CONNECTWISE Cloud Backup™

5 Principles of Ransomware Resistant Cloud Backup

The National Cyber Security Centre (NCSC) provides cyber security guidance and support helping to make the UK the safest place to live and work online. NCSC created principles for ransomware-resistant cloud backups. These principles assess the resilience of a cloud-based backup service in the context of the ransomware threat.

Principle	Threat	
1 Backups should be resilient to destructive actions	Ransomware attacks may seek to frustrate or prevent effective recovery by destroying backups. The backup service should therefore be resilient to attempts to destroy backup data and should also protect that data from malicious editing, overwriting or deleting.	✓
2 A backup system should be configured so that it isn't possible to deny all customer access	"If an attacker can stop a victim organisation from accessing its own backup data by disabling or deleting all customer accounts or corporate identities, they won't need to do anything as destructive as deleting the data itself. The backup system should therefore be configured so that it isn't possible for an attacker to deny all customer access, either by deleting the individual accounts used to access backup data, or by deleting the entire customer account. This also includes setting identity and access management (IAM) policies to ensure this."	✓
3 The service allows a customer to restore from a backup version, even if later versions become corrupted	"If an attacker can flood the backup store with corrupted backup data, they won't need to do anything as destructive as deleting the data itself. The backup service should therefore allow customers to store backups for a retention period that aligns with their risk appetite, and system owners should monitor and test the state of their backups regularly."	✓
4 Robust key management for data-at-rest protection is in use	"If a stored backup is encrypted for data-at-rest protection, an attacker doesn't need to actually delete the data itself if they can simply delete or modify the encryption key. Keys used to encrypt data at rest should therefore be protected, to make sure that backup data can be decrypted when necessary."	✓
5 Alerts are triggered if significant changes are made, or privileged actions are attempted	"An attacker hopes that their attempts to compromise a backup won't be detected, since targeting a backup system can be a precursor to an attack on an organisation's main system. If a significant change is attempted, a cloud backup service should raise alerts, and then initiate follow-on actions once those alerts are triggered. The service should offer different types of alert delivery mechanism, so that alerts can still be received if the customer's infrastructure is compromised. Significant changes could include (but aren't limited to) mass deletion requests, backups stopping, altering global retention periods, changes to global encryption policies or changes to administrator account details. The alerts should be raised whether the attempts are successful or not. Alerts are only effective if the customer initiates a follow-on incident management process once triggered."	✓

When it comes to protecting your Microsoft 365 data, 'good enough' is not enough.

ConnectWise Cloud Backup™ is secure & resilient by design. Below is a list of the key features mapped against the ransomware resistant cloud backup principles.

WORM (Write Once, Read Many) Data Storage Principle

Cloud Backup adheres to the WORM (Write Once, Read Many) data storage principle, which means that once snapshots are created, they cannot be modified or deleted.

Principle 1

Modern Authentication

Cloud Backup employs Modern Authentication protocols to ensure that access is granted only to verified and authenticated users.

Principles 1, 2

Role-Based Acces Control (RBAC)

Cloud Backup provides granular controls tailored to the privilege level and role of each user. Unprivileged accounts can't access backups belonging to other accounts.

Principle 1

Automated Snapshots

Cloud Backup snapshots customer data up to 6 times per day and can retain backups for an indefinite time period

Principle 3

Custom Retention Policies

Users can set their data retention policies for the entire organization (tenant level) or for specific areas or types of data (granular level), according to their business needs

Principle 3

Comprehensive Recovery

Cloud Backup provides a range of comprehensive recovery options, including full restorations, individual item or file (granular) restorations, and the ability to restore data from specific moments in time (point-in-time recovery).

Principle 3

Encryption

Cloud Backup encrypts backup both at rest and in transit with Per-contact AES-256 encryption backed by RSA 2048-bit public private key certificates managed via the Windows/Azure infrastructure for both credential management and user content.

Principle 4

Notifications

Cloud Backup delivers detailed notifications to keep customers informed about status updates, existing issues, and potential risks.

Principle 5

Monitoring

Cloud Backup features extensive monitoring tools that allow users to detect and address issues at both the subscription and resource levels.

Principle 5

Want to learn more?

Head to our Trust Center or Book a Demo Today!

Book a Demo

CONNECTWISE