Likewise®

Fact Sheet

FISMA Compliance For File Servers and Storage Systems

This fact sheet outlines Likewise's technical security controls for electronic assets stored on file servers and NAS systems. The fact sheet also discusses how Likewise's architecture provides the foundation and the functionality to perform continuous monitoring of stored assets.

FISMA mandates that you protect information and information systems to provide confidentiality, integrity, and availability. To do so, you must implement security controls in accordance with NIST Special Publication 800-53.

Likewise software helps ensure the confidentiality, availability, and integrity of information in storage systems by implementing security controls that cost-effectively protect against unauthorized access, use, disclosure, disruption, modification, or destruction. In particular, Likewise implements many of the security controls for access control, system monitoring, and audit and accountability.

Information Security

Minimum Security Requirements for Federal Information and Information Systems, the document also know as FIPS 200, defines information security as follows:

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

For FISMA, integrity, confidentiality, and availability are the objectives that security controls are intended to achieve. Federal information policy defines them as follows:

1) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

2) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

3) availability, which means ensuring timely and reliable access to and use of information.

Source: 44 U.S.C., Sec 3542.

Minimum Security Requirements

To provide integrity, confidentiality, and availability, FIPS 200 specifies the minimum security requirements that federal agencies must meet through selecting security controls in NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*. The risk-management process begins by using FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, to categorize information and information systems so you can select appropriate security controls from NIST Special Publication 800-53.

Security Categorization

The generalized format for expressing the security category (SC) of an information system is as follows:

$SC_{\text{information system}} = \{(\text{confidentiality}, \textit{impact}), (\text{integrity}, \textit{impact}), (\text{availability}, \textit{impact})\}$

where the acceptable values for potential impact are low, moderate, or high.

The potential impact values assigned to the respective security objectives are the highest values from among the security categories that have been determined for each type of information resident on those information systems.

The impact levels of a file server or NAS system determined by the security categorization process drive the selection of the initial set of baseline security controls.

Mapping Security Controls from 800-53 to Likewise Capabilities

The following section details the technical security controls that Likewise can put in place to help ensure the security of information and systems.

Likewise makes two software products: Likewise Storage Services and Likewise Data Analytics and Governance.

In general, Likewise Storage Services provides cross-platform authentication and access control.

Likewise Data Analytics and Governance collects, aggregates, stores, analyzes, audits, monitors, and reports on events that take place on file servers and storage systems, including NetApp, HP, and EMC NAS devices.

AU-2: Auditable Events

Likewise collects and stores the following type of events from file servers and NAS systems. You can choose which of them to record as auditable events.

1. Authentication requests and access attempts.
2. Attempts to view, modify, add, or delete directories and files.
3. Attempts to modify the security descriptors of files.

Likewise collects and stores these events and ties them to the identity of users without impairing the system's performance.

AU-3: Content of Audit Records

Likewise collects and stores audit records that show the type of each event and its date, time, source, location, and outcome.

Likewise also captures the identity of the user or application associated with the event.

AU-4: Audit Storage Capacity

The Likewise application allocates storage capacity for audit records by using a uniquely scalable and high-performance NoSQL database that not only reduces the likelihood of its capacity being exceeded but also allocates storage cost-effectively to handle millions of events.

AU-5: Response to Audit Processing Failures

Likewise can send real-time alerts when a variety of events occur, including an audit processing failure. Likewise can provide a warning when allocated audit record storage volume nears or reaches capacity. Likewise lets you configure traffic volume thresholds for event collection and forwarding.

AU-6: Audit Review, Analysis, and Reporting

Likewise analyzes audit records from storage systems. When it finds indications of inappropriate or unusual activity, it sends a security alert to designated sources. You can adjust Likewise's review and analysis thresholds to meet changing levels of risk.

There is support for several control enhancements: Likewise acts as a security event and information management system to correlate and analyze audit records from different repositories, providing organization-wide situational awareness.

AU-7: Audit Reduction and Report Generation

Likewise supports near real-time audit reviews, analysis, and reporting as well as investigations of security incidents without altering the original audit records. In addition, Likewise can automatically process audit records for events of interest based on criteria that you select and display them on a dashboard.

AU-8: Time Stamps

Likewise generates time stamps for all audit records.

AU-9: Protection of Audit Information

Likewise protects audit information and audit tools from unauthorized access, modification, and deletion. Likewise can also limit access to the management of audit functionality to a subset of privileged users, and Likewise protects the audit records of non-local accesses to privileged accounts and the execution of privileged functions.

AU-12: Audit Generation

Likewise lets you generate audit records for all the events it captures and can include the content of the audited events.

AC-2 through AC-11: Access Control

The Likewise Storage Services platform, by connecting Linux and Unix file servers to Microsoft Active Directory, can implement or help implement AC-2 through AC-11. For more information, see Likewise Storage Services.

IA-2: Identification and Authentication

The Likewise Storage Services platform performs identification and authentication of organizational users by using Active Directory or another user directory. For more information, see Likewise Storage Services.

SI-4: Information System Monitoring

Likewise helps your organization monitor events on file servers, NAS systems, and other data storage systems. Likewise tracks specific types of transactions and displays them on a dashboard for situational awareness. For SI-4, Likewise supports several control enhancements, such as providing near real-time alerts when indications of compromise or potential compromise occur and notifying incident response personnel of suspicious events.

SC-29: Heterogeneity

Likewise Storage Services is a multiprotocol file server that runs on Linux and Unix machines to accept connections with SMB/CIFS and NFS. Because the file server runs on Linux computers and furnishes multiprotocol data access to both Windows and Unix machines, you can use it to increase the level of diversity and heterogeneity of your information technologies, reducing the impact of the exploitation of a specific technology. For more information, see Likewise Storage Services at www.likewise.com.

SC-30: Virtualization Techniques

Likewise's multiprotocol file server can run on virtual Linux machines to give you the ability to disguise information systems, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms. The cross-platform file server also works with a diversity of operating systems. For more information, see Likewise Storage Services www.likewise.com.

Architecture for Continuous Monitoring

The architecture of Likewise Data Analytics and Governance can take you beyond fulfilling the minimum requirements of FIPS 200 and into the realm of maintaining situational awareness through continuous monitoring. The Likewise application, for example, collects, correlates, and analyzes all security-related events on file servers and network attached storage, giving you visibility into your storage assets and the users who access them.

The tremendous amount of data from continuous monitoring requires a solution that can scale. Likewise's commercially hardened SQL and NoSQL infrastructure with polyglot persistence can scale beyond a departmental deployment to support storage arrays with hundreds of millions of file objects and high workloads. It can pull data from a variety of information sources through a RESTful interface. It provides reporting with tailored output that spans from high-level, aggregate metrics to system-level metrics. With a built-in dashboard, it acts as a security information and event management (SIEM) tool for storage systems.

The architecture and functionality of the application helps you establish a continuous monitoring program as defined in *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* (NIST Special Publication 800-137).

Trusted by Federal Agencies

In the past, such government agencies as the U.S. Government Printing Office, the U.S. Army, and the U.S. Department of State have trusted Likewise technology for technical security controls.

Next Steps

For more information on Likewise, visit the web site at www.likewise.com. To contact the sales team, call (800) 378-1330 or email info@likewise.com.

About Likewise

Likewise makes an integrated software platform, Likewise Storage Services, for identity, security and storage used by market-leading OEM storage vendors, including Riverbed, EMC and HP. In addition, Likewise Data Analytics and Governance is an application helps enterprise IT organizations mitigate risk and drive greater value from their unstructured data. Likewise Data Analytics and Governance ties identity and other contextual data to unstructured data as metadata for better analytics, governance and compliance, entitlement management, and performance management. Likewise enables organizations to provide both access to and control of their data across mixed network environments. More information is available at the company's website, www.likewise.com.

References

- *Minimum Security Requirements for Federal Information and Information Systems* (FIPS 200)
- *Standards for Security Categorization of Federal Information and Information Systems* (FIPS 199)
- NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*
- NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*
- NIST Special Publication 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*

15395 SE 30th Pl, Suite 140, Bellevue, WA, 98007. (800) 378-1330