Solution Brief

Distributed Services for Regulated Industries

Regulated Industries are at a Crossroads

Large enterprises in regulated sectors are facing immense challenges with their IT infrastructure as they undertake the task of building a private cloud / hybrid cloud architecture. There are several compelling reasons for this shift. Cloud has changed the way data centers are built today with a focus on a distributed "scale out" architecture incorporating homogeneous elements, affording economies of scale, simplified management, and great flexibility in allocating compute and networking resources to ever-changing application workloads.

But there are challenges to this transformation, including:

- Meeting compliance requirements (SOX, PCI-DSS, Dodd-Frank, GLB Act, GDPR, HIPAA) in a cloud infrastructure requires new policy enforcement and auditing capabilities, given the dynamic environment
- Existing monitoring and observability tools are inadequate to handle the scale and complexity of virtualized, bare-metal and containerized environments
- Organizational IT silos often separate the management of compute, networking and security, which gets in the way of providing seamless compliance, in addition to making the operational model complex

Many regulated enterprises require isolated pools of compute resources which are often implemented through a collection of appliances dispersed throughout the data center (Figure 1). This has created limitations imposed by the rigidity of the network, causing problems such as bandwidth bottlenecks and chokepoints at services appliances, operational complexity associated with traffic stitching to ensure symmetric traffic flows for services, all barriers to agility. Disparate management domains and disjointed tooling and siloed teams and processes only act to limit the ability to rapidly deploy applications in the data center.

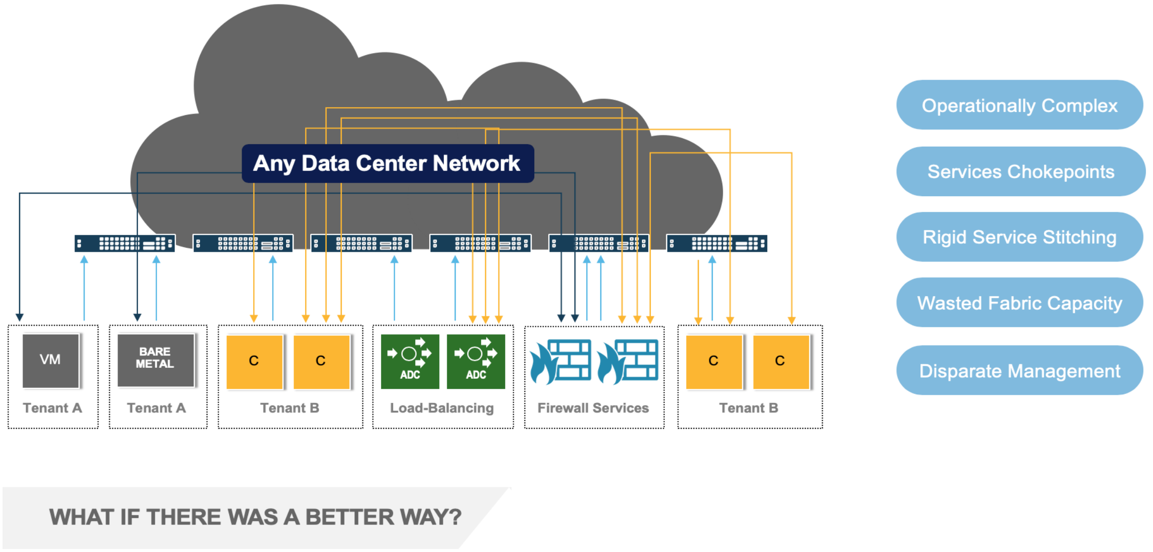


Figure 1: Enterprise Networks Today

These complex legacy "scale up" approaches are expensive, both in CapEx spending and in ongoing staffing needs in order to manage the disparate systems. Furthermore, visibility is hindered by network complexities, separate management systems, and the oceans of data collected from multiple purpose-built appliances with no top-level holistic view. In such a complex environment, the average time to pinpoint problems has become intolerable. An hour of downtime on a critical data center resource can cost an organization over $100K[1].

[1] Study by Ponemon Institute

The key to modern data center efficiency is agility—the infrastructure must support allocating resources to applications and services according to their needs, and dynamically change the allocation quickly when needs change.

A More Efficient, Manageable and Secure Data Center

Just as compute and storage systems are adopting a "scale out" approach, so too the networking and security elements of the data center must adopt a *Scale-out Services Architecture*, and these functions need to find a new home in this model. The ideal place to instantiate these services is the server edge (the border between the server and the network) where services such as firewall, encryption, tunneling and VPN termination can be delivered in a scalable manner. Since each server edge is tightly associated with a single server, its services only need to be aware of the policies related to that server and its users and applications. This approach naturally scales – as more services capabilities come along when new servers are added. It also enables a simple and flatter infrastructure with reduced fault domains for better reliability and availability.

The key elements that capture state-of-the-art cloud architecture principles are:

Distributed Services: Eliminating centralized functions (Firewall, VPN, Load Balancer, Storage, TAP Clusters, etc.) and moving this functionality closer to the workload, directly at the server edge

Pervasive Real-Time Visibility: Enable network and security event visibility, with the ability to monitor at the application level, as close to the workloads as possible

Granular Security: With disparate applications sharing a common infrastructure, security that is immune to workload compromise must be enforced at the server edge with network authorization policies specifying permitted communication (allow list), and encryption of the communication path

Cost-Effective Scale and Performance: Distributed services at the server edge scale intrinsically as servers are added, eliminating the choke-points seen with traditional appliances

Unified Management: Centrally-managed policy-based systems that ensure consistent policy enforcement, even as virtualized workloads migrate from one physical machine to another

Comprehensive Audit Logging: Deep visibility into services and user activities in a segmented environment with auditable logging and reporting to ensure regulatory compliance

In addition, compatibility and integration with existing network Orchestration tools (Ansible, VMware vCenter®, Openshift, Cisco APIC, etc.) is a typical requirement, in order to minimize disruption to ongoing operations and to facilitate a single management view of the Data Center.

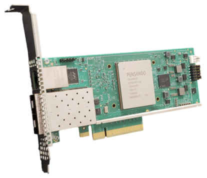
The Pensando Distributed Services Platform

Pensando has developed the **Distributed Services Platform**: a comprehensive offering that delivers software-defined services at the server edge with centralized management and automation. This programmable system delivers:

- Fine-grained firewall, and micro-segmentation between bare-metal, virtualized and containerized workloads
- Software defined networking at the compute edge, with native integration of routing, switching and overlays
- East↔West encryption within the data center, including TCP/TLS termination
- Programmable platform with protocol flexibility to support VXLAN, MPLS, SR-MPLS, SRv6
- Load balancing
- NVMe virtualization, NVME-oF, RDMA, RoCE v2++

The Pensando platform components include:

- The Pensando Distributed Services Card (**DSC**). Installs into servers and provides advanced networking, security and storage services at the server edge, as well as high-speed Ethernet I/O at 10, 25, 40, 50 or 100Gb/s.



- The Pensando Policy and Services Manager (**PSM**). A foundational element of the Distributed Services Platform, built for high availability and fault tolerance using a clustered micro-services architecture. It provides full life cycle management of the platform and all associated security, load-balancing, encryption, and network services, with deep end-to-end visibility.

Software-Defined Services at Wire Speed

The agile nature of data center infrastructure (e.g., new networking protocols, security threats, storage technologies) demands that solutions must be software-defined with the ability to securely update functionality in the field. Pensando offers bundled software packages that can be deployed individually or combined:

Advanced Networking – Switching/Routing, Overlay (VXLAN), MPLS VPN/SR-MPLS/SRv6, NAT, Rate Control

Advanced Visibility & Telemetry – Always-On Telemetry: Application flow information for operational troubleshooting & policy-based security compliance, programmable data plane with flow filtering and export, packet capture with bidirectional ERSPAN and Netflowv9. Programmable data plane telemetry, flow capture/mirroring (bidirectional ERSPAN), intelligent alerting and thresholding, network probing/visibility

Advanced Security – Stateful firewall, detect and protect against different network anomalies and attack vectors, Micro-Segmentation, VPN termination (IPsec), TLS/DTLS encryption, TLS Proxy, AES-XTS data-at-rest encryption

Advanced Storage – NVMe virtualization, NVMe-oF over TCP or RoCE, compression/decompression and dedup offload

Deploying the Pensando Platform

The Pensando Distributed Services Platform can be readily deployed as part of an ongoing server refresh cycle. The platform is fully compatible with bare-metal, virtualized or containerized environments. The DSC PCIe card and driver are the only elements required at the compute nodes – no server agents are needed and existing hypervisor, OS and applications are untouched.

Pensando Distributed Services Card

By bringing a complete package of network, security and storage services into the server edge, powered by the Pensando DSC, significant simplification of the data center is achieved, eliminating network zones, and removing firewall and load balancing chokepoints as shown in Figure 2. The DSC's ability to run wire-speed network services enables implementation of a full routing stack at each server, including segment routing capabilities. This architectural approach delivers streamlined network flows with no tromboning, reducing network latency and jitter. The result is a simpler, flatter network architecture that is easier to manage and ensure regulatory compliance. Micro-segmentation, firewall, encryption and other security services are positioned directly adjacent to the workloads, providing a powerful toolset to the network security administrator.

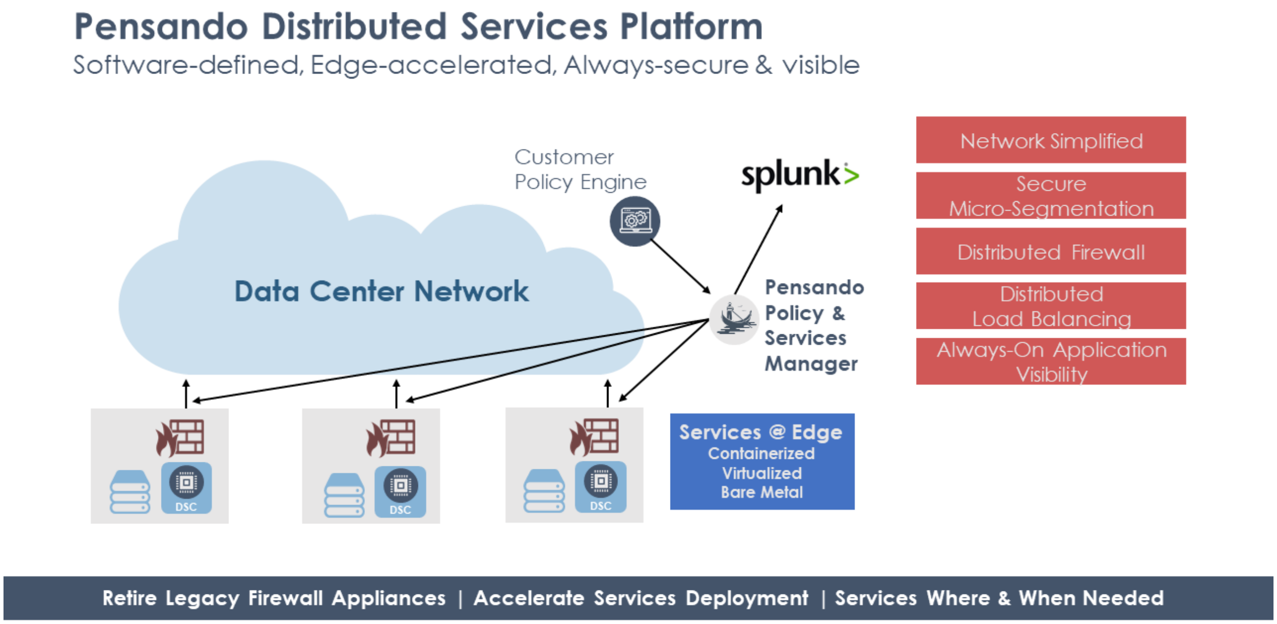

Pensando Distributed Services Platform
Software-defined, Edge-accelerated, Always-secure & visible
Data Center Network
Customer Policy Engine
splunk>
Pensando Policy & Services Manager
DSC
DSC
DSC
Services @ Edge
Containerized
Virtualized
Bare Metal
Network Simplified
Secure Micro-Segmentation
Distributed Firewall
Distributed Load Balancing
Always-On Application Visibility
Retire Legacy Firewall Appliances | Accelerate Services Deployment | Services Where & When Needed

Figure 2: Data Center simplification with services at the server edge

As an independent device at the server edge, the DSC is perfectly situated to provide extraordinary visibility into network performance as well as overall infrastructure health and security. Any workload misconfiguration or compromise which violates policy is automatically detected and reported. The rich telemetry metrics collected by DSCs help to pinpoint performance issues—such as a sudden increase in latency or network jitter—that can be signs of underlying problems. In addition, the DSC can assist in capacity planning with its ability to measure live network performance and latency.

Once installed, services can be dynamically enabled and disabled—including chained services such as micro-segmentation, encryption and network routing—with no degradation to server or network performance. Existing purpose-built appliances may be decommissioned as appropriate and the data center architecture radically simplified, with services tightly coupled to the applications at the compute edge, thereby simplifying operations. Design now is simplified to a traditional leaf/spine switch.

The resulting data center architecture is highly resilient and scalable, since every server is fitted with a dedicated services subsystem. An outage with any individual server does not compromise any of its peers. Just as in the cloud, workloads can be migrated to other servers, while the Pensando platform ensures that the correct policy tracks with the application in its new destination.

Policy and Services Manager

The Pensando **Policy and Services Manager** (**PSM**) manages all DSCs, enabling seamless distribution of policy for networking, security and storage services across the enterprise, service provider and cloud data centers. The tool also provides centralized visibility of the network services, consolidating statistics and telemetry information, thereby simplifying network operations and management. In addition, the PSM handles DSC lifecycle management including discovery, admission, decommission, secure software upgrade and hardware device management.

Integration with Enterprise Management: RESTful APIs enable the PSM to be integrated with Enterprise Management and Automation tools such as VMware vCenter®, OpenShift™, Ansible, Chef/Puppet, as well as SIEM tools such as Splunk for log/event export. The orchestrator can push policy commands into the PSM for deployment to the DSC nodes and all related telemetry, log, and device status can be forwarded to the 3rd party controller or a centralized syslog server.

Dynamic Workload Management: One of the attractions of a Cloud architecture is the ability to distribute workloads and their accompanying services anywhere. The PSM provides the automation to ensure that policy and services follow workloads as they move.

High Availability: The Policy and Services Manager is deployed as a quorum cluster, with 3, 5 or more participating voting nodes. Multiple node failures can be tolerated with no impact to the ongoing operations. Further, the management system is designed to tolerate network interruptions or nodes being down during policy updates.

Scale: A single PSM controller node can manage thousands of DSC nodes, and a federation of PSMs allows scaling to over 1M end points.

Pensando Distributed Services – Tangible Benefits

Benefit	
Simplified Data Center Networking and Services	Removes need for tromboning and rigid network services stitching/chaining, saving fabric bandwidth, lowering application latency and radically simplifying operations Greater flexibility to reconfigure *where* services run, enhancing workload and service mobility A server becomes a first-class network entity, enabling a full networking stack in the compute node Security and Networking services are independent of hypervisor and OS and can be applied on any server where DSCs can be installed.
Compute Efficiency	The DSC offloads multiple compute-intensive services, freeing server CPU cores to be dedicated to running business applications Pensando technology offloads 30% or more of the CPU resources, freeing the server for business workloads, reducing network latency and increasing throughput.
Enhanced Security	Micro-segmentation and firewall can be applied—per application, VM, or container—on the DSC subsystem with full isolation from host-based vulnerabilities The attack surface of the DSC is minimized with Pensando's HardGap™ technology that isolates the host from the DSC's internal processing and memory, preventing unauthorized access Only encrypted/authenticated admin. access allowed from the PSM
Greater visibility and telemetry	Comprehensive and accurate network telemetry with the ability to monitor 100% of traffic at each server at line rate Supports baselining and intelligent alerting NetFlow streaming from any server node with flow-level filtering
Cost savings	Eliminate expensive purpose-built appliances and associated maintenance agreements by consolidating services into DSCs

Pensando Distributed Services – Intangible Benefits

Benefit	
Efficient Troubleshooting	Improved telemetry and visibility together with network simplifications reduces time to trace and root-cause network problems
Operational Simplification	Agile and streamlined management of multiple services through a single pane of glass
Scale	Services scale as the number of servers grows. No need for "forklift upgrades" of service appliances when capacity limits are reached.
Regulatory Compliance	Policy-based data protection assures compliance to SOX, PCI-DSS, GLBA, HIPAA and GDPR with extensive logging and audit capabilities.
Reliability	Fewer appliances, simpler network with straightforward traffic flows enhances reliability, resulting in fewer service disruptions. Distributed, fault-tolerant Policy and Services Manager for high-availability

Summary

Regulated industries are constantly under pressure to streamline their operations, improve security and regulatory compliance while scaling-up to meet new computing demands. Pensando's cloud-scale edge services platform solves the most critical challenges facing enterprise IT management.

About Pensando

Founded in 2017, Pensando Systems is the company pioneering distributed computing designed for the New Edge, powering software-defined cloud, compute, networking, storage, and security services to transform existing architectures into the secure, ultra-fast environments demanded by next generation applications. The Pensando platform, a first of its kind, was developed in collaboration with the world's largest cloud, enterprise, storage, and telecommunications leaders and is supported by partnerships with Hewlett Packard Enterprise, NetApp, Oracle, IBM, Equinix, and multiple Fortune 500 customers. Pensando is led by Silicon Valley's legendary "MPLS" team—Mario Mazzola, Prem Jain, Luca Cafiero, Soni Jiandani and Randy Pond—who have an unmatched track record of disruptive innovation having already built eight $Bn/Year businesses across storage, switching, routing, wireless, voice/video/data, & software-defined networking. The company is backed by investors that include Lightspeed Venture Partners, Goldman Sachs and JC2 Ventures.

For more information, please visit pensando.io .