MigrationWiz®
Security Overview

Table of Contents

Introduction

This whitepaper is targeted to current and potential BitTitan customers who are interested in migrating data using MigrationWiz. MigrationWiz is a patented SaaS product that runs on Azure. This whitepaper is designed to help you understand what measures we use to safeguard your Data, but more importantly, to recommend customer best practices to optimize your security approach for each migration.

Overview

We take the security of our environment seriously. BitTitan's environment security is designed to protect mission critical resources and to provide a secure, robust, and geographically dispersed environment that helps to ensure data integrity and to secure against accidental or deliberate data deletion or leaks. This secure environment is maintained and with encryption and other controls discussed below. This document describes how using best practice recommendations to optimize each migration users can leverage BitTitan's secure SaaS application to efficiently and cost-effectively move data across a variety of environments and platforms.

Customers should leverage our Knowledge Base guidance and documents to enhance the overall security of their data during the migration process.

Definitions

In this Security Overview, the following definitions will apply. All other capitalized terms will have the meaning set out in the User Agreement:

"Customer" means any BitTitan customer or user of the Service Offerings.

"User Agreement" means the applicable User Agreement at www.bittitan.com/legal.

"Application" means the web-based data migration software 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 employee intranet), and any other internet-enabled zone used to support the Application and that handles the Data.

"Customer Environment" 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 employee intranet), and any other system used by 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.

"Good Industry Practices" means methods or techniques to prevent a Security Event as aligned with ISO 27002:2013.

Shared Security Approach

BitTitan designed MigrationWiz as a cloud native product. Using advanced and proprietary cloud infrastructure technologies, we enable scalable network throughput by connecting diverse and powerful networks across the solution. Because we rely on the security of your network to safeguard your migration, our security model is a shared approach. Throughout this document, we will refer to customer best practices to implement a customized security approach.

Our security practices do not cover exposure, breaches or failure resulting from any:

a) use not in accordance with the User Agreement
b) modifications, damage, misuse or other action of user or any third party
c) any failure of a customer environment
d) intentional deviations from our provided guidance.

Customer Best Practices

Creating Strong Passwords. Creating strong passwords applies to both the password to your BitTitan account and the credentials of your Source and Destination data servers. BitTitan maintains password complexity requirements designed to prevent brute forcing of accounts in accordance with industry standards. For those users requiring additional security, we recommend extending the length of your password beyond 8 characters, including special characters, and avoiding guessable passwords. We also recommend regularly changing your account and data server passwords and credentials (e.g., every 90 days) and avoiding recycling any old passwords.

Credential Handling and Storage during and after Migration. We enable users to streamline the process of migrations by using administrative-level credentials (including Office 365 impersonation for increased bandwidth capabilities). Accordingly, we recommend that you create temporary credentials during each migration and change these temporary credentials after the completion of your project. Note that temporary passwords should adhere to standard password policies and should not include any data relevant to your organization or project.

Source Sanitization. MigrationWiz migrates your data “as-is”, meaning that anything currently infected will remain so even after the migration. Accordingly, to ensure sanitation, we recommend that you run an appropriate antivirus scanner on your Source prior to migrating any contents. This practice has the added benefit of ensuring that your data is easily migrated without corruption errors.

Customizing Your Data Purge. MigrationWiz allows you to configure a custom purge policy by setting the number of days after which your project will be auto-deleted if unused. We recommend that you delete a project after completion. By deleting the project, you delete the connection between MigrationWiz and your Source and Destination messaging servers. You should carefully review your account activity to ensure that the project is indeed complete. Note that you can use the Maintenance section of Advanced Options to configure a custom purge policy for each migration project.

Source Maintenance Period. Even after your migration is completed, we recommend that you perform a backup of your source before shutting it down or deleting it and maintaining your Source data server for a period of time to prevent any data loss resulting from failure to migrate, whether as a result of infected or corrupted data. By maintaining some redundancy, you also ensure that mail forwarding is working properly. Since MigrationWiz is a copy and paste tool your source will be exactly as you left it.

Account Review Practices. You should regularly review your account activity to prevent unauthorized use. We enable you to set notifications to ping an email address of your choice in the event of a successful/failed migration. 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). You are responsible for the accounts that have access to the environments. If the account is not being actively used to migrate data you should disable it. You are admins to your environment and have the ability to view where the connections are coming from for any account. If you see anything out of the ordinary or coming from an odd IP, disable the account and contact Support@BitTitan.com.

Understanding your Common Vulnerabilities Exposures (CVEs). Data platforms are not always invulnerable. For example, Outlook Web App (OWA) in Microsoft Exchange Server 2013 SP1 and Cumulative Update 6 does not properly validate redirection tokens, which allows remote attackers to redirect users to arbitrary web sites and spoof the origin of email messages via unspecified vectors, aka "Exchange URL Redirection Vulnerability." A list of common software vulnerabilities is available at https://nvd.nist.gov/ and should be reviewed regularly and at least as often as new software updates are installed.

Least-Privileged Access Controls. Least privileged access control is the concept and practice of restricting access rights for users, accounts, and computing processes to only those resources absolutely required to perform routine, legitimate activities – that is, provisioning accounts with the lowest level of user rights to effectively perform duties. Frequently, a customer's biggest security vulnerability is often their internal team. BitTitan provides best practices security training to all employees. BitTitan recommends that all customers and users adopt a similar process to safeguard systems and data from accidental loss or unauthorized access.

Application Security

BitTitan implements industry best practices for securing the transmission of data and these are continuously updated as technology evolves. We recommend that customers and users follow industry standards for securing systems, services, and data. BitTitan utilizes an AES hashing algorithm to encrypt data connections within the scalable environment.

- All Application endpoints that interact with backend workers, i.e., 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 for invalidated redirects daily.
- All Application endpoints that pass authentication credentials or session tokens are only accessible via HTTPS, using TLS 1.2 (also compatible with TLS 1.1).
- 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 passwords stored by the Application are hashed with a standard hashing algorithm and an appropriate salt.
- User logins enforce password complexity and are protected from brute forcing.
- BitTitan scans the Network perimeter, disables any unnecessary services, and patches any critical CVEs in its infrastructure.

Application end user accounts activity is captured and logged. This is to enable users audit activity and trace it back to the original actor in case of impersonation. Except to the extent related to the secure purging of data, user logs do not roll. Logs are reviewed at the discretion of BitTitan, including upon notice or knowledge of a potential Security Event.

Data Security and Handling

BitTitan does not store or maintain any cache of data processed during migrations. All cache or data used is cleared upon completion of the copy of the item and is not retrievable by any means upon success. You can use temporary administrative credentials and Office 365 impersonation to manage the entire migration project. You control both the source and destination at all times and have the ability to add audit logging to verify the transmission of the data. We highly recommended that you disable these administrative accounts immediately upon completion of the migration to prevent any unintended data breaches.

You control the security of your data. BitTitan does not clean, scan or search for any potential viruses, threats or malware in your data and we do not store any of the transmitted data.

Database Level Security

We authenticate internal users through strong password complexity and change requirements. Further, we store all data in our databases with web endpoints using an AES 256-bit encryption (with ISO 10126 padding and proper random IV initialization). We restrict direct access to databases and limit queries of databases to administrators only and for non-data warehouse systems. We automate the process; there is no human interaction with the servers, software, or migration process. We connect outside of the firewall and never save any data to a physical disk. Data processed on virtual machines may be cached temporarily to optimize throughput, depending on the type and duration of your migration project.

Network Security

Optimize Your Migration Network. MigrationWiz enables geographically dispersed, locally deployable, fault-tolerant cloud computing infrastructure to distribute and optimize migrations. You can choose from a variety of geographically dispersed data centers and implementation methods. Networks are monitored on a 24x7 basis over all Application endpoints, and Network layer ports are monitored on five-minute intervals. BitTitan's patented technology allows you to scale your network to migrate large quantities of data over diverse and distinct technologies.

Logging. Log files are reviewed regularly for security events (failed actions, administrative access, etc.). Logging to a syslog or log sever 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 is reported to the Operations Team for immediate action.

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

Business Continuity

Globally Redundant Continuity. BitTitan maintains and tests an effective business continuity plan (including disaster recovery and crisis management procedures) to provide continuous access to, and support for, the Application.

BitTitan agrees to:

(i) Back up, archive and maintain duplicate or redundant systems that can fully recover the Application on a daily basis. As previously noted, BitTitan *does not house or save migration data*.

(ii) Establish and follow procedures and frequency intervals for transmitting backup data and systems to BitTitan's backup locations. All storage and systems are located in secure Geophysical locations in Azure.

(iii) Update and test BitTitan's primary system(s) archives at least annually to ensure viability of recovery.

Contact Us

For technical information, and to learn more about our pricing and incentives, visit www.BitTitan.com or contact a member of our Sales team at www.BitTitan.com/Contact.

About BitTitan

BitTitan® empowers IT service professionals to successfully deploy and manage cloud technologies through automation. While MigrationWiz® is the industry-leading SaaS solution for mailbox, document and public-folder migrations between a wide range of Sources and Destinations. Since 2009, BitTitan has moved over 13 million users to the cloud for 36,000 customers in 187 countries and supports leading cloud ecosystems including Microsoft, Amazon, Google and Dropbox. The global company has offices in Seattle and Singapore. To learn more, visit www.BitTitan.com.