BitTitan
MigrationWiz

MigrationWiz Security

White Paper

Introduction

MigrationWiz is a web-based data migration platform that uses patented cloud infrastructure to automate the movement of data to the cloud and between cloud tenants. Security, confidentiality, privacy, and compliance are top priority. This security overview will help you understand what measures we use to safeguard your data, and the best practices you should follow to optimize your security approach with each migration.

MigrationWiz uses a shared security approach

BitTitan has met the stringent requirements necessary to receive ISO/IEC 27001 and ISO/IEC 27701 certification, the world's most recognized security and data privacy standards. Still, we recognize that no application vendor can have full control over every potential risk. Security is impacted by a wide range of factors, including employees, third parties, infrastructure design, existing technology, and physical facilities. In addition, organizations must keep up with changing rules and legislation for how they're expected to manage risks within their specific industry. A shared security approach means that BitTitan is doing everything within our scope to decrease risk and protect data during the cloud migration process. But the protection we can provide is only as effective as the measures users take, since many aspects of a secure data migration are not within the control of the MigrationWiz application. This security overview should be studied by everyone using or making decisions about a migration project.

Security best practices and the IT team

In the same way you educate your employees about how cybersecurity begins with them, data protection during a migration relies heavily on your actions before, during, and after each project. Your IT team should implement all applicable best practices discussed below with each project.

In addition, since a major factor in safeguarding any migration is the security of the organization's network, BitTitan cannot assure any level of protection if:

- MigrationWiz is not used in accordance with the User Agreement;
- MigrationWiz is modified, damaged, or misused by any user or third party;
- Users intentionally deviate from the use instructions and security guidance provided by BitTitan;
- Any failure occurs in the customer environment.

Customer best practices

Use strong passwords. Security starts with strong passwords, and this applies to both your BitTitan account password as well as credentials for your source and destination servers. BitTitan follows industry-standard password complexity requirements designed to prevent brute forcing of accounts. We also understand that some users require streamlined use and access. We recommend avoiding guessable words and instead inventing passwords that are longer than 8 characters and include special characters. We also recommend regularly changing your account and data server passwords and credentials – at least every 90 days – and resisting the temptation to recycle old passwords.

Use temporary administrative credentials. You can streamline your migrations by using administrative-level credentials, including Microsoft 365 impersonation for increased bandwidth. To do this, BitTitan recommends creating temporary credentials for each migration, then changing them after the project is complete. Temporary passwords should always adhere to standard password policies and they should not include any data relevant to your organization or project.

Practice least-privileged access. Be mindful that your biggest security threat can be your internal employees. Careless, uninformed, or nefarious activities can have damaging results. In addition to frequent security training for all employees, BitTitan recommends that you adhere to a least-privileged access control protocol. This means restricting access rights for users, accounts, and computing processes to only those resources each individual absolutely needs to effectively perform their everyday duties.

Sanitize sources pre-migration. Since MigrationWiz migrates data “as-is,” anything that’s infected at the source will carry over to the destination. So, as part of your pre-migration process we always recommend that you run an anti-virus scanner on the source prior to executing the migration. In taking this step, you can avoid bringing viruses into the destination, and also ensure that your data is migrated without corruption errors.

Customize your data purge. We recommend that you delete projects after reviewing account activity and verifying that the migration is complete. Deleting the project severs the connection between MigrationWiz and your source and destination servers. You can also set MigrationWiz to auto-delete an unused project within a period of time that you specify. The Maintenance section of Advanced Options is the place to configure a custom purge policy for each migration project.

Maintain source data post-migration. Even after a successful migration, we recommend that you maintain your source data server for a period of time. This redundancy will help recover infected or corrupted data that fails to migrate. It also helps you ensure that mail forwarding is working properly.

Keep track of what’s going on. While MigrationWiz does most of the migration work for you, your core team should do regular monitoring to maintain security. This includes a regular review of account activity to prevent unauthorized use. During a migration, you can set email notifications to alert your team of the project’s success or failures. We further enable you to log subject lines of failed items, which provides better support visibility but may not adhere to your own internal privacy policies.

Understand Common Vulnerabilities and Exposures (CVEs). The simple reality is that you can't depend on every data platform to be invulnerable. For example, Outlook Web App (OWA) in Microsoft Exchange Server 2013 SP1 and Cumulative Update 6 does not properly validate redirection tokens. This allows remote attackers to redirect users to arbitrary web sites and spoof the origin of email messages via unspecified vectors. This is known as "Exchange URL Redirection Vulnerability." This list of common software vulnerabilities should be reviewed regularly; at least as often as new software updates are installed: https://web.nvd.nist.gov/view/vuln/search

Verify the security and compliance of every system you use. MigrationWiz conforms fully with ISO/IEC 27001 and ISO/IEC 27701 standards. ISO/IEC 27001 is the world's best-known standard for information security management systems (ISMS). ISO/IEC 27701 specifies requirements and provides guidance for Privacy Information Management Systems (PIMS) for personal data, including compliance with regulatory requirements for GDPR and the California Consumer Privacy Act (CCPA). Ask your BitTitan sales rep if you need copies of our ISO certificates which are good until the next audit in 2026. BitTitan uses Azure data centers which are compliant with ISO/IEC 27001/27002:2013, SOC 1 Type 2 and SOC 2 Type 2, PCI DSS Level 1, FISMA, HIPAA/HITECH, CJIS, CSA CCM, FERPA and others. You can select from a variety of data center regions based on the requirements of your migration.

How BitTitan protects data

BitTitan follows industry best practices for securing data transmission. Our practices are continually updated and applied to MigrationWiz as technology evolves. We recommend that users follow industry standards for securing systems, services, and data. BitTitan does not clean, scan or search for any potential viruses, threats, or malware in your data, but we do use an AES hashing algorithm to encrypt data connections within the scalable environment. This means:

- All application endpoints that interact with a backend data store have been tested for injection vulnerabilities.
- All application endpoints that accept user input have been tested for cross-site scripting vulnerabilities.
- All application endpoints are tested daily for unvalidated redirects.
- All application endpoints that pass authentication credentials or session tokens are only accessible via HTTPS, using SSLv3 or above.
- Any application endpoint that requires the user to enter their credentials is protected from clickjacking via the use of the ‘X-FRAME-OPTIONS’ header.
- Any stored passwords are hashed with a standard hashing algorithm and an appropriate salt.
- User logins enforce password complexity and are protected from brute forcing.
- Using Advanced Options, Modern Authentication enables authentication features like multi-factor authentication.
- BitTitan scans its network perimeter, disables any unnecessary services, and patches any critical CVEs in its infrastructure.

All activities on your MigrationWiz account are logged to individual end-users so you can monitor any deviations. Except as related to the secure purging of data, user logs do not roll. BitTitan may review logs on any customer account at any time, including when there’s reason to think there’s been a potential security event.

Data handling. MigrationWiz doesn't store any cache of data processed during migrations. All data is cleared when it's been successfully moved and it cannot be retrieved by any means. You control both the source and destination at all times and have the ability to add audit logging to verify data transmission. For convenience, you can use temporary administrative credentials and Microsoft 365 impersonation to manage your migration project. We highly recommended that you disable these administrative accounts immediately upon completion of the migration to prevent breaches.

Database-level security. MigrationWiz uses strong password complexity and change requirements to authenticate internal users. All data stored in BitTitan databases uses web endpoints with AES 256-bit encryption (with ISO 10126 padding and proper random IV initialization). Direct access to databases is restricted and databases queries are limited to administrators only and for non-data warehouse systems.

MigrationWiz connects outside the firewall and is fully automated. There's no human interaction with the servers, software, or the migration process. As a rule, data is never saved to a physical disk, although data processed on virtual machines may be cached temporarily to optimize throughput depending on the type and duration of your migration project.

Network security. MigrationWiz enables geographically dispersed, locally-deployable, fault-tolerant cloud computing infrastructure to customize the network handling your migration. That means you can select from a variety of data center locations and implementation methods to optimize your network security. Networks are monitored 24/7/365 over all application endpoints, and network layer ports are monitored on 5-minute intervals.

Logging. Log files are reviewed regularly for security events like failed actions and administrative access. Logging to a syslog or log server is enabled, and log files are reviewed on an ad hoc basis if suspicious activities are observed. If a potential security event is suspected during log review, it's immediately reported to the BitTitan operations team.

External networks. Every connection to an external network is terminated at a firewall and devices are configured to deny all traffic by default.

Globally redundant continuity. BitTitan maintains and tests an effective business continuity plan that includes disaster recovery and crisis management procedures so we can provide continuous access to, and support for, the MigrationWiz application. This plan includes daily backups and archiving, as well as maintaining duplicate or redundant systems that can fully recover the application and all content. We also follow procedures and frequency intervals for transmitting backup data and systems to BitTitan's backup location. BitTitan's backup storage and systems are located at a secure physical location remote from BitTitan's primary system(s) and is updated and tested at least annually.

Definitions

The following definitions are used throughout this Security Overview:

- ***User Agreemen***t means the applicable User Agreement at https://www.ideracorp.com/Legal/bittitan#tabs-2
- ***Application*** means the web-based data migration software, MigrationWiz, hosted by BitTitan and made available at www.bittitan.com or any subdirectory or successor site.
- ***Network*** means the BitTitan-controlled environment including tables, databases, architecture, and topology, local desktop, or devices used and controlled by BitTitan employees or contractors (including the employee intranet), and any other internet-enabled zone used to support MigrationWiz and handle the data being migrated.
- ***Customer environments*** means the customer or its affiliates' environment including any tables, applications, network, security measures (e.g., firewalls), databases, machines, servers, architecture and topology, local desktop, or devices used by customer employees or contractors (including the employee intranet), and any other system used by the customer, excluding the network and application.
- ***Security event*** means any event attributable to the application or network that results in harm or an unauthorized disclosure in breach of the User Agreement concerning the data.
- ***Best practices*** means methods or techniques to prevent a security event as aligned with ISO 27002:2005.

Contact Us

All migrations start with MigrationWiz, a fully automated, 100% SaaS migration solution that can be accessed at anytime from anywhere. Sign up, configure, and initiate mailbox, document, personal archives, public folders, and cloud storage migration projects from a single, centralized user interface. No special training, personnel, or additional hardware or software installation needed. One of the fastest migration engines on the market, MigrationWiz makes spinning up migration projects a breeze. An enterprise-grade solution designed to scale on-demand, MigrationWiz is easy to use, secure, and industry-tested — by SMBs and Fortune 500 companies alike.

To get started with your migration project, visit www.bittitan.com.