Technical brief

Three ways to simplify and secure your data center network

Data center network volume and velocity have increased rapidly in recent years. Enterprises are moving more of their workloads to the cloud to take advantage of its exceptional speed and flexibility. At the same time, the Internet of Things (IoT) is expanding at a breakneck pace. Many mobile and remote users are joining data center networks every day, working from a variety of connected devices, and creating countless new endpoints to manage and secure. Legacy architectures cannot keep up, which is causing data bottlenecks and pressing security risks. As the shift from centralized to distributed edge-to-cloud data centers continues, new and simpler network architectures are needed to protect networks from evolving threats across a growing number of endpoints.

The network is the central nervous system of the enterprise. It must have the capacity to connect growing volumes of people, data, and things (whether physical or virtual) to keep operations running smoothly. Legacy data center networks can be inefficient and costly to manage, which can cause issues including:

— Long deployment times

— Difficulty integrating with new data center tools

— IT resources wasted on complex manual processes

— Higher IT costs

— More risk exposure

The next wave of data center connectivity requires high performance fabrics, distributed services, and flexible consumption options that support a cloud-first IT strategy. Enterprises need a reliable architecture that can provide fast, secure connectivity and deliver a better quality of experience for users and devices.

Secure your network everywhere

A modern data center network architecture can dramatically enhance security and reduce complexity to meet growing demands without compromising performance.

Here are three effective ways to modernize your network:

1. Ease IT complexity with a distributed services architecture

With many users switching between work environments—at home, in the office, and on the move—traditional router-centric WAN architectures are no longer enough to keep your operations efficient and secure. You need a better way to reduce data center complexity and accelerate automation, integration, and security. The solution is a distributed services architecture.

Integrating stateful service capabilities within the data center fabric provides full visibility into where applications live without impacting existing network architecture or software configurations. This improves data center security while reducing acquisition costs and simplifying IT.

A distributed services architecture simplifies and secures IT by:

— Eliminating appliance sprawl, lowering infrastructure and maintenance costs

— Reducing or eliminating the need to deploy costly software server agents

— Optimizing network performance and bandwidth by reducing latency via deploying services at the fabric edge

— Automating operational initiatives for network and security teams

2. Extend zero trust closer to applications

Users are accessing applications and data from anywhere, on any device, requiring consistent connectivity from campus to branch offices and remote locations. It's critical to deliver consistent experiences, whether applications reside in the data center or the cloud.

Your goal is to enable seamless and secure access for every user, device, and application from anywhere. Modern network architectures make this possible with two key capabilities: edge-to-cloud security (required for any zero trust deployment) and complete network telemetry. Security within the data center is critical to prevent breaches while telemetry supports emerging solutions like artificial intelligence (AI) that can automate security and network operations. By embedding these functions into the network fabric, you can improve network performance by freeing up valuable server CPU cycles that are otherwise tied up in processing compute-intensive network services.

A distributed services architecture expands zero trust security deeper into the data center, to the network-server edge, delivering fine grain micro segmentation that dramatically enhances and scales your data security.

Zero trust is an important enterprise security practice that prevents data breaches and limits internal lateral movement by assuming threats are present in the environment. Continuous monitoring ensures that policies automatically adapt based on changes in identity, location, and device health. This approach can deliver up to 100x the scale and 10x the performance at a third of the total cost of ownership (TCO) compared to traditional solutions.[1] Plus, it makes it easier for you to detect and even prevent suspicious behavior on your network, so you can remain compliant.

Modern network architectures provide benefits that go beyond telemetry:

— Look back at traffic (on a per-application basis) to find the cause of poor application performance

— Provide flow data to a wide variety of network performance and security tools

— Automatically detect anomalies and group-related incidents, and notify teams in real time

— Leverage AI-powered tools with complete high-fidelity telemetry

[1] arubanetworks.com/resource/5-principles-for-a-smarter-data-center/

3. Adopt a flexible consumption model that scales as you need it

Two powerful IT trends are converging in the enterprise: colocation and edge-to-cloud infrastructure as a service (IaaS). Most existing implementations are based on centralized architectures that collect and process data at core data centers, colocation centers, or in the cloud. But in today's world, endless streams of data are generated at the edge—in remote locations like factory floors, retail sites, and healthcare facilities. Instead of infrastructure determining where data lives, the location of data is determining infrastructure decisions.

Managing enterprise data across hybrid environments is driving the expectation for improved availability, performance, and security. Data center networking technology has evolved to provide greater performance, but many security and services architectures have not. You may be unprepared, facing pockets of siloed compute and storage, disjointed network and security architectures, and operations that hinder centralized IT management, orchestration, and visibility. Modernizing your network is more important than ever. That means aligning your network architecture with the cloud-centric architecture and agile service provisioning that hyperscale data centers have been using for years. IaaS makes your environment simpler to deploy, manage, and secure—even as the needs of users, devices, and applications change. Colocation combined with cloud-based services offers significant advantages. These include greater control over your applications and data, enhanced security near your applications, and seamless access to your network—all with a simplified cloud experience.

You gain significant advantages with a pay-as-you-go approach for your infrastructure:

— Deliver low-latency, high-bandwidth connection to all your applications and data

— Improve transaction speed with direct connection to a broad ecosystem of adjacent businesses

— Support your sustainability goals by eliminating overprovisioning

— Optimize IT spend with no up-front payments and pay only for what you use with no egress charges

Prepare your network for the future

Hewlett Packard Enterprise is helping enterprises prepare for the future with a modern network architecture that can support the needs of any environment—even the harshest ones. Our comprehensive network portfolio offers the capabilities and services you need to develop a security-first solution for today's needs and tomorrow's challenges. You can have it all: improved user experiences, more robust security, increased bandwidth, and a cloud-first strategy that helps you work smarter and innovate faster.

Let's turn your network into a powerful, security-first solution—while keeping operations simple.

Visit HPE.com

Learn more at

HPE.com/connected-enterprise

Chat now

a50010481ENW, Rev. 2