SOLUTION BRIEF: SECURITY

Safeguarding AI and HPC Storage Customer Data with VDURA

VDURA High Performance Data Platform

Now in its 11th generation, the VDURA Data Platform delivers industry-leading performance, reliability, and data durability, optimized specifically for HPC and AI workloads. VDURA simplifies complex data management while leveraging cost-effective, commodity hardware to deliver unmatched value and scalability.

VDURA orchestrates multiple storage nodes into a unified storage system, efficiently serving data to HPC compute clusters. Utilizing intelligent software management, VDURA combines nodes featuring HDDs and SSDs, achieving ultra-high throughput (hundreds of GB/s) to support demanding HPC applications.

VDURA autonomously handles failures, continuously balances workloads, proactively protects data integrity, and ensures high availability. It automatically scrubs stored data, rebalances system workloads, and delivers seamless recovery, providing peace of mind with minimal manual intervention.

To safeguard HPC storage and critical customer data, VDURA employs robust security measures to prevent unauthorized access:

- **Online Protection:** Utilizes granular filesystem-level Access Control Lists (ACLs) and Security-Enhanced Linux (SELinux) policies.
- **Offline Protection (Roadmap):** Will implement hardware-based encryption at rest, leveraging industry-standard self-encrypting drives (SEDs)

Data is the Most Valuable Asset

High-performance computing (HPC) systems are essential for organizations in research, academia, commercial, and government sectors, processing massive amounts of sensitive data critical to national productivity and competitiveness.

Protecting this data is vital due to escalating cyber threats, which increasingly involve nation-state actors with sophisticated methods and malicious intent.

Today's HPC environments routinely include tens of thousands of compute nodes with diverse CPUs, GPUs, and accelerators supporting workloads such as scientific computing, engineering simulations, data analytics, and AI/ML. Such environments demand robust, secure, high-performance storage systems like VDURA to maintain data integrity, security, and accessibility.

Multi-Layer Security (Defense in Depth)

VDURA adopts a "Defense in Depth" security strategy, initially popularized by the National Security Agency (NSA). This comprehensive security approach integrates multiple security layers, each providing unique defensive measures, thus creating robust protection against attacks.

The VDURA security model comprises of the below layers:

Policy Layer Includes rigorous certifications, compliance audits, and advanced data handling procedures integrated directly into the system.

Physical Layer Encompasses physical safeguards, environmental controls, access management, and strict enforcement of authorization and authentication policies.

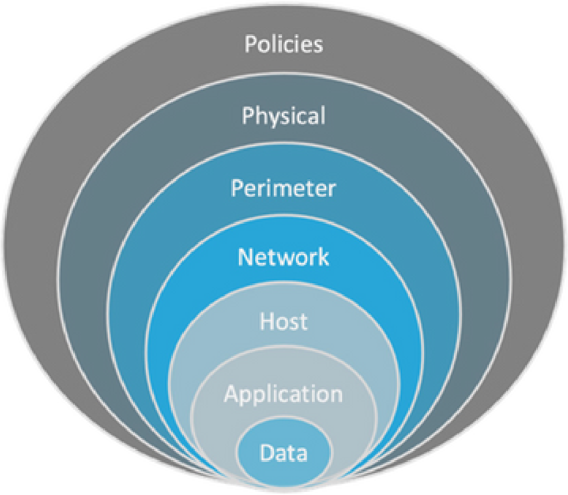

Figure 1: Multi-Layer Security Model.

Perimeter Layer Network-level defenses, including firewalls, IDS/IPS, and SIEM solutions, safeguard data access points.

Host Layer Protects operating systems, servers, virtual machines, containers, with stringent anti-malware and authentication protocols.

Application Layer Ensures secure software development, testing, and rapid patch deployment while maintaining secure application environments.

Data Layer At the data layer, security measures include encryption with hardware-based disk encryption, ACLs, and content-based security such as SELinux security Labels

VDURA's Core Security Features:

Security-Enhanced Linux (SELinux)

VDURA integrates SELinux directly into the filesystem, enforcing mandatory access controls and enabling detailed security labeling. SELinux provides advanced security measures to minimize vulnerabilities, efficiently managing user and system access to data, applications, and processes.

VDURA seamlessly incorporates SELinux security labels as integrated filesystem attributes, streamlining performance and eliminating the complexity typically associated with traditional extended attribute implementations.

The SELinux framework in VDURA includes:

- **Targeted** – The standard and widely-adopted SELinux deployment type.
- **Minimum** – A simplified targeted approach for specific use-cases.
- **Multi-Category Security (MCS)** – Advanced labeling of data based on categories.
- **Multi-Level Security (MLS)** – The highest security level managing comprehensive classified and sensitive data.

This capability allows VDURA customers to share HPC resources securely, dramatically reducing operational, licensing, and hardware costs.

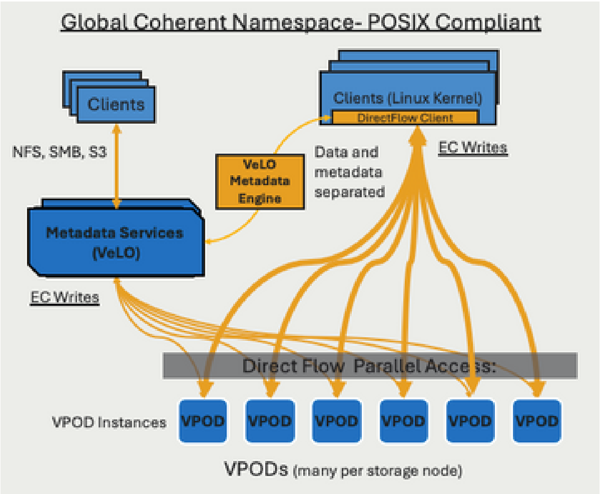

Figure 2: PanFS DirectFlow Client and SELinux Policy Engine Integration.

Filesystem ACLs

VDURA incorporates Filesystem Access Control Lists (ACLs), enabling precise and fine-grained control over data access beyond traditional Linux mode bits. ACLs specify exactly what operations specific users or groups can perform on each file or directory, greatly enhancing security and flexibility in shared computing environments.

ACL management examples include:

- Providing full read/write access for the HPC data of one group.
- Ensuring read-only access for unrelated user groups to specific data directories.
- Completely restricting access across groups where necessary, enabling tight and granular control over organizational data.

Hardware-Based Encryption

VDURA V11 includes plans to incorporate industry-standard Self-Encrypting Drives (SEDs) with hardware-based encryption algorithms, delivering AES-256 encryption-at-rest. These encryption methods ensure minimal impact on storage performance.

VDURA's future roadmap for advanced security capabilities includes:

- Key Management Interoperability Protocol (KMIP) for seamless centralized key management integration with enterprise solutions such as Thales CipherTrust Manager.
- Hardware-based encryption-at-rest designed to transparently safeguard data, preventing unauthorized access if drives become compromised.

Figure 3: Self-Encrypting Drive (SED) with 256-bit AES Encryption Controller.

Safeguarding HPC Storage and Customer Data

The VDURA Data Platform V11 ensures customer HPC storage environments remain highly secure through its multi-layer security architecture, incorporating advanced policy controls, filesystem ACLs, and robust plans for hardware-based encryption. With data security increasingly critical, VDURA remains dedicated to developing state-of-the-art security measures, safeguarding your most valuable asset—data.