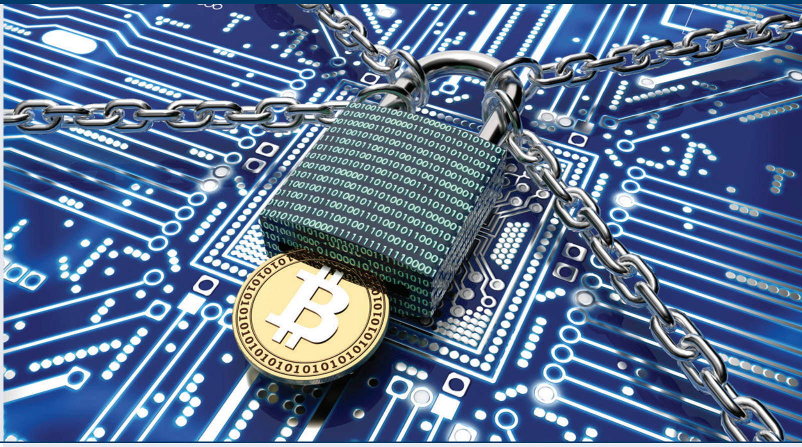
Cloudian Solutions for Ransomware

Ransomware involves the encryption of an organization's data assets by an unauthorized party. To obtain the encryption key, the victim pays a ransom, often in a hard-to-trace crypto-currency such as Bitcoin.



Defense Strategies Have Holes

Strategies for thwarting a ransomware attack usually fall into two categories: preventing the attack and containing its impact.

Attack prevention often involves training programs for users, advising them to avoid "phishing" attacks such as emails whose senders are posing as trusted sources.

Another prevention strategy is to sniff payloads on email for known signatures of malware, or to monitor activities in systems to detect aberrant activities that might connote malware activation.

Finally, you can simply isolate critical systems behind additional layers of firewalls and password challenges to constrain the access of users and programs.

In the long run, these preventive solutions tend to be ineffective. Users become inured to cautions about email hygiene, and technologies designed to block the inroads of malware are quickly rendered obsolete as signatures change rapidly. Firewalls and other blockades irritate users and programmers, who eventually find ways to circumvent their protection for convenience.

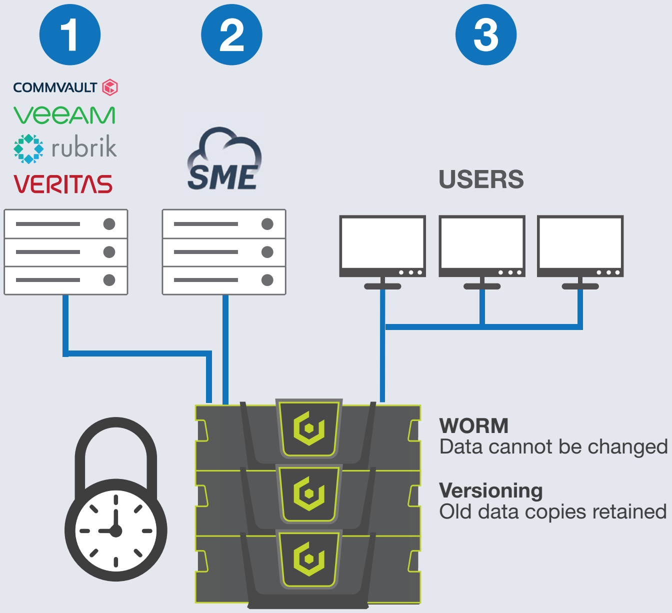
WORM Protects Your Data in the Event of Attack

Attacks can strike even the best-prepared, making it essential to mitigate the effects of a successful breach. Here, the best line of defense is at the storage layer, where the data is written.

The storage technology to preserve data integrity already exists. WORM, which stands for "write once, read many," ensures that data, once written, cannot be changed or deleted until a specified time has passed. Because the data cannot be modified, it therefore cannot be encrypted, thus

3 Ways to Protect Data

1. Backup target for data protection solution
2. Enterprise file synch-and-share
3. File storage for Windows/Mac/Linux clients



rendering the malware ineffective. No one, not even those with admin rights, can change the data, thus also protecting it from employees with malicious intent.

WORM technology is straightforward to implement: it is available as a system-level function of Cloudian® storage.

WORM-equipped storage can be deployed in three ways:

1. **As a backup target:** Cloudian storage can act as a target for popular data protection applications including Veeam, Rubrik, Commvault, and VERITAS. When the WORM feature is activated on this target, the data written is unchangeable for the specified period. This renders hacks pointless.
2. **As part of an Enterprise synch-and-share solution:** Client systems are among the most vulnerable to attacks. Loss of data on those devices may severely impact overall productivity, making a protection strategy critical. The Cloudian/SME enterprise file synch-and-share solution works in conjunction with users' laptops and desktops to maintain a copy of critical files on a central repository where they can be made unchangeable with WORM technology. Data remains on-premises, behind your firewall, immediately accessible when needed.
3. **As a file server:** A straightforward approach is to directly protect files. When configured with Windows/Linux file services plus WORM functionality, Cloudian systems provide a simple means of protecting files as they are stored.

Data Versioning Offers Flexibility

Another option to address the ransomware challenge is data versioning. This creates a new copy of the data when changes are made, while retaining the original copy for a specified period. Thus, if malware encrypts a file, a copy of the unencrypted file will still exist. The benefit of versioning is flexibility: you can erase the old copies at any time to retrieve capacity or comply with data governance rules.

Compared with WORM, versioning offers a lower level of protection: In theory, malware could delete the original, unencrypted data. But ransomware typically does not do this. After all, you can't collect ransom for data that no longer exists.

Both versioning and WORM technologies provide protection where it matters: where the data resides. And they are both easy to integrate and difficult to penetrate.