DELL Technologies

Security Solution Brief

Security Features that Ensure Unity XT HFA Operational and Data Integrity

Security is vital for storage arrays to protect sensitive data, defend against cyberattacks, comply with regulations, ensure business continuity, safeguard intellectual property, and maintain trust and reputation. By prioritizing security in storage arrays, organizations can mitigate risks, protect valuable data, and instill confidence in their stakeholders.

Access Controls

Unity XT HFAs allow administrators to implement robust access controls such as to ensure that only authorized personnel can access the storage resources. This includes features such as role-based access control (RBAC), which allows assigning specific permissions to different users or groups based on their roles and responsibilities.

Data Encryption

Unity XT HFAs supports data-at-rest encryption (DARE), which helps protect sensitive data stored on the storage system. Encryption ensures that even if the physical drives are compromised or stolen, the data remains encrypted and unreadable without the appropriate encryption keys. Additionally, effective key management is a crucial component with Unity XT DARE as it securely generates, stores, and manages encryption keys ensuring that only authorized individuals or systems can access and use the keys.

Secure Protocols

Unity XT HFAs support various secure protocols such as Secure Shell (SSH), Secure Sockets Layer (SSL), Transport Layer Security (TLS) and HTTP Security Headers. These protocols provide encryption and secure communication channels between client systems and the storage system, preventing eavesdropping or tampering of sensitive information during transit.

Security Auditing and Monitoring

Unity XT HFAs provide auditing and monitoring capabilities that allow administrators to track and analyze storage-related events and activities. This helps in identifying potential security breaches, unauthorized access attempts, or unusual behavior that may indicate a security incident.

Security Ecosystem Integrations

Unity XT HFAs can be integrated with other security products and solutions, such as antivirus software, firewalls, intrusion detection/prevention systems, and security information and event management (SIEM) tools. Integration allows for a more comprehensive security posture by leveraging the capabilities of these solutions alongside the storage system.

Authentication Mechanisms

Unity XT HFAs integrate with various authentication mechanisms, such as LDAP (Lightweight Directory Access Protocol), Active Director to centralize and strengthen user authentication. This ensures that only authenticated users can access the storage resources and management interfaces, reducing the likelihood of unauthorized access. Additionally, Unity XT HFAs provide users with the ability to verify VMware Center Certificates helping to ensure the authenticity and integrity of the communication between vCenter components, hosts, and clients, enhancing the overall security of the virtualization infrastructure.

Patching and Firmware Updates

Like other Dell Technologies products, Unity XT HFAs regularly release firmware updates and patches to address security vulnerabilities. Keeping the system up to date with the latest software versions ensures that known security issues are mitigated.

Learn more about Dell Unity XT solutions

Contact a Dell Technologies Expert

DELL Technologies