AHEAD

Networking for the Modern Enterprise

When an organization states that they want to be more ‘modern’ or speaks of becoming ‘a company of the future,’ what exactly do they mean? Is it providing better, more convenient services to their customers? Is it gaining the ability to operate at maximum efficiency? Empowering their employees with cutting edge tools and technologies? Moving their most important business functions to the cloud? The short answer, in most cases, is yes—to all of these things. But regardless of an organization’s definition of ‘modern,’ there are certain connectivity prerequisites that will be necessary to realize those ambitions.

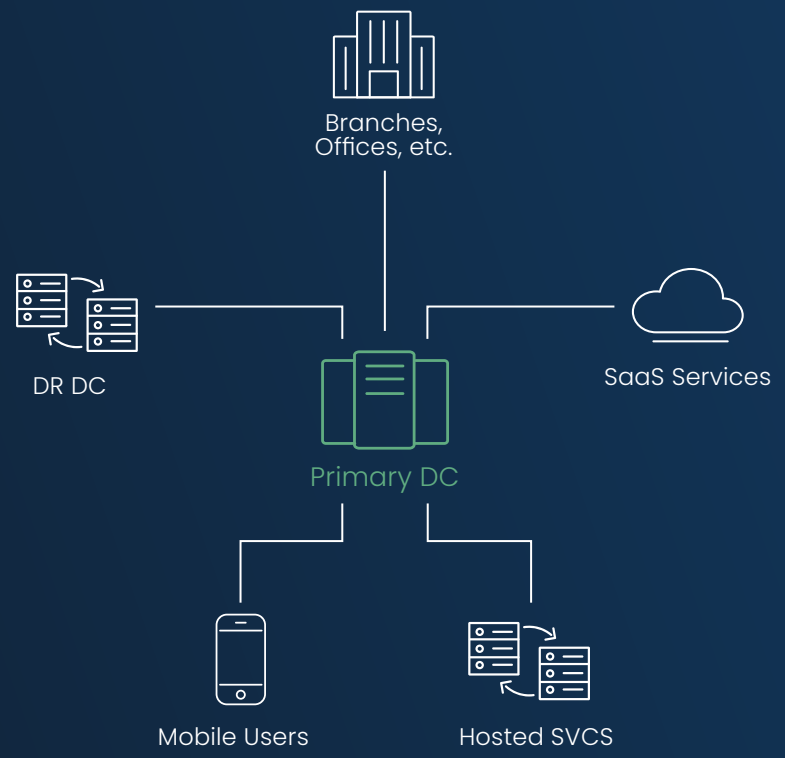
When we consider the enablers of the ‘future’ enterprise, a few key things come to mind. Businesses need to be flexible. They want to see M&A activities happen swiftly and efficiently. They want to optimize performance at all levels of the business. They strive to use automation more effectively, accommodate working from anywhere, and create crystal-clear visibility to make continuous improvements.

The key to achieving all of these things ultimately comes down to one thing: network connectivity. If an organization’s network cannot support its most critical business functions in a way that promotes efficiency, strengthens security, and operates flawlessly, they will struggle to meet even the most modest goals and objectives.

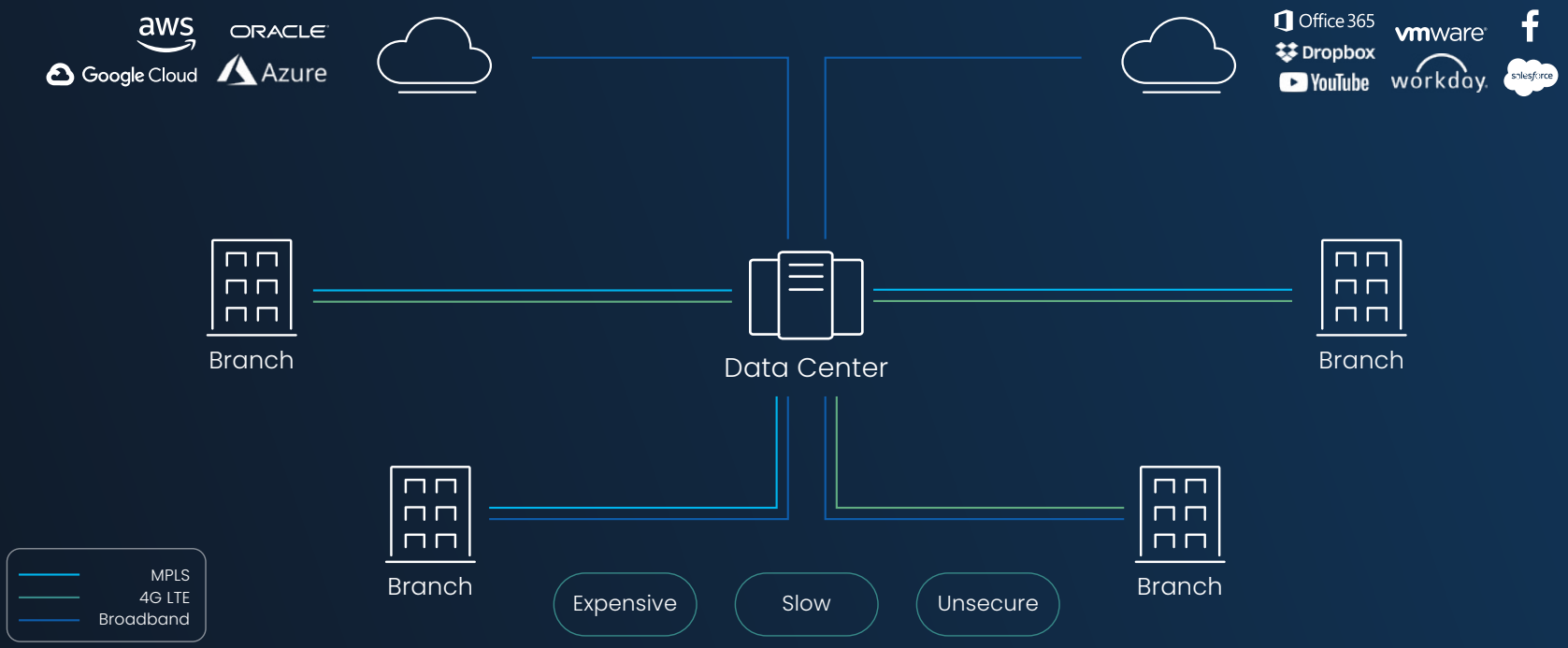
So, let’s explore the hallmarks of a modern network by first looking at where we’ve been and then examining where things are headed.

Legacy Connectivity Structure

What does a legacy network look like? In many cases, organizations used what is called a 'hub and spoke' topology, namely because it made it easy to control activity and place security policies due to the single ingress/egress point for all traffic. This meant that security did not need to be everywhere because there was only one point of focus. Further, the hub and spoke topology made adding services (DNS security, URL filtering, quality of service, etc.) a much simpler task.

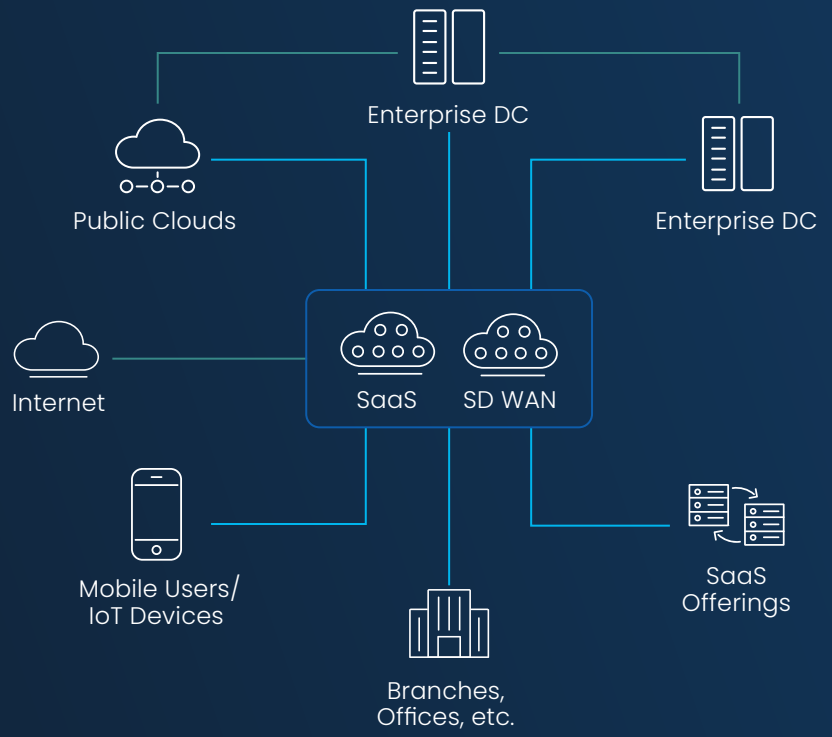


However, while building networks in this way made sense in the past, we've since learned that a hub and spoke method presents a number of issues that make it less optimal for today's modern ways of working. For starters, data could only move from point A to point B within the network, leaving no room for improvement or better efficiency because it could only follow one path. What's more, when attempting to add things like cloud or SaaS to this network structure, performance went down, security became more of an issue, and the entire process became more expensive.



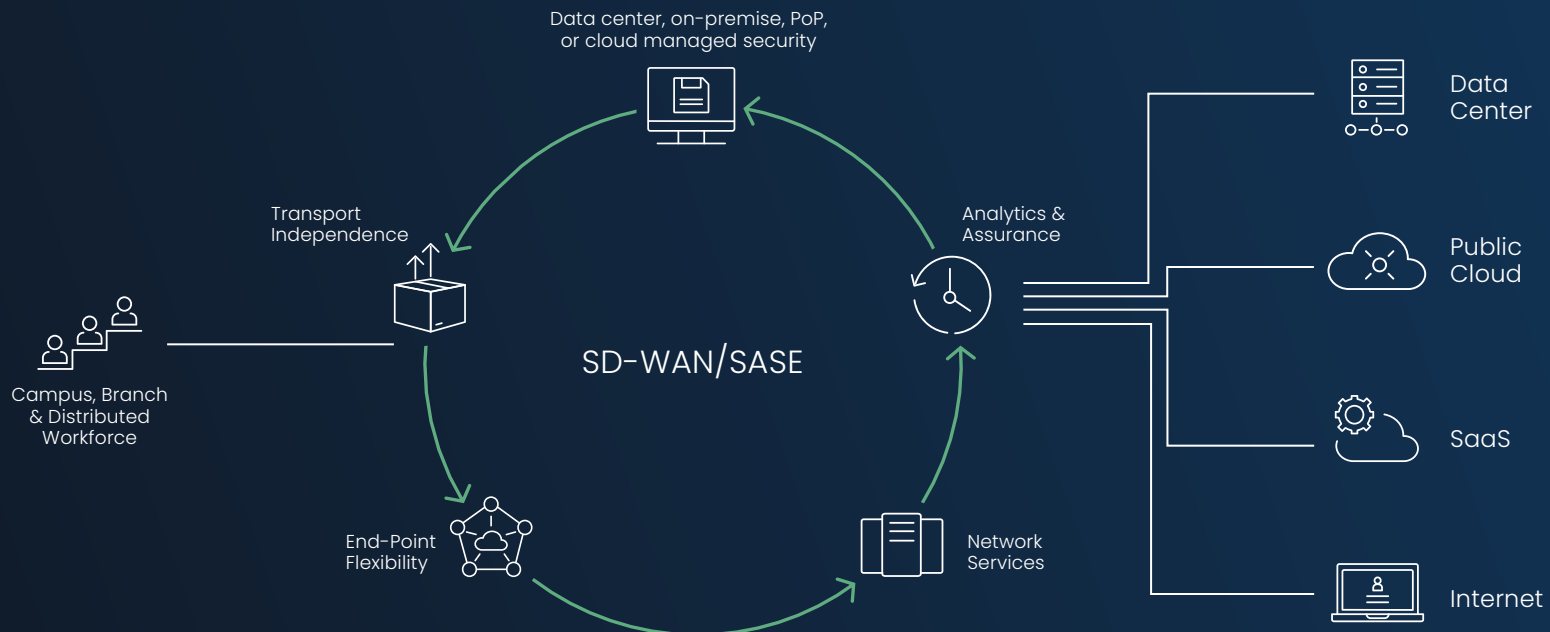
Modern Connectivity Structure

So, what does a modern topology look like? By learning from the past, we knew that it needed to be an intelligent network that could understand the best route for information to flow and make those changes on the fly without manual intervention. Further, this network should perform based on the needs of each specific application. In other words, the applications deemed business critical (e.g., ERP apps) should use more resources than those which don't need as much (e.g., guest Wi-Fi). Additionally, we knew that the network had to be fast to provision so that changes could be rolled out quickly and in an automated fashion to minimize manual errors.



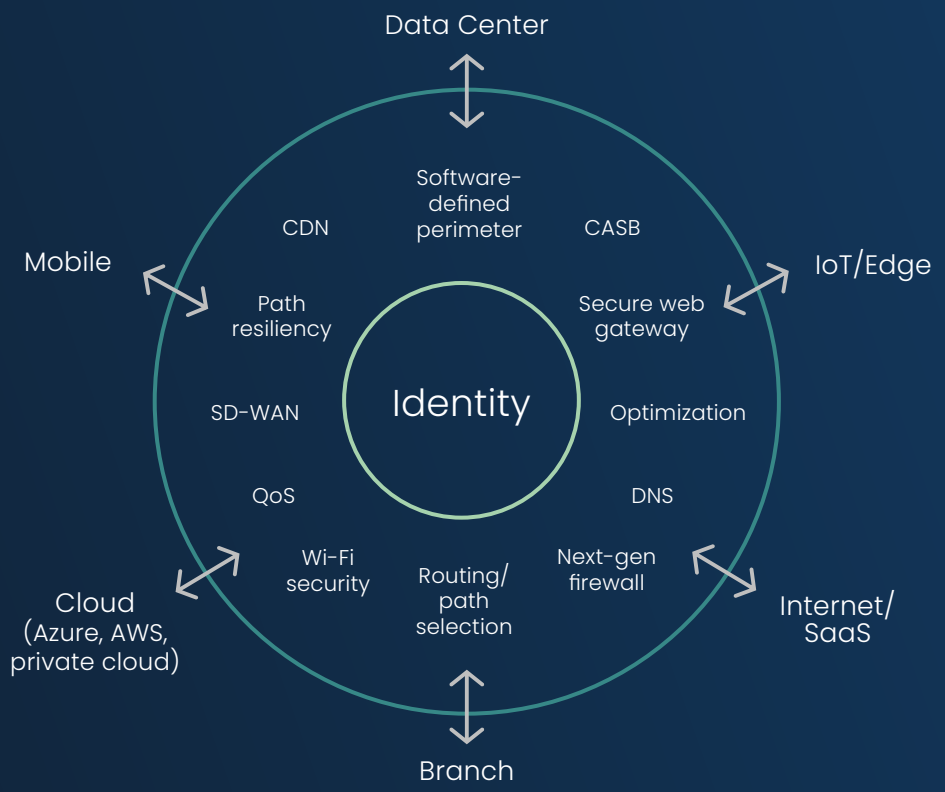
While these improvements were undeniably necessary, they did create a situation where we needed to rethink our security policies entirely. No longer could we rely on the single point of ingress/egress because we now had different points within the network communicating independently. With that, the challenge became figuring out how to design our security in a way that could handle this modern topology.

What we found was that the best way to ensure security across this new topology was to leverage a combination of SD WAN (software-defined wide-area network) and SASE (Secure Access Service Edge). These solutions allowed users to safely access the network from anywhere without compromising security policies.



What is SASE?

Put simply, SASE is the next step in the evolution of SD WAN. The key point to this security model is that identity becomes the new perimeter of the network. Since users are no longer in one place, we cannot rely on IP addressing or access lists because IP addresses are constantly changing. With identity as the perimeter, we can begin to adopt a least-privileged access model where users are given precisely enough access to do their jobs while restricting access to that which is not relevant. This enables secure connectivity from branch offices, mobile devices, home offices, IoT, etc. and allows us to once again build our security policies around one single point within the network. Not only that, but the SASE approach also allows for a number of additional features (CASB, next-gen firewall, URL filtering, DNS security, DLP functionality, etc.) that we used to have in the data center to be tied into one cloud-delivered model.

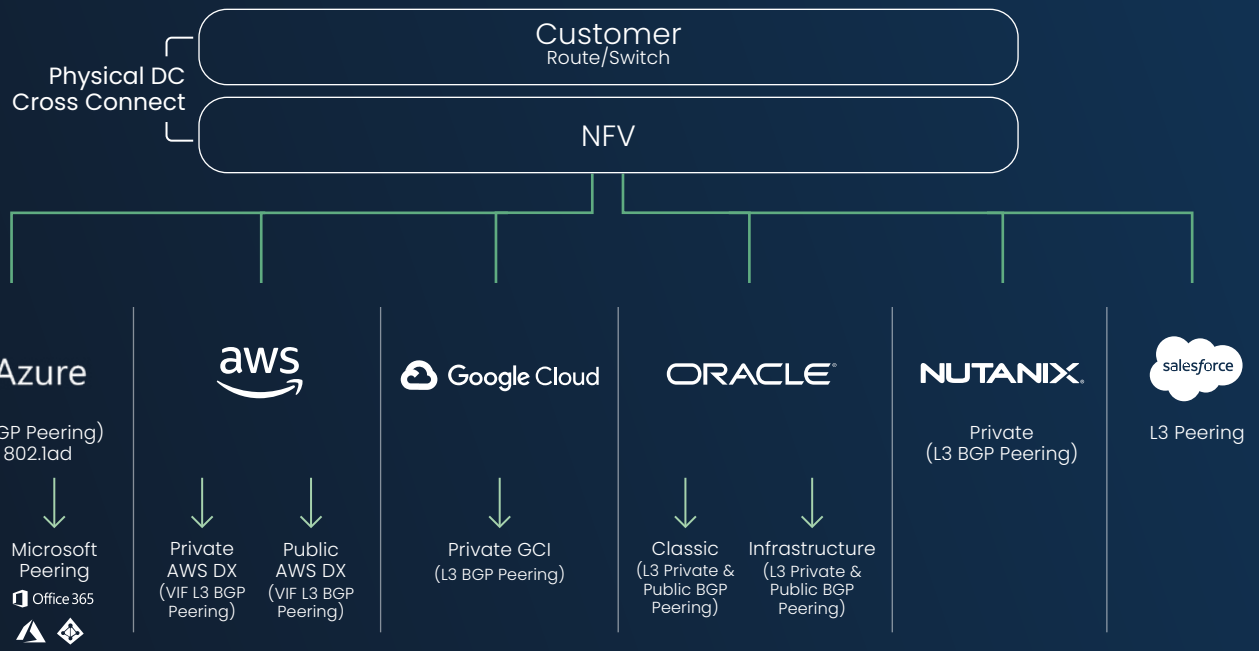


Connecting to Multiple Clouds

Up until now, we've discussed how users get to the cloud, but not necessarily how they get into the cloud. As organizations adopt more clouds into their network, they need to have on-demand connectivity to each one. Using a software-defined direct connect approach will allow organizations to put their applications wherever the business dictates while having a network and security construct that accounts for everything. This means that enterprises can spin up new clouds on-demand, having both visibility and connectivity to multiple clouds without the need for long-term provisioning.

While it's one thing to get into each of these clouds, networking within each cloud can be a bit more complicated, namely because they all tend to operate differently. Because of this variability between different clouds, we often run into issues such as limited visibility or a lack of controls. Further, working within multiple clouds can create a skills gap where teams must be able to work within clouds that are fundamentally different from one another, which means more time spent training employees. Lastly, the disparate nature of these clouds can obstruct repeatability and require more manual intervention, inevitably slowing productivity.

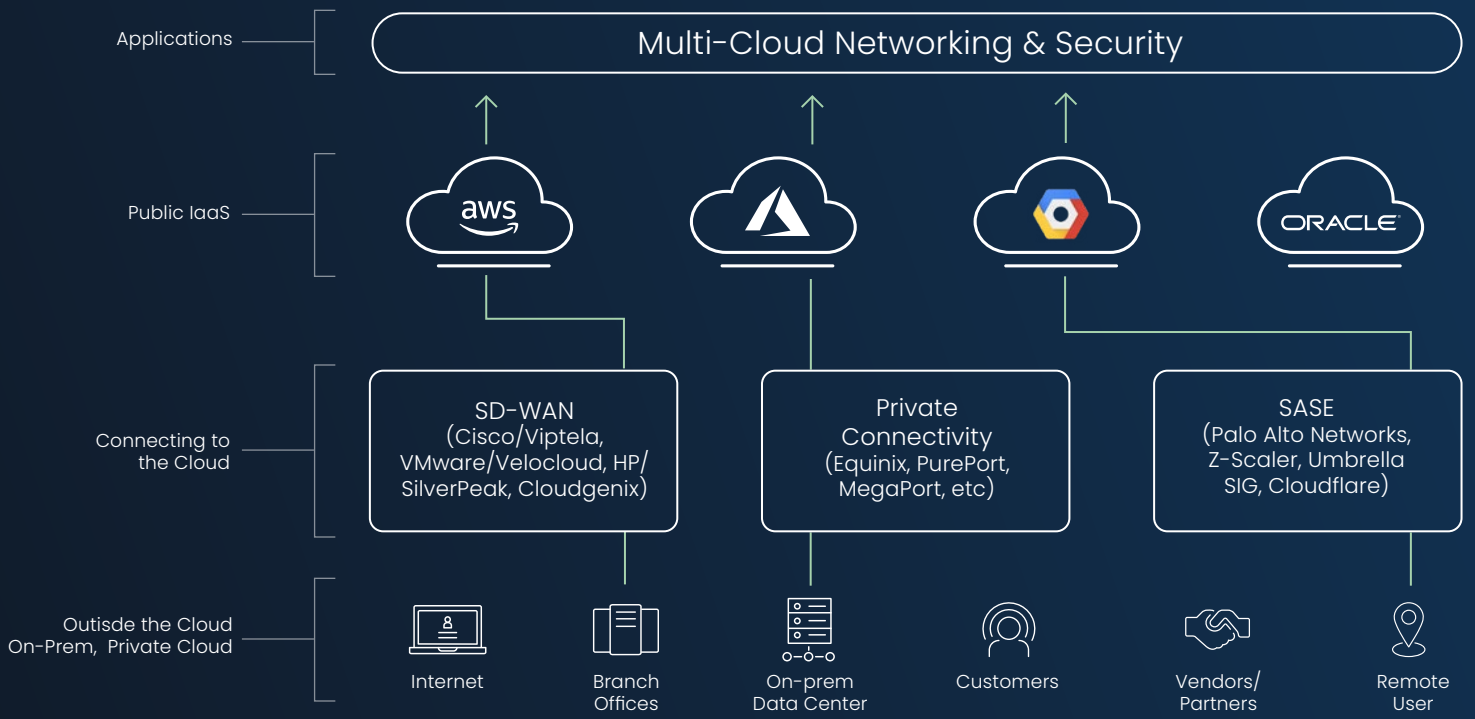
Software Defined Direct-Connects Layer 2 Access



Multi-Cloud Network Architecture

So, how do we create a network and security construct that spans one or multiple clouds so that the business can make decisions and the network and security teams can act quickly? A multi-cloud network architecture allows organizations to instantiate multiple services (such as networking, security, operations, or service insertion) within a singular network. This means that the intricacies between different clouds can ultimately be set aside because we have one network construct that spans across all of them.

The Cloud Network



This approach enables us to leverage the capabilities of everything that has been discussed so far:

01 FLEXIBILITY

Applications can live within just one or many clouds

02 OPTIMIZED PERFORMANCE

SD WAN creates an overall network fabric that has intelligence, self-healing capabilities, and performance based on individual applications

03 WORKLOADS ANYWHERE

SASE allows for a secure direct connection, wherever users are located

04 DIRECT CONNECTIVITY

SD Direct Connect enables connectivity from on-prem data centers to any cloud or SaaS provider

2022 AHEAD SPRING summit

For a more in-depth look into networking for the modern enterprise, check out the on-demand sessions from AHEAD's 2022 Spring Summit: Accelerating to Cloud-Native.

National Hubs

ATLANTA
1117 Perimeter Center
W406
Atlanta, GA 30338

CHICAGO
401 Michigan Ave.
#3400
Chicago, IL 60611

SAN FRANCISCO
2000 Crow Canyon Place
Suite 250
San Ramon, CA 94583