ESG Showcase

The Value of Unified Cloud Networking

Date: March 2022 **Author:** Bob Laliberte

ABSTRACT:. In today's highly distributed cloud-native application environments, organizations need a unified networking fabric to increase security and agility while reducing complexity. This fabric needs to span multiple clouds, devices, distributed locations, and application environments while enabling security services to be deployed and run close to the application without impacting performance. Pluribus Networks has developed the Unified Cloud Fabric to address these needs, providing a common network OS that runs on DPU-powered SmartNICs, open networking switches, and virtual cloud environments. This solution will provide substantial value to organizations, such as improved zero trust security, reduced network complexity, lower total costs, and increased agility. The result: organizations can accelerate business performance securely at webscale speed.

Meeting the Needs of Distributed Application Environments

Digital transformation initiatives are surging: 73% of organizations say they either are implementing new digital transformation programs or have mature implementations already in place.[1] In order to support today's—and especially tomorrow's—digital transformation programs, two requirements are essential: support for distributed environments and dramatic reduction in network complexity to drive performance and improve security.

To achieve the top goals of digital transformation, which, according to ESG research, include becoming more operationally efficient and providing better and more differentiated customer experiences,[2] modern applications are being developed and deployed to run across diverse platforms, including private data centers, multiple public clouds, and edge computing centers. However, these cloud-centric applications will also need to coexist with existing, but essential, legacy applications on a mix of infrastructure types, including bare-metal servers, virtual machines, and containers.

To make that a reality, network topologies and architectures must evolve to deliver the agility and performance typically associated with public clouds in distributed and mixed application on-premises data centers.

It is important to keep in mind that this transformation will not occur over night. The migration will take time and require the ability to manage a mixed network infrastructure environment that supports existing and emerging technologies, such as microservices architectures, distributed processing units (DPUs), and smart network interface cards (SmartNICs).

Another consideration for the network is to provide granular visibility into modern applications that generate increased levels of east-west traffic within a single server and the ability to secure that traffic.

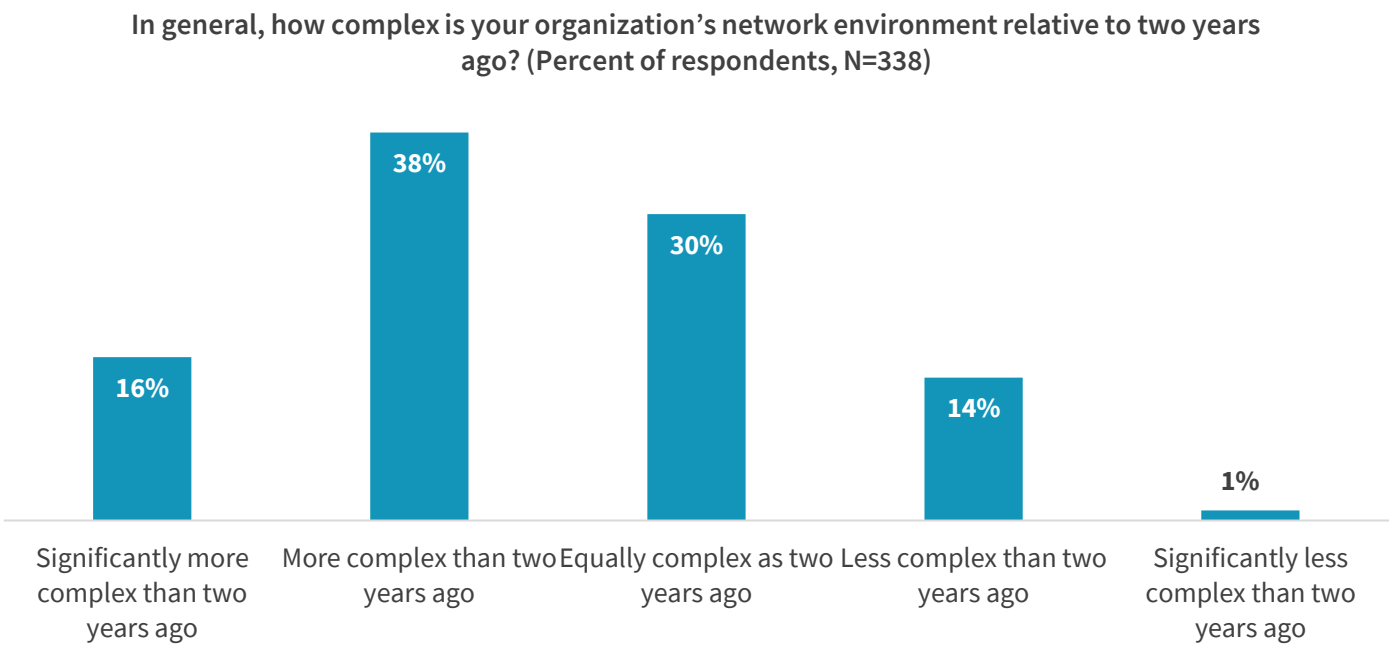
Unfortunately, most legacy security and visibility architectures are not capable of adequately supporting and securing these modern environments, especially those appliance-based visibility solutions or perimeter security solutions.

[1] Source: ESG Research Report, *2022 Technology Spending Intentions Survey*, November 2021.
[2] Ibid.

Security and Visibility Challenges with Distributed Applications

As networks have evolved to support these highly dynamic and distributed environments, they have become substantially more complex to manage and monitor. ESG research points out that 54% of enterprise respondents indicate that their network environment has grown more or significantly more complex over the last two years.[3]

Figure 1. Majority Cite Increased Network Complexity



Source: ESG, a division of TechTarget, Inc.

There are several important reasons why organizations are struggling with network complexity, including:

- The dynamic nature of modern IT environments, where microservices are spun up and down in a matter of seconds, creating significant visibility gaps in relation to network behavior and threats.
- Limited amounts of network automation require operations teams to spend a good portion of time on repetitive manual tasks.
- The numbers and diversity of network management tools for both on-prem and cloud environments have proliferated, especially across multiple sites. This makes it time-consuming for networking teams to learn each new tool and inefficient for them to perform manual correlation between them.
- Staff challenges, both in terms of talent availability and conversance with emerging technologies.
- Challenges in securing and gaining visibility into increased volumes of east-west application network traffic. Centralized appliance-based solutions are not effective in these modern environments, as most employ coarse segmentation, and round-trip latency to and from appliances can impact performance.

[3] Source: ESG Research Report, *Network Modernization in Highly Distributed Environments*, November 2021.

- Distributing security and visibility appliances to additional locations within the data center and across increasingly distributed data centers and edge sites becomes cost-prohibitive and difficult for networking teams to manage.
- Legacy hardware-based appliances lack agility and require additional lifecycle management activities.

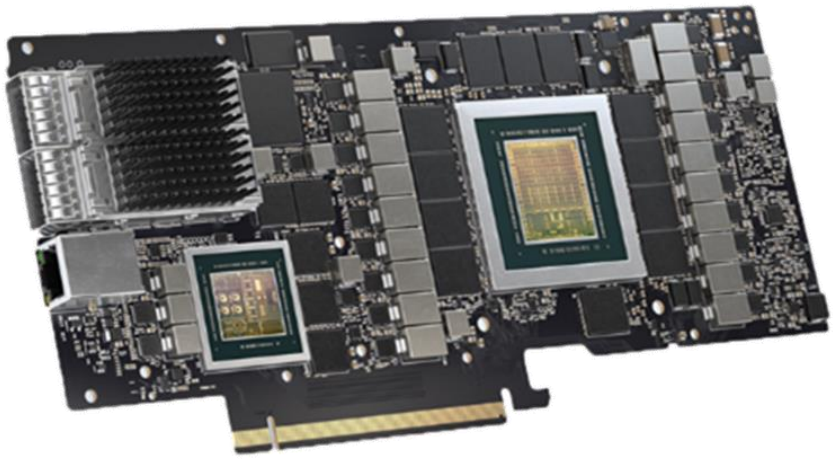
Organizations must address these challenges to deliver consistently secure, positive experiences across modern architectures to create agile, efficient hyperscaler-like environments in on-premises data centers.

Distributed Networking Environments Must Evolve

To transform their existing on-premises or colocation environments for modern application demands, some organizations have adopted an approach of running distributed networking and security in software on the server, but this approach does have several drawbacks. DevOps and NetOps teams lack clear operational separation for "zero trust administration." The overlay network is generally not integrated with the underlay, or physical, network, driving up operations complexity and inhibiting visibility. Networking functions place high demand on server CPUs, increasing server costs or impacting application performance. High software licensing costs can also make for a challenging business case.

Modern SmartNICs and DPUs provide a better platform to achieve those goals of distributing network and security services without the management complexity and performance/cost impacts incurred by software-based solutions. They do this by offloading networking and security services from the CPU on to a card in the server. These devices typically incorporate their own CPU complex to run the networking and security applications along with various hardware accelerators to ensure high performance and throughput. However, this is not just about having the capability to run these services in a SmartNIC—it is also about doing so in a manner that delivers enhanced customer experiences and provides operational scalability and efficiency across networks which may have thousands of SmartNICs and other network edge devices.

Figure 2. Modern SmartNIC Example: NVIDIA Bluefield-2 DPU



Source: NVIDIA

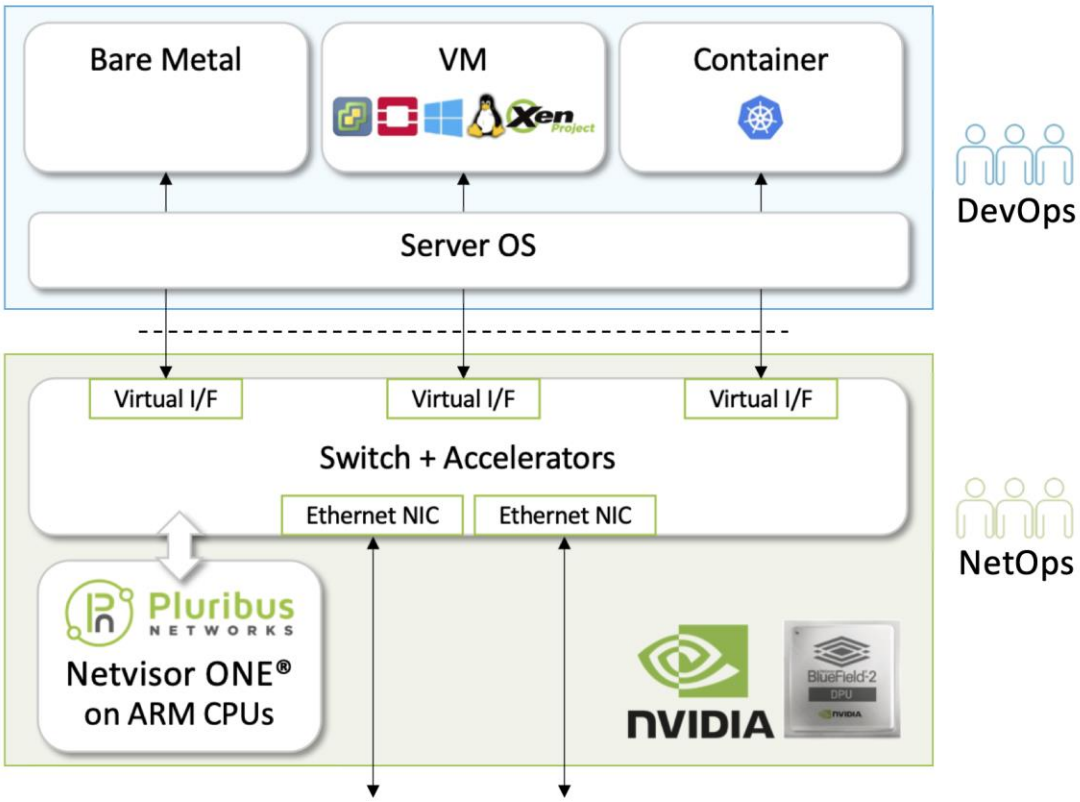
Therefore, organizations need solutions that not only provide the requisite distributed application services but also streamline deployment and management in a cost-effective manner.

The Value of Pluribus Unified Cloud Networking

Pluribus has partnered with NVIDIA to deploy networking and security services as close as possible to the application using NVIDIA DPUs, while also providing a unified network fabric that includes servers without DPUs to enable migration and support for mixed environments. The results are reduced operational complexity, easier administration, and improved sustained performance at scale.

Over the past year, the two companies have worked to integrate NVIDIA Bluefield-2 DPUs with the Pluribus Netvisor ONE network operating system (NOS) so it can take full advantage of Bluefield hardware accelerators and NVIDIA's DOCA software developer kit.

Figure 3. Pluribus and NVIDIA-enabled SmartNIC

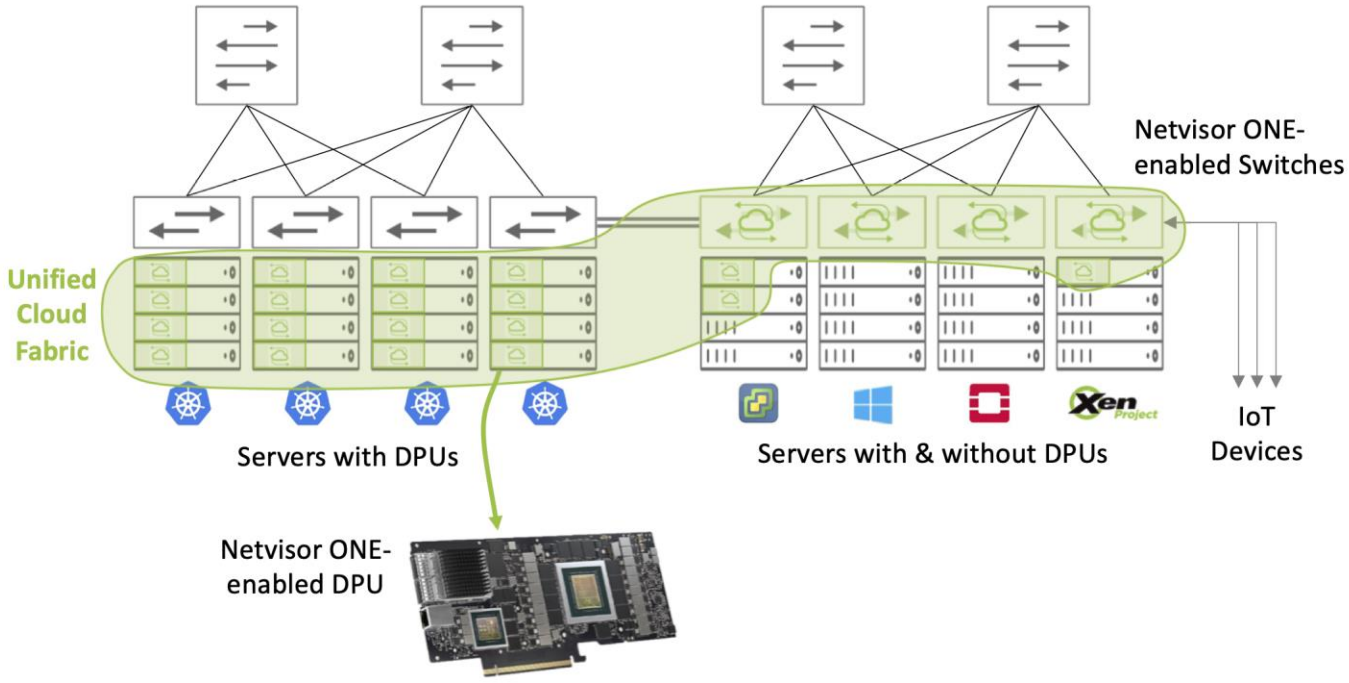


Source: Pluribus

To create operational efficiencies, Pluribus has extended the capabilities of its proven Adaptive Cloud Fabric to create a Unified Cloud Fabric architecture that leverages NVIDIA DPUs.

This ensures that any overlay services available on the switch are now available on the DPU and SmartNIC.

Figure 4. Pluribus Unified Cloud Fabric



Source: Pluribus

As a result, organizations can now implement a unified cloud fabric overlay that supports a heterogeneous, multi-hypervisor environment and deploy new levels of zero trust leveraging micro segmentation with a distributed firewall. Future capabilities will include Kubernetes (K8S) fabric automation and encryption capabilities for east-west traffic, data center interconnects, and hybrid cloud connectivity.

The Pluribus Networks Unified Cloud Networking solution and NVIDIA DPU-enabled SmartNIC provide value across a number of areas. According to Pluribus, these can be broken down into four main categories: unified and automated networking, distributed security, pervasive visibility, and open networking. The potential TCO benefits include the ability to dramatically save time, optimize CPU utilization, and dramatically reduce hardware and software CapEx and OpEx costs (see Table 1).

Table 1. Pluribus Potential TCO Benefits

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, **$60k+ 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

Source: Pluribus

The Bigger Truth

Modern application environments are rapidly gaining ground in the enterprise, and network environments need to evolve in order to better support these dynamic and distributed environments. Organizations deploying these modern application architectures in existing data centers will find numerous network challenges, due to the fact that most data centers still leverage legacy architectures that require multiple network management solutions and individual appliances for each network and security service deployed. While this model worked for prior application architectures, it can impact performance, security, and cost-efficiency.

Organizations need to take advantage of new network architectures that enable unified network management and network services to be distributed with the applications, at scale, and in an operationally efficient manner. These solutions need to provide pervasive visibility, automation, and zero trust-distributed security. Modern solutions also must preserve the value of existing investments in organizations' on-premises data centers or colocation facilities while providing the scale, agility, and performance to embrace modern applications.

Enterprises and service providers deploying cloud-native applications in their existing data centers should explore how the Unified Cloud Fabric from Pluribus and Bluefield DPU from NVIDIA can provide real value to their organizations. The combined solution enables greater operational efficiency, enhanced security, lower total costs, and the ability to deliver high performance at scale.

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188