FileCloud Integrates with Everfox CDR

Solution Brief

Enhancing File Security with Content Disarm and Reconstruction

FileCloud's integration with Everfox Content Disarm and Reconstruction (CDR) technology offers a powerful solution for organizations seeking to bolster their file security and threat prevention capabilities. This partnership combines FileCloud's robust enterprise file sharing and sync platform with Everfox's advanced data first security model technology to create a seamless, secure file handling environment.

Advanced Threat Prevention

Everfox CDR goes beyond traditional malware protection. It works by disassembling incoming files, removing any potentially malicious elements, and then reconstructing the files in a clean, safe format. This process effectively neutralizes hidden threats, including zero-day attacks and advanced persistent threats (APTs), without relying on retroactive signature-based detection methods.

Seamless Integration

FileCloud users can leverage Everfox CDR capabilities directly within the FileCloud UI. When a file is uploaded to FileCloud, it is automatically routed through the Everfox CDR process. This ensures that all files stored and shared within the FileCloud environment are sanitized and free from potential threats, providing an additional layer of security for sensitive corporate data.

Enterprise-grade Security

By implementing this integration, organizations can significantly reduce the risk of malware infections, data breaches, and other security incidents that can arise from compromised files. As part of a Zero Trust security strategy, CDR offers peace of mind for organizations handling sensitive information, enabling them to maintain data integrity while collaborating and sharing files.

Functional Benefits

Enhanced File Security

Organizations can embrace a multi-layered security strategy, where even the content itself is considered. This integration reduces the risk of malware infections and data breaches, protecting sensitive corporate information and maintaining data integrity.

Simplified Compliance

For industries with strict regulatory requirements (e.g., healthcare, finance, and government), the FileCloud-Everfox integration helps meet requirements for data protection by providing an additional layer of security for file handling.

Improved Collaboration Confidence

With the knowledge that all uploaded files are automatically sanitized, users can collaborate and share files with increased confidence. This can lead to improved productivity and more efficient workflows.
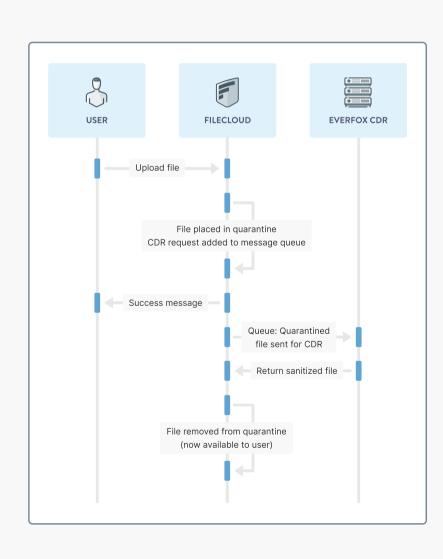
Comprehensive Coverage

The integration works across all connected storage types in FileCloud, as well as clients. Regardless of how users interact with FileCloud, they benefit from the added security of Everfox CDR.

How it Works

When a user uploads a file to FileCloud with the Everfox CDR integration enabled, the system automatically initiates the Content Disarm and Reconstruction process:

- **File Upload:** FileCloud quarantines the file (inaccessible to ensure threats cannot proliferate before being disarmed).

- **Disarm:** The file is sent to Everfox, where it is disassembled and potential threat vectors are removed.

- **Reconstruct:** Everfox returns the sanitized file, which is then made available for normal use. The interaction is captured within FileCloud's audit logs.

- **User Experience:** In an optimally configured environment, the CDR process is transparent to users, taking a matter of seconds.*

*Large files may take longer to fully process.

USER   FILECLOUD   EVERFOX CDR

Upload file

File placed in quarantine
CDR request added to message queue

Success message

Queue: Quarantined
file sent for CDR

Return sanitized file

File removed from quarantine
(now available to user)