EBOOK

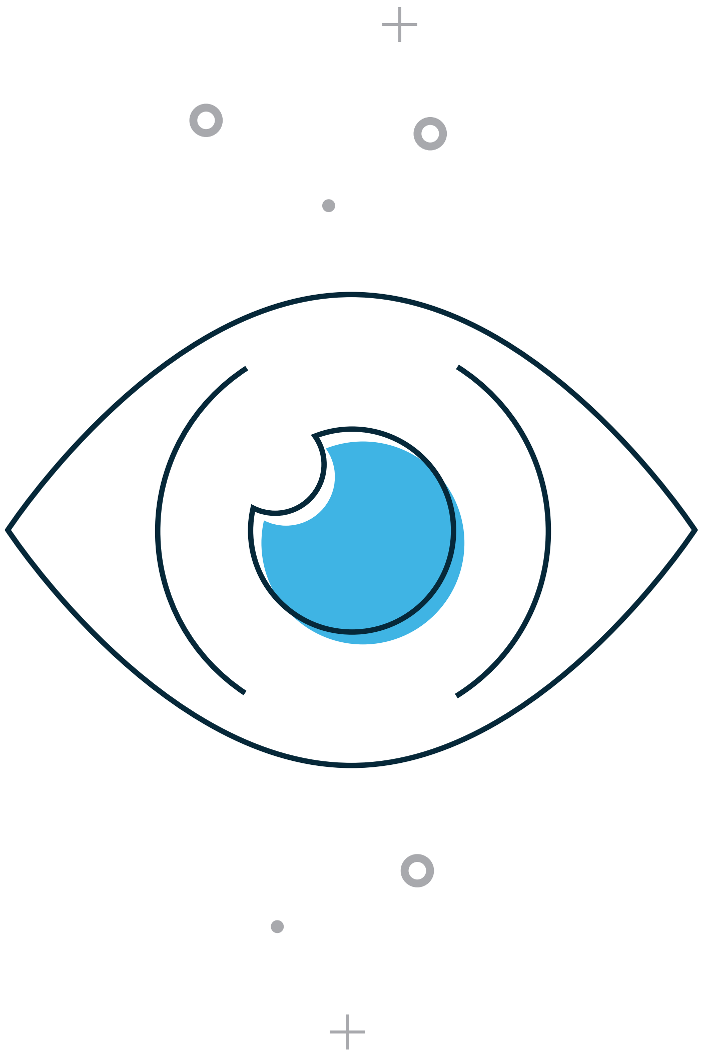
backupify

a datto company

The Complete Guide to Office 365 Security

Office 365 is the fastest growing offering in Microsoft's history, and customers are entrusting the platform to not just meet all of their productivity needs, but to secure and manage their business-critical information assets

Security in Office 365 is a constant effort to monitor, maintain, enhance, report, and verify. Microsoft wants you to know that your data inside Office 365 remains yours – they will never mine your data for advertising campaigns or access your data outside of the scope of delivering your organization with cloud productivity services. In fact, when you sign up to use Office 365 you will see a series of regulatory disclosures describing these governance measures.



Security in Office 365 is a constant effort to **monitor, maintain, enhance, report, and verify**.

Why should I read this guide?

Sure, there's a wealth of content available through various Microsoft websites and documentation, but it is often spread across multiple websites and formats, which can make it difficult to research all of these important topics. We believe there's value in presenting you with a single, comprehensive overview of the data security measures available within the Office 365 platform, giving you a solid baseline from which to build your information management strategies.

The layout of this eBook is very straight-forward: we provide a detailed outline of the various security, compliance, administrative and governance capabilities within Office 365, presenting each topic in a uniform way, as follows:

- A description of each control or data security feature
- An explanation of what it does and how to utilize it
- Directions on where you can go to find more information

We're confident that this guide will become an important resource for your Office 365 administrators and security personnel. Microsoft has invested heavily in easing concerns around data security in Office 365. The Office 365 Trust Center is an essential location to bookmark for detailed explanations on everything we cover here, and the site will keep you up to date with changes to any of the standards that Office 365 supports, the rollout of new security measures, or links to the many national and international certifications the platform receives.

The purpose of this guide is to give you an overview of this content – to help you better understand what Microsoft does to protect the integrity of your data and the quality of service provided by Office 365. The content here can be summarized into four categories: Security, Compliance, Administrative Controls, and Governance.

Microsoft makes continuous improvements to the security of the Office 365 platform, from port and perimeter scanning to regular auditing of operator/administrator activities and access.

Who should read this guide?

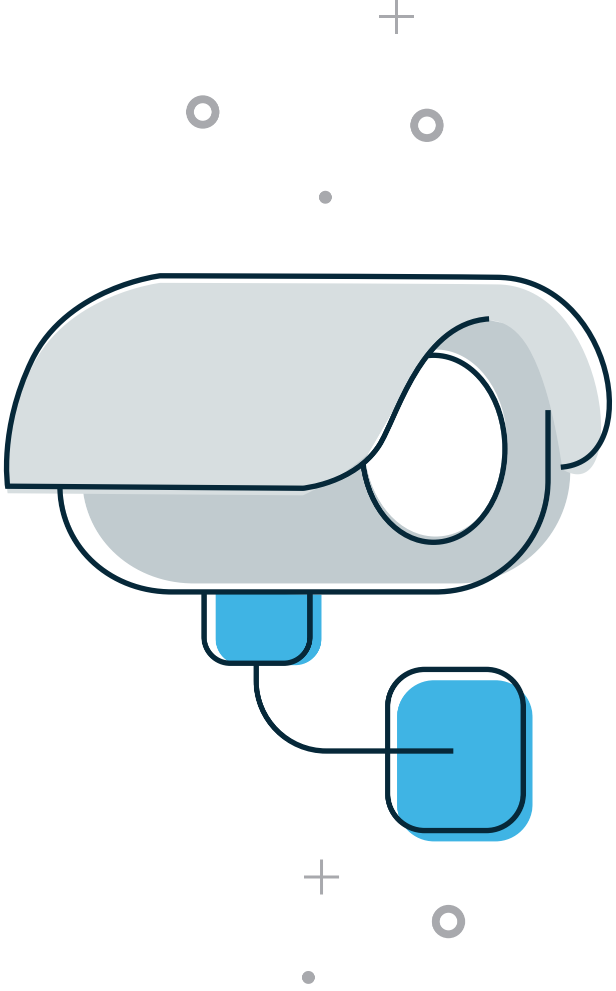
If you own any technical or support duties for the Office 365 platform for your organization, if you are a business stakeholder with concerns about the way in which Office 365 manages your data, or if you're just trying to learn more about the administrative options within the platform, then this guide is for you.

How does Office 365 provide security?

Now that we've provided an overview of what is covered within this eBook, let's go through each of the security, compliance, administrative and governance capabilities available within the Office 365 platform, beginning with data security.

At its core, Office 365 operates some of the most secure data centers in the world, adhering to Microsoft's internally-developed Security Development Lifecycle. Many of the best practices were developed over decades of Microsoft's own enterprise software development efforts, and since the late 1990's, this has included a host of online services.

The Office 365 platform provides enterprise-grade user and administrator controls, giving organizations the ability to manage and scale their environments with the assurance that all physical, logical, and data security layers adhere to industry best practices (or better). Microsoft makes continuous improvements to the security of the Office 365 platform, from port and perimeter scanning to regular auditing of operator/administrator activities and access. If you're interested on keeping up with what Microsoft is doing to keep your data secure, we recommend you bookmark the Office 365 Roadmap site and visit the site often for the latest updates.



Microsoft provides 24-hour security for all of their data center facilities, including multi-factor authentication for all systems, and biometric scanning for physical access.

PHYSICAL SECURITY. WHAT IS IT?

Controls access to systems and data. Microsoft provides 24-hour security for all of their data center facilities, including multi-factor authentication for all systems, and biometric scanning for physical access. All systems on the internal network are segregated from the external network.

In addition, because of role separation, even those employees with physical access to the systems are unable to identify the location of specific customer data. World-class data center procedures ensure that as hardware and systems are updated and optimized, faulty drives and equipment is demagnetized and destroyed. You can sleep soundly at night knowing that the equipment your data resides on is protected within some of the most secure data centers in the world.

Where can I find more information?

Video tutorial: How do we monitor and safeguard your data in Office 365?

Microsoft website: About Microsoft global data centers

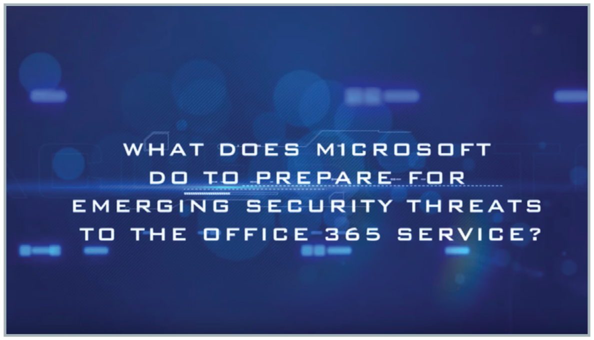
Video overview: Cybercrime: A story of vulnerability, deception, and security

LOGICAL SECURITY. WHAT IS IT?

Safeguards of software and platforms through authentication, passwords, permissions levels and other measures that ensure only the right people have access to your data. Microsoft gives full customer control over their content in the rare instances where Microsoft may need to access the data to resolve a conflict, called the Office 365 Customer Lockbox. Office 365 security provides proactive threat management, port and perimeter scanning, and tightly managed processes from an approved server whitelist, ensuring against malicious code and access.

Encryption at rest and in transit protects your data whether on our servers or in storage devices, or when being transmitted between you and Microsoft.

Where can I find more information:



WHAT DOES MICROSOFT DO TO PREPARE FOR EMERGING SECURITY THREATS TO THE OFFICE 365 SERVICE?

Where can I find more information?

Office blog: Announcing Customer Lockbox for Office 365

Video tutorial: From Inside the Cloud: Who has access to your data within Office 365?

Office support: Set your password expiration policy

DATA SECURITY. WHAT IS IT?

Protection of your data privacy and integrity from natural disaster, system corruption or hardware failure, and human malfeasance. Encryption at rest and in transit protects your data whether on our servers or in storage devices, or when being transmitted between you and Microsoft.

In addition to ongoing threat management, security monitoring, and detection and prevention of any system or data tampering, Office 365 also provides detailed service level agreements (SLAs) around disaster recovery and business continuity, helping meet all of your security requirements.

Where can I find more information?

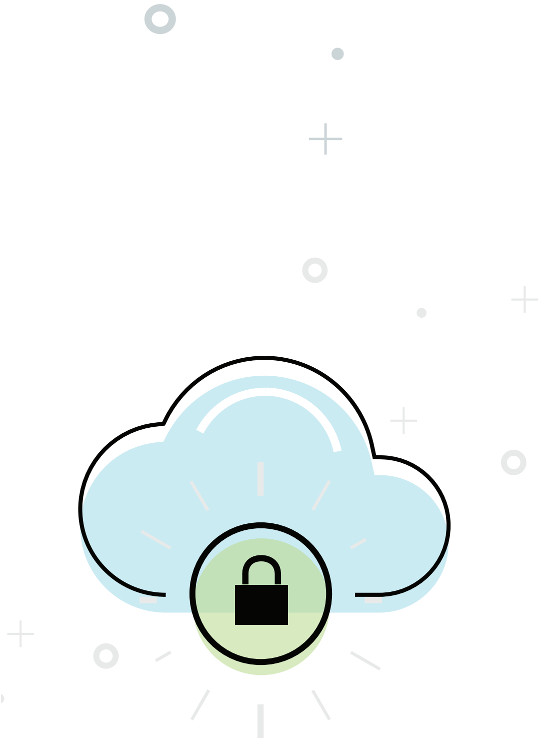
Video tutorial: What does Microsoft do to prepare for emerging security threats to Office 365?

Video tutorial: Explaining data security and your control in Office 365

Office support: Plan for Office 365 security and information capabilities

How does Office 365 manage compliance?

The Office 365 platform supports customers around the world with many different standards and regulations guiding the handling of information assets. As such, Microsoft is constantly adding to the list of compliance and security standards supported.



Another key principle of Office 365 trust is compliance. Commercial organizations have regulations and policies that they must comply with to operate businesses in various industries. These policies can be a mix of external regulatory requirements that vary depending on industry and geographical location of the organization and internal company-based policies.

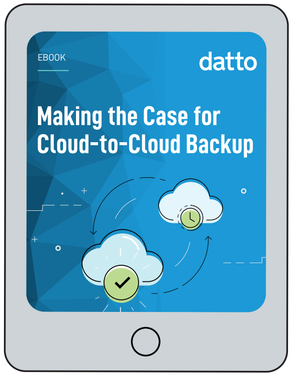
Office 365 provides built-in capabilities and customer controls to help customers meet both various industry regulations and internal compliance requirements, staying up-to-date with many of today's ever-evolving standards and regulations, giving customers greater confidence. To bolster this and to continue earning your confidence, Microsoft undergoes third-party audits by internationally recognized auditors as an independent validation that they comply with all policies and procedures for security, compliance and privacy.

Key aspects of built-in compliance capabilities include third-party audits verifying that Office 365 meets many key world-class industry standards and certifications. Office 365 utilizes a control framework that employs a strategic approach of implementing extensive standard controls that in turn, satisfy various industry regulations. Office 365 supports over 600 controls that enable Microsoft to meet complex standards and offer contracts to customers in regulated industries or geographies, like ISO 27001, the EU Model Clauses, HIPAA Business Associate Agreements, and FISMA/FedRAMP.

In addition, Microsoft employs a comprehensive Data Processing Agreement to address privacy and security concerns around customer data, helping customers comply with local regulations. Read more in Microsoft's Regulatory Compliance FAQ. To give customers the most control over compliance in Office 365, Microsoft provides three useful services.

DLP is a strategy and tools to help administrators **control the flow of sensitive or critical information** outside of the corporate network.

You may also be interested in:



Making The Case For Cloud-to-Cloud Backup

DOWNLOAD NOW

DATA LOSS PREVENTION (DLP). WHAT IS IT?

DLP is a strategy and tools to help administrators control the flow of sensitive or critical information outside of the corporate network.

What does it help me do?

DLP enables administrators to configure policies based on your organization's compliance needs to help reduce the chance that financial information, personally identifiable information (PII), or other key intellectual property data might be inadvertently released. DLP policy tips place notifications directly into your users' email in order to alert them of a potential risk prior to sending an email. These notifications can also act as an educational tool for employees on your corporate compliance policies.

Where can I find more information?

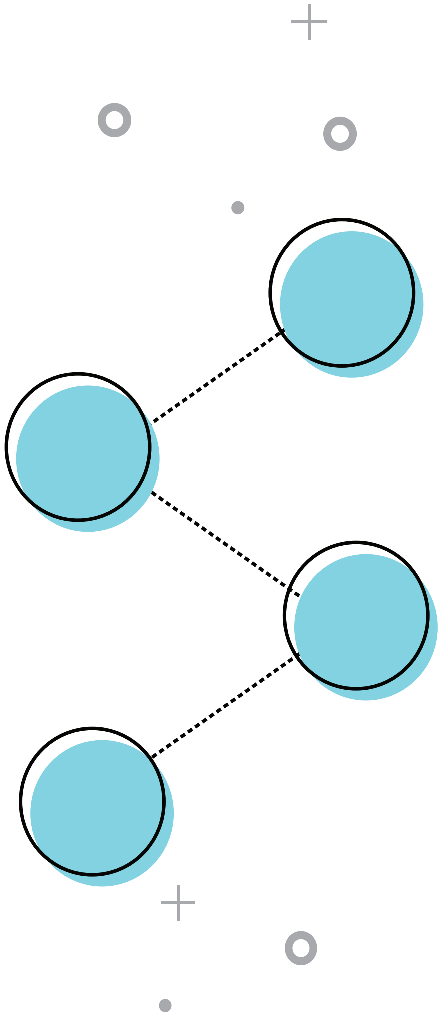
Video tutorial: Data Loss Prevention (DLP) in Microsoft Office 365

Office blog: Office 365 compliance controls: Data Loss Prevention

TechNet article: Technical overview of Data Loss Prevention

EDISCOVERY CENTER. WHAT IS IT?

Electronic Discovery, or eDiscovery, is the process through which electronic records are sought, searched, located, and secured with the intent of using it for legal matters.



Audit logging and reporting is available to **track anything** from Administrator actions to document access and deletion.

What does it help me do?

This capability on Office 365 allows you to search for content across SharePoint Online sites, Exchange Online mailboxes, OneDrive for Business accounts, or across all of them. The eDiscovery center allows you to create “cases” which will provide a collaborative space for you to gather key components required for your evidentiary requirements. With eDiscovery in Office 365, you are able to discover any of the content stored in your environment, including archived emails.

Messaging records management (MRM) is the technology at the heart of data retention in Office 365. The configuration options allow you to apply records management policies to both Exchange Online and SharePoint content in order to specify content that should be retained and clean-up content that is no longer needed. Audit logging and reporting is available to track anything from Administrator actions to document access and deletion. There are many logging and reporting options that can be configured to fit your needs. Combining email archiving and eDiscovery can make life easier for both users and administrators by reducing the amount of inbox organizing to be done, and automatically applying data retention policies based on the type of content being used. The added benefit of email archiving is that your users are no longer storing their emails in independent archive files on local machines that may be outside the reach of your IT team.

Where can I find more information?

Video tutorial: Introducing Office 365 auditing and investigation workflow with eDiscovery

Office support: eDiscovery in Office 365

Office support: Assign eDiscovery permissions to OneDrive for Business sites

Microsoft is constantly reviewing evolving and changing industry standards to ensure that Office 365 compliance framework is current.

Where can I find more information:

How does Office 365 continuously meet your compliance needs?
From Inside The Cloud

CONTINUOUS COMPLIANCE SERVICES. WHAT IS IT?

A framework of processes and over controls that Office 365 uses to proactively monitor and manage the platform. With over 1,000 controls in place, and more being added every month, Microsoft is continually reviewing its own data handling policies and procedures to ensure that evolving customer and industry standards are being upheld.

What does it help me do?

Stay compliant. As new customers are added to the service, each customer agreement details the privacy, security, and data handling processes necessary for you to comply with local data regulations. Microsoft is constantly reviewing evolving and changing industry standards to ensure that Office 365 compliance framework is current.

Additionally, legal hold and eDiscovery capabilities are built into the system to help you find, preserve, analyze, and package electronic content for legal request or investigation, and Data Loss Prevention to help you identify, monitor, and protect sensitive information.

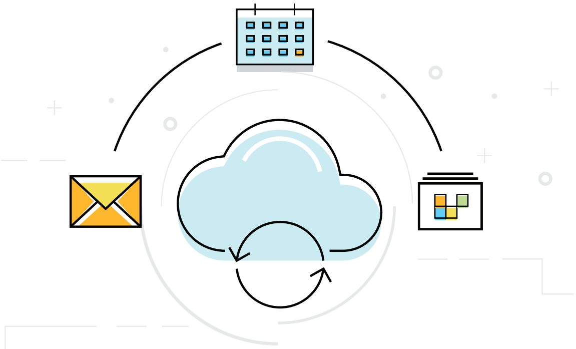
Where can I find more information?

Video tutorial: How does Office 365 continuously meet your compliance needs?

Office Blog: From inside the cloud: How does Office 365 continuously meet your compliance needs?

International Compliance Standards and Certifications

Microsoft recognizes that customers around the world are subject to various laws and regulations. The legal requirements and standards in one country or region may not be applicable in other regions.



As Microsoft expands into more regions, countries, and economic zones, the company is constantly expanding their services and capabilities to enable compliance across a wide range of regulations and privacy mandates to meet their customer needs.

The list below provides an overview of some of the leading compliance standards and certifications provides through the Office 365 platform. However, it is ultimately up to the customer to determine whether these standards satisfy your regulatory requirements.

- Health Insurance Portability and Accountability Act (HIPAA)
- Data processing agreements (DPAs)
- Federal Information Security Management Act (FISMA)
- Federal Risk and Authorization Program (FedRAMP)
- ISO 27001
- European Union (EU) Model Clauses
- U.S.–EU Safe Harbor framework
- Family Educational Rights and Privacy Act (FERPA)
- Statement on Standards for Attestation Engagements No. 16 (SSAE 16)
- Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)
- Gramm–Leach–Bliley Act (GLB)

Customers have the ability to **identify, monitor, and protect their sensitive data** using Data Loss Prevention (DLP) capabilities.

Where can I find more information?

Microsoft website: Security, Audits, and Certifications

Video tutorial: Microsoft Office 365 Security, Privacy, and Compliance Overview

Video tutorial: Microsoft Office 365 Security, Privacy, and Compliance DeepDive

What are the Office 365 administrative controls?

While Office 365 is a service that is managed by Microsoft, there are still many tools and controls within the platform whereby customers can manage security, compliance, and ongoing platform governance to meet the more granular controls of the platform. Customers have the ability to identify, monitor, and protect their sensitive data using Data Loss Prevention (DLP) capabilities, and can establish custom rules around archiving, auditing, and eDiscovery across the different workloads.

RIGHTS MANAGEMENT SERVICES. WHAT IS IT?

Enables a user to encrypt information using 128-bit AES and use policies on email or documents so the content is appropriately used by specified people. Prevents file-level access without the right user credentials.

What does it help me do?

Allows individuals and administrators to specify access permissions to documents, workbooks, and presentations. This helps you prevent sensitive information from being printed, forwarded, or copied by unauthorized people by applying intelligent policies

Where can I get more information?

TechNet article: What is Azure Rights Management?

SharePoint Online, a key component service of Office 365 that provides collaboration functionality **has a number of privacy controls**.

MULTI-FACTOR AUTHENTICATION. WHAT IS IT?

Simply put, it's a security measure that requires more than one method of authentication when accessing a system, usually from independent categories of credentials to verify a user's identity.

What does it help me do?

It enhances security in a multi-device, mobile, and cloud-centric world by using a second factor, such as a password or a personal identification number (PIN), in addition to the primary factor, which is identity. In short, it helps you to better understand who is accessing your system.

Where can I find more information?

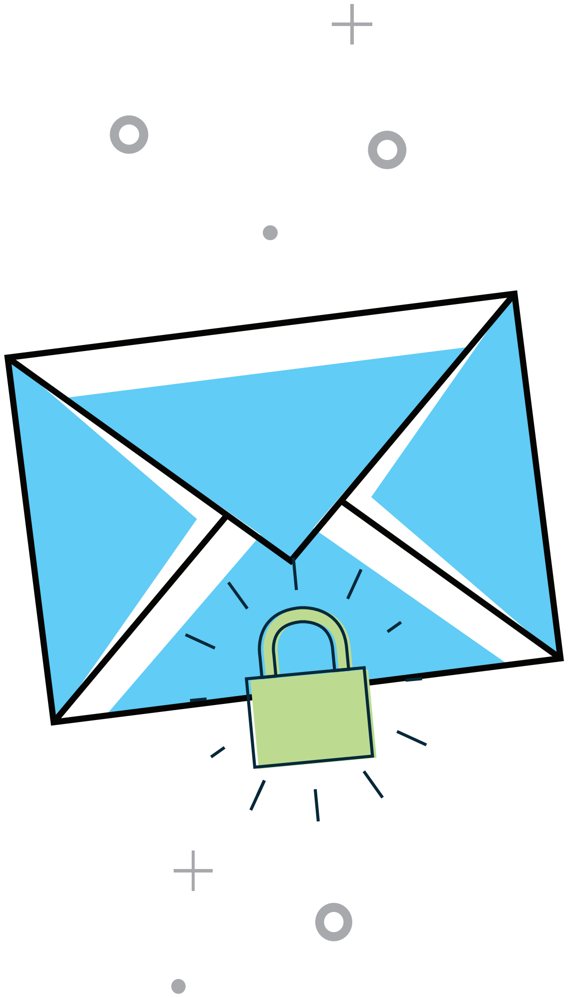
Office support: Set up multi-factor authentication for Office 365

PRIVACY CONTROLS FOR SITES, LIBRARIES AND FOLDERS. WHAT IS IT?

Methods and APIs, primarily the Office 365 Management Activity API, that give organizations greater visibility into actions taken on content, and the ability to manage access.

What does it help me do?

SharePoint Online, a key component service of Office 365 that provides collaboration functionality has a number of privacy controls. These privacy controls allow you to review a wide range of logs on user interactions with content so you can create better policies for ongoing monitoring, analysis, and data visualization. Besides greater visibility and permissions management around what is happened to your content, you can use these signals as input in areas such as your security incident and event management (SIEM) system.



Secure/Multipurpose Internet Mail Extension, or S/MIME, is a widely-accepted standard for public key encryption and MIME data (digital signatures), and it **provides secure certificate-based email access**.

Where can I find more information?

Office support: Control user access with permissions

Office blog: Enhancing transparency and control for Office 365 customers

S/MIME. WHAT IS IT?

Secure/Multipurpose Internet Mail Extension, or S/MIME, is a widely-accepted standard for public key encryption and MIME data (digital signatures), and it provides secure certificate-based email access.

What does it help me do?

It enables encryption of your email messages and allows for the originator to digitally sign the message to protect the integrity and origin of the message.

Where can I find more information?

Office support: S/MIME encryption now in Office 365

Video tutorial: Encryption in Microsoft Office 365

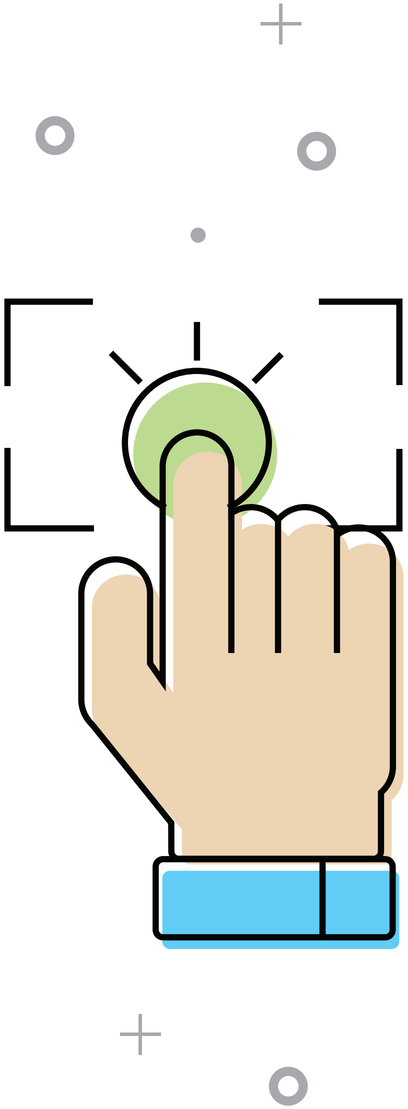
PRIVACY CONTROLS FOR COMMUNICATIONS. WHAT IS IT?

In Skype for Business (Lync), another key component of the Office 365 platform that provides real-time communication, there are various administrator level controls as well as user level controls to enable or block communication with external users and organizations.

What does it help me do?

Allows you to control the level of visibility of your organization presence awareness inside and outside of your company, ensuring privacy of your content and communication.

Encryption helps you to protect sensitive information and data from leaving your system, based on policy rules and compliance standards that you control.



Where can I find more information?

Office Support: Control access to your presence information in Skype for Business

OFFICE 365 MESSAGE ENCRYPTION. WHAT IS IT?

Allows you to send and receive encrypted email as easily as normal email. What does it help me do? Encryption helps you to protect sensitive information and data from leaving your system, based on policy rules and compliance standards that you control. Using Office 365 message encryption, you avoid the cost of other third-party infrastructure, and eliminate the need for certificates, using the recipient's own email as the public key.

Where can I find more information?

TechNet article: Encryption in Office 365

TechNet article: Office 365 Message Encryption FAQ

Video tutorial: What controls do we provide to protect your data in transit in Office 365?

ROLE BASED ACCESS CONTROL. WHAT IS IT?

This feature allows you to enable access to authorized users based on role assignment, role authorization, and permission authorization.

What does it help me do?

It helps you to delegate administrative controls across your organization, if needed. Some organizations may have administrators or experts in SharePoint who are not Exchange or communications admins, and therefore just need admin permissions to a subset of the Office 365 environment. This features gives you the ability to segment administration by roles.

It is the process of **identifying individuals** in a system and **controlling the access you give them** to resources within that system.

Where can I find more information?

Office support: Assigning admin roles in Office 365

TechNet article: Permissions in Exchange Online

EXCHANGE ONLINE PROTECTION. WHAT IS IT?

A hosted email security service within Office 365 that looks for and removes malware, spam, and computer viruses.

What does it help me do?

These features allows you to manage your company's anti-virus and antispam settings from within the Office 365 administration console, with near real-time reporting, policy-based filtering, and message tracing so you can ensure your security and compliance requirements are being actively met.

Where can I find more information?

TechNet article: Exchange Online Protection details

TechNet article: EOP General FAQ

IDENTITY MANAGEMENT. WHAT IS IT?

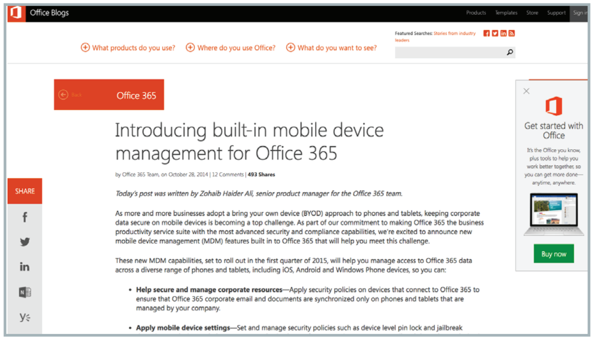
It is the process of identifying individuals in a system and controlling the access you give them to resources within that system.

What does it help me do?

It provides you with various options for identity management, such as cloud-based identity, identities mastered on-premises with secure token based authentication, or federated identities (also known as Single Sign-On, or SSO) to integrate into the Office 365 identity management system based on the security needs of your organization.

A cohesive, holistic and practical approach to governance is required for platforms like Office 365, where **the reach is extensive**.

Where can I find more information:


Office Blogs
Products
Templates
Store
Support
Sign in
Featured Searches: Stories from industry leaders
What products do you use?
Where do you use Office?
What do you want to see?
Back
Office 365
SHARE
Get started with Office
It's the Office you know, plus tools to help you work better together, so you can get more done—anytime, anywhere.
Buy now

Introducing built-in mobile device management for Office 365

by Office 365 Team, on October 28, 2014 | 12 Comments | **493 Shares**

Today's post was written by Zohaib Haider Ali, senior product manager for the Office 365 team.

As more and more businesses adopt a bring your own device (BYOD) approach to phones and tablets, keeping corporate data secure on mobile devices is becoming a top challenge. As part of our commitment to making Office 365 the business productivity service suite with the most advanced security and compliance capabilities, we're excited to announce new mobile device management (MDM) features built in to Office 365 that will help you meet this challenge.

These new MDM capabilities, set to roll out in the first quarter of 2015, will help you manage access to Office 365 data across a diverse range of phones and tablets, including iOS, Android and Windows Phone devices, so you can:

- **Help secure and manage corporate resources**—Apply security policies on devices that connect to Office 365 to ensure that Office 365 corporate email and documents are synchronized only on phones and tablets that are managed by your company.
- **Apply mobile device settings**—Set and manage security policies such as device level pin lock and jailbreak

Where can I find more information?

Office Support: Understanding Office 365 identity and Azure Active Directory

TechNet article: User Account Management

Microsoft Virtual Academy: Office 365 Identity Management

MOBILE DEVICE MANAGEMENT. WHAT IS IT?

Tools that help you manage access to your Office 365 environment through a diverse range of phones and tablets, regardless of operating system (iOS, Android, or Windows).

What does it help me do?

These features will help you to better manage security policies across the devices that connect to your Office 365 environment, ensuring your security, compliance, and governance policies and procedures extend to every access point for your environment.

Where can I find more information?

Office blog: Introducing built-in mobile device management for Office 365

What are the Office 365 governance best practices?

While governance is important, the governance of your Office 365 environment has less to do with the technology and more to do with the practices and procedures you put in place to administrate your information assets. Office 365 provides the tools and capabilities you require to develop sound governance standards, and meet your internal and industry-defined governance requirements. A cohesive, holistic and practical approach to governance is required for platforms like Office 365, where the reach is extensive. With the simplification of development practices in the move to a cloud environment, you now are able to more easily shift resources to concentrate on process and governance where doing so was difficult in the past.

Thanks to this shift, there have been some successful overhauls in how we view governance practices and where it is important to focus our time.

When approaching governance of your Office 365 environment, is it important to holistically review your strategy and tactical plans to execute that strategy. Consider each of these four areas:

Foundation

Set the ground rules for how your platform operates and what information technology security parameters it must operate in to remain compliant. Address the structure and support your organization will provide to keep your environment in working order.

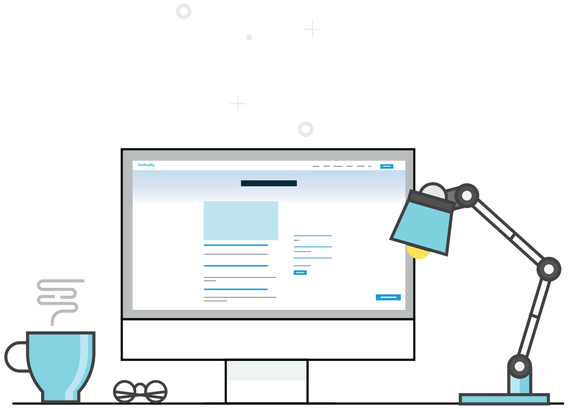
Administration

Placing an emphasis on teamwork between your administrative teams will streamline issue resolution and promote the nature of the platform's collaboration core. As with any team environment, definition of roles and responsibilities will be key to success. Also be sure to set a clear vision for the future in order for your administrators to manage your environment with the future in mind.

Communication

One of the clearest forms of collaboration is through communication. Be very straightforward and open when it comes to governance of your new platform. Gone are the days of running everything from a dark closet behind the curtain. Bring your voice and vision to the forefront and afford your employees the ability to have a voice -- truly productive collaboration is sure to follow!

It's important to remember that **your data needs protection** beyond what Office 365's security settings can offer.



Adoption

Focus some resources on user engagement, awareness and recognition in order to ensure adoption of new features. Placing some power and authority into the hands of your users will encourage them to explore and become personally invested in the technology and how it can benefit their day to day work.

There are many great online resources available with guidance on how to approach governance in Microsoft's cloud first/mobile first world. While Office 365 provides many of the tools and features you need to maintain your governance standards, many organizations elect to invest in third-party solutions to help them better manage their governance activities. Start your planning by understanding your governance goals and priorities, and look to the Office 365 community for advice on where to begin.

TechNet article: Governance Planning in Sharepoint Server 2016

CONCLUSION

With a platform as comprehensive as Office 365, there are many moving parts. While the core features are fairly intuitive and easy to deploy for a small organization, it quickly gets complex when the number of end users increases or your security, compliance, and governance requirements are well-defined.

It's important to remember that your data needs protection beyond what Office 365's security settings can offer. Even with all of Office 365's security settings enable, the safety of your data depends heavily on other people. Between Microsoft data center employees and your own users, data remains in a constant state of risk. Human error is the leading cause of data loss in the cloud, so having a secure second copy of that data is a must. A third party backup solution like, Backupify, keeps data secure and easily recoverable at all times. To learn more, visit www.backupify.com.