# Office 365™ Security

## White Paper

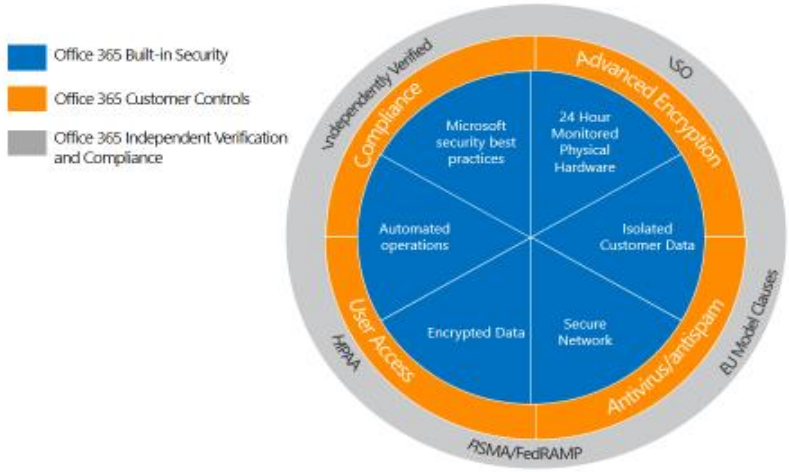
# Introduction

The ability for organizations to control and customize security features in cloud-based productivity services, such as email, calendars, content management, collaboration, and unified communications, is becoming an essential requirement for virtually every company. Today, IT teams are being required to deliver access to productivity services and associated documents and data from more devices, platforms, and places than ever before. While user benefits are undeniable, broader access makes security management more challenging. Each endpoint represents a potential attack surface and another point of management for security professionals. At the same time, organizations face ever-evolving threats from around the world and must manage the risk created by their own users accidentally losing or compromising sensitive data. For these reasons, organizations require a cloud service that has both (a) built-in robust security features and (b) a wide variety of customizable security features that organizations can tune to meet their individual requirements. Organizations expanding remote access while maintaining security best practices may find it difficult and expensive to add this combination of security functionality if they deploy productivity services solely on-premises.

# Office 365™ Security

Microsoft is an industry leader in cloud security and implements policies and controls on par with or better than on-premises data centers of even the most sophisticated organizations. Office 365 security consists of three parts. First, Office 365 is a security-hardened service that has security features built into the service by default. Office 365 customers benefit from in-depth security features that Microsoft has built into the service as a result of experience gained from two decades of managing online data and significant investment in security infrastructure. Office 365 has implemented and continues to invest and improve processes and technologies to proactively identify and mitigate security threats before they become risks for customers.

Second, Office 365 offers security controls that enable customers to customize their security settings. Office 365 is trusted by customers of all sizes across virtually every industry, including highly regulated industries such as healthcare, finance, education, and government. Since Office 365 manages productivity services for such a wide range of industries and geographies, it offers feature choices that customers can control to enhance the security of their data. Third, Office 365 has scalable security processes that allow for independent verification and compliance with industry standards. This paper describes all three aspects of security that are available in the new Office 365.



# Built-In Security

## 24-Hour Monitored Physical Hardware

Office 365 data is stored in the Microsoft network of data centers, run by Microsoft Global Foundation Services and strategically located around the world. These data centers are built from the ground up to protect services and data from harm by natural disaster or unauthorized access. Data center access is restricted 24 hours per day by job function so that only essential personnel have access to customer applications and services. Physical access control uses multiple authentication and security processes, including badges and smart cards, biometric scanners, on-premises security officers, continuous video surveillance, and two-factor authentication. The data centers are monitored using motion sensors, video surveillance, and security breach alarms. Security in the event of natural disaster includes seismically braced racks where required and automated fire prevention and extinguishing systems.

## Isolated Customer Data

One reason Office 365 is both scalable and low cost is that it is a multi-tenant service (that is, data from different customers shares the same hardware resources). Office 365 is designed to host multiple tenants in a highly secure way through data isolation. Data storage and processing for each tenant is segregated through Active Directory® structure and capabilities specifically developed to help build, manage, and secure multi-tenant environments. Active Directory isolates customers using security boundaries (also known as silos). This safeguards a customer's data so that the data cannot be accessed or compromised by co-tenants. For additional cost, a version of Office 365 that stores data on dedicated hardware is available.

## Automated Operations

Within Microsoft data centers, staff's access to the IT systems that store customer data is strictly controlled via role-based access control (RBAC) and lock box processes. Access control is an automated process that follows the separation of duties principle and the principle of granting least privilege. This process ensures that the engineer requesting access to these IT systems has met the eligibility requirements, such as a background screen, fingerprinting, required security training, and access approvals. Engineers request access for particular tasks into a lock box process. The lock box process determines the duration and level of access independently of determining whether another engineer needs to be involved in a monitoring capacity. Such requests are logged as service requests, which are later auditable.

## Secure Network

Networks within the Office 365 data centers are segmented to provide physical separation of critical back-end servers and storage devices from the public-facing interfaces. Edge router security allows the ability to detect intrusions and signs of vulnerability. Client connections to Office 365 use SSL for securing Outlook, Outlook Web App, Exchange ActiveSync, POP3, and IMAP. Customer access to services provided over the Internet originates from users' Internet-enabled locations and ends at a Microsoft data center. These connections are encrypted using industry-standard transport layer security (TLS)/secure sockets layer (SSL). The use of TLS/SSL establishes a highly secure client-to-server connection to help provide data confidentiality and integrity between the desktop and the data center. Customers can configure TLS between Office 365 and external servers for both inbound and outbound email. This feature is enabled by default.

## Encrypted Data

Customer data in Office 365 exists in two states: at rest on storage media and in transit from datacenter over a network to a customer device. All email content is encrypted on disk using BitLocker 256-bit AES Encryption. Protection covers all disks on mailbox servers and includes mailbox database files, mailbox transaction log files,

search content index files, transport database files, transport transaction log files, and page file OS system disk tracing/message tracking logs.

Office 365 also transports and stores secure/multipurpose Internet mail extensions (S/MIME) messages. Office 365 will transport and store messages that are encrypted using client-side, third-party encryption solutions such as PGP.

# Microsoft Security Best Practices

Security in Office 365 is an ongoing process, not a steady state. It is constantly maintained, enhanced, and verified by experienced and trained personnel, and Microsoft strives to keep software and hardware technologies up to date and refined through robust designing, building, operating, and supporting processes. Security Development Lifecycle, Traffic Throttling, Prevent Detect and Mitigate Breach are examples of processes that Microsoft uses to keep Office 365 security the best in the industry.

## Security Development Lifecycle

Security at Microsoft begins before the public ever hears of a given application or service. The Microsoft Security Development Lifecycle (SDL) is a comprehensive security assurance process that informs every stage of design, development, and deployment of Microsoft software and services, including Office 365. Through design requirements, analysis of attack surface, and threat modeling, the SDL helps Microsoft predict, identify, and mitigate vulnerabilities and threats from before a service is launched through its entire production lifecycle. Microsoft continuously updates the SDL using the latest data and best practices to ensure that new services and software associated with Office 365 are highly secure from day one.

## Traffic Throttling to Prevent Denial of Service Attacks

Exchange Online tracks usage baselines and accommodates normal traffic bursts without affecting the user experience. When traffic from a given user exceeds typical parameters, that traffic is throttled until usage returns to normal. Whether the excessive traffic is caused by user behavior or a malicious attack such as a Denial of Service (DoS), Exchange automatically responds to ensure that other users are not affected. Office 365 also uses a third-party commercial DoS monitoring platform for monitoring and throttling capabilities.

## Prevent, Detect, and Mitigate Breach

Prevent Breach is a defensive strategy aimed at predicting and preventing a security breach before it happens. This involves continuous improvements to built-in security features, including port scanning and remediation, perimeter vulnerability scanning, OS Patching to latest updated security software, network level DDOS (Distributed Denial of Service) detection and prevention, and multi-factor authentication for service access. From a people and process standpoint, preventing breach involves auditing all operator/administrator access and actions, zero standing permission for administrators in the service, “Just-In-Time (JIT) access and elevation” (that is, elevation is granted on an as-needed and only-at-the-time-of-need basis) of engineer privileges to troubleshoot the service, and segregation of the employee email environment from the production access environment. Employees who have not passed background checks are automatically rejected from high privilege access, and checking employee backgrounds is a highly scrutinized, manual-approval process.

Preventing breach also involves deleting unnecessary accounts automatically when an employee leaves, changes groups, or does not use the account prior to its expiration. Wherever possible, human intervention is replaced by an automated, tool-based process, including routine functions such as deployment, debugging, diagnostic collection, and restarting services. Office 365 continues to invest in systems automation that helps identify abnormal and suspicious behavior and respond quickly to mitigate security risk. Microsoft is continuously developing a highly effective system of automated patch deployment that generates and deploys solutions to problems identified by the monitoring systems—all without human intervention. This greatly enhances the security and agility of the service. Office 365 conducts penetration tests to enable continuous improvement of incident response procedures. These internal tests help Office 365 security experts create a methodical, repeatable, and optimized stepwise response process and automation.

# Customer Controls

Office 365 combines the familiar Microsoft Office suite with cloud-based versions of our next-generation communications and collaboration services: Microsoft Exchange Online, Microsoft SharePoint® Online, and Microsoft Lync® Online. Each of these services offers individualized security features that the customer can control. These controls allow customers to adhere to compliance requirements, give access to services and content to individuals in a customer's organization, configure anti-malware/anti-spam, and encrypt data where a customer holds the keys.

## Enabling Advanced Encryption

In addition to the robust encryption features detailed above, customers can choose to use Active Directory Rights Management Services (ADRMS) in Office 365. These features provide customers the flexibility to select items they want to encrypt. Encrypting data at rest with ADRMS is also available. Email encryption with non-federated users is available with Office 365, enabling ad hoc encryption services with any recipient. Office Professional Plus offers advanced security with native support for Cryptographic Agility by integrating with the Cryptographic Next Generation (CNG) interfaces for Windows. Administrators can specify cryptographic algorithms for encrypting and signing documents.

## Enabling User Access

Office 365 data and services are secured at the data center, network, logical, storage, and transit levels. In addition, it is critical for customers to be able to control who can access data and how they can use data. Office 365 uses Windows Azure Active Directory as the underlying identity platform. This enables Office 365 customers with strong authentication options granular control over how IT professionals and users can access and use the service. Office 365 also allows integration with On-Premises Active Directory or other directory stores and identity systems such as Active Directory Federation Services (ADFS) or third-party secure token systems (STSs) to enable secure token-based authentication to services.

### Customer-End Federated Identity and Single Sign-On Security Provisions

Administrators can federate on-premises Active Directory or other directory stores with Windows Azure Active Directory, which is the identity platform for Office 365. Once federation is configured, all Office 365 users whose identities are based on the federated domain can use their existing corporate logon to authenticate to Office 365. Federation enables secure, token-based authentication. This also allows administrators to create additional authentication mechanisms such as:

- Two-factor authentication
- Client-based access control, allowing organizations to control how users access information from specific devices or specific locations or a combination of both (for example, limiting access from public computers or from public open Wi-Fi)
- Role-based access control, similar to the access control procedure described above in the Automated Operations section for Microsoft personnel

With IM federation, Lync Online users can IM in a highly secure environment with users in other organizations that use Lync Online, on-premises Lync Server 2010, and even the Skype public IM network. All federated communications are encrypted between the IM systems using access proxy servers. In addition, Lync Online allows administrators to save IM conversations.

### Two-Factor Authentication

Two-factor authentication enhances security in a multi-device and cloud-centric world. Microsoft provides an in-house solution for two-factor authentication with the phone option and also supports third-party two-factor

authentication solutions. The Microsoft phone-based two-factor authentication solution allows users to receive a PIN sent as a message to their phone and enter that PIN as a second password to log on to their services.

## Enabling Compliance

Office 365 delivers a range of compliance features, including data loss prevention (DLP), eDiscovery, and auditing and reporting functionality. Across these capabilities, the user experience is preserved and productivity is not impacted, leading to greater user acceptance.

### Data Loss Prevention (DLP)

While malware and targeted attacks can cause data breaches, user error is actually a much greater source of data risk for most organizations. Exchange Online provides data loss prevention (DLP) technology that identifies, monitors, and protects sensitive data and helps users understand and manage data risk. For example, DLP proactively identifies sensitive information in an email, such as social security or credit card numbers, and alerts users via "PolicyTips" before they send that email. Administrators have a full range of controls and can customize the level of restrictions for their organization. For example, users can simply be warned about sensitive data before sending, sending sensitive data can require authorization, or users can be blocked from sending data completely. DLP features scan both email messages and attachments and comprehensive reporting about what data is being sent by whom is available to administrators.

### Auditing and Retention Policies

Office 365 auditing policies enable customers to log events, including viewing, editing, and deletion of content including emails, documents, task lists, issues lists, discussion groups, and calendars. When auditing is enabled as part of an information management policy, administrators can view the audit data and summarize current usage. Administrators can use these reports to determine how information is being used within the organization, manage compliance, and investigate areas of concern.

### eDiscovery

The new, easy-to-use eDiscovery Center can be delegated to specialist users—such as a compliance officer or human resources personnel—to conduct e-discovery tasks, without having to generate additional overhead for the IT department. eDiscovery allows customers to retrieve content from across Exchange Online, SharePoint Online, Lync Online, and even file shares. With the integrated Office 365 eDiscovery, customers have one single experience for searching and preserving email, documents, and site mailboxes. With eDiscovery customers can be specific about what they want to search for and preserve. The ability for customers to find only what they want and nothing more allows for reduction of discovery costs. The eDiscovery process places no burden on the user for preserving and searching for data, since all of these processes are done in the background.

### Data Spillage Management

Office 365 has compliance features to support customers' dealing with a data "spillage." For example if a federal government customer were to transmit classified data into Office 365, there are ways for the customer to remove the data by themselves. Compliance and security officials with appropriate RBAC privileges can use eDiscovery to search for the message or document and hard-delete them. The hard drives used to store the "spilled" data are never re-purposed or repaired or otherwise moved out of the physical security of the Office 365 data center. They are destroyed if they are no longer used in the Office 365 infrastructure.

## Enabling Anti-Spam/Anti-Malware

Customers have configuration options for anti-malware/anti-spam in the service. Customers also have the choice of using their own anti-malware service and routing to and from Office 365 via that third-party service. Office 365 uses multi-engine anti-malware scanning to protect incoming, outgoing, and internal messages from malicious software transferred through email.

Office 365 evaluates received messages and assigns a spam confidence level (SCL) value. Messages with high SCL values are deleted at the gateway, and messages with low SCL values are delivered to users' inboxes. Messages with borderline SCL values are placed in users' Junk Mail folders, where they are automatically removed after 30 days. Administrators can use the Office 365 Administration Center to manage anti-spam/anti-malware controls including advanced junk mail options and organization-wide safe and blocked sender lists. Individual users can manage their safe and blocked senders from within their inboxes in Microsoft Outlook or Microsoft Outlook Web App.

Content controls and multi-engine malware scanning also help eliminate documents containing malicious code. Based on file name extensions, Office 365 blocks certain file types that can contain malicious code from being uploaded to or retrieved from the service. Office 365 uses an intelligent instant message filter (IIMF) to help protect the service and customer networks against malware and spam via IM. Microsoft developed the IIMF based on years of experience operating secure global IM systems.

# Independent Verification and Compliance

Office 365 has operationalized security into a scalable process that can quickly adapt to security trends and industry-specific needs. Microsoft engages in regular risk management reviews, and it develops and maintains a security control framework that meets the latest standards. Internal reviews and external audits by trusted organizations are incorporated into the Office 365 service lifecycle. Close working relationships with other Microsoft teams result in a comprehensive approach to securing applications in the cloud.

Operating a global cloud infrastructure creates a need to meet compliance obligations and to pass third-party audits. Auditable requirements come from government and industry mandates, internal policies, and industry best practices. Office 365 ensures that compliance expectations are continuously evaluated and incorporated. As a result, Office 365 has obtained independent verification, including ISO 27001 and SSAE16 SOC 1 (Type II) audits, is able to transfer data outside of the European Union through the U.S.-EU Safe Harbor Framework and the EU Model Clauses, is willing to sign a HIPAA Business Associate Agreement (BAA) with all customers, has received authority to operate from a U.S. federal agency under FISMA, and has disclosed security measures through the Cloud Security Alliance's public registry. Office 365 extends the controls implemented to meet these standards to customers who are not necessarily subject to the respective laws or controls.

## ISO 27001

Office 365 service was built based on ISO 27001 standards and was the first major business productivity public cloud service to have implemented the rigorous set of global standards covering physical, logical, process, and management controls.

## FISMA

Office 365 has been granted FISMA moderate Authority to Operate by multiple federal agencies. Operating under FISMA requires transparency and frequent security reporting to our US Federal customers. Microsoft applies these specialized processes across our infrastructure to further enhance our Online Services Security and Compliance program for the benefit of customers who are not subject to FISMA requirements.

## HIPAA BAA

Office 365 is the first major business productivity public cloud service provider to offer a HIPAA BAA to all customers. HIPAA is a U.S. law that applies to healthcare entities and that governs the use, disclosure and safeguarding of protected health information (PHI), and imposes requirements on covered entities to sign business associate agreements with their vendors that have access to PHI.

## EU Model Clauses

Office 365 became the first major business productivity public cloud service provider to sign the standard contractual clauses created by the European Union (known as the "EU Model Clauses") with all customers. The EU Model Clauses address the international transfer of data. Office 365 is one of very few if not the only cloud service that has received broad validation from European data protection authorities (DPAs) regarding its approach to the EU Model Clauses, including from Bavaria, Denmark, France, Ireland, Luxembourg, Malta, and Spain.

## Cloud Security Alliance

Office 365 fulfills compliance and risk management requirements as defined in the Cloud Security Alliance (CSA) Cloud Control Matrix (CCM). The Cloud Control Matrix (CCM) is published by a not-for-profit, member-driven organization of leading industry practitioners focused on helping customers make the right decisions when moving to the cloud. The matrix provides a detailed understanding of the security and privacy concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains. Office 365 has published a detailed overview of its capabilities for the CCM requirements that illustrates how these capabilities meet these requirements and empowers customers with in-depth information to evaluate different offerings in the marketplace today.

# Conclusion

Businesses today need productivity services that help users get more done from virtually anywhere while maintaining security in the face of ever-evolving threats. Office 365 supports both of these needs at once with a highly secure, cloud-based productivity platform. Information regarding Office 365 security, privacy, compliance, transparency, and service continuity can be found in the Office 365 Trust Center. The Office 365 platform incorporates security at every level, from application development to physical data centers to end-user access. Today, fewer and fewer organizations have the ability to maintain an equivalent level of security on-premises at a reasonable cost.

Importantly, Office 365 applications include both (a) built-in security features that simplify the process of protecting data and (b) the flexibility for administrators to configure, manage, and integrate security in ways that make sense for their unique business needs. When businesses choose Office 365, they get a partner that truly understands business security needs and is trusted by companies of all sizes across nearly every industry and geography.