FLEXENTIAL®

Planning a Hybrid IT Strategy for Today and Tomorrow

Authors:

Jason Carolan
Chief Innovation Officer

Tim Parker
SVP, Network Strategy

Two of the main drivers for customers adopting hybrid IT are: improving the customer experience in a highly dynamic market and providing the agility necessary to keep up with such dynamics.

During the COVID-19 pandemic, users in every dimension shifted to web and mobile online services for nearly everything. Companies that were unable to make the pivot quickly suffered more than others. Some segments are still recovering but are using this time to radically change business models to be more online-driven, contactless and secure. Hybrid IT is the key to improving innovation, application response times, security models and reliability. In general, "one-size-fits-all" models constrain developers and IT staff and don't provide all the best tools to meet demand.

Public cloud computing works great for core use cases, development, and quick scale-up and scale-down, while private cloud and edge may provide enhanced cost controls and faster response times by reducing latency.
To achieve this, consider these five elements:

- **Connectivity:** Data centers, 5G, clouds, servers, end-users, branches, edge, IoT
- **Control:** Multi-cloud capable, DevOps, management servers, portals
- **Observability:** Transparency, monitoring, response time, feedback response
- **Governance:** Application portfolio rationalization, cost management, GRC (Governance, Risk & Compliance) programs
- **Security and Assurance:** Service resilience, physical to logical security, privacy, standards, controls, regulatory data, trust

Connectivity

The first step toward hybrid adoption is connectivity. In the hybrid world, network connectivity needs to become more fluid and more application-aware. As applications span multiple cloud platforms at any one time, IT managers need a combination of network services and capabilities to provide optimized connections between users, content providers, cloud providers and branch offices. Content delivery networks work in conjunction with content providers to optimize network traffic.

IDC estimates that 20% of CIOs will adopt connected cloud architectures in 2021.

Enterprises and medium-sized businesses will continue to adopt new clouds, optimize their content needs, re-factor existing deployments and right-size applications. Data gravity will be an essential consideration in connecting new applications and driving deployments. Because of this, the flexibility and security of the network are paramount. AI and machine learning are hungry for data and can be easily impacted by additional network latency.

Many CIOs and IT leaders are making serious investments in networking to meet current and future needs. IDC estimates that 20% of CIOs will adopt connected cloud architectures in 2021; frankly, just the beginning as these issues will continue. Leaders are also making considerable investments over the next two to three years in 5G and upgraded wireless connectivity.

The importance of the user, or the "branch of one," has also increased over the last 12 months and is expected to remain over the coming two to three years. Connectivity and security of data go hand-in-hand, hence the growing consolidation of networking functions like SD-WAN and security features like VPNs. Expectations for solid APIs and "as-a-service" models will continue to grow as well, just like with everything else in IT. The industry refers to this as SASE: Secure Access Service Edge. Traditionally, SD-WAN was targeted to larger branch offices as networking overlays of multiple users. But with today's growing hybrid workforce, we can expect one or many to be solved by similar solutions, with added security features to address new risks.

According to the latest IDC forecast, SD-WAN continues to be one of the fastest-growing segments of the network infrastructure market—poised to reach $5.25 billion in 2023.[1]

- A business-driven SD-WAN eliminates the need for legacy branch routers, firewalls and costly MPLS backhaul.
- A business-driven SD-WAN makes it easy for enterprises to increase and leverage bandwidth and even run their entire business on shared, public broadband.
- A business-driven SD-WAN expedites and automates onboarding of new sites, cloud-delivered security services and applications with true zero-touch provisioning and automated service chaining. Apps/policies are consistently auto-deployed to thousands of remote locations in accordance with business intent.

Content delivery is a critical component for both public and private use and is the number one driver for increased network demand and growth. Whether the content is streaming video or critical business application data or images, the demand is part of the growing dependency on hybrid computing.

According to the latest IDC forecast, SD-WAN continues to be one of the fastest-growing segments of the network infrastructure market—poised to reach $5.25 billion in 2023.

Control

Controlling resources and applications on the cloud can be challenging in one environment vs. many. Applications have tentacles that stretch between databases and app-tiers as new use cases are solved. Enterprises struggle with planning, identifying and maintaining application dependencies, even for the most static of applications. Combine that with easy to obtain public cloud resources, and the problem gets even more challenging. It's not uncommon to hear, "I don't know what to shut down," when a leader is confronted with out-of-control cloud spend.

One solution is governance, the model and toolkit that helps enterprises better maintain application sprawl and resources. The second solution is technical (and the focus of "Control" in this paper)—the use of tools and software to help manage the platforms. These tools may be called "CMP" or "cloud management platforms," but the line is being blurred with traditional infrastructure management tools.

Observability

A vital issue for IT managers today is to understand what they have. It's also challenging to know how applications and underlying resources are performing against stressed SLAs to keep up with new customer needs. Instrumentation is necessary to help close this gap and must work across clouds, networks, providers and application tiers. Unfortunately, many monitoring platforms today are deployed on only a subset of infrastructure domains, siloed from each other.

Providers must expose underlying infrastructure layers to help IT managers correlate environment conditions, all the way to cooling and power consumption for advanced environments. Often, the developer may be in the best spot to provide this instrumentation, so it's closer to the application and its real performance. As compute-intensive applications powered by GPUs for AI/ML use cases grow, this need will continue to expand. In addition, large-scale Software-as-a-Service (SaaS) platforms desire more hardware control, being able to disable servers when not necessary.

An example of common control environment is Flexential's advanced VMware vCenter offering. This capability enables interoperability and compatibility with industry-leading third-party tools for an optimal application development environment, across cloud infrastructures.

Flexential's new single-tenant cloud offering, is the industry's only cloud offering that allows you to have complete administrative control over the provider-owned vCenter. This capability enables customers to utilize tools that require access to cloud administration domain functionality and enables a greater degree of personalization. While you will be provided with significantly more access to the cloud infrastructure, Flexential will perform the initial configuration, ensuring the solution is compliant up to the hypervisor level and provide ongoing management of the shared hypervisor.

Advanced vCenter Access also powers data protection use-cases by enabling the implementation of a custom backup/snapshot strategy using tools that the client has already invested in like Veeam, Rubrik or Zerto. It's also ideal for providing integration with DevOps tools that are critical for Continuous Integration and Development (CI/ CD) solutions like Rightscale, Terraform and Ansible.

A hybrid IT platform must tackle these areas and allow IT managers and buyers visibility into how resources are being used across physical and logical domains. Mobile devices and network-enabled platforms will also need additional instrumentation to help predict capacity or performance issues before they occur.

Governance

Successful organizations strive to balance control and autonomy, no different than being successful with hybrid IT. Cloud helps IT be much more agile with on-demand resources and the ability to deploy applications all over the world. However, it can come at a cost both in direct cost related to cloud usage and in complexity.

A good hybrid IT model involves a level of governance to ensure business needs and architecture principles are being followed. The worst-case scenario for an organization might be discovering that an important application is sitting somewhere unmanaged and uncontrolled, and managing through an unknown set of failures. Also bad is not knowing what resources map to what application and inability to disable resources (and costs) without impacting the end users.

Governance can play a significant role in ensuring the right platform is used for the proper purpose, with the correct high-level requirements to help protect the business from increased spend and risk. Enterprises should provide ground rules to support line of business and other IT consumers make the right decisions and measure how well hybrid IT is working. Most companies require ongoing optimization efforts as IT needs change.

Security and Assurance

Security continues to be a top-three concern for most public cloud IT users. As highlighted in the connectivity discussion, security models are ever-converging with IT consumption changes. As IT resources get easier to consume, the risk can increase as applications and their data span multiple

platforms and perhaps management domains. Most of the concerns surround IT skillsets in managing new public cloud deployments. Further, corporate IT's governance model may not have matured to take these issues into account.

Secondly, as more transactions occur online, the reliability of services becomes more critical—are they done timely and quickly? Building IT architectures for highly available services can be difficult, but there are many more capabilities available today than ever before. More online services mean higher expectations and more competition. Over the last few years, fiber expansion has continued at a rate never seen before. There are three-times more fiber services in the ground today than in 2005, reaching more homes and businesses (Fiber Broadband Association). This expansion powers terrestrial and wireless connectivity, enabling 5G towers that are necessary to see the benefits of 5G speeds.[2]

Today's laptops have Ethernet, Wi-Fi and 5G modems built in. If IT services go down, it's likely not going to be the fault of the last mile in the coming years. But more networks and more deployment choices can strain existing security models and implementations. Most, while applicable to multi-cloud and hybrid scenarios, are just frankly not implemented that way.

The industry is moving toward zero-trust models, tighter authentication standards like biometrics, stronger encryption and multi-factor by default. Threats, unfortunately, have increased during this time as well, with ransomware and data leaks up more than 500+% over last year, according to some reports.[3] So-called "bad actors" can be hired with Bitcoin for a few hundred dollars as the barrier to entry continues to fall to "hire out" disruption. The impact to an enterprise can be in the millions or billions of dollars.

Finally, soft targets like back-end infrastructure tools such as monitoring software (i.e., SolarWinds) are large targets due to the vast scale of systems they are attached to—often "behind the firewall" with greater access.

Hybrid IT managers will need a security-first strategy when implementing and should expect increased investment to maintain risk, service assurance, uptime and compliance with security requirements. Private clouds can be easier to secure, but not necessarily. Often, the network complexity on private cloud and colocation can be minimized and keep data more contained through a single connectivity provider or set of managed services.

Security solutions should be deployed comprehensively across platforms and IT management domains to provide the best visibility and fast response times when things do go wrong. IT endpoint security in the "branch of one" needs to be a top concern, with broader usage of behavioral advanced threat detection, reduced access to operational systems, and stringent use of multi-factor authentication and encryption whether at home, the office or the coffee shop.

Conclusion

In December 2020, Andy Jassy, now the new CEO of Amazon and the former leader of AWS, estimated that only 4% of workloads were in the cloud. More applications are being written as cloud-native, virtualized or with containers like Kubernetes. As the customer experience becomes more sensitive and competitive, applications will need service layers or to be edge-enabled. More IoT data sources will require more processing and will need to be more distributed to meet demands—at the edge and integrated with core and cloud data services. The reality is, a variety of platforms will continue to be the norm for hosting IT services. Learning how to best optimize various platform capabilities and ensure that "IT doesn't escape" is key—which requires solid architecture and governance.

Flexential's end-to-end solutions portfolio includes colocation, cloud, connectivity, data protection, managed and professional services. Building on this platform, Flexential provides individual assessment to ensure infrastructure requirements are met
with dynamic hybrid IT solutions that flex as an enterprise's needs evolve.

Visit Flexential.com to find out how your business would benefit from a hybrid IT model.

Sources:
(1) https://www.businesswire.com/news/home/20190724005072/en/SD-WAN-Infrastructure-Market-Poised-to-Reach-5.25-Billion-in-2023-According-to-New-IDC-Forecast
(2) https://medium.com/@fiberbroadband/fiber-growth-remains-strong-now-passing-30-million-homes-in-the-u-s-5461eb03216b
(3) https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html