

Solution Brief

ShardSecure integrates with Nextcloud to strengthen security for collaboration platform



Overview: secure, efficient collaboration for workplaces

Content collaboration platforms have become a crucial tool for the modern workplace. By reducing the need for constant back-and-forth communication through email and messaging, they streamline workflows, enhance productivity, and facilitate teamwork. For hybrid and remote teams, these platforms also provide an efficient, centralized way for employees across the world to collaborate on critical files, documents, and projects.

Because so many teams are sharing sensitive files on collaboration platforms, however, there's a pressing need for cutting-edge data security. Creators of collaborative software must implement strong data protection solutions that can mitigate the impact of outages, accidental and malicious exposure of data, and more.

About Nextcloud's collaboration platform

[Nextcloud](#) is an industry-leading, open-source content collaboration platform. Its technology includes solutions for file syncing and sharing, video conferencing, and real-time document collaboration for governments, enterprises, schools, and service providers.

With a wide range of features that enable teams to communicate, share files, and collaborate in real-time, Nextcloud makes it easier for organizations to manage their projects and deliver quality work. Their products offer powerful capabilities to control and monitor data exchange and communication, including file access controls and workflow features, extensive audit logs, in-grained sharing controls, and more.



ShardSecure and Nextcloud integration

Together, ShardSecure's and Nextcloud's technology are providing a secure, resilient way for teams to collaborate on confidential and sensitive projects.

ShardSecure's Data Control Platform offers the necessary security and resilience features for data at rest. By making data unreadable to all unauthorized users and third parties, we keep data private and protected from both accidental and malicious exposure.

Both ShardSecure and Nextcloud's solutions center on keeping the customer in control of their data. Nextcloud does not store customer data files; rather, they allow organizations to collaborate using their own on-prem data storage or the third-party storage of their choice. ShardSecure provides the necessary security features for this storage to further ensure the security and protection of data created and shared in Nextcloud.

Addressing data security and sovereignty concerns

ShardSecure helps companies meet requirements for both data security and data sovereignty. Sensitive data should never be exposed to unauthorized users, but it's all too common in modern architectures. Everyone from server and data center administrators to cloud providers may have access in modern architectures, causing problems with security and compliance.

ShardSecure addresses these problems by ensuring that unauthorized users cannot access sensitive data.

Our technology enables Nextcloud customers to securely adopt any storage solution of their choice without giving up control of their data to those third party storage providers. We also enforce data residency within the Nextcloud solution, helping customers ensure that their data is not only secured wherever it's stored but also residing within a predefined jurisdiction.

Seamless, transparent integration

ShardSecure offers easy integration with storage APIs, and its architecture allows for an easy plug-and-play integration with any application, including Nextcloud's collaboration platform. It is transparent to customers' storage locations, making deployment quick and efficient.

Our integration with Nextcloud is completely transparent to both Nextcloud admins and Nextcloud users. We introduce data protection (including data security and data sovereignty) without any changes in Nextcloud's architecture, user workflows, or data workflows.

ShardSecure's solution is also a zero-downtime event, providing advanced security with no impact to applications and no visible changes or significant lag for users. If a Nextcloud customer needs to migrate data from one of their storage locations to another, the process can be started with just a few clicks.



Summary

With the need for content collaboration tools growing, modern workplaces are on the hunt for centralized, secure solutions that allow their team members to share projects. The ShardSecure-Nextcloud integration responds to this market need by adding ShardSecure's innovative data security and resilience capabilities to Nextcloud's industry-leading collaboration platform. Together, our joint solution is providing a centralized, secure, and resilient platform that enables teams to work collaboratively while keeping their data safe from outages, cyberthreats, and other disruptions.

About NextCloud

Nextcloud Hub is the industry-leading, fully open-source, on-premises content collaboration platform. Teams access, share and edit their documents, chat and participate in video calls and manage their mail and calendar and projects across mobile, desktop and web interfaces.

To learn more about Nextcloud, visit www.nextcloud.com.

About ShardSecure

In the face of rising data security and sovereignty challenges, cyberattacks, and operational complexity, ShardSecure helps companies simplify their data protection. Our innovative data control platform lets organizations enjoy the flexibility of securing their data wherever they want: on-premises, in the cloud, or in hybrid-cloud architectures.


With strong data security and resilience, agentless file-level protection, support for cross-border compliance, native ransomware protection, easy plug-and-play integration, and more, ShardSecure helps you stay in control of your data.

To learn more about ShardSecure, visit us at <https://shardsecure.com>

 @ShardSecure

 @ShardSecure

 @ShardSecure

 101 Avenue of the Americas
9th Floor, New York, NY 10013
United States of America

 info@shardsecure.com

**SHARD
SECURE**