyrus: Thank you, Andrew, for speaking with us. It's been quite interesting especially given that you deal with almost all the global FSIs on the Fortune 500 list.

In Conclusion

Regardless of its digital, network infrastructure or cloud maturity, if a financial institution's KPIs are to create or augment that moment of truth in customer journeys in a compliant manner — which includes, but not limited to digital and mobile banking, secured digital payments, virtual customer service, and various highly-personalised financial products — then the **IDC-Tata Communications framework** offers a powerful approach to assist the organisation in identifying its current inhibitors and in enabling it to achieve that future-proof enterprise status.

ABOUT THE FEATURED ANALYST AND EXECUTIVE

Cyrus Daruwala

Mr Daruwala is the Managing Director for IDC Financial Insights. Cyrus Daruwala and his teams focus on all aspects of "run the firm" or "change the firm". His research and advisory practices cover banking, insurance, and capital markets and topics such as legacy modernisation and transformation, hybrid cloud, big data and analytics, customer life-cycle management, digital experience, ecommerce ecosystems, Internet of Things, cognitive, blockchain, and fintech. For the past 20 years, Mr. Daruwala has been working with financial institutions to help them assess their business and operational and technical challenges, select the right vendors/partners, better understand their IT total cost of ownership, and grow their customer base.

Andrew Yeong

Mr Yeong is Vice President, Customer Success Group, APAC at Tata Communications. In his role, Andrew Yeong is responsible for the growth of Tata Communications' business across all industry verticals, focusing on providing digital transformation services to corporations in the region. He also supports the company's strategic efforts in growing and maintaining its leadership position in the network infrastructure market, as well as in building deeper penetration with its mobility, IoT, cloud enablement and cyber security solutions.

IDC Asia/Pacific
83 Clemenceau Avenue
#17-01 UE Square,
West Wing
Singapore 239920
T 65.6226.0330

IDC Custom Solutions

Doc no: AP77121X