Secure Delete for Azure Storage

Securely and permanently delete all files and data stored on Azure.

Public clouds such as Azure are growing in popularity as more companies use them for archiving, backups and production workloads. Public clouds, including Microsoft Azure, keep 3 copies of your data by default to ensure it is protected and recoverable. One concern when using a public cloud is how to ensure your data is permanently removed. Modern storage and file systems can make this process difficult and leave many concerned that their data might still be accessible. Atmosera's Secure Delete for Azure Storage is an application designed to address this specific concern.

Go nuclear on your Azure storage with a purpose-built app.
Erase all files and data from Azure storage and remove all traces of them.

Leverage government approved processes.
Use US Department of Defense (DoD) 5220.22-M data sanitization method.

Control how the data is overwritten.
Ensure the data is overwritten multiple times and not just deleted.

The reasons to use Secure Deleted for Azure Storage.

There comes a time when data needs to be deleted. The three most common cases are:

> **Delete data uploaded by mistake and ensure it is gone forever —** Mistakes happen and there are instances where data that should never be in a public cloud, such as credit card and login details, need to be removed immediately and permanently.

> **Purge expired or archived data which is under mandate to be deleted securely —** Some data types have a finite value and may no longer be relevant or need to be available. Many compliance frameworks, covering such industries as healthcare and financial services, require that all data be completely deleted and unrecoverable.

> **Leave Azure and decommission your environment with all its data —** Sometimes customers want to exit their Azure environments. This applies to temporary, development and production deployments. Customers want to guarantee that all their data is also removed and not recoverable.

How the application works.

This is an extreme measure but ensures your data is deleted and not recoverable — ever again. It works on all types of storage including Solid State Drives (SSD) and Hard Drives used in Azure data centers. Since networked storage doesn't give direct access to the real disks (it's all virtualized) and files are scattered using the Write Anywhere File Layout (WAFL), the application conducts the process over the entire drive.

The application stripes all logical sectors of the disk and securely deletes data from blob containers by salting the drives and wiping all data. The current blob size limitation is 500 TB and the application is calibrated to target 500 TB. The number of passes defaults to 7 and is user configurable. Each pass uploads a garbage file containing random data in 128 MB, 256 MB, 512 MB or 1 GB increments. The data is then deleted after each pass and repeats until all passes are completed.

Any other copies held in the cloud follow suit and all get wiped as well. The process ensures that all data remanence are effectively eliminated. The duration to wipe a disk can take time to complete but delivers the peace of mind that the data and files are indeed securely removed. This process cannot be undone and is used at the customer's own risk.

How the application is priced: Starts at US$0.30 per Hour

The cost of running this application is a combination of the selected software plan charges plus the Azure infrastructure costs for the virtual machines (VMs) on which you will be using this software. Costs may vary by region.

Where to get the application.

Azure MARKETPLACE | Microsoft Azure Certified

The application is available on the Azure Marketplace at the following link:

https://azuremarketplace.microsoft.com/en-us/marketplace/apps/atmosera.secure-delete

atmosera®

A leading Azure service provider leveraging both Microsoft Cloud Platform and Azure

atmosera.com **P** +1.503.222.2202 **T** +1.800.903.4852 **F** +1.503.646.1400