5-STEP MULTICLOUD MIGRATION FRAMEWORK FOR HEALTHCARE

A simple path to secure and automated multicloud for providers, payers, and life sciences

While healthcare organizations were initially cautious about moving to the cloud, that reticence is quickly receding. In fact, the cloud market in healthcare is growing 18 percent annually and is predicted to reach nearly $45 billion by 2023.

Healthcare providers, payers, and life sciences are attributing this newfound enthusiasm to the fact that cloud technology provides easy, secure, and uninterrupted access to clinical and administrative applications—everything from electronic medical records to business productivity tools aimed at increasing overall collaboration and efficiency. Cloud makes it simpler to meet end users' expectations with anywhere, anytime access. In fact, 65 percent of healthcare providers use cloud services in some form, according to the Healthcare Information and Management Systems Society (HIMSS).

While using multiple cloud environments can help organizations separate applications with different security requirements, applications often change security levels throughout their lifecycle. This means healthcare organizations need to be adequately prepared for this shift. Applications may need to be quickly redeployed in other environments or modified to meet different backup, redundancy, or security requirements. Organizations must be able to redeploy workloads easily.

Data volumes are also surging, collaborative research is improving, and there is a tremendous need to enable data, information, and knowledge transparency across organizations. Cloud deployments help shift the focus from data to information-centricity, empowering users with quicker access to translational and outcome data resources. Connected medical and consumer devices are now the norm, and the resulting data can be used to analyze a patient's well-being, streamline R&D, and lower costs. The associated increase in devices, however, creates more opportunities for cyber criminals to breach an organization's network and potentially wreak havoc on intellectual property, not to mention patient and financial data.

Managing Complexity in Healthcare Environments

Managing multicloud environments is challenging. Due to the sensitivity of clinical data, hybrid cloud strategies are common, as healthcare organizations rely on a mix of public cloud services combined with private clouds and data centers. Many healthcare providers are struggling to manage a complex hybrid IT environment while meeting the rapidly growing needs of clinical systems, big data and business intelligence, and connected medical devices and machines.

In any industry, network complexity is an inhibitor to progress. In fact, that complexity is so debilitating that simply managing it has become a core function of the networking team. Draconian change controls, common in many IT Infrastructure Library (ITIL) shops, have brought operations to a near standstill. The very network architectures that support healthcare delivery are based on the belief that the best approach to handling complexity is to contain it.

In fact, IT in general—and networking in particular—have historically employed an aggressive isolation and containment strategy to deal with complexity. Highly attuned to patient privacy and cybersecurity challenges, healthcare organizations create domains with hard boundaries around a data center, campus, the backbone, or between clinical and administrative applications. Resources are grouped and quarantined. Operations are handled by teams of specialists.

As a coping mechanism, this was absolutely the right approach. However, in creating these boundaries, healthcare organizations have unintentionally added overhead and erected roadblocks that are simply unacceptable to any entity that needs to improve outcomes while reducing cost.

Each boundary imposes a "crossing tax" as people, systems, and processes navigate between contexts. Visibility and control tend to stop at the boundaries, rendering workloads immobile and operations domain-centric.

If the IT world were static, a divide-and-conquer approach to managing complexity might work. But if the transformative promise of the cloud in healthcare is to be realized, these hard boundaries must be eliminated. That means healthcare providers lose containment, making complexity not just an inconvenience but a debilitating obstacle to progress.

Multicloud as the Driver for Change

Multicloud is the natural conclusion for healthcare providers, payers, and life-sciences companies moving to the cloud. It's the recognition that economic, data privacy, application, and latency requirements drive the adoption of more than one cloud across an organization's IT infrastructure.

However, "multiple clouds" and "multicloud" are not the same thing. For example, most healthcare providers already rely on multiple cloud services for applications, storage, and compute resources. Multicloud is more than just tacking on another cloud to an existing deployment—it is about delivering infrastructure that is essentially invisible to the user. This requires several architectural tenets:

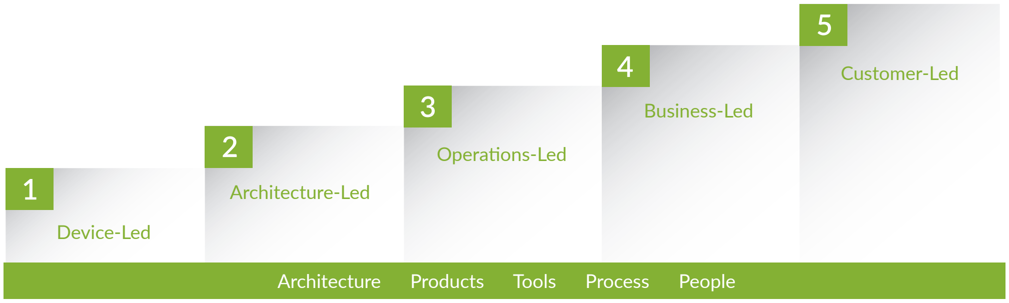
- **Security:** With data at the center of the IT universe, security is more than an add-on. It has to be a top-tier architectural consideration, especially when users and workloads are distributed.
- **Ubiquity:** One of the central theses of multicloud is that applications and services need to be everywhere. Indeed, if the clinician or patient experience is dependent on location, the full promise of cloud will go undelivered.
- **Reliability:** Networks are expected to be as reliable as public utilities. Everything must be available all of the time. Even small gaps in availability are intolerable and jeopardize patient safety. Reliability must be guaranteed in a multicloud world.
- **Fungibility:** To drive application and service ubiquity in a highly reliable way without breaking the bank, resources must be fungible. That means workloads cannot be bound to specific resources such that it impedes availability.

Making the Move to Multicloud

Ultimately, healthcare organizations will not purchase a shrink-wrapped multicloud infrastructure. Migrating from contained silos to a more fluid operational environment involves more than just product; it requires architectural planning, tooling, and process considerations—not to mention cultural and people changes. Having the right people and tool sets is critically important, as multicloud strategies typically involve multiple APIs and management modules.

The 5-step multicloud migration framework is designed to provide an agnostic way of thinking about staging the changes IT requires to adopt multicloud and what's important in delivering operational excellence.

As healthcare organizations navigate their way from conventional networks to multicloud architectures, they will naturally shift how they approach architectural design, deployment, and operations, evolving from a device-led to a customer-led design.



Methods-driven approach to lay out the path and coordinate decisions across initiatives

Figure 1: Multicloud Migration Framework

From Device-Led to Operations-Led

Most organizations are device-led, meaning they identify capacity requirements coupled with power and space constraints, then select a network or security device that matches the need. When they interact with their infrastructure, they work device-by-device, frequently using CLI or lightweight scripts as the preferred tool.

More mature enterprises, however, are architecture-led. They might settle on a data center architecture (leaf-spine or IP fabric, for example) and then use it to drive requirements into the individual devices. When they interact with the infrastructure, they operate at an architectural level, bringing tools like Puppet, Chef, and Ansible into play.

Cloud companies, however, are fundamentally operations-led. They decide first on their data models, telemetry, and data distribution strategies, allowing them to drive requirements into the architecture and ultimately the devices. By elevating operations to the top tier in terms of design criteria, they optimize for automation. This is in stark contrast to organizations that look at automation as a thing to add after deployment, relegating operations personnel to late-comer status in the entire design process.

Healthcare organizations must adopt the operations-led philosophy, driving architectural decisions from a set of clinical and operational requirements that include SLAs around application or service deployment, or the establishment of new clinics. While the evolutionary path will vary from organization to organization, and will naturally evolve from the device-oriented approach so common today, these business-level requirements will over time yield to customer needs, like specific clinical or patient application experiences or data privacy requirements.

A Simple Path to Secure and Automated Multicloud

The path to secure and automated multicloud cannot be traversed using only high-level guidelines. Complexity is not a problem in abstract representations of the network; it exists in the details that determine how a network actually operates.

This means that healthcare organizations need to develop multicloud migration paths for each of the major places in their network: data center, campus, branch, and cloud. Additionally, they must consider how to evolve pan-enterprise disciplines like automation and security. While these domains and disciplines might initially evolve independently, if multicloud truly offers a seamless infrastructure experience, migration plans will need to converge on a common set of architectural principles and capabilities.

The key will be orchestrating the simultaneous yet decoupled efforts, maintaining constant progress towards a multicloud objective. Healthcare organizations that understand their future state and use every refresh and expansion opportunity to ensure that their networking environment evolves to multicloud-ready will find that they are well positioned to take advantage of everything these emerging trends have to offer. By breaking the migration into consumable steps, organizations, people, and even budgets will be spared the jarring changes typical of larger transformations.

Put simply, the healthcare industry should view refresh and expansion events as opportunities for change. The committed organization will ensure that they use these opportunities to do two things: make progress toward deploying better technology, and avoid making any decisions that unnecessarily limit the number of paths forward. In this way, the set of decisions and changes build towards a true multicloud infrastructure, where teams can manage policies and resources as a whole.

Next Steps

To learn more about Juniper's network solutions for healthcare, visit https://www.juniper.net/us/en/solutions/healthcare/.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

JUNIPER NETWORKS | **Engineering** Simplicity