FORNETIX®

Enterprise-Grade Key Management for Dell PowerMax Data Storage

Fornetix VaultCore™ and Dell EMC PowerMax

The **Dell EMC PowerMax** line was purpose-built to meet the rapidly expanding needs of modern data storage. The exponential growth in technologies like cloud computing, machine learning, internet-of-things, big data analytics, and artificial intelligence are generating mountains of data and traditional methods for protecting that data are being disrupted. As a PowerMax certified product, **Fornetix VaultCore** is built to deliver scalability, automation, access controls, and policy tools to secure data-at-rest while keeping up with even the highest-performing storage solutions.

PowerMax Redefines Modern Storage

The PowerMax data storage array is a powerful architecture with extreme performance that consolidates demanding, mixed workloads. It is designed for unparalleled speed, optimization, reliability, and efficiency without compromise. PowerMax features end-to-end NVMe flash drives and storage-class memory for sustained bandwidth up to 350GB per second along with 99.9999% availability in a single array.

Rapid and intuitive storage provisioning, workload consolidation, workflow automation, and non-disruptive migration allow for simple and easy operation even in complex environments. Built-in tools for inline deduplication and compression operate with virtually zero impact on performance and increase the overall efficiency of the architecture.

VaultCore Is the Foundational Layer for PowerMax Storage Encryption

Fornetix VaultCore has been certified by Dell for seamless integration with PowerMax via the **Key Management Interoperability Protocol** (KMIP) to bring the benefits of dedicated encryption key management to every storage drive from a unified central platform.

Access Controls & Policy Engine — VaultCore utilizes an **Attribute-Based Access Control** (ABAC) model that allows for the use of fine-grained, least-privilege policies to centrally govern whether a user can access the desired data. Instead of rigid user roles, ABAC leverages a wide variety of attributes as building blocks to construct meaningful policies.

For example, a policy might dictate specific locations, approved devices, certain hours of the day, whitelisted IP addresses, security classifications, department membership, and many other contextual details. Access to the resource is denied if the circumstances fail any of the policy's requirements. VaultCore acts as a **Policy Decision Point** (PDP) in a Zero Trust architecture following NIST SP 800-162 guidelines.

POLICY A   POLICY B

A/B   B

A/B   A/B   A/B/C   POLICY C
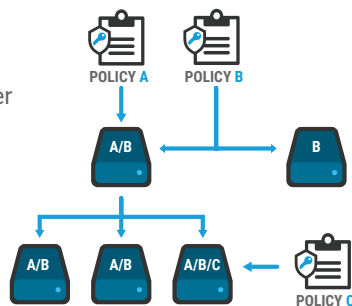
Key Points

- High-performance encryption key management to match the scalability of PowerMax
- Maintain compliance with regulatory requirements for data security
- FIPS 140-2 validated with deployment options for Level 1 through Level 3
- Attribute-Based Access Controls (ABAC) and Policy Decision Point (PDP) for Zero Trust
- Rapid and seamless integration via KMIP industry standards
- Combined architecture fully certified by Dell
- Built on Dell hardware for a secure "Made in America" supply chain
- Available on PowerMax OS: 5978.711.711 + Cumulative Epack 9402 and up
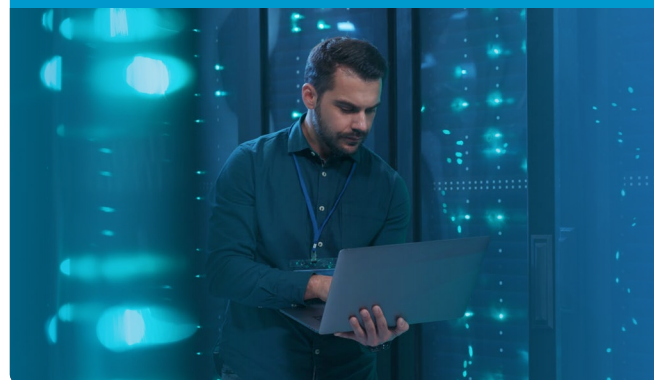
Unmatched Scalability & Automation — VaultCore has an industry-leading capacity that exceeds 100 million encryption keys and certificates, an ideal match for the massive storage capabilities delivered by PowerMax arrays. VaultCore was designed with powerful workflow automation to simplify the arduous tasks of the key management lifecycle, cutting down on human error and reducing overall IT expenditures. Deployment options include virtual appliances as well as rack-mounted hardware appliances with High-Availability configurations available.

Regulatory Compliance — For many organizations, data and privacy regulations like GDPR, HIPAA, CCPA, PCI-DSS, and others have inadvertently created more key material than can adequately and successfully be managed without a dedicated key management solution. This has left organizations struggling to effectively protect their customer's data and balance the burden of costs necessary to protect that data. The combination of VaultCore's scale, policy tools, and logging makes it simple to put in place strategies that automate compliance demands. In addition, VaultCore technology is compliant with government FIPS 140-2 requirements with deployment options ranging from Level 1 to Level 3 (with added hardware security module).

Secure, Trusted Supply Chain — VaultCore is engineered, developed, and supported in the United States, meeting requirements for recent 'Made in America' Executive Orders that impact government procurement. Our hardware is built using proven Dell components and supply chains for maximum reliability and security.

Separation of Encryption Keys — VaultCore enables PowerMax users to secure their encryption keys off-device. This ensures that encryption keys are isolated from the main storage array. If the PowerMax becomes compromised, all data remains safely encrypted since all keys are shielded within a separate cryptographic boundary.

About Fornetix

Fornetix is a cybersecurity platform enabling a Zero Trust future, while delivering critical encryption automation, access controls, authorization services, and machine identity to the federal government and commercial enterprises around the globe. For more information, please visit our website at www.fornetix.com.

Authorized User

VAULTCORE

KMIP

Dell PowerMax

CERTIFIED