TitanHQ™

Powered by
CYBERSENTRIQ

Entra ID Back Up

Safeguard your business with Entra ID Protection.

Entra ID is the foundation of your IT estate. If it's compromised, your business could come to a standstill. Formerly known as Azure Active Directory, Entra ID faces over 25 billion attacks a year. With millions of passwords breached daily, basic protection is no longer enough. Even Microsoft recommends using third-party services to back up your data.

TitanHQ's Entra ID Backup ensures business continuity by securing access to your Entra ID's user information and permissions.

Why built-in protection isn't enough

Microsoft Entra ID comes with only basic safeguards, leaving critical security gaps. Failure to address these weaknesses exposes your business to significant risk, particularly when facing sophisticated threats.

Limited backup and recovery capabilities

Entra ID offers limited built-in backup and recovery for critical configurations and data. If compromised, you're not just restoring user data, but also piecing back together complex roles, group memberships, and relationships, which slows down your recovery and keeps your business offline when it matters most.

Short retention periods

With Entra ID's 30-day audit log limit, incidents such as cyberattacks, data breaches, or unauthorized access could go undetected for months. TitanHQ offers unlimited retention periods, providing you with the time and data necessary to thoroughly investigate, respond to, and fully recover from any breach.

Increased risk during attacks

Rising cyber threats can easily overwhelm Entra ID's default protection. A sophisticated attack could lock you out of Microsoft 365 and other critical apps, paralysing your entire business. TitanHQ's solution ensures you're always one step ahead by securing backups and allowing fast, efficient recovery in the face of any threat.

Credential stuffing attacks

Attackers exploit weak or reused passwords to infiltrate your identity system. With TitanHQ's Entra ID protection, you can swiftly restore compromised users, group memberships, and access permissions, reducing the damage and downtime caused by stolen credentials.

Zero-day vulnerabilities

When zero-day vulnerabilities hit, identity systems are often the first target. TitanHQ's Entra ID backup and recovery enables you to instantly restore user identities, roles, and relationships, ensuring your business remains operational even during unexpected breaches.

Phishing and business email compromise

Phishing attacks don't just compromise email; they can open the door to your entire identity system. With TitanHQ, compromised accounts can be rolled back, and business access restored in minutes, stopping attackers.

Insider threats

Not all threats are external. Whether due to malicious intent or accidental misconfiguration, insider threats can pose serious risks to identity systems. TitanHQ quickly reverses unauthorised changes, ensuring your critical user configurations are always recoverable.

CAPs and Intune misconfigurations

Conditional Access policies (CAPs) determine the trustworthiness of users and their devices. Microsoft Intune helps organisations manage those devices. These systems can take months to build and weeks to recover in the event of a misconfiguration. TitanHQ recovers CAPs and Intune data in seconds.

Our approach to effortless recovery

Backup

Capture Entra ID data, including user attributes, configurations, groups, roles, and CAPs, with immutable, off-site backups. Your data is kept with no time limits, ensuring rapid recovery without the risk of tampering or deletion.

Compare

Track and compare changes in user configurations over time. Instantly identify discrepancies and restore settings in seconds, cutting time spent digging through audit logs.

Granular recovery

Recover user attributes, licences, and relationships. With detailed change logs and version history, you can quickly revert to any previous version of a user or configuration to maintain smooth operations.

Complete recovery for Entra ID

Recovery isn't just about data; it's about restoring full user functionality. TitanHQ's solution ensures you recover all attributes and relationships necessary to keep your workflows intact. Restore user attributes and licences. Reinstate users with all original attributes so they have the tools they need instantly, and re-establish relationships. Restore critical group memberships, role assignments, and the user's manager for effortless continuity.

Maximise efficiency, minimise disruption.

Speed and simplicity are key. Recover faster, reduce complexity, and cut costs to keep your business on track. Recover in seconds, not hours. Cut recovery times by restoring only what's needed. Solve admin headaches. Troubleshoot user access issues effortlessly, freeing up time from digging through audit logs.

Stay compliant and secure.

TitanHQ's solution keeps you compliant with global regulations, such as ISO 27001, HIPAA, GDPR, and SOC2, offering data retention far beyond Entra ID's 30-day limit.

Ready to safeguard your business?

Deploying TitanHQ's cloud solution is quick and painless, with no hardware and no downtime. Don't leave your business exposed. Protect your users, groups, and configurations today.

Contact us to find out more

Powered by
CYBERSENTRIQ