Propelling the Hybrid Cloud into a New Era of Accelerated Infrastructure with VMware vSphere

Project Monterey – Prepare your infrastructure to meet the needs of next-gen apps

Get Started

vmware

Next-Generation Applications Are Influencing Changes to Data Center Architecture

Modern applications are not what they used to be. They are often distributed in nature and utilize a complex set of microservices to accomplish their tasks. Today's apps process lots of unstructured data such as text, images and log files, and utilize advanced AI/ML techniques and analytics. Many require real-time data processing. Above all, they are more varied and numerous than ever.

However, CPUs are not always fully suited to serve the needs of these new types of workloads. To improve application performance, specialized accelerators such as data processing units (DPUs, also known as SmartNICs), GPUs (graphics processing units) and FPGAs (field programmable gate arrays) are used to accelerate application-specific functions, like image processing. This trend has resulted in the creation of application-specific infrastructure silos, which leads to operational inconsistencies among different types of workloads.

With the ubiquity of 5G connectivity and the migration of workloads to multi-cloud architectures, the volume of modern microservices applications is rising exponentially. These workloads often increase east-west data center traffic, resulting in higher demand for infrastructure services and lower yield of computing resources for business and mission-critical applications.

In addition, as enterprise computing expands into a distributed scaled-out infrastructure across the data center, edge and cloud, the nature of security vulnerabilities and overall impact of threats is changing constantly.

These application-driven macro trends are making it difficult for IT infrastructure managers to manage costs, performance and efficiency. Enterprise IT infrastructure teams are looking for an agile, on-demand infrastructure that is easily scalable and that can manage new as well as legacy applications.

IDC predicts that over 500 million new applications and services will be developed using cloud native methods by 2023.[1]

1. IDC FutureScape. "Worldwide IT Industry 2020 Predictions." IDC #US45599219. October 2019.

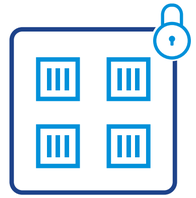
Challenges of Traditional Infrastructure Architectures

Traditional infrastructure architectures are not equipped to handle the demands of heterogeneous, distributed, multi-cloud applications.

Some AI/ML inference services spend as **little as 33% serving** the application needs and the rest in orchestrating services.[2]

Increased operational complexity from infrastructure silos – With the increase in application-specific infrastructure silos to meet the needs of workloads such as AI/ML, IT operations teams need to create and maintain specialized infrastructures in addition to the traditional IT infrastructure. The divergence in the operating models of these specialized silos results in increased complexity and cost.

Higher server scale-out costs to meet infrastructure services demands – Traditional and network server scale-out techniques don't work as, paradoxically, an ever-increasing portion of the newly added server capacity is used by infrastructure services.



Unacceptable security risks to mission-critical applications from a CPU- and OS-centric security model – The current data center architecture where the application and infrastructure services both run on the same CPU must be strengthened with additional layers of defense against low-level threats. Enterprises are looking for ways to offer more robust security models that isolate the workload from the infrastructure domains.

2. IEEE Micro. "Understanding Acceleration Opportunities at Hypescale." Akshitha Sriraman, Abhishek Dhanotia, May/June 2021.

Project Monterey Reimagines the Virtual Infrastructure

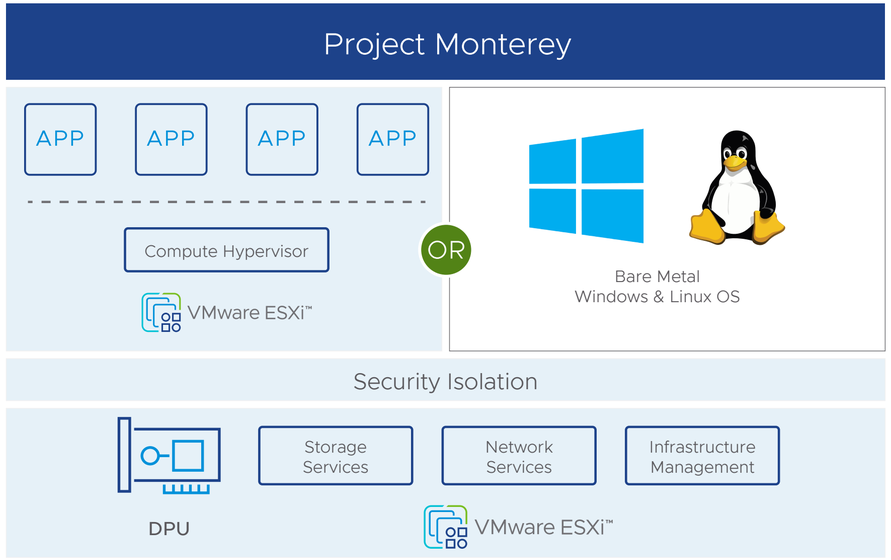
Without a redesign of the software and hardware infrastructure management layer, supporting modern applications on existing infrastructures will lead to an unsustainable increase in both total cost of ownership (TCO) and security risks. It is clear that a new approach is required.

Project Monterey is a new way to architect the core infrastructure by orchestrating and managing infrastructure services with DPUs that

- Run and administer core infrastructure services including composing and consuming hardware resources on demand
- Can manage the lifecycle of new kinds of workloads such as bare-metal, in addition to traditional virtualized and containerized workloads
- Can offload infrastructure services from CPUs, such as security and network processing

By integrating tightly with DPUs, Project Monterey creates an alternate control fabric comprised of DPUs.

Project Monterey leverages existing tools and user experiences to preserve the existing Day 0, Day 1 and Day 2 experience that customers are familiar with.



Project Monterey reimagines virtual infrastructure as a distributed architecture that is enabled by the DPU and offers a single, secure operating model for traditional, cloud native and bare-metal workloads for VMware vSphere®.

Project Monterey Helps Enterprises Respond Rapidly to Application-Driven Infrastructure Needs

Unified and consistent manageability

Project Monterey provides a single, secure operating model that unifies management for traditional, cloud native and bare-metal workloads. It proactively monitors, identifies and mitigates network infrastructure bottlenecks. It reduces the operational overhead of managing DPU lifecycle by leveraging familiar and known VMware tools and methods.

Improved performance

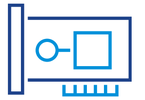
Project Monterey enables the offload of infrastructure functions from host or server CPUs to DPUs, thus freeing up CPU cycles to serve applications. This results in higher workload consolidation per host and lower infrastructure TCO. Additionally, the latency and throughput of the infrastructure are improved by accelerating infrastructure services on the DPU.

Enhanced infrastructure security

Project Monterey hardens the security posture of the infrastructure by providing an air-gapped isolation between infrastructure and workload domains. Project Monterey enables a uniform security control model across virtualized and bare-metal workloads.

Single, secure operating model across workload types

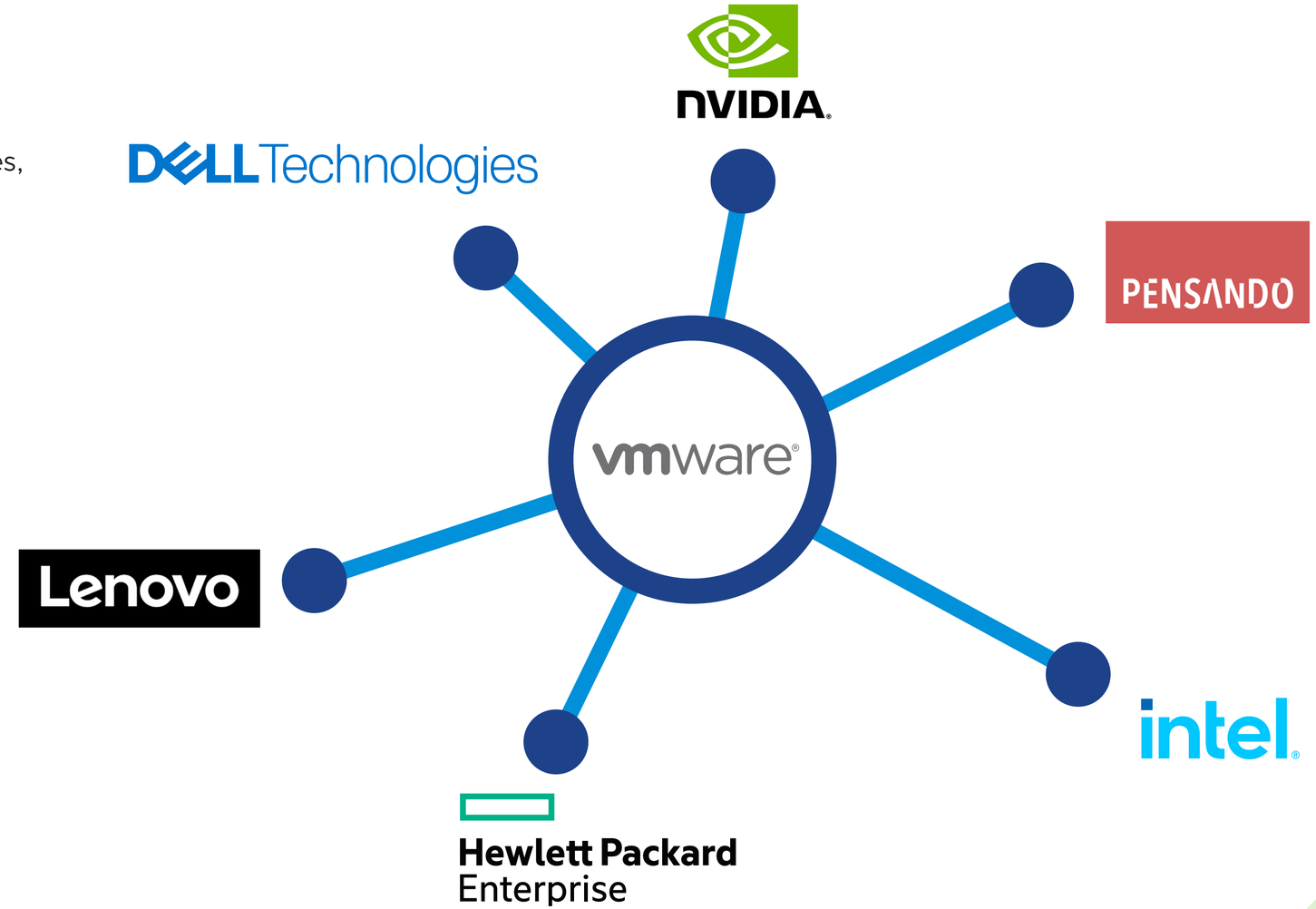
Isolation of workload domain from the infrastructure domain



Offload infrastructure service functions to DPUs

Partner Ecosystem

VMware is bringing together a broad ecosystem of leading DPU (NVIDIA, Pensando and Intel) and server vendors (Dell Technologies, HPE and Lenovo) to deliver flexible and integrated solutions.



Efficiently Support the Needs of Next-Gen Applications

Project Monterey, through its ecosystem of DPU and server vendors, enables the infrastructure to deliver maximum performance for services and applications.

It reduces operational overhead by establishing a common operating model across bare-metal, traditional and cloud native workloads.

Project Monterey provides an enhanced Zero Trust model by separation of infrastructure and workload domains.

Get Started Today

To learn more about Project Monterey and VMware's collaborative approach to developing a vibrant ecosystem, visit our website.

LEARN MORE