FileCloud

NIST 800-171 Compliance Guide

WWW.GETFILECLOUD.COM

Note: This white paper is intended to provide an overview and is not intended to provide legal advice. For more comprehensive information on regulations and their implications, please consult your legal counsel.

Introduction

The U.S. government requires federal contractors to comply with the NIST 800-171 security standard to ensure the security of Controlled Unclassified Information (CUI) in non-federal systems and organizations.

In addition to general requirements for contractors to comply with NIST 800-171, the U.S. Department of Defense (DoD) mandates that all DOD contractors that process, store or transmit CUI "meet the Defense Federal Acquisition Regulation Supplement (DFARS) minimum security standards by December 31, 2017 or risk losing their DoD contracts." Compliance with NIST 800-171 enables contractors to meet those minimum DFARS security standards. This document explains how CodeLathe's product, FileCloud Server, can be used to manage the CUI in non-federal systems and organizations.

CUI is defined as a categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the federal government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination.

FileCloud Server is a highly scalable, self-hosted Enterprise File Sharing and Sync solution (EFSS). The Unique selling proposition of FileCloud are: total control of an organization's data, complete security, unparalleled branding options, and excellent user experience. Security, privacy, and data ownership is fundamental to FileCloud's security architecture. FileCloud security starts with 256-bit Advanced Encryption Standard (AES) Secure Sockets Layer (SSL) encryption at rest, two-factor authentication, SSO (single sign-on), granular user and file sharing permissions, client application security policies, automatic anti-virus scanning of files when uploading, unlimited file versioning, file locking, endpoint device protection, and comprehensive HIPAA compliant audit trail. FileCloud also uses FIPS 140-2 validated crypto module for all its crypto operations (encrypting data at rest and in transit). With FileCloud, you can be rest assured that CUI data is well protected on your servers. FileCloud provides a variety of deployment options: Private Cloud (behind firewall and proxy) and Public Cloud (AWS or Azure Gov Cloud).

Features of FileCloud Server

- Access and sync all your files on all your devices
- Share files to internal and external users
- Mount your remote files as a local drive on Windows and Mac OS
- Integrate mobile apps, Outlook, and Office Add-ons
- Set up Team Folders around projects or departmental needs and allow both employees and partners to securely access their files from anywhere
- White Label Solution - Can be branded for your organization
- Unlimited file versioning and recycle bin support
- Versatile, granular folder permissions to mimic any kind of file share and permissions hierarchy
- Ensure appropriate level of access for every user by assigning individual folder level permissions
- Administrators can manage all devices accessing FileCloud data and monitor suspicious activities in real time
- In case of any suspicious activity, administrators can selectively block devices or permanently remove users from accessing the data
- Complete data security, ownership, and total privacy
- Detailed Audit Trail (What, When, Who, Where, and How)
- DLP - FileCloud's unique capabilities to monitor, prevent, and fix data leakage assures corporate data is protected across all your devices (Laptops, Desktops, Smartphones and Tablets).
- Governance: FileCloud's detailed activity logs, connected devices inventory, and access logs provide all the right tools to satisfy any data compliance needs.
- Ransomware protection, workflow automation, federated search, admin reports, meta data system, policy management capabilities and more ….

The following table maps the NIST 800-171 requirements to FileCloud Server that is hosted by you in your private cloud or public cloud infrastructure like AWS or Azure GovCloud.

NIST 800-171 Requirement	Details	How FileCloud Server Supports NIST 800-171 Compliance
3.1.1	Limit information system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	The FileCloud platform provides comprehensive access controls and device management capabilities to manage and access the CUI.
3.1.2	Limit information system access to the types of transactions and functions that authorized users are permitted to execute	FileCloud's granular access permissions (view only, download, upload, share, sync, and delete) allow System admins to limit authorized user access to CUI.
3.1.3	Control the flow of CUI in accordance with approved authorizations.	FileCloud's powerful workflow capabilities provide control mechanisms (copy, move, delete, verify integrity and notify owners) to manage the flow of CUI.
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	The FileCloud platform offers RBAC, groups, and powerful policy management capabilities to separate the duties of individuals who will be using the FileCloud system.
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	FileCloud's role, group, and policy-based access management capabilities allow system administrators to define access policies that employ the principle of least privilege.
3.1.6	Use non-privileged accounts or roles when accessing non-security functions.	FileCloud offers role-based access controls and different user types to access non-security functions
3.1.7	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	FileCloud prevents non-privileged users from performing administrator duties. Privileged administrator actions are also kept in audit records.

3.1.8	Limit unsuccessful logon attempts.	The FileCloud platform allows the administrators to set the maximum number of unsuccessful logon attempts.
3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	FileCloud Server is a self-hosted product. Customers can create their own privacy, Terms of Service (TOS), and security policies.
3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity.	FileCloud provides the ability for system administrators to set session locks. After a defined period of time, the user sessions are terminated. However, FileCloud does not use pattern hiding displays.
3.1.11	Terminate (automatically) a user session after a defined condition.	FileCloud provides the ability for system administrators to set default login sessions using the session timeout parameter. This will keep users actively logged into their account for a limited time only. Once the user exceeds the inactivity period then the session expires, and the user's sessions are terminated. The user must log in again to get access.
3.1.12	Monitor and control remote access sessions.	FileCloud's powerful audit capabilities monitors "what, when, who, why, and how," attributes of every user action (preview, download, upload and other actions) within the system. Administrators can easily monitor the audit transactions and control the user access if needed.
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	FileCloud protects the confidentiality and integrity of your files in transit and at rest. • AES 256-bit encryption to store files at rest • SSL/TLS secure tunnel for files transmission

3.1.14	Route remote access via managed access control points.	FileCloud allows administrators to control which nodes or ports are allowed for remote access. System administrators can also choose to deploy FileCloud behind a reverse proxy.
3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	FileCloud provides a separate administrator portal to execute privileged operations. This portal can be further protected by IP access restrictions and two-factor authentication (2FA) mechanisms.
3.1.16	Authorize wireless access prior to allowing such connections.	FileCloud can be deployed behind a corporate firewall or reverse proxy to authorize wireless access. FileCloud can also restrict based on client IP addresses and disable the ability for client applications to connect.
3.1.17	Protect wireless access using authentication and encryption.	All FileCloud communications (On Transit, At Rest) are protected by NIST-recommended encryption technologies.
3.1.18	Control connection of mobile devices	FileCloud policy management and device management capabilities allow disabling and enabling the connection of mobile devices to FileCloud.
3.1.19	Encrypt CUI on mobile devices and mobile computing platforms.	FileCloud utilizes native encryption provided by the popular mobile platforms (iOS and Android). Administrators can also disable the ability to open content from other mobile applications.
3.1.20	Verify and control/limit connections to and use of external systems.	All external systems (like S3 compatible storage) are controlled by authentication keys.

3.1.21	Limit use of organizational portable storage devices on external systems.	Not Applicable.
3.1.22	Control CUI posted or processed on publicly accessible systems	FileCloud offers a variety of deployment options to control CUI: Host it on-premises servers (private deployment), or host on hybrid or secure public cloud deployments (AWS/Azure GovCloud).

3.2 Awareness And Training

NIST 800-171 Requirement	Details	How FileCloud Server Supports NIST 800-171 Compliance
3.2.1	Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems.	FileCloud Alerts are available in FileCloud's Admin portal which tracks all unhandled exceptions, security issues, and system error messages generated on the server. The number of alerts is shown on the FileCloud Dashboard and the Alerts page will show detailed information about the various errors encountered.
3.2.2	Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.	FileCloud alerts and notifications help the administrators and end users to follow the best practices when it comes to security.
3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	FileCloud audit logs, notifications, and share analytics can be used for user training to identify potential indicators of insider threats.

3.3 Audit And Accountability

NIST 800-171 Requirement	Details	How FileCloud Server Supports NIST 800-171 Compliance
3.3.1	Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.	FileCloud provides comprehensive audit logging (what, when, who, where and how) details. Administrators can export or archive the audit logs for safe keeping.
3.3.2	Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	By providing options to record every action with What, When, Who and How attributes, FileCloud gives customers the best possible audit data to satisfy any type of compliance.
3.3.3	Review and update audited events.	The FileCloud platform helps system administrators and personnel with privileged access to view the audited events.
3.3.4	Alert in the event of an audit process failure.	FileCloud Audit interface clearly shows the audit time line. Administrators can check it periodically to make sure actions are audited properly. FileCloud also sends an alert to the System Administrator if audit archival fails for some reason.
3.3.5	Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.	FileCloud Audit logs can be exported to Security Information and Event management (SIEM) systems and can also be integrated with syslog to analyze and identify suspicious or unusual activity.
3.3.6	Provide audit reduction and report generation to support on-demand analysis and reporting.	The FileCloud platform offers built-in and configurable reports for on-demand analysis and reporting.

3.3.7	Provide an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	FileCloud can be integrated with NTP servers to provide authoritative time stamps.
3.3.8	Protect audit information and audit tools from unauthorized access, modification, and deletion.	FileCloud can auto archive the audit logs to a safe location to prevent unauthorized access, modification, and deletion. The FileCloud Admin portal also offers role-based access to restrict unauthorized access to audit transactions.
3.3.9	Limit management of audit functionality to a subset of privileged users.	The FileCloud Admin portal offers role-based access to manage and limit the audit transaction to a subset of privileged users.

3.4 Configuration Management

NIST 800-171 Requirement	Details	How FileCloud Server Supports NIST 800-171 Compliance
3.4.1	Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	FileCloud provides system check reports that give the baseline configuration of the FileCloud software and its components.
3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational information systems.	The FileCloud Admin portal provides security settings (Password policy, Authentication, Access, and Share settings) for the platform that can be easily configured by the system administrators. FileCloud Device and Policy management also offers security settings that can be enforced for mobile and client device access.

3.4.3	Track, review, approve/disapprove, and audit changes to information systems.	The FileCloud platform records administrator actions in the audit log.
3.4.4	Analyze the security impact of changes prior to implementation.	FileCloud offers the best security practices documentation. System administrators can configure the system as per guidelines to run the system securely.
3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.	FileCloud enforces logical access as defined by the system administrators. Further, FileCloud audit logs track all logical access applied to the CUI data.
3.4.6	Employ the principle of least functionality by configuring the information system to provide only essential capabilities.	FileCloud can be configured to provide the least and essential access to the CUI data.
3.4.7	Restrict, disable, and prevent the use of nonessential functions, ports, protocols, and services.	FileCloud can be configured to run on a secure port. Administrators can allow only the necessary functions for end users.
3.4.8	Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	FileCloud offers MDM capabilities to enforce black listing of other mobile applications to open or edit FileCloud data.
3.4.9	Control and monitor user installed software.	FileCloud prevents unauthorized apps from accessing the CUI. Only FileCloud mobile apps can access the data.

3.5 Identification and Authentication

NIST 800-171 Requirement	Details	How FileCloud Server Supports NIST 800-171 Compliance
3.5.1	Identify information system users, processes acting on behalf of users, or devices.	FileCloud assigns unique IDs to users and devices to track activity on the platform across all devices.
3.5.2	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	FileCloud offers advanced policy options to enable authentication for users as well as devices before allowing access to organizational information systems.
3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	FileCloud supports 2FA for users and administrators local and network access.
3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and nonprivileged accounts.	FileCloud user accounts will be locked out if they try using the wrong password for “n” times. The “n” number can be configured to meet your organization security requirements.
3.5.5	Prevent reuse of identifiers for a defined period.	FileCloud prohibits duplicate identifiers within the system and user identifiers can also be disabled for a defined period.
3.5.6	Disable identifiers after a defined period of inactivity.	FileCloud allows disabling of user accounts after a specified time period of user inactivity.
3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	FileCloud supports strong password policy. Enabling this option will require the password to contain at least one uppercase, lowercase, number, and a special character in the password.

3.5.8	Prohibit password reuse for a specified number of generations.	FileCloud prohibits password reuse. An administrator can specify the number of previous passwords that cannot be reused when password is changed.
3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.	FileCloud provides an option that will force the new user, on login, to change the password.
3.5.10	Store and transmit only encrypted representation of passwords.	All passwords are stored and transmitted only in encrypted format.
3.5.11	Obscure feedback of authentication information.	FileCloud provides obscure feedback when wrong password is entered to make it harder to guess the password.

3.6 Incident Response

NIST 800-171 Requirement	Details	How FileCloud Server Supports NIST 800-171 Compliance
3.6.1	Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.	N/A
3.6.2	Track, document, and report incidents to appropriate organizational officials and/or authorities.	The FileCloud platform logs incidents and generates system alerts when malicious incidents occur.
3.6.3	Test the organizational incident response capability.	N/A

3.7 Maintenance

NIST 800-171 Requirement	Details	How FileCloud Server Supports NIST 800-171 Compliance
3.7.1	Perform maintenance on organizational information systems.	N/A
3.7.2	Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	FileCloud offers a separate Admin portal to limit access to configuration and maintenance controls to authorized users such as system administrators.
3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	FileCloud supports remote erasing of FileCloud data in PCs and mobile devices.
3.7.4	Check media containing diagnostic and test programs for malicious code before the media are used in the information system.	FileCloud can be configured to scan for malware using an anti-virus program before content is uploaded to FileCloud.
3.7.5	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	The FileCloud Admin portal can be configured to require 2FA access. It can also be configured to time out those sessions after a threshold of idle time has been reached.
3.7.6	Supervise the maintenance activities of maintenance personnel without required access authorization.	The FileCloud audit function logs all user transactions irrespective of their privilege levels.

3.8 Media Protection

NIST 800-171 Requirement	Details	How FileCloud Server Supports NIST 800-171 Compliance
3.8.1	Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital.	N/A
3.8.2	Limit access to CUI on information system media to authorized users.	FileCloud protects CUI by encrypting content at rest and enforcing proper access controls.
3.8.3	Sanitize or destroy information system media containing CUI before disposal or release for reuse.	FileCloud can remotely erase CUI on client devices (PCs, Mobile Phones).
3.8.4	Mark media with necessary CUI markings and distribution limitations.	N/A
3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	FileCloud enforces access controls on mobile devices regardless of their location. FileCloud can remotely block or erase FileCloud data on mobile devices if needed.
3.8.6	Implement cryptographic mechanisms to protect the confidentiality of information stored on digital media during transport outside of controlled areas unless otherwise protected by alternative physical safeguards.	FileCloud encrypts all CUI at rest with AES encryption.
3.8.7	Control the use of removable media on information system components.	N/A
3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.	N/A

3.8.9	Protect the confidentiality of backup CUI at storage locations.	FileCloud encrypts and enforces access controls for all CUI under management, including CUI on redundant servers.

3.9 Personnel Security

NIST 800-171 Requirement	Details	How FileCloud Server Supports NIST 800-171 Compliance
3.9.1	Screen individuals prior to authorizing access to information systems containing CUI.	The FileCloud platform allows access to CUI only to authorized users.
3.9.2	Ensure that CUI and information systems containing CUI are protected during and after personnel actions such as terminations and transfers.	When employees and contractors are terminated, FileCloud can revoke permissions of the users and block the access to CUI. Further, personnel devices can be remotely blocked and erased by the FileCloud platform.

3.10 Physical Protection

NIST 800-171 Requirement	Details	How FileCloud Server Supports NIST 800-171 Compliance
3.10.1	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	N/A
3.10.2	Protect and monitor the physical facility and support infrastructure for those information systems.	N/A

3.10.3	Escort visitors and monitor visitor activity.	N/A
3.10.4	Maintain audit logs of physical access.	N/A
3.10.5	Control and manage physical access devices.	N/A
3.10.6	Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites).	Remote access to CUI is protected by strong authentication and access controls. The data is encrypted in transit and at rest.

3.11 Risk Assessment

NIST 800-171 Requirement	Details	How FileCloud Server Supports NIST 800-171 Compliance
3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of CUI.	The FileCloud platform offers an administrative dashboard (system summary, recent access locations, File type distribution), detailed audit logs, and built-in reports to periodically assess the risks.
3.11.2	Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.	FileCloud can be integrated with ClamAV or other anti-malware software via Internet Content Adaption Protocol (ICAP) interface to block any viruses or malware from being uploaded to FileCloud.
3.11.3	Remediate vulnerabilities in accordance with assessments of risk.	FileCloud alerts system administrators about suspicious files that fail signature checks as well as files blocked by the AV software.

3.12 Security Assessment

NIST 800-171 Requirement	Details	How FileCloud Server Supports NIST 800-171 Compliance
3.12.1	Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.	FileCloud offers administrative dashboard, alerts, and reports to perform security assessments quickly.
3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.	FileCloud provide functionalities to protect the system from ransomware and malware attacks (Requires integration with Ant-Virus Software with ICAP capabilities).
3.12.3	Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.	N/A
3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	N/A

3.13 System and Communications Protection

NIST 800-171 Requirement	Details	How FileCloud Server Supports NIST 800-171 Compliance
3.13.1	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	FileCloud monitors, controls, and protects organizational communication in transit and at rest via encryption using FIPS 140-2 validated encryption module.

3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	FileCloud provides end-to-end data protection with multiple levels of security at each layer. Security is a first-order citizen with FileCloud and is built from the ground up – not as an afterthought. FileCloud is available on private or hybrid cloud or as a private hosted deployment is an isolated environment on AWS GovCloud. This enables customers to adopt the deployment model that best suits their security needs.
3.13.3	Separate user functionality from information system management functionality (e.g., privileged user functions).	FileCloud offers an Admin portal which is separate from the end User portal. Further, the Admin portal can be configured with role-based access control for privileged user functions.
3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.	FileCloud prevents unauthorized access or sharing of CUI. Only authorized users can share information via FileCloud. FileCloud also has the option to disable public sharing and disabling new user invites in such a way that the information is kept only within the organization and authorized users.
3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	FileCloud's 3-tier architecture allows web interfaces and other system functions to be deployed outside network DMZs for public access, while ensuring that application logic and CUI storage remains on internal networks. FileCloud can be also deployed behind a reverse proxy for further protection.
3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	By configuring the underlying web server, you can whitelist the IP addresses used to access FileCloud.

3.13.7	Prevent remote devices from simultaneously establishing non-remote connections with the information system and communicating via some other connection to resources in external networks.	N/A
3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	FileCloud encrypts CUI in transit using TLS 1.2 (Transport Layer Security).
3.13.9	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	FileCloud provides session timeout for both the end User and Admin portal that can be configured by the system administrators. After a defined period of inactivity, the user as well as the admin session expires.
3.13.10	Establish and manage cryptographic keys for cryptography employed in the information system.	FileCloud enables system administrators to set encryption for data at rest and in transit.
3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	FileCloud uses FIPS 140-2 validated cryptographic module for all cryptographic operation including encryption of CUI data at rest and in transit.
3.13.12	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	N/A
3.13.13	Control and monitor the use of mobile code.	FileCloud clients (web browser or desktop clients) don't use any mobile code such as applets or active x controls.

3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	N/A
3.13.15	Protect the authenticity of communications sessions.	FileCloud invalidates the session upon user logout or upon a defined period of inactivity.
3.13.16	Protect the confidentiality of CUI at rest.	FileCloud uses FIPS 140-2 validated encryption module to encrypt (AES 256) CUI data at Rest

3.14 System and Information Integrity

NIST 800-171 Requirement	Details	How FileCloud Server Supports NIST 800-171 Compliance
3.14.1	Identify, report, and correct information and information system flaws in a timely manner.	CodeLathe monitors vulnerabilities in the FileCloud platform regularly and resolve these vulnerabilities based on impact and severity.
3.14.2	Provide protection from malicious code at appropriate locations within organizational information systems.	FileCloud can be integrated with anti-malware products to scan for viruses, APTs and zero-day attacks. FileCloud also provides built-in ransomware protection by comparing the file signature.
3.14.3	Monitor information system security alerts and advisories and take appropriate actions in response.	The FileCloud platform can be configured to export audit logs and system alerts from Security Information and Event Management (SIEM) systems being used for security monitoring and alerts.
3.14.4	Update malicious code protection mechanisms when new releases are available.	FileCloud can be integrated with anti-malware products via an ICAP interface. These products can be updated periodically as new definitions are released by the vendor. By default, FileCloud can be integrated with the open source ClamAV product which can be updated periodically.

3.14.5	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	When you integrate FileCloud with an anti-virus product via ICAP, all uploaded files are scanned for viruses and malware.
3.14.6	Monitor the information system, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	FileCloud monitors all the communications for signs of ransomware and our audit logs, dashboards and geoIP features can be used to look for traffic anomaly.
3.14.7	Identify unauthorized use of the information system.	The FileCloud platform doesn't permit unauthorized access of the system. FileCloud's audit logs record all user transactions.

FileCloud Architecture

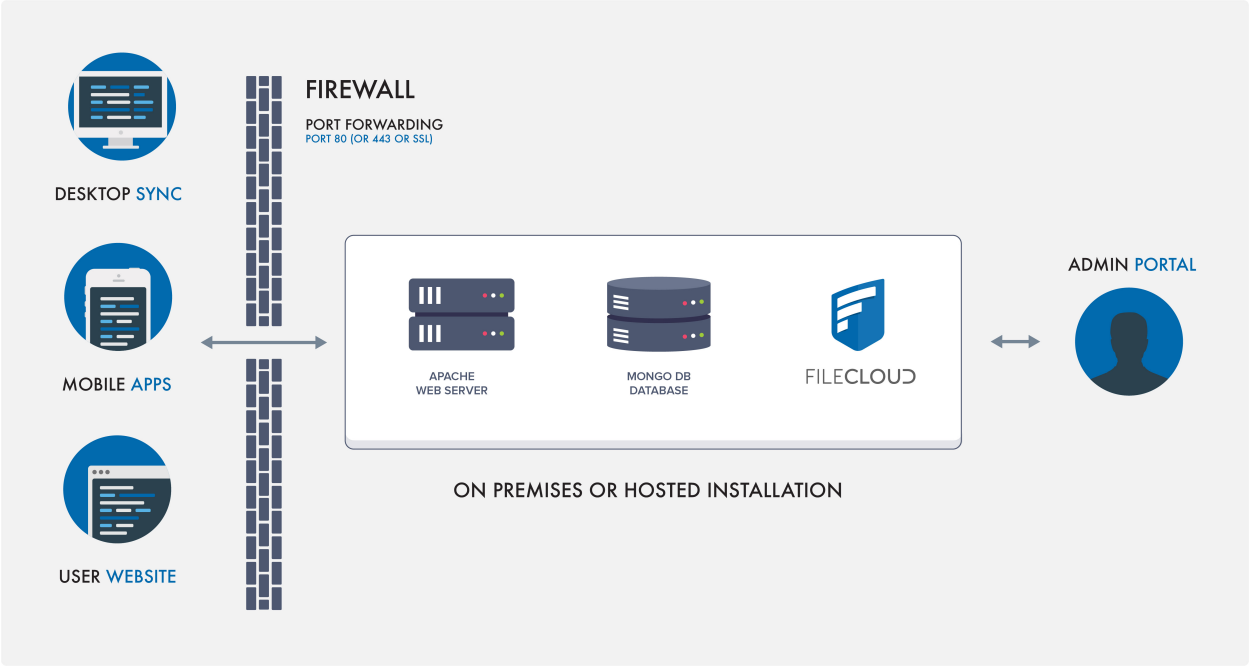

Diagram 1. FileCloud Architecture

FileCloud software is typically installed on a server (Linux or Windows). After installation, an Admin portal is available to configure and manage the system. Once configured by an administrator, users can access the FileCloud installation using the web browser, mobile apps, or even keep their desktop folders in sync using the FileCloud's desktop sync clients.

FileCloud High Availability Architecture

The FileCloud solution can be implemented using the classic 3-tier high availability architecture. The first tier consists of the load balancer and access control services. Tier 1 will be a web tier made up of load balancers. Tier 2 will be stateless application servers and for FileCloud implementation. This layer will consist of Apache nodes. Tier 3 will be the database layer. The advantage of this architecture is separation of stateless components from state-full components allowing great flexibility in deploying the solution.

To learn more about how the FileCloud platform can help your organization comply with NIST 800-171 regulations, please contact us at sales@codelathe.com.

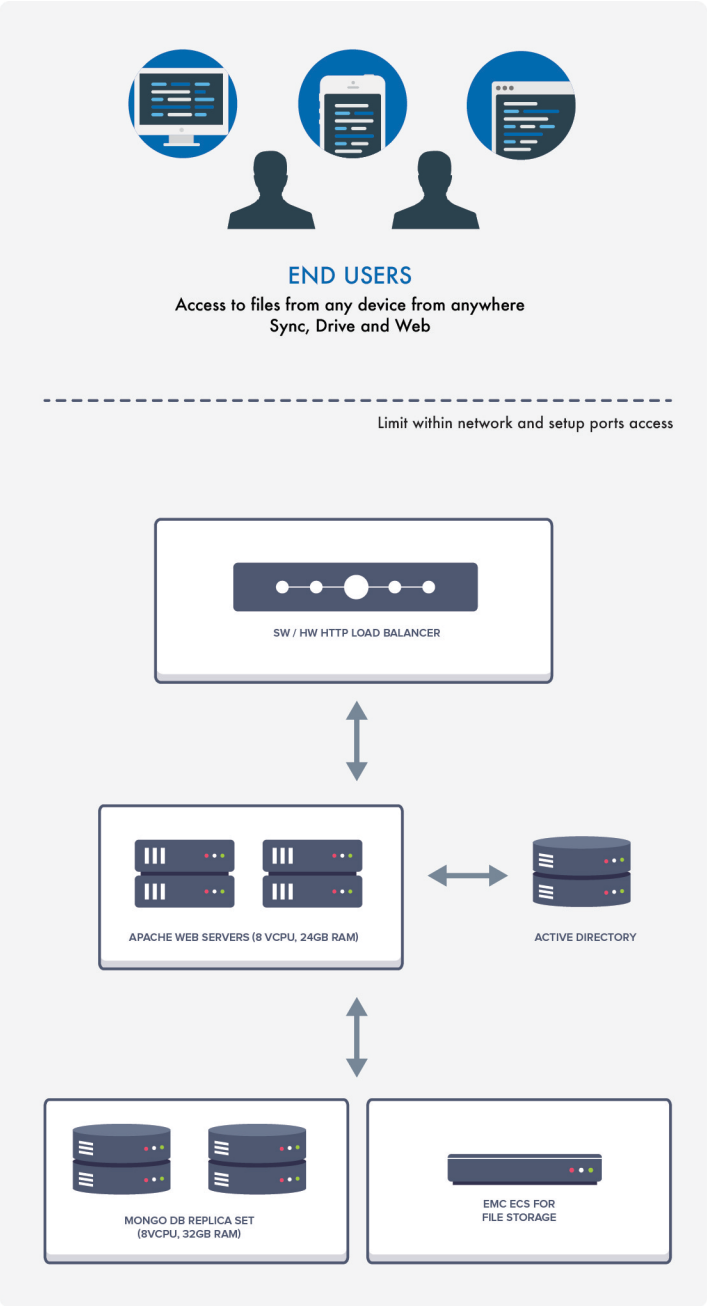

Diagram 2. FileCloud High-Availability Architecture

13785 Research Blvd, Suite
125 Austin TX 78750

Email:
sales@codelathe.com

Website:
https://www.getfilecloud.com

Phone:
+1 (888) 571-6480

Fax:
+1 (866) 824-9584