Microsoft

Exposing the top 4 myths of cloud security

Get started with Office 365

Introduction

With security breaches and their impact on businesses frequently in the headlines, the need for stringent security measures has never been more evident. A third of U.S. businesses report having had a breach of customer information, and the costs can be significant. One in five organizations have lost customers due to a cyberattack and nearly 30% have lost revenue, with the average cost of single data breath reported at $4 million.

However, 74% of IT leaders say security concerns are holding back their move to the cloud. Are you one of them?

While reservations about the security capabilities of cloud environments concerns used to be a reason for companies to delay migration, investment by Microsoft into new security tools and resources are challenging those misperceptions and providing compelling reasons to make the move.

Get the real story. Here are four common myths about cloud security, and some facts about the Microsoft cloud.

Myth 1

Microsoft employees will have unfettered access to my data if I move to the cloud.

Fact: With Microsoft, your data is always yours.

Microsoft's multi-tenant architecture sets the industry standards for security, confidentiality, and privacy. Multiple layers of protection prevent access to information from other tenants. To deliver an enterprise-grade hyper scale cloud service, Microsoft operations are automated with self-healing mechanisms. In addition, Microsoft engineers don't have standing access to customer data and there is a process in place to grant access when it is required for service operations.

Myth 2

We don't need to worry because we haven't had a problem so far.

Fact: Hope is not a strategy. Your approach to security needs to assume there will be active —and successful— attempts to breach your firewall.

A third of US companies have experienced a data breach.1 It's no longer a question of if, but when an incident will occur. Businesses need security systems and solutions that provide maximum defense against security breaches, as well as an agile, effective response when a breach does occur.

Myth 3

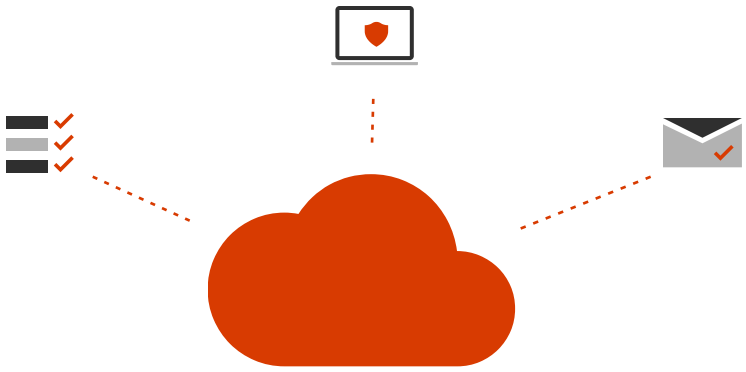
Moving to the cloud makes compliance issues, such as categorizing data and reporting, more difficult.

Fact: Microsoft integrates compliance requirements and features throughout cloud services and datacenters. The Microsoft cloud can also help organizations meet xyz percent of their requirements.

Security and compliance are inextricable. Regulatory requirements are constantly evolving. That's why Microsoft has a compliance team dedicated to keeping up-to-date on any changes. We work closely with businesses and regulators to ensure our solutions comply with the General Data Protection Regulation (GDPR) and other applicable regulations, whether they're global, regional, or associated with a specific industry.

Office 365 have net late sundis deliquis voluptatem re, si as rem in prestibus magnatint volum fugia dolutatem excerum quo magnietur aliciis

Our data processing agreements detail our protocols and policies regarding customer data, which is helpful with regard to meeting documentation requirements for privacy regulations. **Office 365** includes access to features and tools like Compliance Manager and Content Search to assess and manage your risk, as well as Advanced Data Governance and Data Loss Prevention to help classify, protect, and monitor your data.



Myth 4

My company can always spends enough on security to keep our systems protected.

Fact: It's not only how much you spend, it's how smart. Microsoft investments in research, development, and services provide enterprise-grade security even for companies without enterprise-size budgets.

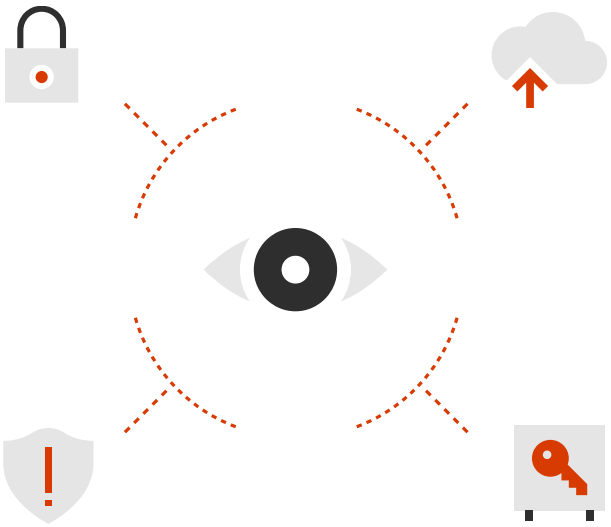
Increasingly complex attack methods have made creating adequate defenses more difficult. Resources need to be allocated to protect against multiple vulnerabilities (e.g., identities, devices, infrastructure) and types of attacks (e.g., phishing, zero-day, etc.). While threats continue to grow in frequency and sophistication, companies still resort to costly point solutions to address specific threats rather a systemic approach. Managing exponential growth in controls can be a costly nightmare.

With Office 365, you gain a trusted partner in Microsoft, who provides up-to-date tools and capabilities to help keep your data secure.

And when your infrastructure is on-premises, you are solely responsible for updating and maintaining your systems to keep them protected, as well as responding effectively when a breach occurs.

What does enterprise-grade security mean with regard to **Office 365**? It means providing intelligent security across five key dimensions: identity and access management, information protection, threat protection, security management, and compliance.

In addition, Microsoft patches over one billion windows devices, scans 400 billion emails for malware, and processes 450 billion authentications every month. By analyzing the resulting data, Microsoft can provide unique insights into emerging threats.



Office 365 is hosted in geo-redundant datacenters protected by motion sensors, video surveillance, and other measures 24 hours a day.

Multiple authentication procedures, including badge identification and biometric scanners, protect our centers against unauthorized entry.

With an on-premises solution, security protection procedures for hardware, operating systems and applications are manual and prone to human error. In the cloud, that process can be automated. Automating security procedures allows Microsoft to address security threats on a large scale and reduce the risk of data breach from employees.

Is your business prepared to dedicate the funds and resources it now takes to maintain an adequate security posture? Does that even make sense for your business? Do you have the expertise to keep pace with constantly evolving security threats? When you move to **Office 365** you resolve these questions, and more, by sharing burdens such as endpoint protection and identity and access management with Microsoft as a trusted partner, while completely shifting the burden of application- and network-level controls, host infrastructure, and physical security.

Office 365: your secure entry into the cloud

If you're looking to take advantage of the cost savings and security advancements available in the cloud, **Office 365** is a great place to start. Here's a look at some of the security capabilities of **Office 365**.

Secure Score

Microsoft Secure Score helps you understand your current **Office 365** security configuration and suggests you how implementing additional controls can help increase security and reduce risk. It is based on how many security configurations you have partially or fully adopted compared to all security configuration you have available. You can also track your score over time using the Score Analyzer or take action to increase your score.

Encryption

When you move to **Office 365** your data is encrypted by default—both at rest and in transit—through multiple encryption technologies, including Bitlocker, service encryption, and transport layer security (TLS). Additional controls are provided for more granular protection, such as **Office 365** Message Encryption. For added compliance and control, there are a variety of encryption key options such as Customer Key, or bring your own key (BYOK) and hold your own key (HYOK) with Azure Information Protection.

Redundancy

Microsoft's distributed data centers mean that if one location experiences problems, your instances can be redirected to a different center with little to no downtime.

Manage user logins

Office 365 uses Azure Active Directory (Azure AD) to manage user logons, authentication and federation services. These services can be used with an on-premises Azure AD deployment, or to support a third-party identity provider. Administrators can manage user accounts with a choice of three identity models: cloud, synchronized, or federated.

Security incident response

With **Office 365**, you are in effect shifting a certain amount of security risk and responsibility to Microsoft. This is yet another reason Microsoft is so committed to security. Our incident response teams work around the clock to monitor, detect, and respond to security incidents and protect our cloud services—and your data.

Data governance

Implement a comprehensive data governance strategy including retention, disposition, and supervision to make sure you are keeping what you need and getting rid of the rest. Use labels to detect your sensitive data and then use labels to ensure your data is retained, protected and disposed of according to your policies and requirements.

eDiscovery

Respond to internal investigations, regulatory requests or prepare for litigation with in place eDiscovery tools. Create a case, implements legal holds and refine the content relevant to your investigation. Reduce the overall content required for review with advanced analysis including themes, de-duplication of threads and additional analysis designed to reduce time and costs of review.

Protect eMail from security threats

Office 365's Exchange Online Protection helps keep email communication free from spam, viruses, and malware.

Security for mobile devices

Office 365 uses Intune mobile-device management to ensure that the information stored on Windows, Apple or Android mobile devices remains secure.

Tracking threats

Office 365 Threat Intelligence provides an interactive dashboard for IT administrators to analyze the prevalence and severity of threats in near real-time, real-time and customizable threat alert notifications, remediation for suspicious content, and expansion of the Management API to include threat details and enabling integration with SIEM solutions. Available with **Office 365** E5 or as an add-on to your subscription.

Cloud App Security

Use **Office 365** Cloud App Security to protect access to your data by identifying abnormal usage, security incidents, shadow IT, and other high-risk scenarios. Cloud App Security features the Cloud Discovery Dashboard, which shows information about cloud app usage in your organization, including users, traffic, and transactions. Available in **Office 365** E5 or as an add-on to your **Office 365** subscription.

Multi-Factor Authentication

Managed from the **Office 365** admin center, Multi-Factor Authentication provides an extra layer of security. Administrators have a choice of several secondary authentication factors, including mobile apps, phone calls, SMS or application passwords for non-browser clients.

Advanced Threat Protection

Office 365's Advanced Threat Protection (ATP) helps defend against unknown virus and malware attacks with robust zero-day protection, including features that guard against malicious links in real time. ATP provides rich reporting and URL trace capabilities to provide administrators with security insights specific to your organization. Available with **Office 365** E5 or as an add-on to your subscription.

Compliance Manager

Gauge your compliance standing in real-time with the Compliance Manager tool . Understand what Microsoft implemented controls are in place, and where you are with your customer managed controls as related to specific regulations that are relevant to your organization.

Data Loss Prevention

Detect, protect, and monitor sensitive data with **Office 365** Data Loss Prevention across Exchange Online, OneDrive for Business, and SharePoint Online.

FastTrack migration support

In addition to modern security features, when you move to **Office 365** your migration is includes support by FastTrack, the Microsoft success service to help you evaluate your environment, plan your rollout, and drive adoption.

Make the move

Want to learn more about making the move to **Office 365**? Compare **Office 365** to legacy Office apps in:

"What you're missing with your legacy Office Apps vs. O365."

More resources:

Sign up for an E3 trial now

Sign up for the Office 365 Enterprise E5 trial

Office 365 Trust Center

Office 365 security whitepaper