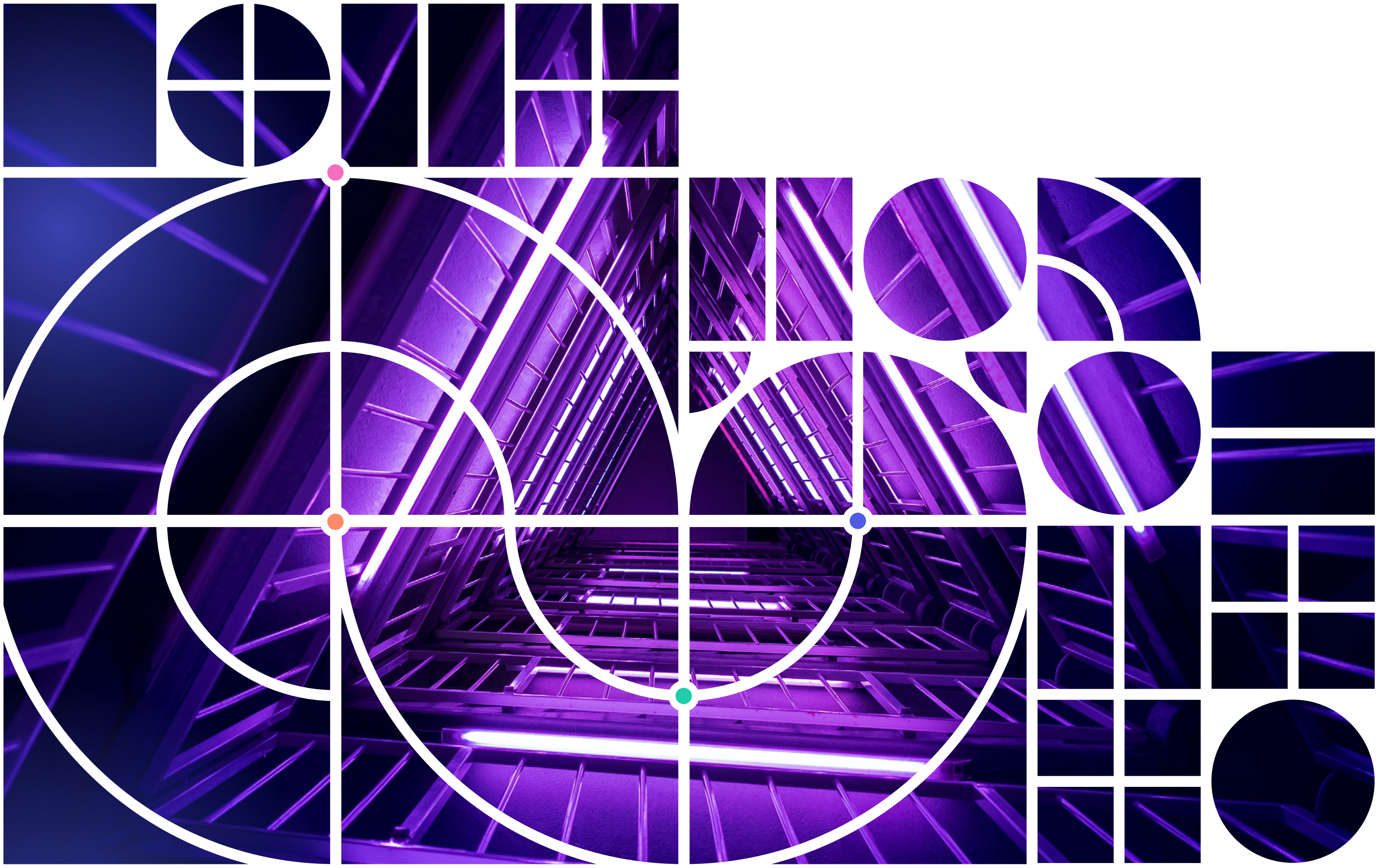
ctera your files. your cloud.

CTERA White Paper

Never Trust Your Filers: Embracing Zero Trust in a Global File System



Never Trust, Always Verify: Adapting Enterprise Data Security to Remote Work Models

Enterprises traditionally based their network security on a “castle-and-moat” concept. The castle is the corporate network, and the moat has a single drawbridge that is heavily guarded (firewall, VPN, etc.). Any traffic passing the security point is considered an “insider” and can access any file or application within the network.

Unfortunately, this traditional trust model doesn’t hold up well for today’s distributed enterprise. Over the past decade enterprises have transitioned to remote work models to support users spread across dozens and hundreds of branch offices. In parallel, dynamic workloads move across multiple data centers and public, private and hybrid clouds, while Bring Your Own Device (BYOD) and work-from-home (WFH) have become common practices.

This fundamental shift in the way enterprises work has expanded their attack surface and compelled them to reassess how they protect data in their network. Security and IT teams understand that user identities can be compromised, and that the communication source is now meaningless from a security standpoint. Even the LAN – once the bastion of corporate security – is no longer automatically trusted.

Once inside the network with user credentials, a malicious actor can move laterally to access, corrupt or exfiltrate sensitive corporate data. The increasing sophistication of cyber-attacks, stricter regulations, and greater awareness of the risks involved have also contributed to this new “Zero Trust” mindset. In short: Never Trust, Always Verify.

A Flat Architecture for a New Flat World

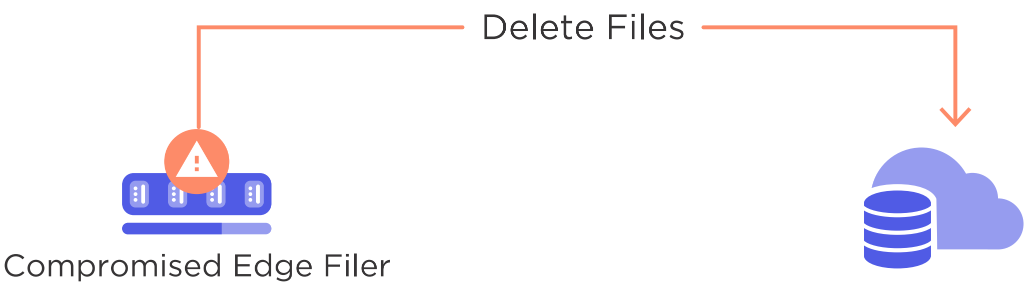
Based on the Zero Trust approach, enterprises should not automatically trust anything inside or outside their perimeters. Every access attempt should be considered “suspicious” until proven otherwise. Systems should never rely on the communication source and should authenticate each access attempt from every endpoint, including devices on the LAN or VPN.

Zero Trust architectures are not dependent on location. And this leads to a very important advantage of the zero trust architecture that is rarely appreciated. Zero Trust allows enterprises to treat the new flat world as one flat, cloud-centric network, where employees can work just as effectively at home as they can sitting at their corporate HQ desk.

Why CTERA Chose Zero Trust for Its Global File System

CTERA is the only global file system provider with a Zero Trust architecture. Unlike other solutions, we built our platform with a “security first” approach. We understood from Day 1 that no edge devices (filers, desktops, laptops) should be trusted when it comes to branch offices or WFH users.

Many of our competitors sell large and expensive filers that are often regarded as part of the core IT infrastructure. Initially deployed in centralized locations with tight security, these filers were assumed to be secure and were granted highly privileged credentials to access the underlying object storage buckets. The problem is that as enterprises scale up, they also need to deploy filers at remote locations that are less tightly controlled. Without a Zero Trust approach, their data is at serious risk. For example, if an edge filer with the necessary credentials to directly modify objects in the object storage becomes compromised, it could corrupt or erase essential data for the entire organization. The result of such attack would be devastating.



In other words, a global file system that provides the credentials for accessing the underlying object storage system to endpoint devices is fundamentally unsuited for any large-scale deployment, particularly when branch offices and home workers are involved.

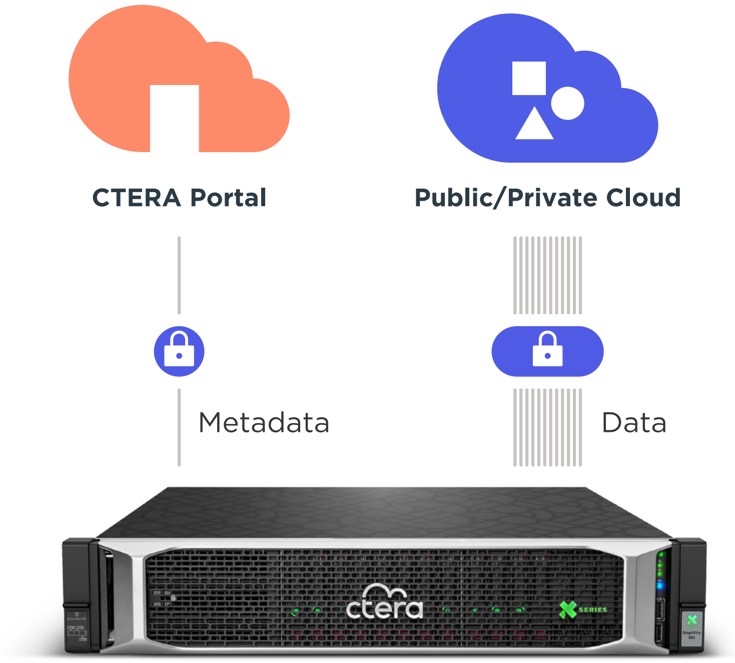
How We Implement a Zero Trust Architecture

CTERA's Global File System consists of edge devices, core servers, and object storage. Edge devices include CTERA Edge Filers installed at remote offices, CTERA Drive software installed on users' PCs and laptops, and the CTERA Mobile app. The core servers (aka CTERA Portal) are an orchestration layer responsible for managing the Global File System and its clients. Object storage (cloud or on-premise) is where the bulk of the data is stored.

Based on our Zero Trust architecture, edge devices are inherently untrusted and are not given default privileges to object storage. Before CTERA 7.0 (released in October 2020), edge devices were completely isolated from the object storage. All traffic from the edge devices to the object storage went through the CTERA Portal, which enforced strict security and file access controls. Despite the additional cost and complexity of routing all the data indirectly, we chose this method because we prioritized security above all else.

CTERA's Zero Trust architecture contrasts with other solutions on the market that took a more naïve security approach. These solutions distributed highly privilege credentials for object storage to each of the edge filers, ignoring the risk that a compromised edge filer could potentially lead to a data breach.

CTERA Direct: Taking Zero Trust Architecture to the Next Level



CTERA’s Zero Trust architecture was built around a hub-and-spoke centralized security authority. Based on this concept, edge devices communicate only with the core servers and are never granted credentials to access the object storage.

From a cost/performance perspective, however, the hub and spoke architecture had a drawback. Sending all the traffic through the core servers may create bottlenecks in those servers, increasing their cost (since they must decrypt and process the entire storage bandwidth of the global file system) and adding another “hop” of latency.

CTERA Direct, our patented technology introduced in CTERA 7.0, eliminated this trade-off by enabling edge devices to communicate **directly** with the nearest object storage buckets - without compromising security. This technology combines the same proven, zero trust architecture with the speed and cost savings of a disaggregated architecture. By reading and writing data to object storage, CTERA Direct save time , data transfer costs, and compute demands.

At the same time, devices never possess any access keys for object storage. Instead, **every request** to access data is first submitted to a core server. If the request is approved, the core server digitally signs the request and returns the signature to the endpoint. The endpoint then uses the signed requests to perform the requested activity directly with the object storage.

The World is Your Office

CTERA chose a zero trust architecture from Day 1 because we didn’t want to restrict global file system access to only highly secure centralized devices. We wanted to help enterprises extend their file systems to remote branch office, laptop and mobile client users, where it’s imperative not to trust any device without proper verification.

However, as time passed, a much more important implication of Zero Trust security became apparent. Companies that implemented the “Never Trust, Always Verify” paradigm early on were the first to realize that their employees should be able to work equally well from anywhere. And the importance of this has never been clearer than in the last six months, where working remotely has become “the new normal.”

The primary objective of any CIO today is to enable employees to work productively in this brave new world. CTERA provides distributed enterprises with a proven tool for achieving just that objective: the world’s most secure, globally-accessible file system.