====================
H1: Cross-Platform Storage Access Control

Subtitle: Securing Access to File Servers

====================

As heterogeneous networks increasingly spawn data silos -- file servers segmented by storage protocol -- the files of Unix users are usually stored on separate servers from the files of Windows users, making it hard to secure unstructured data with a centralized access control system.

By providing a cross-platform file server with an integrated access control system, Likewise Storage Services secures access to unstructured data regardless of whether a user is accessing it from a Unix computer or a Windows computer. Likewise can authenticate and authorize users with Microsoft Active Directory or another directory service like LDAP.

The benefits of cross-platform storage access control for file servers and NAS systems will instantly please IT administrators, auditors, and security managers:

<!-- bulleted list -->
*Secure sensitive files with a uniform security model and common access controls.

*Show compliance with regulations and standards.

*Mitigate the risk of security breaches, data loss, fraud, noncompliance, and legal problems.

*Reduce the costs associated with identity management, storage, and security.

=============================
Problems in Storage Access Control
It's easy to store unstructured data: The relatively low cost of storage lets it pile up in file servers unmonitored and unsecured.

The worries begin when you realize that the file servers might contain sensitive, proprietary, and confidential information. Even though the cost of storing it is low, the cost of a data breach or incident of noncompliance, whether internal or external, can be high -- risks that heighten the importance of securing it.

Several problems, however, stand in the way of protecting it:

1. Data silos. Because of different storage access protocols, the data of Windows users and Unix users ends up in separate silos, making it difficult to secure Unix and Windows file servers with a common access control system and uniform security policies.

2. Different identity management systems. If platform-specific data silos aren't bad enough, there are often different access control systems for Unix and Windows users. Multiple identity management systems subvert attempts to protect both Unix and Windows file servers with uniform security policies.

3. Monitoring access based on identity. Unstructured data that is segmented into storage silos and controlled by disparate access control systems compounds the problem of determining the users and groups who are accessing sensitive material. Multiple identity management systems can also disassociate access events from user identities.

Likewise solves all three problems by integrating a multiprotocol file server with an access control system that can authorize users with Active Directory or another directory service.

=============================
The Likewise Solution

Consolidating Data Silos into Multiprotocol Storage

Data silos resolutely block efforts to consolidate storage and apply uniform security policies. Compacting stored data into a multiprotocol file server or NAS system is the first step toward securing it.

Likewise Storage Services provides a multiprotocol file server that is accessible by Unix clients using NFS and Windows clients using SMB/CIFS. As a multiprotocol file server, it lays the foundation for cross-platform access control.

Cross-Platform Access Control
Likewise integrates a cross-platform access control system with its file server to authenticate both Unix and Windows users with Active Directory or another directory service. A common point of access control for stored data serves as a technical bridge for implementing uniform security policies.

Managing and securing unstructured data with a common access control system and uniform security policies is crucial to complying with regulations, mitigating the risk of security incidents, and cutting costs.

Associating File Events with User Identities

A file server with an access control system provides a a framework for identity-aware monitoring -- a framework that the Likewise Data Analytics and Governance application uses to show who accesses what data. In addition, the Likewise application features compliance reports that tie access events to user identities.

==========================

Tackle Unstructured Data with Likewise

Companies that put in place systems and policies to protect unstructured data can comply with regulations, mitigate the risk of security incidents, and cut the costs associated with identity management, storage, and security. Likewise technology provides the following functional steps to achieve these goals:

*Consolidate data silos into a multiprotocol file server that works with NFS and SMB/CIFS.
*Secure unstructured data with a cross-platform access control system that works with Active Directory and other directory services.
*Implement consistent security policies for both Windows and Unix users.
*Monitor and report on access based on user identities with Likewise Data Analytics and Governance.

==========================

<!-- sidebar box with list of features; consider setting in same way as the features list in file-activity-monitoring.txt -->

Features
*Active Directory authentication with Kerberos and NTLM
*Additional directory services for LDAP and NIS
*Multiprotocol file server works with both SMB/CIFS and NFS
*File server accessible by Linux, Unix, Mac, and Windows clients
*Identity-aware monitoring of access
*Compliance reports that link access with identity

==