

# Secure File Services for Government and Defense

Military-Grade Global File System Ensures Full Data Availability and Privacy for Mission Owners



Available through the DODIN  
Approved Products List (APL)

## Secure Data Management for Government and Military Organizations

The modernization of file services and data storage is a major priority for federal and defense agencies as they embark on digital transformation initiatives. These organizations aim to leverage cloud technologies to accommodate massive data growth, securely share files across various locations, and gain new insights from data analytics.

CTERA's global file system technology offers government organizations a modern, cloud-based solution for unstructured data management that delivers full privacy and protection for sensitive and classified data.

CTERA technology allows federal and defense agencies to deploy private file services that deliver the same resiliency, productivity, and elasticity as civilian cloud-based services, while meeting stringent military-grade data security requirements and mission-critical availability.

Trusted by military and homeland security organizations in the U.S. and abroad, the CTERA platform is available through the Department of Defense Information Network Approved Products List (DODIN APL).

## Built for Mission-Critical Requirements



### Common Data Repository with Caching Endpoints

Distributed presentation of file access (SMB/NFS) across remote locations with caching of frequently accessed data-sets for high speed access. The CTERA platform enables virtually unlimited local file storage and enables collaboration across multiple locations.



### Secure and Efficient File Transfer

CTERA employs source-based de-duplication and compression, minimizing impact on available WAN bandwidth and reducing storage capacity in your cloud or data center by up to 90%. Work efficiently over high latency connections and move large files over long distances at high speeds.



### Military-Grade Security

Deploy private file services that deliver the same resiliency, productivity, and elasticity as civilian cloud-based services, while meeting stringent military-grade data security requirements and mission-critical availability. The CTERA platform utilizes a zero-trust architecture, 100% on-premise deployment model, CAC enablement, read-only audit logs, and much more.

## Trusted by the Department of Defense to Protect Classified Data



**100% In-Firewall**  
on premises, VPC or hybrid



**Strong Authentication**  
AD, 2-factor, smartcard, CAC/PIV



**FIPS 140-2 Certified**  
data encryption suited for top-secret files



**Seamless ACL Migration**  
NT-ACL enforcement over NAS and FSS



**Secure Data Transfer**  
files protected at rest and in-transit



**File Sharing Policy**  
control by file name, user, group

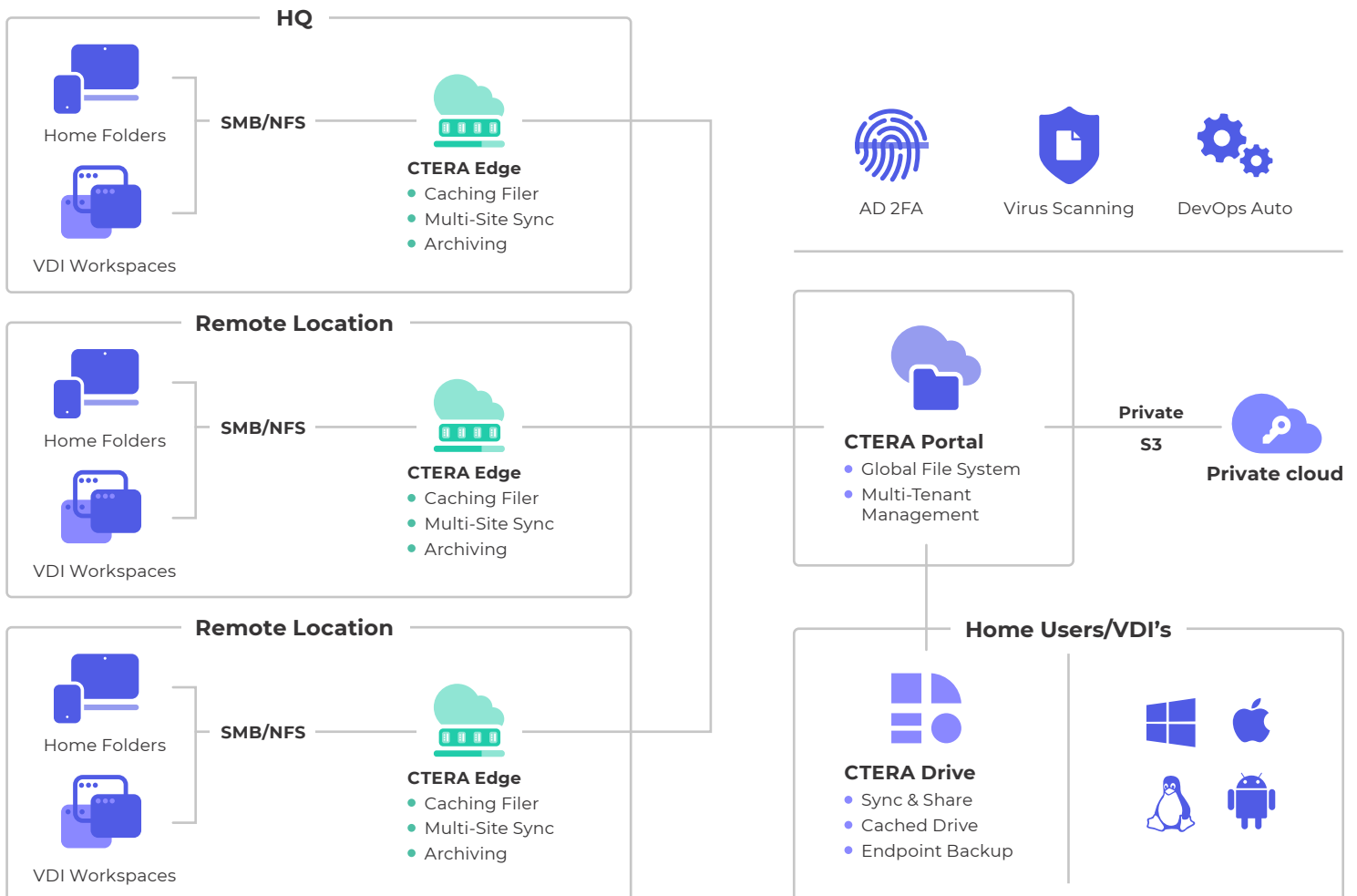


**Private Key Management**  
no 3rd party access to your keys



**Zero-Trust Architecture**  
"Never Trust, Always Verify" for all edge devices

## Architecture



## CTERA Natively Migrates Legacy NAS Data Sources



### Automated Data Migration

Seamless transfer of corporate file shares from legacy NAS systems such as NetApp, Dell EMC, and Windows Server with full preservation of existing file system structure and permissions.



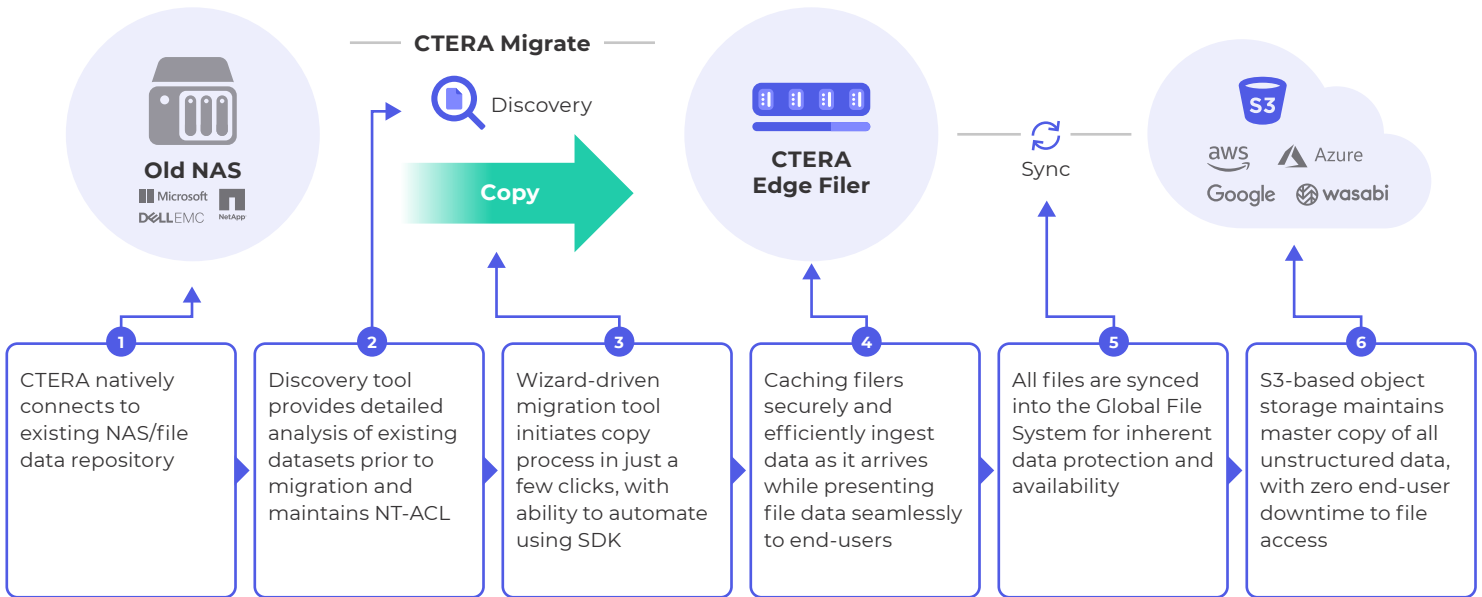
### Data Visualization

Use advanced data discovery to gain insight into your file assets so you can easily plan and scope your cloud migration project.



### Reduced Cost and Complexity

Built-in, easy-to-use migration tools accelerate deployment and eliminate the need for external servers, third-party software, or professional services teams.

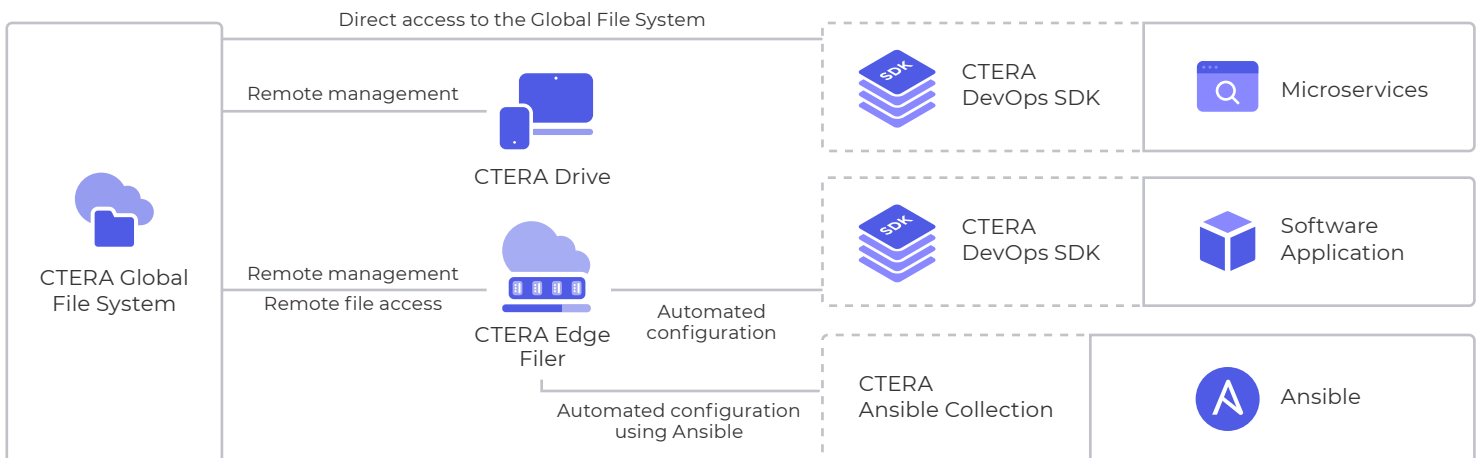


## CTERA DevOps for Automation of Global File Services



### SDK for Modern, Direct Access and File System Provisioning

CTERA provides a robust SDK and APIs for building modern file system architectures, scaling file services to any size, and reducing multi-cloud gateway and storage provisioning down to minutes or even seconds.





### U.S. Air Force

A major command of the United States Air Force has modernized desktop and backup management processes and enabled secure file access and collaboration for users anytime, anywhere. The CTERA solution efficiently replicates sensitive data across a dozen highly distributed command bases for global file sharing, while maintaining a simple mapped-drive experience.

CTERA's smartcard authentication, advanced audit logs, and multi-tenant architecture ensure rigid compliance with security protocols, while data migration tools allowed the major command to seamlessly migrate existing file shares, including folder structure and ACLs, to the CTERA solution.



### U.S. Navy

The United States Navy uses CTERA's global file system technology to enable edge-to-core data tiering, fast local performance, and compliance while meeting stringent federal IT data security and mission-critical availability requirements. In choosing CTERA's platform, built on top of a zero-trust security architecture with FIPS 140-2 validation and offers 100% private deployments, the U.S. Navy can securely modernize legacy infrastructure while ensuring high-performance data transfer for remote users even over high latency links.



### Department of Veterans Affairs

The VA has over 150 medical centers and 100s of petabytes (PB) of mission-critical data from business operations data to medical images used in veteran care. They had challenges managing the scale of data, the speed of processing data at each facility (the edge), no centralized control, lack of collaboration, and security concerns.

CTERA provided a proven solution that enabled the VA to embark on an edge-to-cloud file services strategy without compromising on stringent data security requirements. The speed and flexibility of this solution provides better availability for veterans and hospitals, faster access to critical resources, and an on-ramp into the public cloud.