Proxima

Datasheet

Cloud to Cloud Backup for Microsoft Office 365

If you are one of the many organizations embracing Microsoft Office 365, you may not realize there is a risk that your data could be lost.

With Office 365, all your data, including emails, calendars, and files, live in a Microsoft cloud that is beyond your control. Does it matter? After all, Microsoft offers a financially backed guarantee of 99.9% uptime with state-of-the-art redundancy at every layer.

But scratch beneath the surface and you'll find good reasons to back up your Office 365 data to a central backup repository in your own secure data center or a trusted third party service provider's data center.

Four Reasons Your Office 365 Data isn't as Safe as You May Think

1. **Compliance.** Many organizations fall under strict email and document retention regulations, where failure to comply can lead to expensive fines or worse. By default, deleted Office 365 data is non-recoverable after a maximum of 30 days. Longer retention times are only possible with more costly or expensive editions of Office 365. And if your Office 365 subscription is ever cancelled, all your data is automatically deleted after 90 days. Having your own backup copies of your Office 365 data ensures you can comply with regulations regardless of your Office 365 edition or whether or not your subscription is cancelled.
2. **Liability.** The Office 365 terms of service currently limit Microsoft's liability to $5,000 or your last 12 months subscription fees should anything happen to your data—assuming you can prove it was Microsoft's fault. In contrast, the liability you might face if your Office 365 data were lost is potentially unlimited. Given the amount of risk you bear, it's prudent to keep a copy of your Office 365 backup data in a secure, non-Microsoft location.

Proxima Software Solutions
T: 0203 6422270
W: proxima-software.com

POWERED BY Asigra.

3. **Audit Rights.** The Office 365 terms of service give you no audit rights. This is problematic if, as part of an audit, you are required to show the physical location where your data is stored. Maintaining a backup copy of your Office 365 data in a secure location that you are able to audit may be an acceptable way to work around this problem.
4. **Vendor Lock-in.** Having all your Office 365 data in the Microsoft cloud effectively marries you to Microsoft, for better or for worse. If you want to keep your options open, then maintaining a backup copy of your Office 365 data makes it much easier to consider migrating to another vendor's office productivity service.

Take Control of Your Office 365 Data Protection

Our solution powered by Asigra can help you securely protect your Office 365 data:

- Easily schedule automatic creation of point-in-time backup copies of your data in key Microsoft Office 365 services like Exchange Online, SharePoint Online, and OneDrive
- Backup copies are deduped, compressed, encrypted, and then stored to the secure private, public, or hybrid cloud of your choice (Figure 1)
- An intuitive user interface allows you to establish and automatically apply backup rules—no recovery settings need to be configured in Office 365
- The interface also helps you quickly recover your data—accidently deleted emails and files, corrupted calendars, or even entire mailboxes—either back into Microsoft Office 365 or to another location
- Define Office 365 backup rules with complete flexibility to meet the needs of your business, such as applying different point-in-time backup intervals and retention periods for OneDrive data versus Exchange data

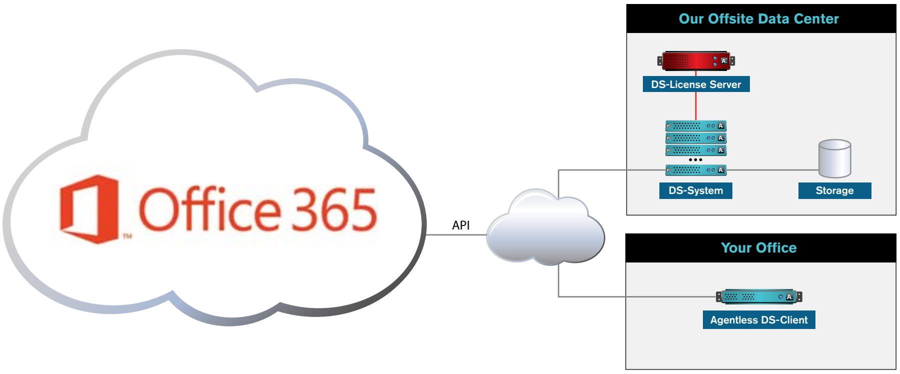


Figure 1

Business Benefits

- Granular backups of data in Office 365
- Recovery and restore assurance
- Standardized backup and recovery approaches
- Advanced administration options
- Peace of mind through automation – set it and forget it
- Deploy in the computing style of your choice: as a service to our data center; as a private cloud in your own data center; or a hybrid cloud. If your preferences evolve over time, you can change your deployment style easily.

Key Features and Capabilities

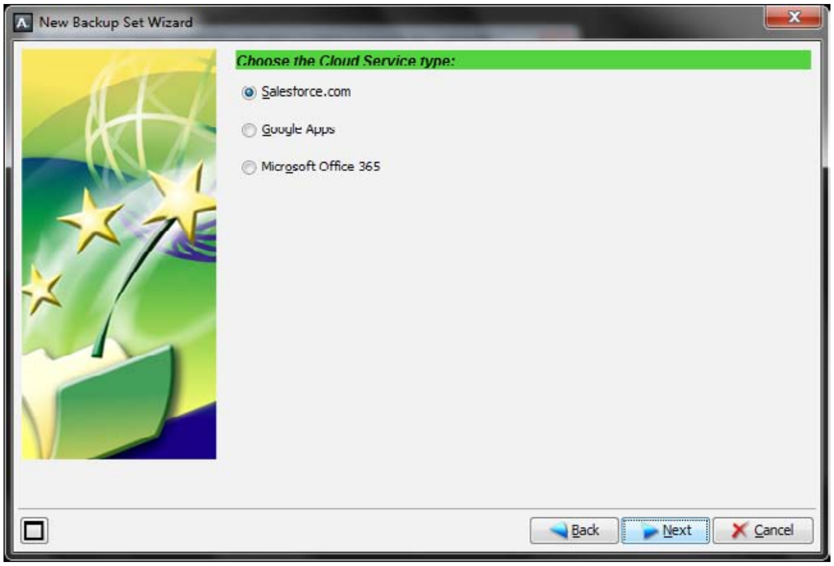
- Secure Backup and Recovery for all Corporate Data Sources
- Agentless
- Autonomic Healing and Validation Restore
- Continuous Data Protection
- Selective Data Destruction
- NIST FIPS 140-2 Certified
- AES 256 Encryption at rest and in-flight
- Bandwidth Throttling
- WAN Optimized

Proxima Software Solutions
T: 0203 6422270
W: proxima-software.com

POWERED BY
Asigra.

Proxima

- Easily accommodate different levels of protection for different groups of Office 365 users with custom backup sets (Figure 2)—for example, more frequent backups of Marketing's Exchange data and less frequent backups of Development's Exchange data


New Backup Set Wizard

Choose the Cloud Service type:

● Salesforce.com

○ Google Apps

○ Microsoft Office 365

Figure 2

- Define protection rules for hundreds of users at the same time, to create backup domain schedules, and to view the status of the last backup, which is saves a lot of time in organizations with hundreds or thoursands of Office 365 users
- Protect all editions of Office 365, without needing to purchase minimum edition levels or special add on features

Comprehensive Data Protection for Office 365 and the Entire Enterprise

Our solution protects much more than your Office 365 data, easily scaling to all other critical data sources in your organization, including physical or virtual machines, mobile endpoints, and other cloud sources like Salesforce, Google Apps or Amazon Web Services. With our solution, you can enjoy peace of mind knowing that your enterprise data is protected and safe.

Microsoft Office 365™ Services protected by our service

Microsoft Exchange Online™

- mailboxes
- email (including any attachments, meta data)
- calendars
- contacts
- tasks

Microsoft Sharepoint Online™

- sites
- calendars
- contacts
- discussion lists
- document libraries
- list content

Microsoft OneDrive™

- all files

Contact us today to learn more about our secure backup and recovery solution.

Proxima Software Solutions
T: 0203 6422270
W: proxima-software.com

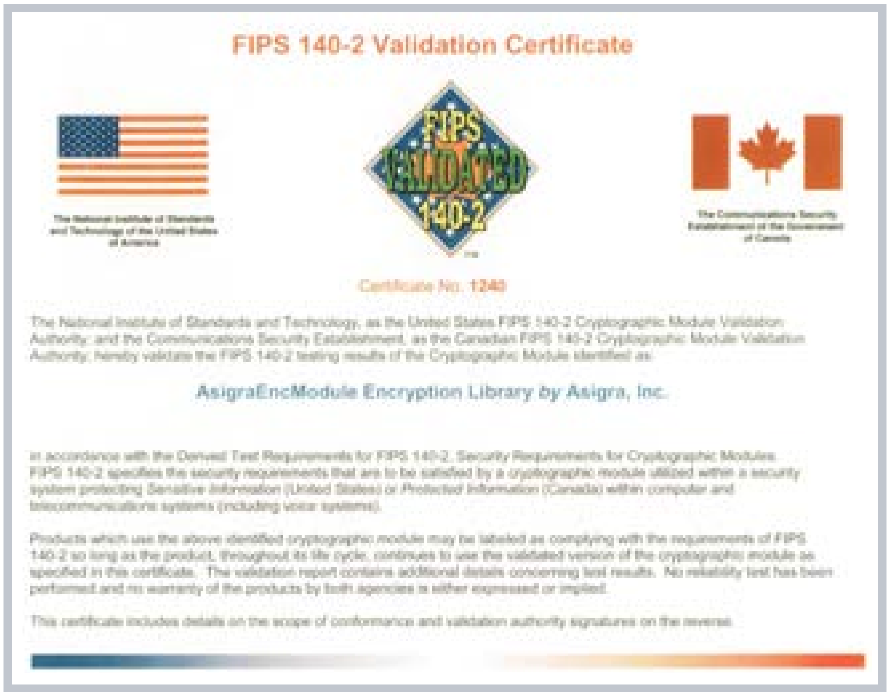
POWERED BY
Asigra.

The importance of FIPS Certification

The Cloud Backup & DR services MPR IT Solutions provide are Powered by Asigra, a FIPS 140-2 certified application, certificate #1240. FIPS is important as it is an internationally recognised, independent standard, that is recommended for use by the UK Information Commissioners Office (ICO). The ICO regulate, investigate and prosecute data loss and data breach incidents under the UK Data Protection Act and the newly implemented General Data Protection Regulations (GDPR).

Please see the ICO guidance on “choosing the right software”, as it applies to data encryption and the prevention of data loss and data breach

Asigra has the Highest Internationaly recognised Software Standard for Security & Encryption NIST - FIPS 140-20 Certificate



FIPS 140-2 Validation Certificate

The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

Certificate No. 1240

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

AsigraEncModule Encryption Library by Asigra, Inc.

in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting Sensitive Information (United States) or Protected Information (Canada) within computer and telecommunications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

Choosing the right software

The way that encryption software is put together is also crucially important. Software can use a state of the art algorithm and a suitably long key to output encrypted data, but if its development did not follow good practice, or the product itself is poorly tested or subject to insufficient review, there may be vulnerabilities or other opportunities for attackers to intercept data or break the encryption without the users’ knowledge. It is also possible that the encryption software includes an intentional weakness or backdoor to enable those with knowledge of the weakness to bypass the protection and access the protected data.

ico.
Information Commissioner's Office

It is therefore important to gain an external assessment of encryption software where it is of critical importance to have an assurance that such vulnerabilities do not exist. Such an assessment may also assist in defining an appropriate algorithm and key size.

It is recommended that data controllers ensure that any solution that they, or a data processor acting on their behalf, implement meets the current standards such as FIPS 140-2 (cryptographic modules, software and hardware)

Reference: https://ico.org.uk/for-organisations/guide-to-data-protection/encryption/implementing-encryption/

Proxima Software Solutions
T: 0203 6422270
W: proxima-software.com

Business Benefits of Asigra Cloud Backup with FIPS 140-2 for Office 365

- Reduces the risk of data loss
- Reduces the risk of data breach
- Follows UK Information Commissioners Office recommended best practice
- Automated encryption, no human intervention
- Backup data is encrypted at rest and in transit
- May mitigate the level of fine or sanction if loss did occur
- Assists readiness for General Data Protection Regulations (GDPR)
- Assists readiness for Data Protection for Data Insurance

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

The National Institute of Standards and Technology (NIST) independently certify products containing encryption that IT vendors provide them.
All FIPS 140-2 certified products can be searched for online through NIST

Reference: http://csrc.nist.gov/groups/STM/cmvp/validation.html

POWERED BY
Asigra.