Ensuring Data Protection and Privacy in Office 365 Multi-Tenant Environments

EXECUTIVE SUMMARY

This is the era of cloud-first. From public and private clouds to multi-cloud, hybrid cloud, and multi-tenant clouds, the growth and penetration of cloud technology is enabling enterprises to transform and innovate their business. With this growth comes new challenges and complexity with managing the various cloud deployments and ensuring their security.

While protecting your data is always a top-of-mind concern, it is even more imperative when you need to move vast amounts of it between cloud tenants to support a merger, acquisition, divestiture, or a similar business initiative. This paper outlines some key data protection and privacy compliance considerations when planning to integrate or migrate Microsoft Office 365 tenants and how the Binary Tree Power365® platform can safeguard your sensitive information in these types of business transformations.

INTRODUCTION

Keeping your applications and data safe from intrusion and breaches remains, of course, one of IT's highest- priority functions. Today, Microsoft spends over $1 billion annually on security, and there are various forms of protections offered by cloud providers and technology providers, including:

Physical security of the cloud datacenter, including background checks and biometric two-factor authentication for employees

Breadth of security offerings, ranging from cloud anti-virus to distributed denial-of-service protection to encryption to key management

Identity and access controls including secure directory and single sign-on

Defense-in-depth capabilities providing protection at every level of the stack

Microsoft assumes some of the responsibilities of information security in the Microsoft Azure cloud, while you are responsible for others.

As you plan or evolve your cloud strategy, it's important to understand the shared responsibility of both security and regulatory compliance in the cloud. Meaning that the cloud vendor, such as Microsoft, assumes some of the responsibilities of information security in the Microsoft Azure cloud, while you are responsible for others.

For example, Microsoft is responsible for ensuring the security of their datacenters and, for managed services, system software. **However, you 'the customer' retain responsibility for systems software, other managed services and for the security of your applications and data.**

SECURING DATA AT ALL STAGES

Data is the foundation for all things computing and is especially true for financial and healthcare industries. Data breaches are an ever-increasing threat to every industry that needs to be protected against both internal and external threats.

Data encryption is the most powerful tool that helps secure and prevent the compromise of your data. For financial institutions and large health systems that routinely deal with large volumes of highly confidential (financial records, patient records, trade records), confidential (PII, IP, regulatory requirements), sensitive (emails, docs) and public (unrestricted) data, security is of utmost importance.

Moving to Azure for the first time or consolidating a multi-tenant environment resulting from a merger, acquisition or divestiture means you need to be sure that your data is secure during cloud migration and once it is in destination Azure cloud. Protecting data in transit, at rest and in use should be an essential part of your data protection strategy as data could be exposed to risks in all stages. With a constantly evolving economy, businesses are even more data-driven and data security is most instrumental for them. Today, having the right set of controls and tools can help you secure the data in all the stages – in transit, at rest and in use.

DATA AT REST

Data can be exposed while it is not actively moving from device to device or network to network, when instead, it is stored in the cloud. The Encryption at Rest designs in Azure uses a symmetric encryption (Data Encryption key – DEK) to encrypt and decrypt the data and protect the data encryption key with a Key Encryption Key (KEK) for ease of management, access control, and auditing of encryption. Microsoft always protects your data, but Key Encryption Keys allow you, the customer, to meet regulatory requirements to bring your own keys, manage your own keys, and rotate them as mandated by regulations. Encryption at Rest protects against unauthorized data access. You can manage the KEK in your own Azure Key Vault, including bringing your own keys (BYOK) from your HSM to encrypt data with customer managed keys (CMK). By keeping the data encrypted on disk, it prevents compromise of data by the attacker.

DATA IN TRANSIT

Data can be accessed over the network while moving back and forth between locations – whether it's in motion between user and service, between or across datacenters, or end-to-end encryption. Azure recommends end-to-end encryption for data moving between cloud services with standard protocols such as Transport Layer Security (TLS). Azure also uses the Internet Protocol Security (IPsec), to provide authentication, integrity, and confidentiality of data at the IP packet level as the data is transferred across the network.

DATA IN USE

Data can even be exposed while in use, for example while being processed or in memory. An attacker with admin privileges, a malware or a hacker can have access to your data or code while it is being used. Use of technologies such as full memory encryption, enclave technologies, such as Intel's Secure Guard Extensions (SGX), and cryptographic techniques, such as homomorphic encryption (HE), can be used to create secure, trusted execution environments

(TEE). HE allows computations to be done on encrypted data, without requiring access to a secret (decryption) key. The results of the computations are encrypted and can be revealed only by the owner of the secret key. With Azure Confidential computing through TEE, you can now build, deploy, and run applications that protect data confidentiality and integrity in the cloud. TEE is the secure area that runs in an isolated environment protecting data being processed from access outside the TEE. Only authorized codeis permitted to run and to access data, so code and data are protected against viewing and modification from outside of TEE. SQL Always Encrypted with Secure Enclaves protects sensitive data in use while preserving rich queries and providing in-place encryption.

Establishing Cloud Governance

A key function in all cloud strategies is governance. As your use of the cloud grows, you'll want to maintain control by establishing standards for its usage and monitoring to ensure those standards are adhered to. Examples of such standards include:

- which cloud provider(s) is allowed;
- which services are approved (e.g., which relational database(s) is the "standard");
- cost guidelines;
- adherence to reference architectures;
- architecture reviews; and
- compliance reviews and audits.

How to get started with cloud governance?

Think about your business, IT, and organizational goals, as well as your risks; then establish a methodology to help you achieve your end-state. Take the time to benchmark your current state relative to your goals and risks, then build your initial governance foundation, that is, the initial core set of principles to govern against (e.g., deployment rules to ensure security best practices, cost guidelines.

Cloud Operations

Digital transformation is a significant event, and to protect and secure your cloud investment, you'll want to establish a solid cloud operations strategy.

Cloud operations consist of these five disciplines:

1. **Inventory and visibility,** that is, having a detailed knowledge and visibility into the existence and state of each asset.
2. **Operational compliance,** ensuring that cloud assets are properly sized and configured to achieve the desired performance and reach agreed-upon metrics.
3. **Protection and recovery**, that is, the tools and processes to ensure business continuity and minimizing operational interruptions.
4. **Platform operations**, a consistent set of management guidelines and processes for commonly used application platforms (e.g., for Azure SQL, which may have many instances supporting many applications).
5. **Workload operations,** tools and processes to ensure the workload or application as a whole (infrastructure, OS, database, integration, and so on) meets the needs of the business

Effective cloud operations require focus and attention to detail, and when properly designed is a set of commitments between IT and your business partners.

TEN STEPS TO IMPROVING PROTECTION AND COMPLIANCE IN THE CLOUD

In a recent Microsoft survey, "Data Protection and Privacy Compliance in the Cloud: Privacy Concerns Are Not Slowing the Adoption of Cloud Services, but Challenges Remain," organizations surveyed are not confident that their SaaS and PaaS applications meet privacy and data protection requirements. And between 50-60% of these organizations are not even vetting software vendors for critical security capabilities.

A key function in all cloud strategies is governance.

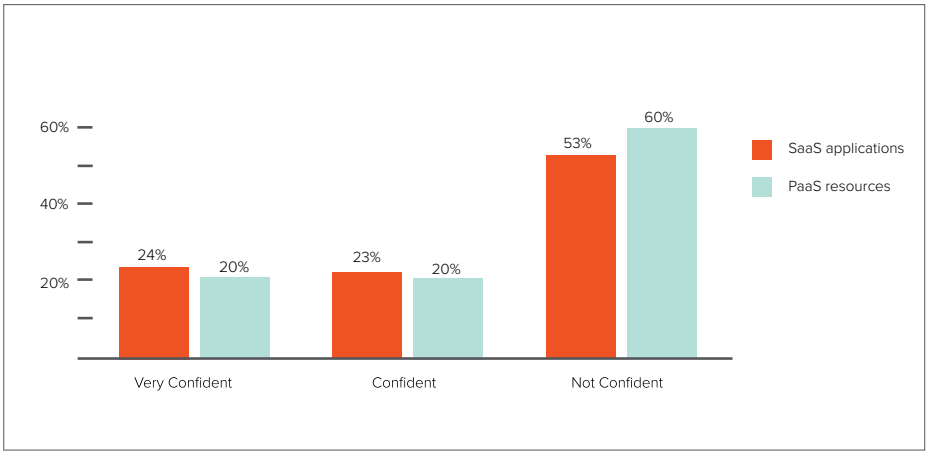

Figure 1. How confident are you that SaaS and PaaS applications used within your organization meet privacy and data protection requirements?

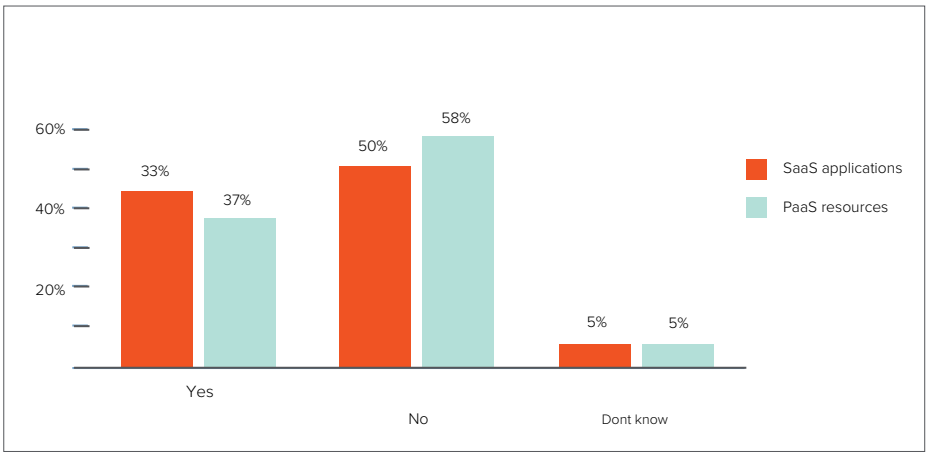

Figure 2. Are SaaS and PaaS applications evaluated for privacy and data security requirements prior to deployment within your organization?

Educate yourself about all the cloud applications and platforms already in use in the orginization.

To improve confidence in your ability to protect data and achieve compliance with privacy regulations in the cloud, the following are recommended steps from the Microsoft report that you can take to address these concerns.

1. Improve visibility into the organization's sensitive or confidential data collected, processed, or stored in the cloud environment.
2. Educate yourself about all the cloud applications and platforms already in use in the organization.
3. Simplify the authentication of users in both on-premises and cloud environments.
4. Ensure the cloud provider offers event monitoring of suspicious and anomalous traffic in the cloud environment.
5. Implement the capability to encrypt sensitive and confidential data in motion and at rest.
6. Make sure that the organization uses and manages its own encryption keys (BYOK).
7. Implement multifactor authentication before allowing access to the organization's data and applications in the cloud environment.

8. Assign responsibility for ensuring compliance with privacy and data protection regulations and security safeguards in the cloud to those most knowledgeable: the compliance and IT security teams. Privacy and data protection teams should also be involved in evaluating any cloud applications or platforms under consideration.

9. Identify information that is too sensitive to be stored in the cloud and assess the impact that cloud services may have on the ability to protect and secure confidential or sensitive information.

10. Thoroughly evaluate cloud-based software and platforms for privacy and security risks.

OVERVIEW OF BINARY TREE POWER365 PLATFORM PROTECTIONS

This section provides a brief overview of the key security considerations in Binary Tree Power365® platform that are designed to safeguard your sensitive information end-to-end in any Binary Tree Power365 multi-tenant integration or migration project.

Microsoft 365 Connectivity and Authentication

FULLY ENCRYPTED CONNECTIVITY

Binary Tree Power365 connects to Office 365 using multiple protocols and APIs, all of which use certificate-based encryption to protect data in-transit. In addition, Binary Tree Power365 is certified with the EU-U.S. and Swiss-U.S. Privacy Shield Framework. The framework certification was designed by the U.S. Department of Commerce, and the European Commission and Swiss Administration, respectively, to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce. More information is provided below.

OAUTH 2.0 TOKEN-BASED APP AUTHENTICATION

Most Binary Tree Binary Tree Power365 functionality leverages token-based authentication to achieve its connectivity to Office 365, meaning credentials are not stored or transmitted between Binary Tree Power365 and Office 365.

OAUTH 2.0 TOKEN-BASED USER AUTHENTICATION

Binary Tree Power365 relies on OAuth tokens for all user activity, from logging in to Binary Tree Power365, to connecting Office 365 tenants to the system. Users log in directly to Office 365's Azure AD, with no credentials ever passing through Binary Tree Power365.

INTEGRATED APP AUTHENTICATION WITH MICROSOFT 365

Microsoft 365 administrators enjoy an integrated authentication experience where you can move from the Binary Tree Power365 app portal to a Microsoft portal seamlessly, without multiple logins and passwords. All while keeping your account security under your organization's policies, rules and security protocols.

MULTI-FACTOR AUTHENTICATION (MFA)

With integrated app authentication, Binary Tree Power365 also supports MFA-enabled users. If your organization leverages MFA within Microsoft 365, then Binary Tree Power365 is ready to provide an integrated login experience.

MANAGED SERVICE ACCOUNTS

For advanced functionality, Binary Tree Power365 generates and manages a dedicated service account in each Microsoft 365 tenant. The account credentials are randomly generated to be unique, highly complex and the password is encrypted at inception and never processed in its unencrypted form. In addition, encryption keys are randomized and never stored.

Power356 connects to Office 365 using multiple protocols and APIs, all of which use certificate-based encryption to protect data in-transit.

All data synchronized or migrated via Binary Tree Power365—including mailbox, OneDrive and public folder data—is encrypted from end-to-end.

MAILBOX DELEGATION

Binary Tree Power365 assigns access rights for its service accounts only to individual mailboxes that are in scope for mailbox migration activities, and only when those rights are necessary for data synchronization activities.

STRICT SSL/TLS ENFORCEMENT

All user connectivity to Binary Tree Power365 must be via HTTPS, with all content delivered directly from Binary Tree Power365 servers, protecting against mixed-content exploits and potential data leaks from external sources.

Binary Tree Power365 Data Transfer Protections

END-TO-END ENCRYPTION FOR DATA MIGRATIONS

All data synchronized or migrated via Binary Tree Power365—including mailbox, OneDrive and public folder data—is encrypted from end-to- end. This includes:

- Reading data from the source mailbox using an encrypted data channel
- Temporarily storing objects using message-level encryption, with each message using a unique, randomly generated encryption key that is only held in memory
- Writing data to the target mailbox using an encrypted data channel
- Performing a secure delete of the temporary message file on the internal Binary Tree Power365 storage as soon as the message is written to the target mailbox

END-TO-END ENCRYPTION FOR THE EMAIL REWRITE SERVICE

All messages that traverse the Binary Tree Power365 Email Rewrite Service are encrypted throughout the process. This includes:

- Accepting messages from Office 365 only through TLS-encrypted interfaces
- Temporarily storing objects using message-level encryption, with each message using a unique, randomly generated encryption key that is only held in memory
- Performing the address rewrite functionality in encrypted memory space
- Delivering rewritten messages back to Office 365 only through TLS-encrypted interfaces for delivery to their destination mail system

END-TO-END ENCRYPTION FOR BINARY TREE POWER365 DIRECTORY SYNC

All data synchronized via Binary Tree Power365—including Active Directory on-premises and cloud-based data—is encrypted from end-to-end. This includes:

- Reading data from the source environment using an encrypted data channel
- Writing data to the target environment using an encrypted data channel

Application Security

VERACODE VERIFIED TEAM TIER SEAL

Binary Tree Power365 is subject to weekly security threat assessments conducted by Veracode to evaluate 3rd party and source code libraries for vulnerabilities and threats. Veracode is recognized as leader in Application Security by Gartner. Binary Tree Power365 has the Veracode Verified Team seal.

THIRD-PARTY SECURITY SCANS AND PENETRATION TESTING

Binary Tree Power365 is subjected to a comprehensive vulnerability scan monthly and thorough penetration tests annually from a leading security provider. Any potential vulnerabilities that are detected are automatically categorized as Severity 1 bugs and are addressed immediately.

Certifications

ISO 27001:2013 CERTIFIED

Binary Tree Power365 is certified and conforms with the requirements of ISO/IEC 27001:2013. ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.

PRIVACY SHIELD ALLIANCE CERTIFIED

Binary Tree Power365 is certified and conform with the requirements of the EU-U.S. Privacy Shield framework and Swiss-U.S. Privacy Shield framework. The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks were designed by the U.S. Department of Commerce, and the European Commission and Swiss Administration, respectively, to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce.

ISO 27018:2014 "CLOUD SECURITY" CERTIFIED

Binary Tree Power365 is certified and conform with the requirements of ISO 27018:2014. ISO/IEC 27018:2014 establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.

Compliance

GENERAL DATA PROTECTION REGULATION (GDPR)

We value adherence to international data protection and security initiatives, including without limitation Article 28 of the General Data Protection Regulation (EU 2016/679). We are committed to implementing an information security program that contains administrative, technical and physical safeguards reasonably necessary to protect against anticipated threats to the security, confidentiality and integrity of data with respect to applicable security standards.

Art. 94 of GDPR repealed Directive 95/46/EC (EU Model Clauses), in which Binary Tree Power365 was compliant. However, we continue to adhere to the standards set by that directive for the transfer of personal data to processors.

CONCLUSION

Data security and privacy are among the topmost concerns for all organizations. Quest provides confidentiality, integrity, and availability of customer data, while enabling seamless integration. Binary Tree Power365 provides customers with features that enable rapid change acceleration with the confidence that customer sensitive data is secure and protected.

NEXT STEPS

We hope you found the guidance in this document helpful. With the right planning and the right solutions, you can protect and secure your multi-tenant projects with confidence.

Contact us today!

Learn more at www.quest.com/binarytree

Data security and privacy are among the topmost concerns for all organizations.

ABOUT QUEST

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (www.quest.com) for regional and international office information.