ctera your files. your cloud.

# CTERA RANSOMWARE PROTECTION

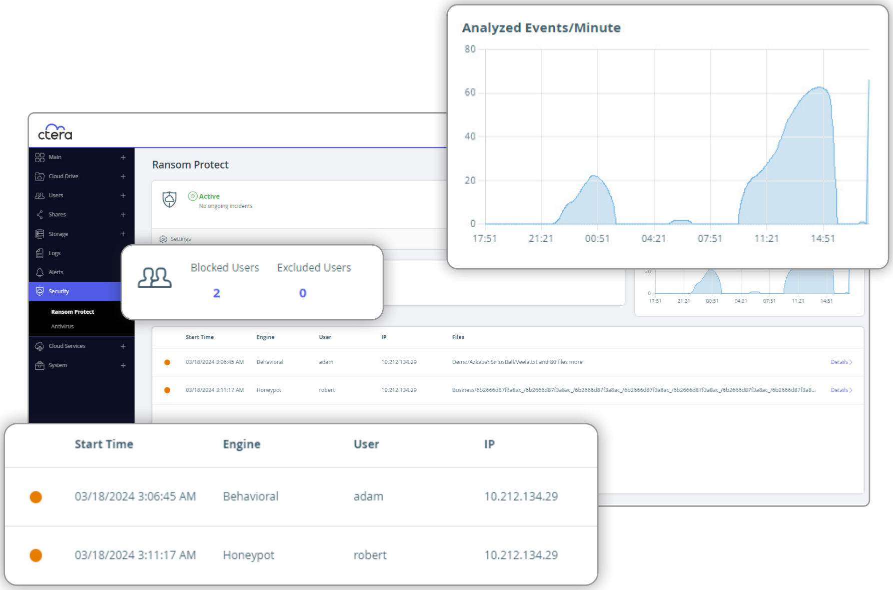
Identify, Block, & Recover

Fighting back against ransomware requires a risk management strategy that goes beyond data security or backup products. While you can't prevent your organization from being targeted by a ransomware attack, you can take steps to protect your data.

CTERA's global file system features Ransom Protect, a state-of-the-art AI-driven ransomware defense mechanism that identifies and halts ransomware attacks in real time. Furthermore, should a ransomware attack occur, organizations have the ability to virtually instantly recover the 'locked' data from immutable snapshots.

## CTERA Ransom Protect

CTERA Ransom Protect employs advanced machine learning algorithms to swiftly identify and block suspicious file activities. Now enhanced with honeypot capabilities, Ransom Protect utilizes the strategic deployment of decoy files within the organization's file system and enables CTERA to identify and stop unauthorized access or attempts at data theft, effectively neutralizing threats before significant damage can occur. With an incident management dashboard, administrators can monitor attacks in real time. The system securely stores extensive incident evidence and logs, aiding in post-attack forensics. Integrated into CTERA Edge Filer, Ransom Protect is easily activated with a single click for streamlined deployment.



| Blocked Users | Excluded Users |
|---|---|
| 2 | 0 |

| | Start Time | Engine | User | IP | Files | |
|---|---|---|---|---|---|---|
| ● | 03/18/2024 3:06:45 AM | Behavioral | adam | 10.212.134.29 | Demo/AzkabanSiriusBall/Veela.txt and 80 files more | Details > |
| ● | 03/18/2024 3:11:17 AM | Honeypot | robert | 10.212.134.29 | Business/6b2666d87f3a8ac_/6b2666d87f3a8ac_/6b2666d87f3a8ac_/6b2666d87f3a8ac_/6b2666d87f3a8ac_/6b2666d87f3a8... | Details > |

| | Start Time | Engine | User | IP |
|---|---|---|---|---|
| ● | 03/18/2024 3:06:45 AM | Behavioral | adam | 10.212.134.29 |
| ● | 03/18/2024 3:11:17 AM | Honeypot | robert | 10.212.134.29 |

### Real-time AI Detection

Ransomware threats can be detected and shut down almost immediately. Advanced machine learning algorithms identify behavioral anomalies suggesting fraudulent file activity, and block offending users within seconds.

### Data Exfiltration Prevention

With use of honeypot decoy files, malicious exfiltration attempts are immediately detected and shut down, neutralizing threats.

### Zero-Day Protection

Ransomware starts working and encrypting files within seconds. When it comes to protection, there is no time to delay – certainly not the length of time that traditional signature-based services take to recognize a ransomware attack. CTERA's Ransom Protect provides true zero-day protection.

### Incident Management

Ransom Protect includes a complete administrator dashboard that enables real-time attack monitoring, comprehensive incident evidence logging, and granular post-attack forensics. Administrators can also re-add any blocked users when it's deemed safe to do so.

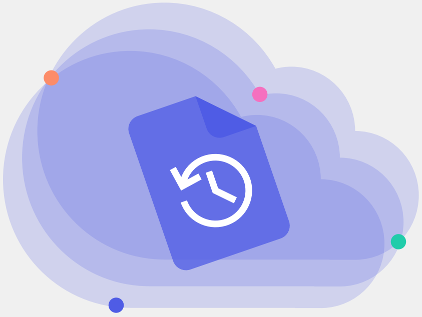
## The Backup Gap

Traditional backup systems are ill-equipped to handle fast-moving ransomware attacks. Backup products for endpoints and servers typically back up data every 8 to 24 hours. This amount of potential data loss is unacceptable in today's fast-paced business environment.

In contrast, CTERA offers continuous real-time protection, synchronizing the data to air-gapped, immutable object storage. This provides a superior defense against ransomware attacks, with RPO (recovery point objective) measured in minutes or seconds.

**24 Hours of Exposure**

2.5 years worth of productivity
for a 1,000 person office

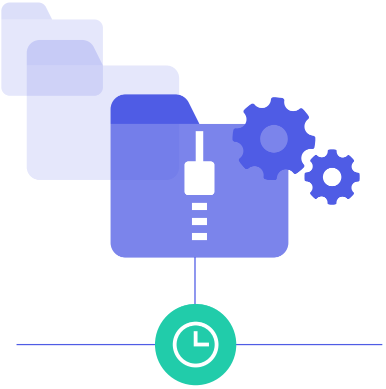


## Instant Recovery

CTERA's caching technology not only replicates the data continuously to the cloud, but offers near-immediate disaster recovery following a ransomware incident, even when tens of terabytes need to be rolled back. When rolling back a folder to a previous version in the cloud, the edge filer is populated nearly instantly with stubs that enable users to immediately regain access to the recovered files on their mapped network drives. There is no need to wait for all the damaged data to be restored.

## Immutable Storage

Over 90% of ransomware attacks target backups. To combat this, CTERA securely stores data in both immutable snapshots and immutable WORM folders in air-gapped object storage. These cannot be deleted or modified during the retention period, effectively creating a safe haven for your data. This strategy thwarts ransomware from destroying your recovery options.



## Zero-Trust Architecture

CTERA is the only global filesystem to have a Zero-Trust architecture. Edge filers never store or receive credentials for the object storage. All storage operations are performed with single-use tokens provided by an authorization service in the CTERA Portal.