SHARDSECURE®

DISRUPTING THE CYBER CRIME ECONOMY

SOLUTION BRIEF:

SHARDSECURE FOR MICROSOFT 365

ShardSecure natively integrates with Microsoft 365 to provide organizations who want:

- Additional protection and privacy for sensitive documents such as those containing intellectual property, regulated and compliance data, customer and employee data, company financials, etc.
- A seamless experience for Microsoft 365 Online users
- The flexibility to select their backend storage solution whether it be single-cloud, multi-cloud, multi-region, and/or on-prem storage configuration

A smooth Microsoft 365 Online experience

Because we are a certified Microsoft Cloud Partner, we use native Microsoft APIs to create a smooth experience for Microsoft 365 Online users with support for Excel, Word, and PowerPoint. Therefore, documents can be shared with other users and users may still collaborate on a file online and in real-time. And you have the benefit of Microsharding working continuously in the background to keep your files protected and making your data undesirable to attackers and unauthorized users.

Copy files from OneDrive

It's also easy to copy your files from OneDrive. Copy one, several, or all your files from OneDrive to the ShardSecure for Microsoft 365 application with the click of a button for any file type.

Storage flexibility

ShardSecure provides native support for multi-cloud, multi-region, and/or on-prem storage support, and our Microsoft 365 integration gives you the same flexibility in choosing the storage configuration that you want.

How our patent-pending Microshard technology protects your sensitive data

Microsharding is a technology created to protect sensitive data in a manner that is easy-to-deploy, simple to manage, and unusable in the wrong hands. We created a three-step process that consists of shredding, mixing, and distributing your data.

Here's how it works:

Shred: We eliminate data sensitivity by shredding files into Microshards, which are single-digit bytes that are too small to contain sensitive information.

Mix: Next, we randomly mix the Microshards into multiple containers that are unidentifiable and unintelligible. We also add poison data to those containers to increase the level of difficulty for an attacker who may try to reassemble the data in a Microshard container.

Distribute: Lastly, we distribute the containers across multiple, segmented locations in the cloud or datacenter to ensure data is always incomplete. We support multi-cloud, multi-region, and/or on-prem storage configurations. If an attacker is able to compromise one of your storage locations, the Microsharded data provides no value. This is how we make your data undesirable to an attacker.

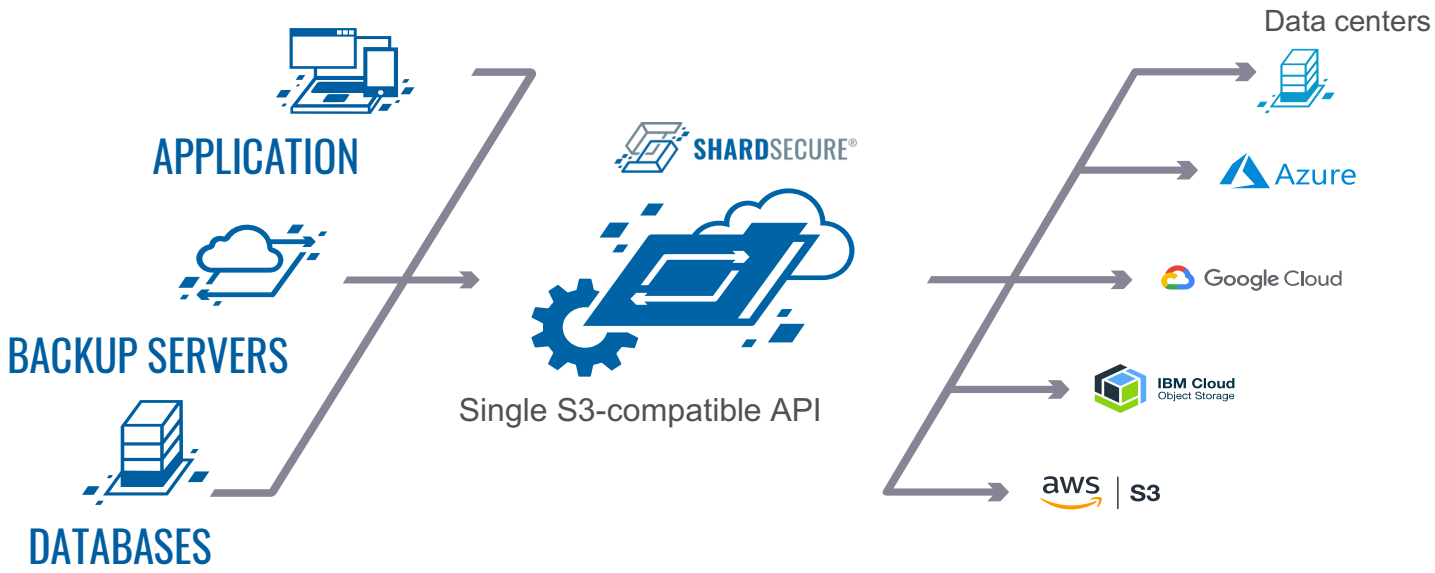
Technology Overview

The ShardSecure virtual appliance cluster can be deployed in the cloud or datacenter. The solution ingests unstructured and structured data via S3 Compatible Object Storage API, iSCSI, SMB and NFS.

Data is compressed then shredded into Microshards that are too small to contain sensitive data. Microshard data is thoroughly mixed, poison data is added, and new shards (containers holding many Microshards) equal to the number of configured storage destinations are formed to eliminate any value in the data.

To ensure data is always incomplete at rest, it is distributed following a user-set policy to multiple independent locations, which may include on-premises/datacenter or cloud storage. The appliance will reassemble Microshard data whenever needed for authorized applications and users.

ShardSecure can be deployed in as little as 15 minutes and works with your existing security controls.



SHARDSECURE®

+1 (800) 760 9445

info@shardsecure.com

@ShardSecure

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