Solutions Overview

PENSANDO

Pensando Response to Cybersecurity Executive Order

In response to persistent and increasing threats to public and private infrastructure, in May 2021 President Biden signed the Executive Order on Improving the Nation's Cybersecurity, noting that "protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector" in both responding to cyber attacks and sharing information to detect and mitigate threats.

The **Pensando Distributed Services Platform** is uniquely positioned to deliver software-defined visibility, network, and security services via a highly programmable, centrally managed architecture implemented at the server edge. Since it is securely isolated from server resources, the Pensando platform can be used to address several key requirements outlined in the executive order:

- Zero Trust network security
- Encryption of data in flight
- Extended Detection and Response (XDR): aligning network telemetry with endpoint telemetry to detect attacks in a data center
- Long-term network telemetry to provide a source of truth for investigating and remediating risks and incidents

The Pensando platform can meet these goals with zero impact on the server itself and no changes required to the underlying network. Server resources are freed to scale for workload hosting while the Pensando data processing units (DPUs) host these mission-critical services. Pensando DPUs can be implemented either within servers equipped with the **Pensando Distributed Services Card** (**DSC**), or through the **Aruba CX 10000 with Pensando Distributed Services Switch** (**DSS**), a new class of switch providing distributed stateful services for the top-of-rack networking layer.

Although the directives outlined in this executive order are primarily aimed at both the Federal Government and its service providers, its recommended changes and investments can be a guideline for private sector entities looking to strengthen their own security posture and evaluate how they coordinate with their IT and OT partners.

Pensando Overview

Just as data centers are adopting a "scale-out" approach for compute and storage systems, the networking and security elements of the data center must also adopt a scale-out services architecture, and the network, security, and visibility functions need to find a new home in this model. The ideal place to instantiate these services is at the server edge, where services such as encryption, firewall, visibility, and networking can be delivered in a scalable manner.

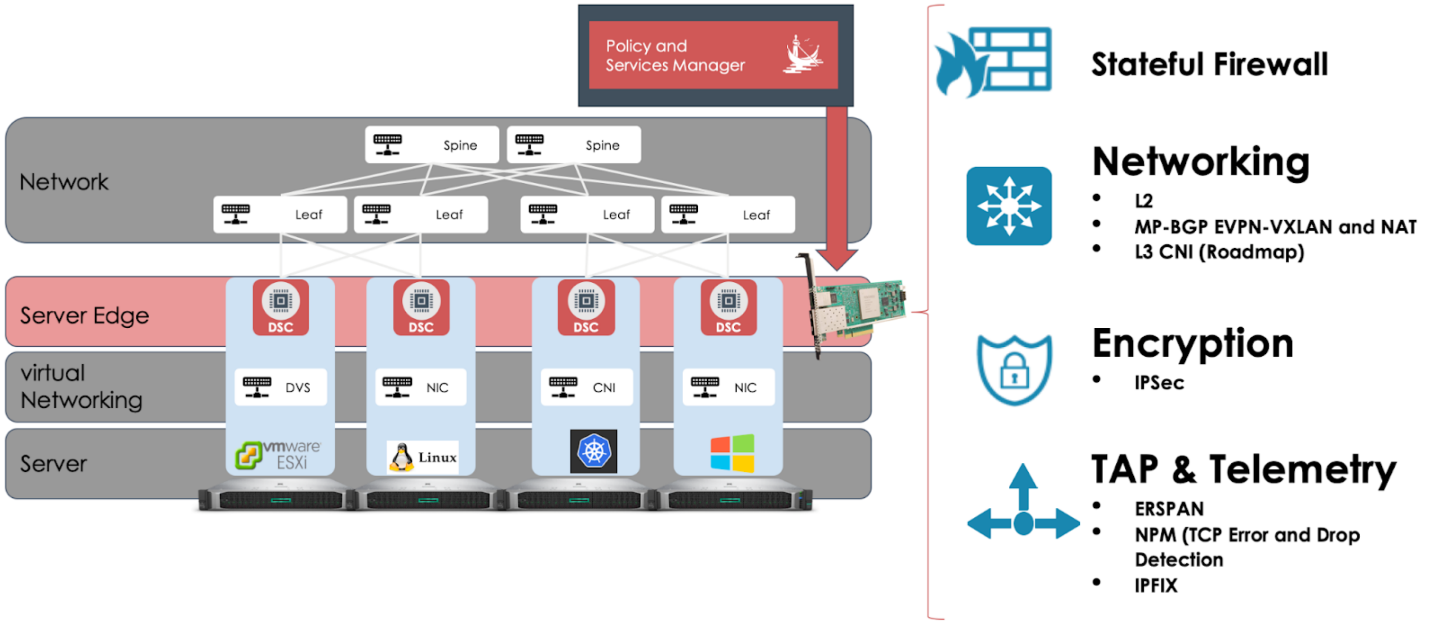
The heart of the Pensando platform is a custom, P4-programmable DPU, which can be easily added as a network card to any server via the Pensando DSC, or to network environments via the CX 10000 top-of-rack

DSS. Since each DSC becomes the network interface on a host server, it only needs to be aware of the policies related to that server and its users; similarly, each DSS can be configured to enforce policy as appropriate for the hosts it connects to the network. This approach naturally scales, as more services capabilities are made available as each new server or switch is deployed.

The Pensando Distributed Services Platform delivers a powerful suite of software-defined services at the compute edge. Pensando's technology provides high-performance scalable networking, security, and visibility functions, eliminating an assortment of discrete appliances throughout the data center, and dramatically simplifying IT operations while providing unmatched telemetry, I/O visibility, and security insights.

The Pensando DPU is optimized to execute a software stack delivering network, telemetry, visibility, and security services at cloud scale with minimal latency and jitter, and very low power requirements (~30W for a 100G DSC).

The **Pensando Policy and Services Manager** (**PSM**) controls all aspects of the platform, including life cycle management and health monitoring for all deployed DSCs and DSSes. Resources can be automatically provisioned and new software-defined services deployed from a single pane of glass. The PSM handles seamless distribution of network configuration, encryption keys, firewall rules, etc. to active distributed services nodes to consistently manage network performance while also ensuring compliance. The PSM enables always-on telemetry and deep end-to-end observability across the entire environment, integrating with popular analytics, orchestration, and management tools via open APIs.



Stateful Firewall

Networking

- L2
- MP-BGP EVPN-VXLAN and NAT
- L3 CNI (Roadmap)

Encryption

- IPSec

TAP & Telemetry

- ERSPAN
- NPM (TCP Error and Drop Detection
- IPFIX

Pensando's Approach to Key Executive Order Mandates

Zero Trust Network Architecture

Section 3 (b) states:

> [Agencies shall] develop a plan to implement **Zero Trust Architecture**, which shall incorporate, as appropriate, the migration steps that the National Institute of Standards and Technology (NIST) within the Department of Commerce has outlined in standards and guidance.

Pensando's approach:

Zero Trust networking is based on the premise that flows destined for hosted workloads cannot be trusted, even if both endpoints are within the data center. One of the fundamental requirements for Zero Trust is that all flows should be distrusted by default:—both North/South traffic from outside the data center to applications, and East/West traffic between applications in the data center—and must be verified.

While North/South security requirements have long been understood, the DSC and DSS address a more challenging problem: deploying distributed firewall services to inspect all flows in and out of each server. This service runs on the DSC or DSS at line rate, and can inspect and protect all flows between the server and other workloads in the data center.

Legacy models for East/West firewalling require either a virtualized (VM) firewall to be hosted on the server, other hosted software consuming server resources, or a separate firewall appliance added to the data center, with all flows rerouted ("tromboned") through the appliances. With DPUs in each server (DSC) or top-of-rack switch (DSS), this is no longer required: all flows as they enter or leave the server/workload can be inspected against specific firewall rules to ensure that all inter-workload communication is properly controlled. In addition, all flows are tracked via Flow logs and FW Syslog—which can be easily exported to external systems or used to validate the security posture over time. Stateful firewall logs are time-stamped and logged on a per-rule basis, with a session ID, rule ID, source/destination IP, port and protocol.

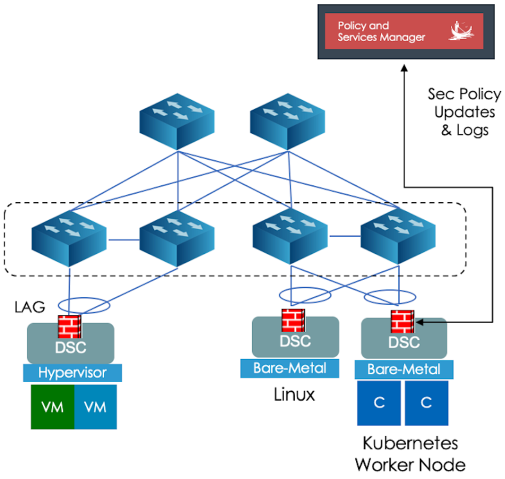
- Stateful Connection Tracking Firewall with ALG & DDoS Protection
- Security policy centrally managed with PSM
- Firewall logs per rule with connection counters, in PSM or exportable to SIEM with syslog

Security Group Policy Definition:

- Policy Rules: IPs, Port/Protocol, Subnets
- Support ingress and egress security policy

DoS & ALG Support:

- DOS: Session Metric Thresholds (TCP/UDP/ICMP) guards against brute-force flooding attacks
- ALG: FTP, SUNRPC, ICMP, DNS, TFTP, RTSP



Encryption of Data in Flight

Section 3 (d) states:

> Within 180 days of the date of this order, agencies shall adopt multi-factor authentication and **encryption for data** at rest and **in transit**, to the maximum extent consistent with Federal records laws and other applicable laws.

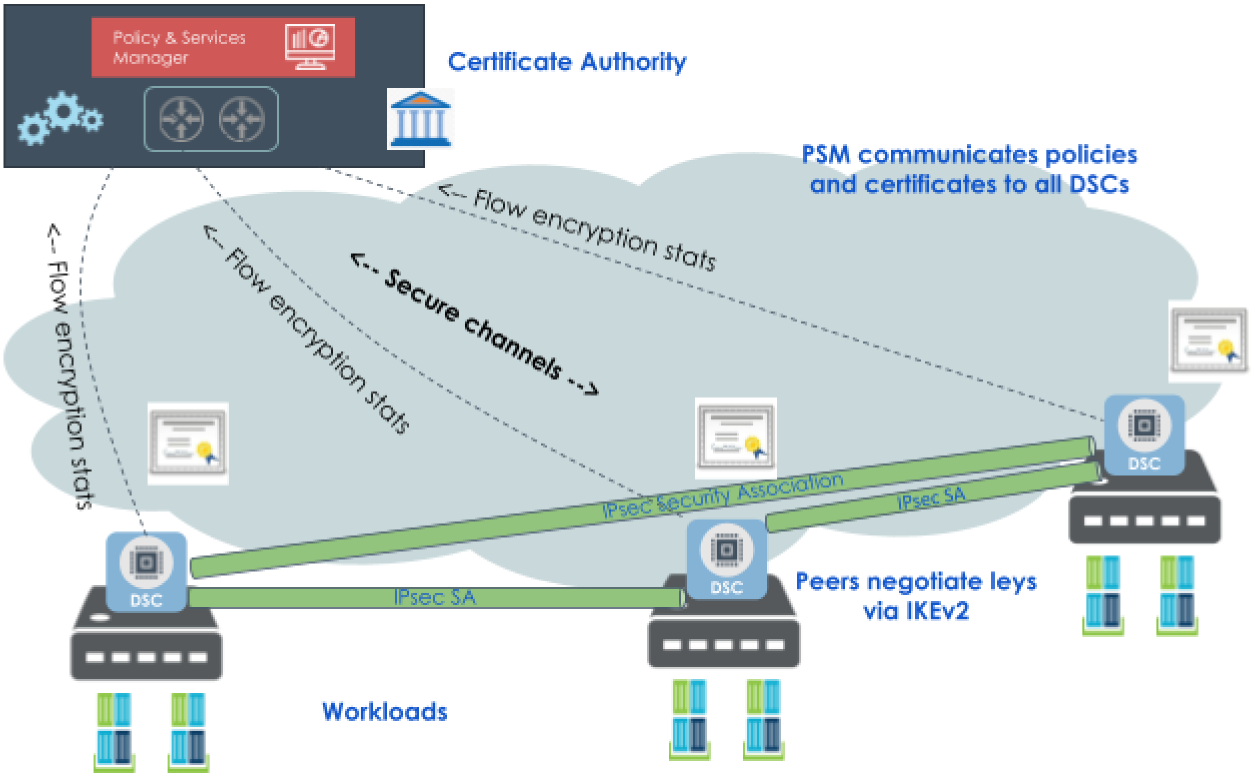
Pensando's approach:

The Pensando DSC supports IPsec encryption between any DSC-enabled servers. Each DSC encrypts all flows between bare-metal, virtualized, and containerized servers transparently, without compromising visibility, and is transparent to applications, developers, and end users. **Always-on encryption** services run on the DSC, at wire speed, and can be configured on a per-workload basis—allowing for "in the clear" flows where required.

There is no requirement to update, modify, or enhance any of the applications in the data center, and there is no impact on workload performance. Encryption is provided by the DSC opportunistically, and supports servers connected at 10G, 25G, or 100G—all at line speed.

The Pensando PSM provides a centralized control point that allows operators to identify where encryption is required, and provision a full mesh of encryption among all DSC-supported servers. Even with encryption enabled, full telemetry, the ability to TAP/ERSPAN flows, and distributed firewalling are also supported—all without any impact on the server.

Policy definitions are used to enable encryption of flows between workloads and between subnets, as well as encrypting access to IP storage. All in-flight IP traffic can be encrypted. The encrypted paths leverage the IPsec protocol and support the ability to configure key rotation on the encrypted links. For additional details, please see the *Pensando IPsec Solutions* white paper.


Policy & Services Manager
Certificate Authority
PSM communicates policies and certificates to all DSCs
<-- Flow encryption stats
<-- Flow encryption stats
<-- Flow encryption stats
<-- Secure channels -->
IPsec Security Association
IPsec SA
IPsec SA
DSC
DSC
DSC
Peers negotiate leys via IKEv2
Workloads

The Pensando Policy and Services Manager simplifies identification of which workloads should be encrypted, and automates the creation of secure connections.

EDR/XDR Support

Section 7 (b) states:

> [Federal Civilian Executive Branch (FCEB)] Agencies shall deploy an **Endpoint Detection and Response (EDR)** initiative to support proactive detection of cybersecurity incidents with Federal Government infrastructure, active cyber hunting, containment and remediation, and incident response.

Pensando's approach:

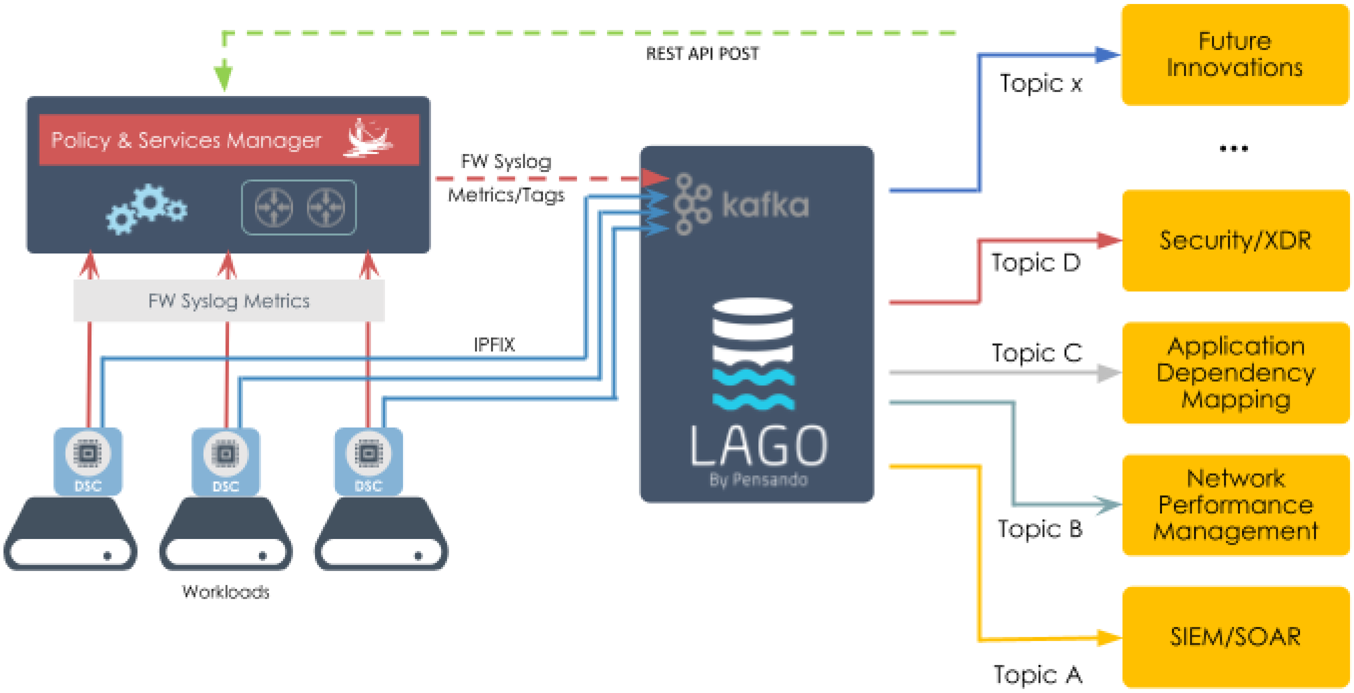
Pensando provides the network telemetry used by EDR/XDR machine learning algorithms to couple agent-based insights with network-based telemetry. Extended Detection and Response (XDR) is a more powerful form of EDR, taking a broader view, integrating security across endpoints, cloud computing, email, and other solutions. A complete view of the threat can be determined by marrying the endpoint and network statistics, assisting in threat hunting and quarantine/mitigation responses.

For this challenge, the unique value of the Pensando platform lies in the intelligence it delivers at the server edge, giving access to full telemetry in the data center—a data source that has been difficult to obtain for most EDR/XDR vendors. The Pensando platform has unparalleled visibility of all flows into and out of each server, and in most cases, visibility to flows between workloads within the same server. This telemetry is captured and exported in the standard IPFIX format for consumption by third party ML engines. The Pensando DSC additionally enables pervasive traffic mirror functions using its hardware bi-directional flow streaming and traffic mirroring capabilities, which can stream server I/O captures to security analytic engines.

Pensando telemetry can feed any EDR/XDR ML engine on the market today. In addition, Pensando has active engagements with several EDR/XDR vendors, allowing them to leverage this telemetry as part of their ML processing of data center flows. All data gathering is performed by the DSC or DSS, removing any overhead burdens from the workload hosts. There are no clients to load, providing no-penalty visibility to the ML tools of interest to allow them to investigate the flows for threats.

Pensando has created an open-source Kafka bus, called *Lago*, to stream this telemetry to as many ML tools as necessary for each agency. Lago is designed to support multiple ML engines if desired, increasing an organization's ability to determine if a breach is taking place.

The output of these EDR/XDR tools can be presented to a SIEM, or the ML tool can directly push commands back to the PSM via open REST APIs, to modify the appropriate DSC or DSS configurations in the network and simplify any mitigation needs.



DSC and DSSes act as sensors close to workloads to collect quality data.

Network and System Logs

Section 8 (a) states:

> Information from network and system logs on Federal Information Systems (for both on-premises systems and connections hosted by third parties, such as [cloud service providers]) is invaluable for both investigation and remediation purposes. It is essential that agencies and their IT service providers collect and maintain such data and, when necessary to address a cyber incident on FCEB Information Systems, provide them upon request to the Secretary of Homeland Security through the director of CISA and to the FBI, consistent with applicable law.

Pensando's Approach:

As described earlier in this overview, the DSC and DSS can provide complete packet captures and full network telemetry via ERSPAN, IPFIX, and Syslog records for all flows in the data center, enhanced by integrations with partners such as Splunk and Elastic to collect, visualize, and store this telemetry. These capabilities dramatically simplify the process of gathering network telemetry. The DSC in each server or switch provides the ability to accurately capture all flows in the data center, without placing any operational or resource burden on other network elements or hosted workloads. (The DSS has the same capabilities today, except for encryption between workloads, which is being evaluated for inclusion in a DSS software update.)

Since the telemetry is collected before encryption of data in flight, the DSC can provide a distributed firewall, and encrypt all E/W flows in the data center simultaneously, without impacting data gathering, increasing latency/jitter, or using additional server resources.

The Lago framework can be used to share any telemetry source (IPFIX, Syslog, and DSC statistics), as seen with the Splunk and Elastic integrations already described. Its extensibility and open interface design are well-suited to the evolving needs of long-term telemetry storage; a new topic can be easily added in support of any additional data collection requirements.

Summary

The Pensando platform is ideally suited to satisfy key provisions of the May 2021 Cybersecurity Executive Order. The solutions described in this brief have been built to grow beyond the needs of today's hyperscalars and can be easily added to any new or existing server with no negative impact on performance or scale. The Pensando Distributed Services Platform is fully software-programmable, enabling the deployment of new capabilities, services and protocols through secure software updates as future requirements are placed on agencies. For further information, please contact us on the web at pensando.io, or via email at info@pensando.io.