Pluribus
NETWORKS

Pluribus Unified Cloud Networking

Unified, simplified, secure networking across distributed clouds

Highlights

- The industry's only open, SDN-automated solution that unifies networking across data center switches and servers with distributed security, built-in automation, end-to-end visibility and hardware-accelerated performance

- Unified and simplified cloud networks: any cloud, any workload, any device

- Distributed security without compromises: microsegmentation, distributed firewall, encryption

- Pervasive visibility: every application, every flow

- Comprehensive automation: controllerless SDN, underlay + overlay + services

- Open networking: disaggregated hardware + software, choice of switches and DPUs
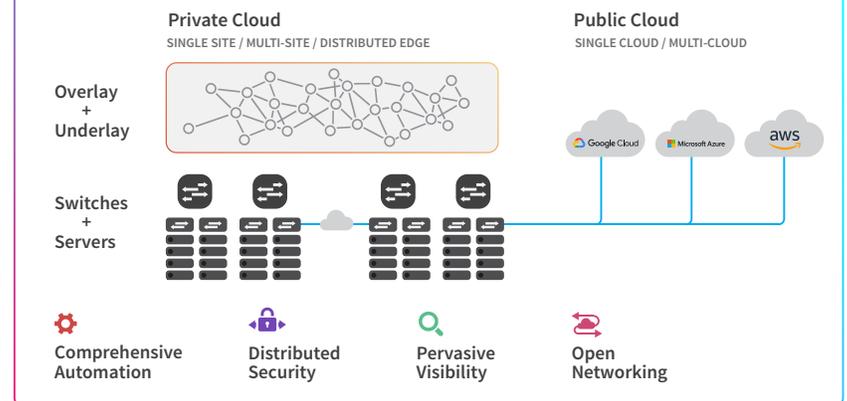
Introduction

Pluribus Unified Cloud Networking is the industry's first architecture enabling a unified networking model across distributed clouds and across switches and server-based data processing units (DPUs) with zero-trust distributed security, built-in automation and pervasive visibility. Built on disaggregated, open networking hardware, the Pluribus Netvisor ONE® network operating system, and the Pluribus Unified Cloud Fabric™, this revolutionary architecture enables cloud operators to transform their cloud networks with a smooth migration path. With Pluribus Unified Networking, cloud operators can realize enhanced security, dramatically reduced complexity, lower total cost and increased agility to accelerate their businesses and move at cloud speed.

Pluribus Unified Cloud Networking

Applications

The Unified Cloud Networking architecture can benefit any type of cloud network operator including:

- **Enterprise Hybrid Clouds** – Enterprises are embracing hybrid cloud models and retaining the majority of their workloads in private cloud environments, especially those with mission-critical performance, security and privacy requirements. Private cloud infrastructure is expanding, spanning on-premises data centers, colocation sites and increasingly distributed edge sites.

- **Cloud Service Providers (CSPs)** – A wide variety of CSPs providers differentiate themselves from hyperscale public clouds by catering to local market requirements, such as data sovereignty and privacy, and providing managed and hosted cloud services more closely tailored to their customers' requirements.

- **Telco Clouds** – Telecom service providers operate highly distributed cloud infrastructure to support their network services, including 5G and emerging edge computing services.

Target applications of Unified Cloud Networking include:

- Unified networking across heterogeneous networks with a mix of switches and data processing units (DPUs) and mixed application environments, from bare metal to virtual machines with multiple hypervisors to containers orchestrated by Kubernetes

- Distributed zero-trust security services including microsegmentation, distributed firewall and encryption

- Distributed and pervasive visibility, with application-aware flow monitoring and analytics

Challenges

To remain competitive, cloud network operators of all types need to evolve their cloud network infrastructure in two ways:

1. Transform cloud networks to become as agile, highly available and simple to operate as the hyperscale public clouds.

2. Move rapidly toward a new, more highly distributed networking and zero-trust security architecture to address increasing cybersecurity risks.

Achieveing these goals requires addressing several challenges in today's networking environments and solutions:

- **Cloud networking is fragmented and complex.** Overlay networks are decoupled from underlay networks and fail to stretch across distributed clouds. Each cloud network has its own operations model, increasing operations cost.

- **Security solutions are lacking.** Today's cloud networks demand distributed security, including micro-segmentation for zero-trust environments, to protect distributed applications against increasingly sophisticated security threats. Security appliances cannot scale cost-effectively to meet this requirement, while software-based virtual firewalls are expensive and compromise server performance.

- **Visibility is an afterthought.** Limited traffic monitoring and application visibility lead to reactive, slow troubleshooting. Separate monitoring networks add substantial cost yet deliver incomplete coverage.

- **Automation is brittle and incomplete.** Bolt-on automation tools and do-it-yourself (DIY) scripting are hard to implement and even harder to maintain. Multi-vendor incompatibility, script drift and lack of change control increase risks of outages or security breaches.

Unified Cloud Networking Solutions

The Pluribus Unified Cloud Networking architecture and the Unified Cloud Fabric address these challenges with comprehensive capabilities.

- **Unified and simplified cloud networks.** Pluribus eliminates fragmented networks with separate operating models, enables smooth migration toward the new distributed architecture and lowers operational complexity and cost by delivering a consistent network operations model across underlay (physical) and overlay (virtual) networks, across switches and servers and across heterogeneous, distributed clouds.

- **Distributed security without compromises.** Pluribus enables security to be distributed to the server, including fine-grained microsegmentation and distributed firewalls, with substantially better performance and lower total cost of ownership compared to hardware appliances or purely software-based solutions.

- **Pervasive visibility.** Pluribus delivers built-in application-aware visibility and analytics for every application and every traffic flow, improving proactive trouble detection and resolution, while eliminating the extra cost and incomplete coverage of separate monitoring networks.

- **SDN-enabled Automation.** Pluribus solutions incorporate industry-leading controllerless SDN automation to enable network operations teams to manage highly-distributed networks with thousands of DPUs and other network endpoints, while avoiding the challenges of integrating third-party automation tools or building and maintaining do-it-yourself (DIY) scripts.

Solution Architecture

Open Network Platforms

The foundation of Unified Cloud Networking is open networking hardware platforms. Pluribus has embraced open, disaggregated networking for years, with its Netvisor ONE operating system (OS) running on data center leaf and spine switches from multiple vendors, including Pluribus Freedom Series switches, to create unified data center fabrics.

With the introduction of Unified Cloud Networking, the Netvisor ONE OS now also runs on open data processing units (DPUs) from leading vendors, which are inserted into servers to provide more highly distributed networking and security capabilities closer to applications.
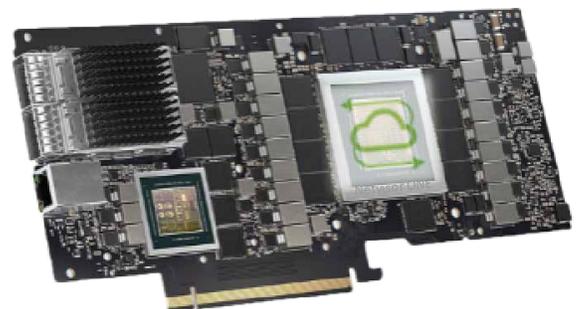
Pluribus Netvisor ONE OS on Open DPU

Netvisor ONE OS

Netvisor ONE is the foundation of Unified Cloud Networking, a common network operating system that runs on diverse network platforms from switches and DPUs to edge devices and virtual instances in the public clouds. Netvisor ONE is the industry's only network OS that can run across all of these environments, enabling a unified fabric and network operations model for cloud networking.

Unified Cloud Fabric

The Pluribus Unified Cloud Fabric is the heart of Unified Cloud Networking. It unifies and simplifies diverse cloud networks with network virtualization services, distributed security, built-in automation and pervasive visibility.

The Unified Cloud Fabric is the next generation of the award-winning Adaptive Cloud Fabric, which has been deployed for years in mission-critical networks around the world. The Unified Cloud Fabric builds on that proven fabric technology and extends it to more highly distributed networks with new features and capabilities.

A key benefit of the Unified Cloud Fabric is its ability to unify networks that include servers with DPUs and other servers and devices without DPUs. As cloud operators move toward a target architecture that is more fully distributed, with networking and security enabled by DPUs in every server, they need a smooth migration path that doesn't require DPUs to be deployed everywhere overnight. They also need a common network fabric that can accommodate servers and devices that will never have a DPU, including special purpose appliances and IoT devices. Enabled by Netvisor ONE instances running in both switches and in DPUs, the Unified Cloud Fabric achieves that goal.
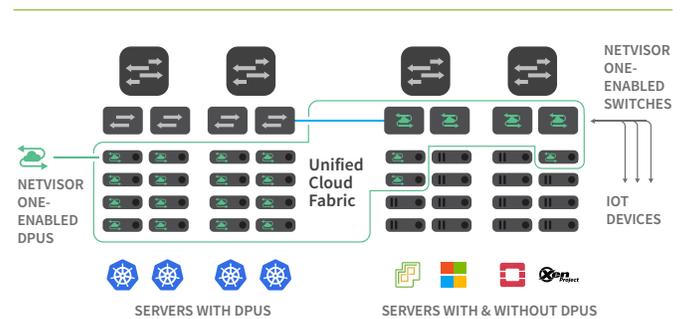
Unified Cloud Fabric Across Switches and DPUs

UNUM Fabric Manager and Insight Analytics

Pluribus UNUM, a robust, widely deployed platform incorporating management and analytics for distributed network fabrics, has been extended to manage Unified Cloud Networks. The platform includes the UNUM Fabric Manager, providing comprehensive GUI-based life-cycle management of unified cloud networks, and UNUM Insight Analytics, delivering rich network performance and security monitoring, analysis and problem solving.

Unified Cloud Networking Benefits

The most important benefit of Unified Cloud Networking is dramatically reduced complexity and increased business velocity.

Unified Cloud Networking also offers substantial total cost of ownership (TCO) benefits in multiple ways.

Unified Cloud Networking Attribute	TCO Benefit	Savings
⚙ Unified Networking with Comprehensive Automation	Lower ops complexity Opex savings	• Eliminate multiple networks with different operating models • Built-in automation reduces service delivery time up to **95%**
🔒 Distributed Security	Capex savings	• Avoid cost of scaling out HW appliances, **$20k+ per rack** • Avoid separate licenses for SW-based firewalls, **$100k+ per rack** • Offloading networking + security from CPU reduces servers **25%+**
🔍 Pervasive Visibility	Capex savings	• Eliminate overlay visibility infrastructure, **$15k+ per rack**
↻ Open Networking	Capex savings	• Best-of-breed open HW saves **20-50%** vs. proprietary HW

Summary

Pluribus Unified Cloud Networking uniquely enables operators to achieve their goal of transforming their cloud networks for high agility, availability and distributed zero-trust security.

Pluribus Networks, Inc.
www.pluribusnetworks.com