Microsoft Security Guidance for Nonprofits

Planning and implementation guidance for fast-moving organizations that have an increased threat profile

This topic is 1 of 12 in a series 1 2 3 4 5 6 7 8 9 10 11 12

Introduction

Nonprofits around the world are dynamic organizations working in many areas who face security risks that rise with the impact they can achieve. They face challenges from sophisticated actors that can deploy significant resources to breach an organization. This solution demonstrates how to build an environment with essential cloud services. It includes prescriptive security design for protecting identities, email, and access from mobile devices.

This solution includes capabilities across Office 365, Enterprise Mobility + Security (EMS) suite, and Azure Platform as a Service (PaaS). EMS makes it possible to integrate other cloud services and use the same identity provider, secure access capabilities, and monitoring solutions across your entire environment.

This guidance includes only cloud services but you can also use these recommendations with a hybrid on-premises environment.

Core cloud capabilities in this solution

Office 365 enterprise capabilities

Secure email and calendars	Business-class email protected with Exchange Online Protection and Office 365 Advanced Threat Protection.
Office suite and Office Online	The latest Office apps for your PC and Mac, including updates to protect your environment. Create and edit documents from a browser.
Office on PCs, tablets, and phones	Fully installed Office experience across PCs, Macs, Windows tablets, iPad® and Android™ tablets, and most mobile devices.
OneDrive for Business	1 TB of personal cloud storage that can be accessed from anywhere and syncs with a PC/Mac for offline access. Easily share documents with others and control who can see and edit each file.
SharePoint Online	Communications sites to keep your organization up to date. Team sites and document libraries protected at the appropriate level for the sensitivity of your data and projects.
Online meetings	Host online meetings with audio, HD video, and web conferencing over the Internet. Join meetings with a single touch or click from the smartphone, tablet, or PC of your choice.
Meeting broadcast	Broadcast Skype for Business meetings on the Internet for up to 10,000 people, who can attend in a browser on nearly any device. Meetings include real-time polling and sentiment tracking.

Azure PaaS analytics environment

Azure PaaS Analytics	Build and secure an analytics environment in Azure using SQL Data Warehouse and Azure Data Lake. Protect access to this environment using the same capabilities as Office 365.

Enterprise Mobility + Security (EMS) suite

Simplified identity management	Centrally manage single sign-on across devices and all of your Software as a Service (SaaS) and cloud applications.
Multi-factor authentication	Strengthen sign-in authentication with verification options, including phone calls, text messages, or mobile app notifications.
Conditional access	Define policies that provide contextual controls at the user, location, device, and app levels to allow, block, or challenge user access.
Risk-based conditional access	Protect apps and critical data in real time using machine learning and the Microsoft Intelligent Security Graph to block access when risk is detected.
Advanced security reporting	Monitor suspicious activity with reporting, auditing, and alerts, and mitigate potential security issues using focused recommendations.
Mobile application management	Publish, configure, and update mobile apps on enrolled and unenrolled devices, and secure or remove app-associated corporate data.
Mobile device management	Enroll corporate and personal devices to provision settings, enforce compliance, and protect your corporate data.
Persistent data protection	Encrypt sensitive data and define usage rights for persistent protection regardless of where data is stored or shared.
Microsoft Cloud App Security	Gain visibility, control, and protection for your cloud-based apps Identify threats, abnormal usage, and other cloud security issues.

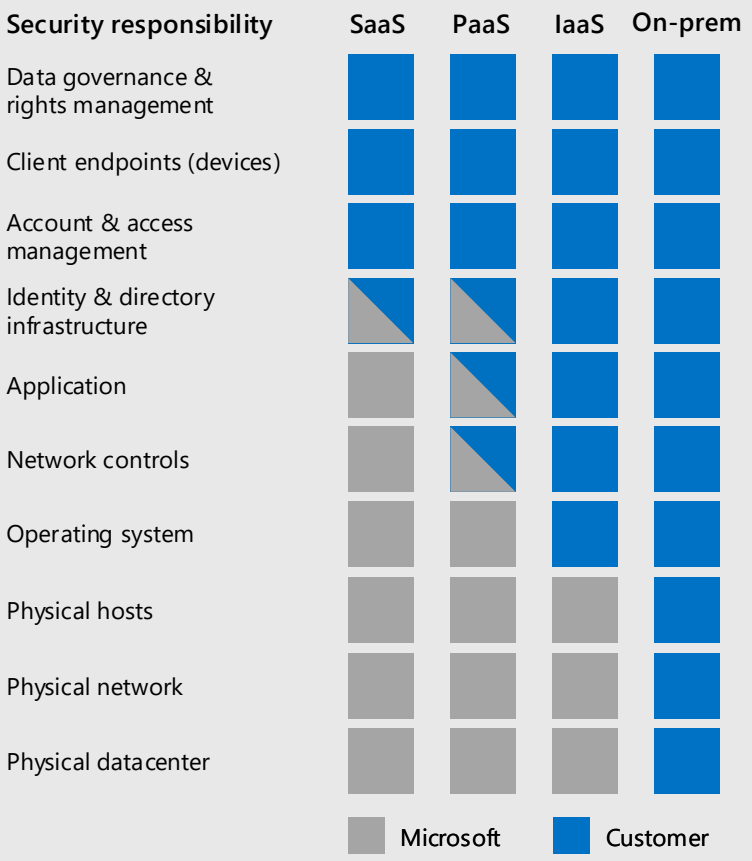
Reduce your security responsibility

By using Microsoft cloud services, you greatly reduce the attack surface you are responsible for. This solution shows you how to configure the controls that are provided for you to secure your data, devices, and identities with Office 365 (SaaS). The same approach can be used with other cloud services.

"Identity & directory infrastructure" refers to integration with on-premises directories. If you're using cloud-only accounts, this doesn't apply to you. The guidance in this solution is designed for cloud-only environments, but can also be used with hybrid environments with on-premises directories.

When you use Office 365 and EMS, you don't have responsibility for securing these layers. By using Microsoft cloud services, you greatly reduce the amount of work required to keep your environment secure. Decades of engineering experience has enabled Microsoft to develop leading-edge best practices in the design and management of online services. Through industry-leading security practices and unmatched experience running some of the largest online services around the globe, Microsoft delivers enterprise cloud services you can trust.

For more information, see Microsoft Cloud Security for Legal and Compliance Professionals



See topics 2-12 for more information and resources.

November 2017

Microsoft

Common attacks and Microsoft capabilities that protect your organization

Capabilities with blue text are included in this guidance.

Identity-based attacks

Begin attack

Phishing

Attacker targets employees by email or other unsafe links or websites.

Spear-phishing

Attacker uses information specifically about a user to construct a more plausible phishing attack.

Brute-force attack

Attacker tries a large list of possible passwords for a given account or set of accounts.

Other similar attacks: Watering hole attacks, leaked passwords.

Any employee clicks on a link and enters their credentials.

Exchange Online Protection blocks malicious hyperlinks in a message.

Office 365 Advanced Threat Protection protects against links in mail and files that are redirected to unsafe sites. Protection continues dynamically after mail is delivered.

Windows Defender SmartScreen checks sites against a dynamic list of reported phishing sites and warns users.

Weak passwords are systematically identified.

Azure AD password protections enforce minimum requirements for passwords, dynamically ban commonly used passwords, and force reset of leaked passwords.

Azure AD Smart Account Lockout temporarily locks out accounts with high-risk login activity.

For on-premises networks, Advanced Threat Analytics detects brute-force activity targeted to the domain.

Enter

Attacker uses stolen credentials to gain access to the user's mail and files.

Multi-factor authentication prevents password-only access to cloud services, including Exchange Online mailboxes and OneDrive for Business files.

Azure AD conditional access rules block access from unmanaged PCs.

Azure AD Smart Account Lockout temporarily locks out accounts with high-risk login activity.

Risk-based conditional access protect apps and critical data in real time using machine learning and the Microsoft Intelligent Security Graph to block access when risk is detected.

Traverse

Attacker moves laterally, gaining access to cloud services and resources in the environment.

Azure AD conditional access rules can protect all SaaS apps in your environment with multi-factor authentication and other protections.

Cloud App Security detects and alerts on anomalous activity for all SaaS apps in your environment, including activity originating from new and infrequent locations, suspicious locations, new and untrusted devices, and risky IP addresses.

Securing Privileged Access Roadmap is guidance to mitigate lateral traversal and credential theft techniques for your on-premises and hybrid cloud environments.

For on-premises networks, Advanced Threat Analytics identifies abnormal activity by using behavioral analytics and leveraging Machine Learning.

Exfiltrate data

Attacker removes data from the environment.

Cloud App Security detects and alerts on anomalous activity, such as download activity, and can suspend user accounts.

Intune Mobile Application Management rules prevents business data from leaving approved business apps on mobile devices.

Windows Information Protection (WIP) protects business content on devices with file level encryption that helps prevent accidental data leaks to non-business documents, unauthorized apps, and unapproved locations.

Office 365 Exchange mail flow rules prevent auto-forwarding of mail to external domains.

Office 365 data loss prevention (DLP) rules prevent sensitive data from leaving the environment.

Azure Information Protection and Azure Rights Management encrypts and permissions sensitive files. Protection travels with the files.

Azure technologies provide encryption for disks and storage, SQL Encryption, and Key vault.

SQL Database dynamic data masking limits sensitive data exposure by masking it to non-privileged users.

SQL Threat Detection alerts on suspicious database activities, potential vulnerabilities, and SQL injection attacks, as well as anomalous database access patterns.

Azure Backup is a service you can use to back up and restore your data in the Microsoft cloud. This service includes capabilities to protect your backups from ransomware.

Device-based attacks

Devices compromise

Malware is installed on the device. This can include viruses, spyware, ransomware, and other unwanted software that installs without consent.

Malicious files and viruses are introduced into the environment.

Exchange Online Protection scans for and blocks known malware and viruses.

Office 365 Advanced Threat Protection tests incoming files for unknown malware and viruses before they are delivered.

Windows and Office updates protect against new threats to this software.

Windows Defender Application Guard for Microsoft Edge protects against advanced attacks coming from the Internet.

Windows 10 Device Guard only allows trusted applications (defined by you) to run.

Any employee clicks on a malicious link or opens a malicious file.

Windows Defender Antivirus scans for malware, viruses, and security threats.

Windows Defender SmartScreen checks to see if new apps lack reputation or are known to be malicious, and responds accordingly.

Windows Firewall protects against unauthorized access.

Securing Privileged Access Roadmap provides guidance for protecting workstations used for privileged access.

Attacker moves laterally, gaining access to cloud services and resources in the environment.

Intune device compliance policies define criteria for healthy and compliant devices.

Azure AD conditional access rules block access from noncompliant devices and enforce multi-factor authentication for access to cloud services.

Cloud App Security detects and alerts on anomalous activity.

Windows Defender Advanced Threat Protection **is** a service that helps detect, investigate, and respond to advanced attacks on your networks.

Windows 10 Credential Guard prevents attackers from gaining access to other resources in the organization through Pass-the-Hash or Pass-the-Ticket attacks.

Lost or stolen device

Possession is unknown.

Intune device configuration policy enforces password and/or pin requirements and wipes the device after a specified number of failed login attempts.

Attacker gains access into the device.

Windows 10 UEFI Secure Boot helps protect the boot process and firmware against tampering, such as from a physically present attacker.

Windows 10 BitLocker protects files from access without the user credentials.

This topic is 2 of 12 in a series

Microsoft

Microsoft Security Guidance for Nonprofits

Planning and implementation guidance for fast-moving organizations that have an increased threat profile

Solution deployment

Planning for your solution is an iterative process. As you move through the topics in this guide, you'll understand how earlier decisions affect components planned later in the process. Revise your design as needed.

1. Outline your cloud solution and plan for accounts and Azure AD groups.

In this first step you identify the needs of your users and map these to the appropriate cloud capabilities. The available capabilities for collaboration and secure access depend on the account types. This topic helps you make initial decisions that lead to a high-level design for your environment. You'll also design your strategy for Azure AD groups to support the solution both for licensing and for protection. See the **Identity and capability planning** topic (4).

2. Make licensing decisions.

The **Subscriptions and licensing** topic (5) recommends plans for this solution based on the desire to protect an organization with a higher-than-average threat profile. Review this plan and make adjustments for your own organization.

3. Configure and protect your tenants.

In the **Tenant setup and configuration** topic (6) we walk you through the process of setting up your Office 365 and EMS tenants. This includes configuring tenant-wide settings that are recommended as starting-points for a secure environment, configuring the Azure AD groups you planned, and getting started with Cloud App Security.

4. Plan for device protection.

Before you can secure access to cloud services you need to account for devices. In the **Device protection and access** topic (7), plan how you expect users to access cloud services from devices (PCs and phones). Plan the desired protection for each category. This topic includes a starting-point recommendation that you can adjust for your organization.

5. Plan and implement conditional access rules and related policies.

After making decision for identity management and device protection, the Conditional access rules for protecting identities and access from devices topic (8) shows you how to put your plan into action with Azure AD conditional access rules, Intune device policies, and Intune app protection policies. This topic illustrates a plan based on the starting-point recommendations provided in the Device protection and access topic. You can adjust this plan for your organization.

6. Protect your global administrator accounts.

Cloud administrators are valuable targets for cyber criminals. The **Securing administrative access** topic (9) shows you how to protect your global admin cloud accounts.

7. Plan and provision SharePoint team sites and file protection.

SharePoint Online and OneDrive for Business are the core of your collaboration environment. The **SharePoint and OneDrive for Business** topic (10) recommends tenant-wide settings for these services. It also recommends and demonstrates how to configure team sites with protection that allows for the appropriate level of open or secure collaboration. Finally, this topic demonstrates how to implement Azure Information Protection to protect highly confidential files. Use these recommendations to design an environment that meets the needs of your organization.

8. Add users and enable multi-factor authentication.

With protection in place, you can now add users to the environment and enable them for multi-factor authentication. Adding users to the appropriate Azure AD groups provisions them with licenses, gives them permissions to resources, and enforces conditional access rules and related policies. See the **Add users to your environment** topic (11).

9. Create a secure analytics environment with Azure PaaS services.

The **Azure analytics** topic (12) illustrates a recommended secure environment for working with large data sets. This includes a combination of Azure SQL Data Warehouse and Azure Data Lake.

November 2017

Microsoft

Microsoft Security Guidance for Nonprofits

Planning and implementation guidance for fast-moving organizations that have an increased threat profile

Identity and capability planning

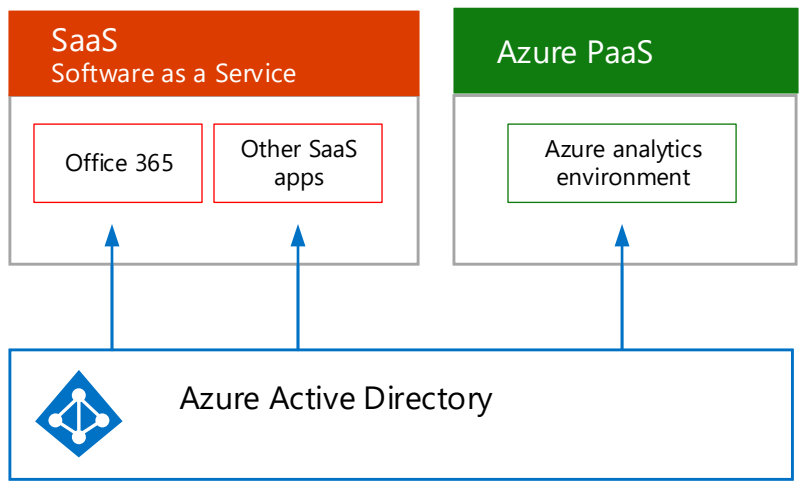
Identity management is the first line of defense against cybercrime

Protecting your environment begins with identity management. This includes:

- Maintaining control over who has access to resources in your environment.
- Securing access with controls that ensure strong assurances of identity (users are who they say they are) and access from safe devices.
- Provisioning resources in your environment with appropriate permissions to reduce the potential for harm and data leakage.
- Monitoring your environment for anomalous user behavior and automatically taking action.

Azure Active Directory (Azure AD) is a leading provider of cloud-based Identity as a Service (IDaaS) and provides a broad range of capabilities for managing and protecting your environment.

- Manage all accounts in one place for all of your cloud applications.
- Use the same set of controls to protect access to applications across your environment.
- Collaboration with partners.
- Monitor anomalous account behavior and automatically take action.



For more information about Azure Active Directory capabilities, see Microsoft Cloud Identity for Enterprise Architects.

Plan for users, account types, and Azure Active Directory groups

Agile organizations can be made up of users with a variety of purposes. Some are permanent contributors while others might only work for a few weeks or months. Some contributors might be employed by partner organizations. A few contributors might be experts that you consult with rarely but at critical moments for your organization, such as a university researcher.

Planning for identity is an iterative process. This topic is designed to get you started. As you learn more about how identity choices influence implementation you can fine-tune your plan.

1. Categorize your users

Take stock of the types of contributors to your organization. What are the logical groupings? Group users by high-level function or purpose to your organization.

For this example solution, we've identified a variety of user categories for a nonprofit to demonstrate the planning and implementation process.

- Senior and strategic staff
- IT staff
- Operations staff
- Analytics staff
- Regular core staff
- Field staff
- Consultants and vendors
- Hourly-paid contract staff
- Unpaid volunteers

Your organization can be composed of more or fewer user categories.

Example agile organization dev/test environment
Configure users and groups

2. Decide what type of accounts to use

Azure Active Directory lets you manage accounts for partners (B2B accounts) in addition to accounts for users you manage directly (tenant domain accounts). Some cloud capabilities extend to users who have no association with your directory (no account management).

This topic details capabilities and protections that can be applied to each type of account. This will help you decide which users belong directly in your tenant domain, which users can be managed using B2B accounts, and which users require no management at all.

This mapping of categories to account types is used as an example.

Tenant domain accounts

- Senior and strategic staff
- IT staff
- Operations staff
- Analytics staff
- Regular core staff
- Field staff

Azure B2B accounts

- Consultants and vendors
- Hourly-paid contract staff

No account management

- Unpaid volunteers

3. Plan for Azure AD groups

Groups in Azure AD are used for several purposes that simplify management of your cloud environment.

Use group-based licensing to assign services to your users automatically as soon as they arrive in the cloud.

Some groups can be populated dynamically based on attributes.

Use groups to automatically provision users for SaaS applications and to protect access to those applications with multi-factor authentication and other conditional access rules.

Groups can be used to provision SharePoint team sites. Groups can also be used in Azure Rights Management templates to protect files with encryption and permissions.

Example Azure AD groups for this solution are provided later in this topic.

The Access Panel lets users view and launch cloud-based applications they have access to.

https://myapps.microsoft.com

Continued on next page (page 1 of 4 in this topic)

How account types work with cloud services

Azure Active Directory provides some flexibility in how users are managed. **Tenant domain accounts** are users within your organization that you license for cloud services. **B2B accounts** are users outside your organization that you invite to participate in collaboration. Both of these account types can be managed within your Azure Active Directory environment. Some cloud services can be shared with users outside your organization without any account management.

This illustration shows how cloud services relate to account types. It's important to understand which services can be used by each account type. This will help you plan for different types of users who contribute to your organization.

This illustration lists the example user categories under each account types as an example.

Cloud services

Azure Active Directory provides identity access to any cloud service, including non-Microsoft cloud providers such as Amazon Web Services.

This example includes Office 365 and an analytics environment in Azure using Platform as a Service (PaaS) capabilities.

Types of accounts

Tenant domain accounts — accounts you add to your tenant and manage directly.

B2B accounts — accounts for users outside your organization you invite to collaborate with. These can be other Office 365 accounts, other organization accounts, or consumer accounts (such as Gmail).

No account management — these are users you communicate with outside your organization who do not use services that require account management in Azure AD.

Capabilities

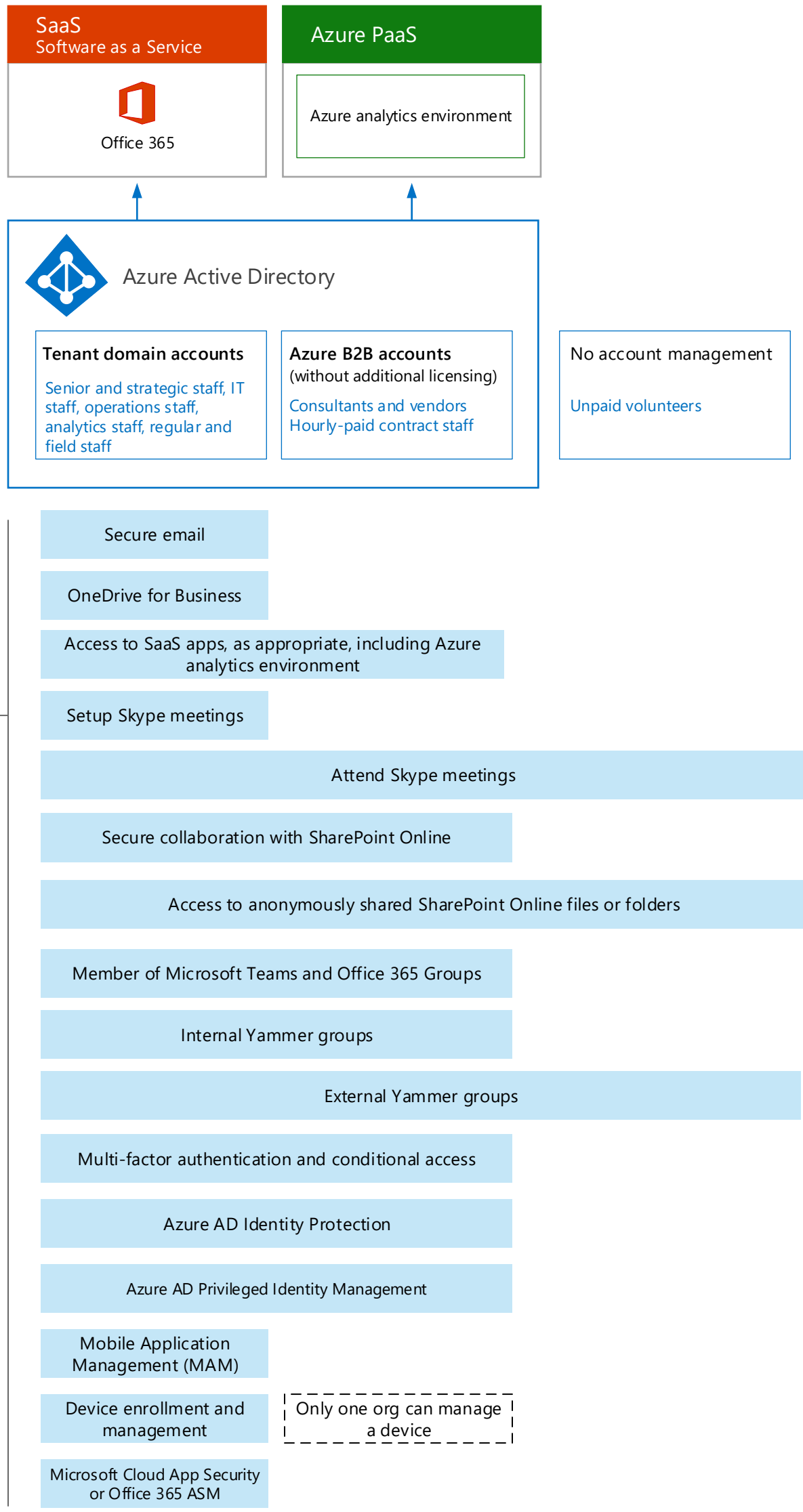
This illustration shows which capabilities are available for each account type.

Capabilities in the B2B column are available without additional licensing. You can add licenses to B2B accounts to give these users additional capabilities.

This illustration doesn't include all capabilities.

Azure Active Directory capabilities are available for B2B accounts at a ratio of 1 licensed user to 5 B2B users.

For example, if you assign 10 licenses to users for Azure Active Directory P2, you can also use these capabilities with up to 50 B2B users without assigning additional licenses.

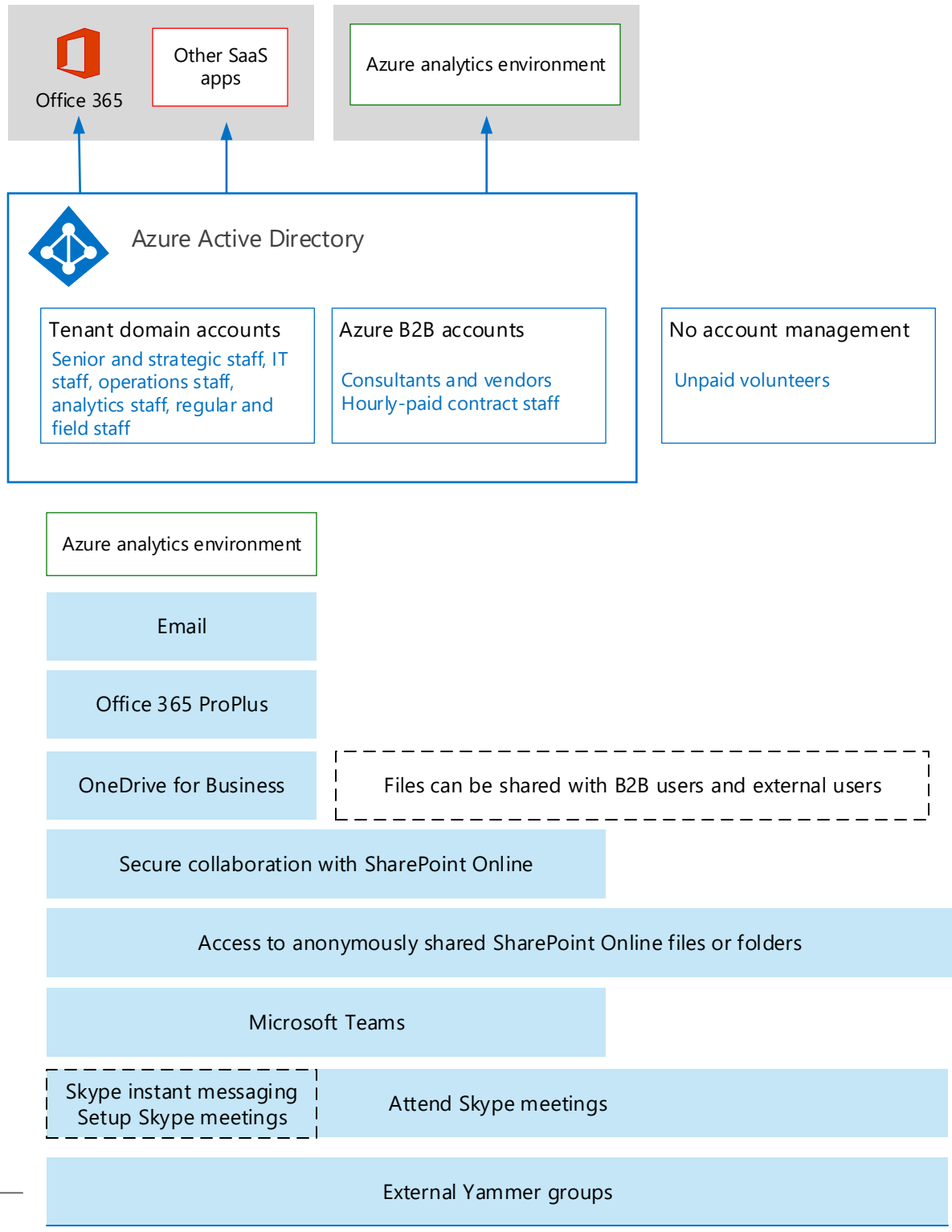


Continued on next page (page 2 of 4 in this topic)

Example cloud environment

For this solution we'll focus on core cloud capabilities for an agile and collaborative organization. This includes collaborative capabilities of Office 365 and secure access to other SaaS apps and an Azure analytics environment.

Use this as an example for sketching your own environment. This will help you design Azure AD groups and plan for licensing.



For an agile environment you can use External Yammer groups to communicate with people who are important to your organization but who's accounts you are not managing. Using SharePoint and Microsoft Teams for internal collaboration and Yammer for external communication makes it easy for your staff to know when they're posting to a public-external audience. External users are required to log in with an email account. You can create external groups for different uses, such as field offices or special interest groups.

Tune your account decisions

By now you have a good idea of what type of accounts to use for the various contributors to your organization. Use this information to learn more about B2B accounts and to discover users who might be better served with a different type of account.

Why use B2B accounts?

Azure AD business-to-business (B2B) collaboration capabilities enable any organization using Azure AD to work safely and securely with users from any other organization, small or large. Those organizations can be with Azure AD or without, or even with an IT organization or without. You can provide access to documents, resources, and applications to your partners, while maintaining complete control over your own corporate data.

- Give external users access to apps in your environment (SharePoint team sites and other SaaS and PaaS applications) without adding them directly to your domain.
- Reduce licensing costs (compared to adding domain accounts).
- Protect access with conditional access rules, including multi-factor authentication.

Should my regular staff member be added as a B2B account instead?

- Does this person also work for another organization? Does that organization manage their devices?
- Does this person use current Office 2016 apps and receive updates through a subscription with another organization?
- Do I need to provide a secure mailbox for this person?

If another organization is providing these services for a staff member, they might just need a B2B account.

Does my B2B partner need a tenant domain account?

- Do I need to monitor B2B accounts using cloud app monitoring tools? These tools will alert on B2B accounts if they haven't been scope out. But these tools cannot automatically take action on B2B accounts, even if these accounts are licensed for these tools. If you need the ability to take automated action on user accounts for anomalous behavior, add them as tenant domain accounts.
- Do I need to apply mobile app management policies to B2B users accessing organization data? In this case, you can license B2B users for these capabilities. You don't need to give them a tenant domain account.
- Will my B2B user have access to sensitive and highly confidential data and the ability to download this data to their devices? Does this B2B user have access to multiple libraries of sensitive and highly confidential data? If this is true, consider the risks of the device becoming compromised or stolen. If this risk is not acceptable, consider using a tenant domain account and managing their devices. This also gives you the opportunity to use cloud app monitoring tools to take action on anomalous behavior, such as downloading large amounts of data.

Continued on next page (page 3 of 4 in this topic)

Azure Active Directory groups and group-based licensing

Azure AD groups greatly simplify many IT responsibilities, including licensing and provisioning users for resources.

This table includes example Azure AD groups for this solution, including groups used for group-based licensing.

More information

Managing access to resources with Azure Active Directory groups

What is Microsoft Azure Active Directory licensing?

Dynamic group membership in Azure Active Directory

Azure AD group	Description	Licenses
IT admins	Administration of services. Use dedicated accounts, not user accounts. Create separate user accounts for non-admin activity. Use one of the groups below, as appropriate. This group is licensed with a mailbox to receive alerts from cloud app monitoring tool. Members of this group are higher value targets for hackers, so additional protection can be applied using this group.	EMS E5 Office 365
IT global and security administrator accounts	Global administrators and security administrators of your cloud services. This is a sub-set of your IT admins. These accounts are the highest-value targets for cyber criminals.	
All tenant domain accounts (dynamic group)	Used for licensing. This group can be used to configure baseline-protection rules for access to services. More restrictive rules can be applied to other groups and the results are additive.	Office 365 EMS E5
All B2B accounts (dynamic group)	View and manage all B2B accounts in one place. Apply conditional access rules for B2B users that don't require device enrollment and management.	No Licensing
Senior and strategic staff	This group is used for access to data with sensitive and higher levels of protection. Members of this group are higher value targets for hackers, so additional protection can be applied using this group.	
Operations staff	Permissions for SharePoint team sites and other resources, as appropriate.	
Analytics PaaS app users	Users with access to the PaaS analytics environment. Use this group for additional licensing for this environment, if needed, including permissions for SharePoint team sites related to analytics work. Members of this group are higher value targets for hackers, so additional protection can be applied using this group.	
Regular core staff	Permissions for SharePoint team sites and other resources, as appropriate.	
Field staff	Permissions for SharePoint team sites and other resources, as appropriate.	
Additional sensitive data users	Add regular users to this group who have access to one or more libraries of sensitive data but are not members of the 'Senior and strategic staff' group.	
Select AIP-protected data users	Add users to this group to give access to AIP-encrypted files. Before adding users to this group, see "Adding permissions for external users" in the SharePoint topic (10). Monitor the membership of this group frequently. Setting this group up early allows you to account for individuals outside your organization who might need to create an individual account in Azure AD to be included in secure access to highly confidential data.	
Conditional access exclusion group	Use this group in conditional access rules to give your organization a way to quickly resolve access issues for highly mobile individuals who find themselves locked out based on conditional access policies. In the event a user is locked out and you do not suspect suspicious activity, temporarily add the user to this group while you resolve their access issue.	

Microsoft Security Guidance for Nonprofits

Planning and implementation guidance for fast-moving organizations that have an increased threat profile

Subscriptions and licensing

There are a variety of plans available for Office 365 and the identity and security capabilities included in the Enterprise Mobility + Security (EMS) suites.

[Compare all O365 Plans]

[Compare E3 and E5 Enterprise Mobility + Security]

This page shows how deploying O365 E5 and EMS E5 provide the combination of security and collaboration capabilities that are essential for an organization with a higher-than-average threat profile.

Subscriptions, licenses, and user accounts

To provide a consistent use of identities and billing for all cloud offerings, Microsoft provides an organization/subscriptions/licenses/user accounts hierarchy.

Organization

The business entity that is using Microsoft cloud offerings, typically identified by a public DNS domain name, such as contoso.com.

Subscriptions

For Microsoft SaaS cloud offerings (Office 365, Intune/EMS, and Dynamics 365), a subscription is a specific product and a purchased set of user licenses.

For Azure, a subscription allows for billing of consumed cloud services to the organization.

Licenses

For Microsoft SaaS cloud offerings, a license allows a specific user account to use cloud services.

For Azure, software licenses are built into service pricing, but in some cases you will need to purchase additional software licenses.

User accounts

User accounts are stored in an Azure AD tenant. For organizations with an on-premises directory, user accounts can be synchronized from an on-premises identity provider such as Windows Server AD.

Your Azure AD directory also includes B2B users you add for collaboration.

Recommended E5 plans for user accounts

	Office 365 E5	Enterprise Mobility + Security (EMS) E5	Azure Active Directory P2 for B2B accounts
Capabilities	**E3 capabilities plus:** Advanced Skype for Business meetings and voicemail capabilities Advanced analytics with Power BI Pro and Microsoft MyAnalytics Advanced Threat Protection Advanced Data Governance Advanced Security Management [Compare all Office 365 for Nonprofits Plans]	**EMS E3 capabilities plus:** Risk-based conditional access Privileged identity management Automated classification and encryption for files Microsoft Cloud App Security [Compare all Enterprise Mobility + Security Plans]	This is included with EMS E5. Every Azure AD paid license includes rights to 5 B2B collaboration users (5:1 model). For example, if you assign 10 licenses to users for Azure Active Directory P2, you can also use these capabilities with up to 50 B2B users without assigning additional licenses.
Why this is recommended	Advanced Threat Protection for email drives the recommendation for E5 for all users with a mailbox. Advanced Data Governance capabilities can be used to automate protection for data loss prevention.	Risk-based conditional access and Cloud App Security drive the recommendation for EMS E5. Also, Cloud App Security can't be used for B2B accounts and device management for B2B accounts is limited, even with additional licensing, so risk-based conditional access helps here.	Azure Active Directory P2 includes risk-based conditional access which can be used with B2B accounts.

Plans per type of user

This chart shows a recommended starting point for assigning licenses for the different types of users who are contributing to this type of organization. You might need to add licensing to some B2B accounts depending on what capabilities they require access to. For example, if a B2B user is participating in the analytics environment, add the appropriate licensing for this user.

Azure AD P2 licensing for B2B users are included in the licensing of EMS E5 for tenant accounts. See the chart above for more information.

	Senior and strategic staff	IT Staff	Operations staff	Analytics staff	Regular core staff	Field staff	Consultants / Board Directors (B2B)	Paid volunteers (B2B)
Office 365 E5	✓	✓	✓	✓	✓	✓		
EMS E5	✓	✓	✓	✓	✓	✓		
Azure AD P2 for B2B Included with EMS E5							✓	✓

Microsoft

Microsoft Security Guidance for Nonprofits

Planning and implementation guidance for fast-moving organizations that have an increased threat profile

Tenant setup and configuration

This topic walks you through recommended configuration for tenant-wide settings that affect the security of your cloud environment. Your security needs might require more or less security. Use these recommendations as a starting point.

Create and connect your tenants

Create your Office 365 and EMS tenants and make sure these are connected. You can use these test lab guides to walk through this process. Then you can use this test environment to walk through the rest of the guidance in this topic and guide.

1. Create your Office 365 tenant

   Office 365 dev/test environment
   Create an Office 365 E5 trial subscription

2. Add an EMS tenant to your Office 365 tenant

   Office 365 and EMS dev/test environment
   Add an EMS trial subscription to your Office 365 trial subscription

3. Check Secure Score when done

   Visit your Office 365 Secure Score site.
   https://securescore.office.com
   Access to Secure Score requires the admin account for the trial environment

Admin centers and dashboards

This table includes the admin centers and dashboards that you'll use most for protecting your environment.

Subscription	Management URL	Dashboards and admin centers
Office 365	https://portal.office.com	Office 365 Admin center Security and Compliance center Exchange admin SharePoint admin and OneDrive for Business admin
	https://securescore.office.com	Office 365 Secure Score dashboard
Enterprise Mobility + Security	https://portal.azure.com	Azure Active Directory Azure AD Identity Protection Microsoft Mobile Application Management Microsoft Intune Azure Information Protection
	https://portal.cloudappsecurity.com	Cloud App Security

Office 365 Secure Score

Office 365 Secure Score analyzes your Office 365 organization's security based on your regular activities and security settings and assigns a score.

After setting up your Office 365 subscription, take note of your starting score. The work you do as part of this solution to protect your environment will increase your score.

The goal is not to achieve the max score, but to be aware of opportunities to protect your environment that do not negatively affect productivity for your users.

https://securescore.office.com

Introducing the Office 365 Secure Score

What's next

Use the guidance in the rest of this topic to configure recommended tenant-wide settings that protect your environment.

Continued on next page (page 1 of 4 in this topic)

Tune threat management settings in Office 365 Security & Compliance Center

The Office 365 Security & Compliance Center includes capabilities that protect your environment. It also includes reports and dashboards you can use to monitor and take action.

Some areas come with default policy configurations. Some areas do not include default policies or rules. Visit the areas below to tune threat management settings for a more secure environment.

Mail filtering
Anti-spam settings

Includes default settings **Yes**

What to watch for:
- **Too much spam** — Choose the Custom settings and edit the Default spam filter policy.
- **Spoof intelligence** — Review senders that are spoofing your domain. Block or allow these senders.

More information

Office 365 email anti-spam protection

Anti-malware

Includes a default policy **Yes**

Recommended — edit the default policy:
- Common Attachment Types Filter — Select On.

You can also create custom malware filter policies and apply them to specified users, groups, or domains in your organization.

More information

Anti-malware protection

Configure anti-malware policies

DKIM
DomainKeys Identified Mail

Includes a default DKIM signature **Yes**

DKIM is an authentication process that can help protect both senders and recipients from forged (spoofed) and phishing email. Your tenant includes a default signature for your domain. Create an additional DKIM signature if you add custom domains to your tenant.

More information

Use DKIM to validate outbound email sent from your custom domain in Office 365

Safe attachments

Includes a default policy **No**

Recommended — add this safe attachment policy:
- Block — Block the current and future emails and attachments with detected malware (choose this option).
- Enable redirect — (check this box and enter an email address, such as an admin or quarantine account).
- Apply the above selection if malware scanning for attachments times out or error occurs (check this box).
- Applied To — The recipient domain is (select your domain).

More information

Safe Attachments in Office 365

Safe links

Includes a default policy **Yes**

Recommended — add this setting to the default policy for the entire organization:
- Use safe links in Office 2016 on Windows (select this option).

Recommended policy for specific recipients:
- URLs will be rewritten and checked against a list of known malicious links when user clicks on the link (select this option).
- Use Safe Attachments to scan downloadable content (check this box).
- Applied To — The recipient domain is (select your domain).

More information

Safe Links in Office 365

View the dashboards and reports in the Security and Compliance Center

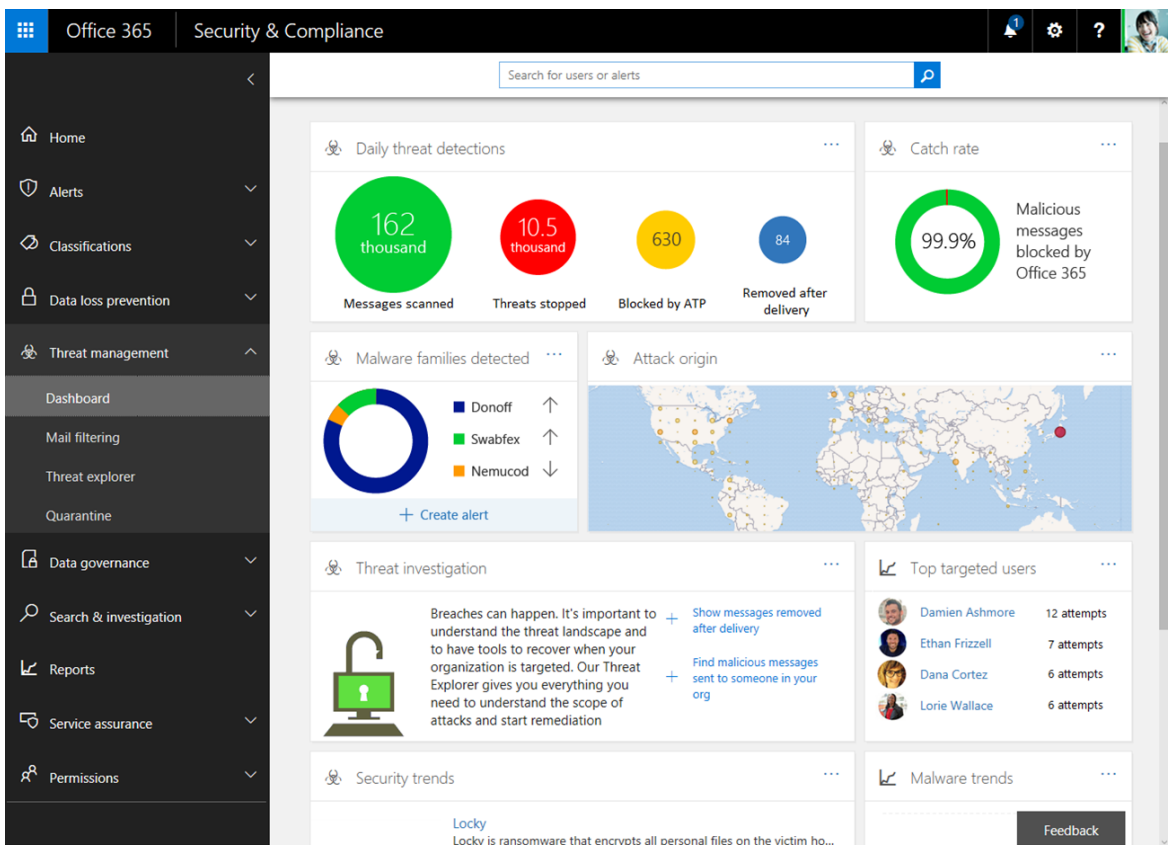
Visit these reports and dashboards to learn more about the health of your environment. The data in these reports will become richer as your organization uses Office 365 services. For now, be familiar with what you can monitor and take action on.

Threat management dashboard
Use this dashboard to see threats that have already been handled, and as a handy tool for reporting out to business decision makers on what Threat Intelligence has already done to secure your business.

Threat explorer
If you are investigating or experiencing an attack against your Office 365 tenant, use the threat explorer to analyze threats. Threat explorer shows you the volume of attacks over time, and you can analyze this data by threat families, attacker infrastructure, and more. You can also mark any suspicious email for the Incidents list.

Reports — Dashboard
View audit reports for your SharePoint Online and Exchange Online organizations. You can also access Azure Active Directory (AD) user sign-in reports, user activity reports, and the Azure AD audit log from the View reports page.

Reports in the Office 365 Security & Compliance Center



Continued on next page (page 2 of 4 in this topic)

Configure additional Exchange Online tenant-wide settings

Many of the controls for security and protection in the Exchange admin center are also included in the Security and Compliance Center. You do not need to configure these in both places.

Here are a couple of additional settings that are recommended.

Mail flow
Transport rules

Includes a default rule — No

Recommended — Add a mail flow rule to help protect against ransomware. See "How to use Exchange Transport Rules to track or block emails with file extensions used by ransomware" in this blog article: How to deal with ransomware.

Create a transport rule to prevent auto-forwarding of email to external domains. For more information, see Mitigating Client External Forwarding Rules with Secure Score.

More information

Mail flow rules (transport rules) in Exchange Online

Enable modern authentication
Exchange Online and Skype for Business

Enabled by default — No

Modern authentication in Office 365 is a prerequisite for using multi-factor authentication (MFA). MFA is recommended for securing access to cloud resources, including email.

Enable Exchange Online for modern authentication

Skype for Business Online: Enable your tenant for modern authentication

Modern authentication is enabled by default for Office 2016 clients, SharePoint Online, and OneDrive for Business.

More information

Using Office 365 modern authentication with Office clients

Configure tenant-wide settings in SharePoint admin center

Configure tenant-wide sharing policies

This guide includes recommendations for configuring SharePoint team sites at increasing levels of protection, starting with baseline protection. SharePoint team sites configured at the baseline level allow sharing files with external users by using anonymous access links. This approach is recommended instead of sending files in email.

To support the goals for baseline protection, configure tenant-wide sharing policies as recommended here.

SharePoint admin center and OneDrive for Business admin center include the same settings. The settings in either admin center apply to both.

Sharing settings for individual sites can be more restrictive than this tenant-wide policy, but not more permissive. This guide includes recommended configurations for team sites protected at higher levels. For more information, see the SharePoint and OneDrive for Business topic (10) in this guide.

Sharing
SharePoint Online and OneDrive for Business

Enabled by default — Yes

- Allow sharing to authenticated external users and using anonymous access links (default setting).
- Anonymous access links expire in this many days. Enter a number, if desired, such as 30 days.
- Default link type—select Internal (people in the organization only). Users who wish to share using anonymous links must choose this option from the sharing menu.

More information

Manage external sharing for your SharePoint Online environment

Configure settings in Azure Active Directory

Configure named locations (under conditional access)

If your organization includes offices with secure network access, add the trusted IP address ranges to Azure Active Directory as named locations. This feature helps reduce the number of reported false positives for sign-in risk events.

Named locations in Azure Active Directory

Block apps that don't support modern authentication

Multi-factor authentication requires apps that support modern authentication. Apps that do not support modern authentication cannot be blocked by using conditional access rules.

For secure environments, be sure to disable authentication for apps that do not support modern authentication. You can do this in Azure Active Directory with a control that is coming soon.

In the meantime, use one of the following methods to accomplish this for SharePoint Online and OneDrive for Business:

- Use PowerShell, see Block apps that do not use modern authentication.
- Configure this in the SharePoint admin center on the "device access' page — "Control access from apps that don't use modern authentication." Choose Block.

Continued on next page (page 3 of 4 in this topic)

Create Azure AD groups and setup group-based licensing

Now that your tenant is configured, you can setup the Azure AD groups for your organization, including dynamic groups and group-based licensing.

If you have created a test lab environment, use the following test lab guide:

Secure SharePoint Online sites in a dev/test environment

For steps 1 and 3 below, see Phase 2: Create and configure your Azure Active Directory (AD) groups and users

1 Create Azure AD groups

Create the groups you have planned in Azure AD

Create a group and add members in Azure Active Directory

2 Add criteria for dynamic membership to the appropriate groups

Managed dynamic rules for members in a group

Criteria for dynamic groups:

- All tenant domain accounts — Enable the All users Group and then remove guest users. See Hardening the All users dynamic group.
- All B2B users — Add users where userType equals Guest

3 Assign licenses to the appropriate groups for group-based licensing

Assign licenses to a group

Get started with Cloud App Security or Office 365 Advanced Security Management

Use Office 365 Advanced Security Management to evaluate risk, to alert on suspicious activity, and to automatically take action. Requires Office 365 E5 plan.

Or, use Microsoft Cloud App Security to obtain deeper visibility even after access is granted, comprehensive controls, and improved protection for all your cloud applications, including Office 365.

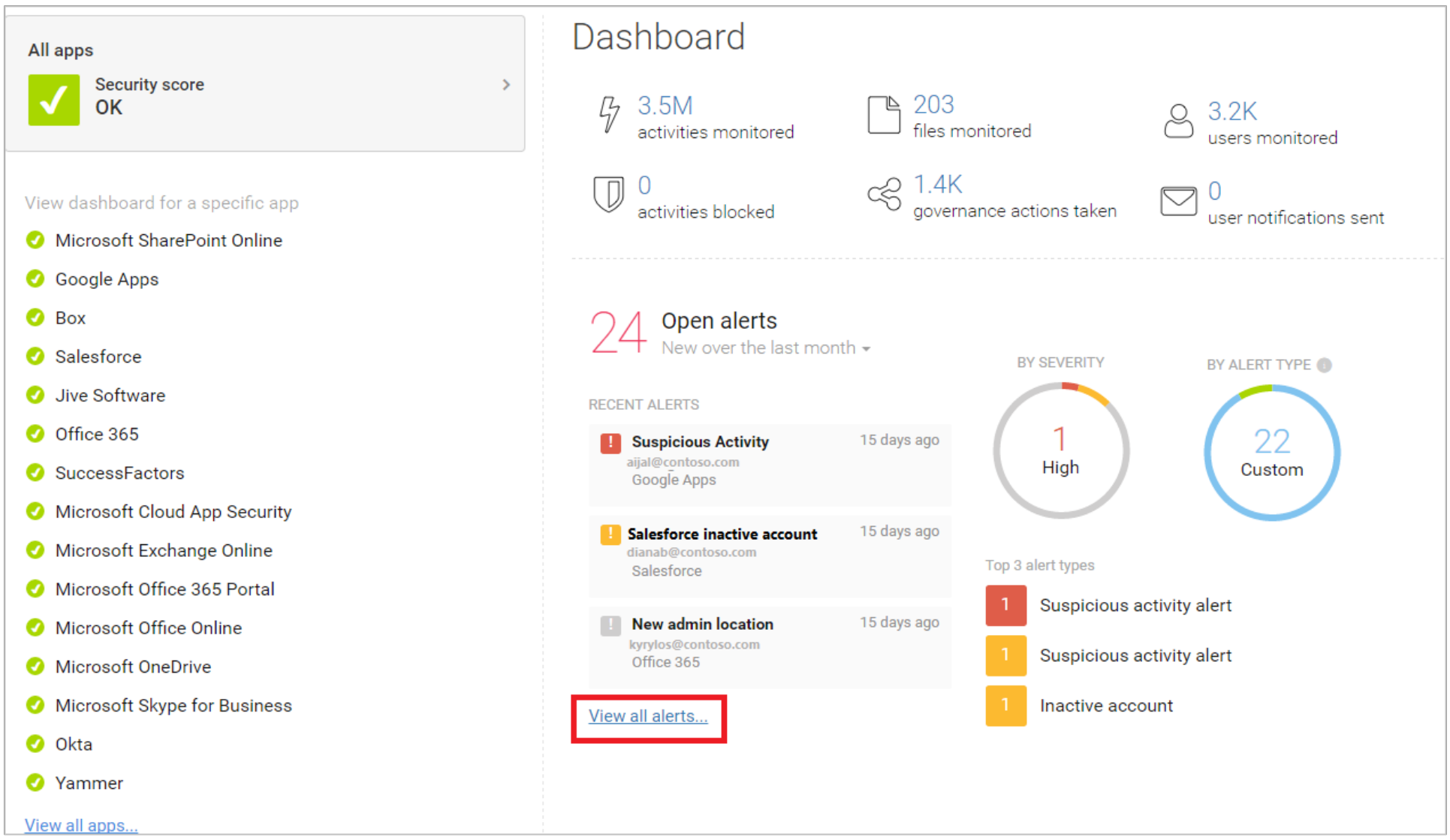
Because this solution recommends the EMS E5 plan, we recommend you start with Advanced Security Management so you can use this with other SaaS applications in your environment.

Start with default policies and settings.

Deploy Cloud App Security

More information about Microsoft Cloud App Security

Overview of Advanced Security Management in Office 365



Microsoft

Microsoft Security Guidance for Nonprofits

Planning and implementation guidance for fast-moving organizations that have an increased threat profile

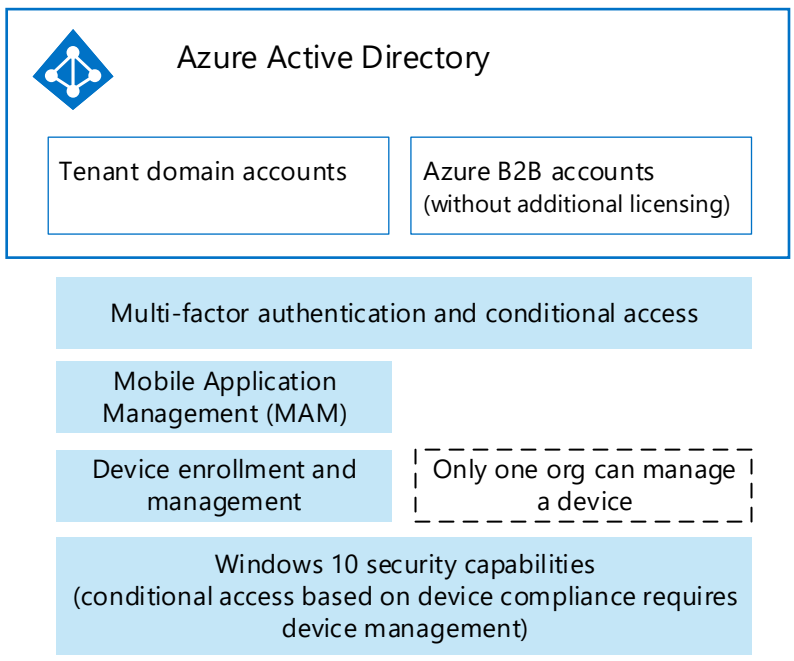
Device protection and access

You can gain a lot of protection on devices, even for unmanaged BYOD devices, by using capabilities in the EMS E5 suite.

First, understand what capabilities are available per account type. See the illustration to the right.

This topic includes recommendations you can use as a starting point. You'll need to make a few decisions to adjust these recommendations for your environment.

- B2B accounts — Intune capabilities require additional licensing for B2B users. For B2B users that have access to sensitive data, consider licensing these with EMS E5 so you can apply Mobile Application Management (MAM) capabilities.
- Managing devices — Choose whether to enroll devices into Intune for management. Only one organization can be a "management authority" for a device. Therefore, managing devices of B2B users might not be an option because these devices might already be managed by another organization.
- Windows 10 — Windows 10 includes compelling security capabilities that make this a recommendation for organizations with a high threat profile. At a minimum, consider using Windows 10 for users who are the highest value targets for cyber attacks.



Starting-point recommendation

This guidance is intended for lightweight, rapidly moving organizations. These starting-point recommendations acknowledge that you might not have a lot of control over the devices users bring to the environment. These recommendations are also intended to provide a variety of options for protecting devices, including data on the devices. Adjust this guidance for your organization based on your threat profile.

This solution provides prescriptive guidance for protecting access to email, files, and other resources with multi-factor authentication, conditional access rules, and Intune management. The guidance is based on these starting-point recommendations. You can adjust this guidance to support the decisions you make for your environment.

Support for managing MAC devices is coming soon.

	Tenant domain accounts	Azure B2B accounts (without additional licensing)
Senior and strategic staff IT staff Operations staff Analytics staff	Intune-managed PCs. Windows 10 with BitLocker, Windows Defender, Windows Firewall, and Windows Information Protection (WIP) as a minimum configuration. If Windows 10 is not used, enroll PCs in Intune and use device compliance policies to ensure the health of these devices. Latest versions of Office 2016, including updates. Intune-managed phones/tablets. Phones registered with Azure AD for phone authentication. Approved phone/tablet apps from the app stores (apps that can be managed by Intune Application Management). Intune app management policies to protect business data on phones.	
Regular core staff Field staff	Intune-managed BYOD PCs with device compliance policies to ensure the health of these devices. Latest versions of Office 2016, including updates. Phones registered with Azure AD for phone authentication. Approved phone/tablet apps from the app stores (apps that can be managed by Intune Application Management). Intune application management policies to protect business data on phones.	
Consultants and vendors Hourly paid contract staff	Conditional access rules requiring multi-factor authentication and apps that support modern authentication. Phones registered with Azure AD for phone authentication. Conditional access rules requiring multi-factor authentication. Approved phone/tablet apps from the app stores (apps that support modern authentication).	

Continued on next page (page 1 of 3 in this topic)

Decide whether to manage devices

You can gain a lot of protection by using Intune Mobile Application Management capabilities on BYOD devices (iPhones and Android phones), and by using multi-factor authentication and conditional access rules to govern access, even on PCs.

For greater security for organizations with a high threat profile, Intune enrollment and management provides the ability to ensure devices are healthy and not compromised. You can also manage security settings and features on devices, rather than relying on users to configure their devices for security. For example, you can ensure that anti-virus software is running and up to date.

Intune capabilities — unmanaged vs. managed devices

Intune App Protection for unmanaged BYOD devices	Intune management for enrolled devices
Send a wipe request. Configure app management policies per platform (without enrolling devices): • iOS • Android Choose which applications to apply a policy to and then configure policy rules. Example settings for iOS: • Prevent iTunes, iCloud backups • Allow app to transfer data to other apps • Allow app to receive data from other apps • Prevent "Save As" • Restrict cut, copy, and paste with other apps • Restrict web content to display in the Managed Browser • Encrypt app data • Disable contacts sync • Require PIN for access (with additional settings) • Require corporate credentials for access • Block managed apps from running on jailbroken or rooted devices • Recheck the access requirements (timeout and offline grace period) • Offline interval (days) before app data is wiped These settings also apply to Company Owned Devices.	Manage more device platforms and types: Android, iOS, Mac OS X, Windows phones and desktops. Block access from unsupported devices. Deploy apps, including LOB apps. Configure finer-grain control of access to corporate resources by configuring policies. Types of policies: • Configuration — manage security settings and features on devices. • Device compliance — Define rules and settings that a device must comply with. • Conditional access — Secure access to email and other services, depending on conditions that you specify. Policies are typically used in combination. For example, define compliance policies and then define conditional access policies that require compliance. Conditional access policies are defined by application: • Dynamics CRM Online • Exchange Online • SharePoint Online & OneDrive for Business • Skype for Business Online

Review options for protection and make a plan

These illustrations demonstrate protection capabilities you can implement for your environment, starting with the most basic capabilities that are recommended.

Windows 10 security capabilities are listed on the next page.

BYOD phone and tablet protection

Unmanaged	Managed
Require apps that support modern authentication and MFA, such as Outlook (these are available in the app stores)	
Require multi-factor authentication	
Intune Mobile Application Management (encrypt app data, prevent leaks to non-managed apps, wipe data, and more) *	
	Require device compliance *

* Requires additional licensing for B2B users

PC protection

Unmanaged	Managed
Use latest versions of Office 2016 and install updates *	
Require the use of apps that support modern authentication	
Require multi-factor authentication	
	Require device compliance and healthy devices *

* Requires additional licensing for B2B users

Continued on next page (page 2 of 3 in this topic)

Windows 10 security capabilities

Windows 10 provides many security capabilities to protect data, devices, and identities. Some of these can be configured manually by administrators. Some capabilities require no additional action. The following table indicates how these capabilities take effect.

For cloud only environments, focus on the capabilities highlighted in light blue.

	Recommended for cloud-only environments					Hybrid on-premises tools
				Device management required		
Capability	**No action necessary**	**Users can configure this**	**Intune MAM**	**Intune device management**	**System Center Configuration Manager**	**Group Policy Object**
Windows Defender Antivirus — scans for malware, viruses, and security threats.	✓	✓		✓	✓	✓
Windows Defender SmartScreen — checks to see if new apps lack reputation or are known to be malicious, and responds accordingly. Checks sites against a dynamic list of reported phishing sites and warns users.	✓	✓				✓
Windows updates — protect against new threats.	✓	✓		✓	✓	✓
BitLocker — encrypts all data at rest and protects it against offline attacks.		✓				✓
Windows Firewall — protects against unauthorized access.		✓		✓	✓	✓
Windows Defender Application Guard for Microsoft Edge (Windows 10 Fall Creators Update) — protects against advanced attacks coming from the Internet.		✓		✓	✓	✓
Windows Information Protection (WIP) — protects business content on devices with file level encryption that helps prevent accidental data leaks to non-business documents, unauthorized apps, and unapproved locations.			✓	✓	✓	
Windows Defender Advanced Threat Protection — a service that helps detect, investigate, and respond to advanced attacks on your networks.				✓	✓	✓
Windows 10 UEFI Secure Boot — helps protect the boot process and firmware against tampering, such as from a physically present attacker.	✓	✓				
Windows 10 Device Guard — only allows trusted applications (defined by you) to run. Not recommended for BYOD environments.		✓				✓
Windows 10 Credential Guard — prevents attackers from gaining access to other resources in the organization through Pass-the-Hash or Pass-the-Ticket attacks. Implement first on computers where privileged accounts are used.		✓				✓

Microsoft

Conditional access rules for protecting identities and access from devices

This page illustrates the set of policies and rules to achieve the starting-point recommendations detailed in the previous topic. Policies and rules are additive. If two of the same type of policy or rule is applied to a user, the most restrictive policy or rule is enforced. Many of these rules are described in more detail in Recommended security policies and configurations.

Prerequisite action for users

Windows 10 PCs:
- Turn on BitLocker device protection
- Protect your PC with Windows Defender
- Turn Windows Firewall on

Mac:
- Use FileVault to encrypt your Mac disk
- Install and use reliable antivirus software
- Turn on firewall protection

Help for users: Protect your account and devices from hackers and malware

In a hybrid enterprise environment administrators can use Group Policy Objects and System Center Configuration Manager to automatically configure these protections on Windows 10 PCs.

Azure AD groups	Azure B2B accounts (without additional licensing)	Device type	Azure AD conditional access policies	Azure AD Identity Protection user risk policy	Intune device policies and profiles		Intune App Protection policies and conditional access rules			
Senior and strategic staff IT staff Operations staff Analytics staff			Require multi-factor authentication (MFA) for access to Office 365 services when sign-in risk is medium or high	High risk users must change password (This forces users to change their password when signing in if high risk activity is detected for their account)	Define compliance policies (one policy for all platforms)	Create a WIP app policy for managed Windows 10 devices				
							Create a device configuration profile for email access	Define app sharing profiles for iOS and Android for Work	Only allow access to Exchange Online and SharePoint Online from apps that support Intune app policies	Define app policy (one policy per platform)
Regular core staff Field staff			Policy 1: Require compliant PCs and mobile devices (This rule enforces device management with Intune) Policy 2: Require compliant PCs or approved apps							
										
Board Members	Consultants and vendors Hourly paid contract staff									
										

Notes for rules									
	Apply to all users, exclude the **Conditional access exclusion** group for temporary exceptions. Cloud apps: Office 365 Exchange Online and Office 365 SharePoint Online. Conditions: Sign-in risk is medium and high. Access controls: Grant access, but require multi-factor authentication.	Apply to the Azure AD groups. Select the same Cloud apps as the MFA policy. Don't select platforms (this enforces compliant devices). Access controls: Grant access, but require device to be marked as compliant. For Policy 2, also select "Require approved app" (coming soon) and "Require one of the selected controls."	Include all users (no exclusions). Conditions: User risk is High. Access: Allow access, but require password change.	**Create one policy for all platforms.** For more information, see "Device compliance policy" in this article: Policy recommendations to help secure email.	Create a Windows Information Protection (WIP) with enrollment policy using the Azure portal for Microsoft Intune	Create a policy for each platform (iOS, Android).	Configure this in the classic Intune portal. One policy for iOS and Android for Work (not available for regular Android). iOS = Select Allow managed documents in other managed apps. Android for Work = Apps in work profile can handle sharing request from personal profile (under Work profile settings).	Create two conditional access rules: • Exchange Online • SharePoint Online Allowed apps = Allow apps that support Intune app policies. Apply to all users.	One policy per platform (Android, iOS). Select targeted apps and policy settings. Recommended: • PowerPoint • Excel • Word • Microsoft Teams • Microsoft SharePoint • Microsoft Visio Viewer • OneDrive • OneNote • Outlook

Microsoft

Microsoft Security Guidance for Nonprofits

Planning and implementation guidance for fast-moving organizations that have an increased threat profile

Securing administrative access

One of the best ways to protect your nonprofit from digital attack is by ensuring that administrative access to your Office 365 subscription is secure. You can do this by protecting your global administrator accounts and delegating day-day administration to specific roles.

Protect global administrator accounts

Security breaches of an Office 365 subscription are typically done by compromising the credentials of an Office 365 global administrator account.

To ensure that these special user accounts are always protected against attack, use:

Dedicated global admin accounts

Sign in with them only for tasks that require global administrator privileges.

Multi-factor authentication (MFA)

Be protected even when an attacker determines a global admin account and its password.

Conditional access policy

Require that all global admin accounts use MFA.

Cloud App Security or Advanced Security Management (ASM)

Get email notification of global admin account and role change activity.

More information

Deploy protected global admin accounts

1. Create an Office 365 group named **IT Admins-Notify** and add the user accounts of IT staff that will be notified of global administrator account activity and changes in roles for user accounts.

   More information

2. Create an Office 365 security (Azure AD) group named **Global Admins**.

   More information

3. Create up to three global admin accounts—such as GlobalAdmin1, GlobalAdmin2, and GlobalAdmin3—with very strong passwords. Enable MFA for each global admin account, and add them to the **Global Admins** group.

   More information

4. Sign in as each admin account and configure the MFA method.

   More information

5. Configure a conditional access policy to require members of the IT Admins group to use MFA (if you haven't already included them in a policy).

   More information

6. Sign in as each global admin account and test MFA and the conditional access policy.

7. Enable Cloud App Security or ASM and configure two policies:
   - An activity policy for **Administrative activity** that sends email alerts to the **IT Admins-Notify** group
   - An activity policy for **Role changes** that sends email alerts to the **IT Admins-Notify** group

   More information

8. Sign in as a global admin account, change the role of one of your other global admin accounts to the user role, and then change it back to the global administrator role.

9. Check the inbox of one of the user accounts in the **IT Admins-Notify** group for emails for the global administrator sign-in and the role changes.

Advanced protection for administrator accounts

Protected access workstations (PAWs)

Create dedicated administrator workstations from which all sign-ins with a global administrator account must be done.

More information

Eligible administrators

Use Azure Privileged Identity Management (PIM) for on-demand, "just in time" administrative access.

More information

Other types of admin accounts

For day-to-day administration, rather than using a global administrator account, assign roles—such as Exchange administrator or Password administrator—to your IT staff based on their responsibilities.

1. Determine the IT staff and the roles to assign for managing the subscription and its services.

2. Sign in with a global administrator account and configure the IT staff user accounts for their customized roles.

   More information

Microsoft

Microsoft Security Guidance for Nonprofits

Planning and implementation guidance for fast-moving organizations that have an increased threat profile

SharePoint Online and OneDrive for Business

SharePoint Online and OneDrive for Business provide experiences that enable communication and collaboration while protecting your data at appropriate levels based on your needs.

OneDrive for Business

OneDrive for Business lets users store, share, and sync their work files. Users can update and share files from any device. They can even work on Office documents with others at the same time.

Users control who they share with and can view who has access to files and change permissions. They can even see who has viewed files.

What is OneDrive for Business?

SharePoint Online communication sites

SharePoint communication sites are beautiful, dynamic sites that let you reach a broad internal audience, and that look great on the web, in the SharePoint mobile app, on PC and on Mac.

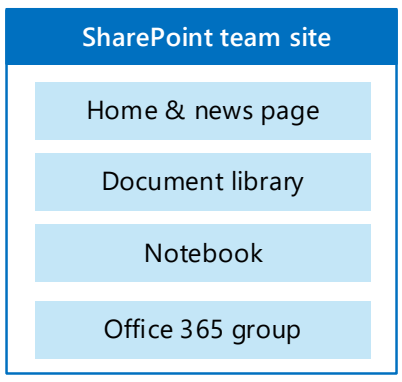
Communication sites are perfect for internal cross-company campaigns, weekly and monthly reports or status updates, product launches, events and more

SharePoint communication sites begin rollout to Office 365 customers

What is a SharePoint communication site?

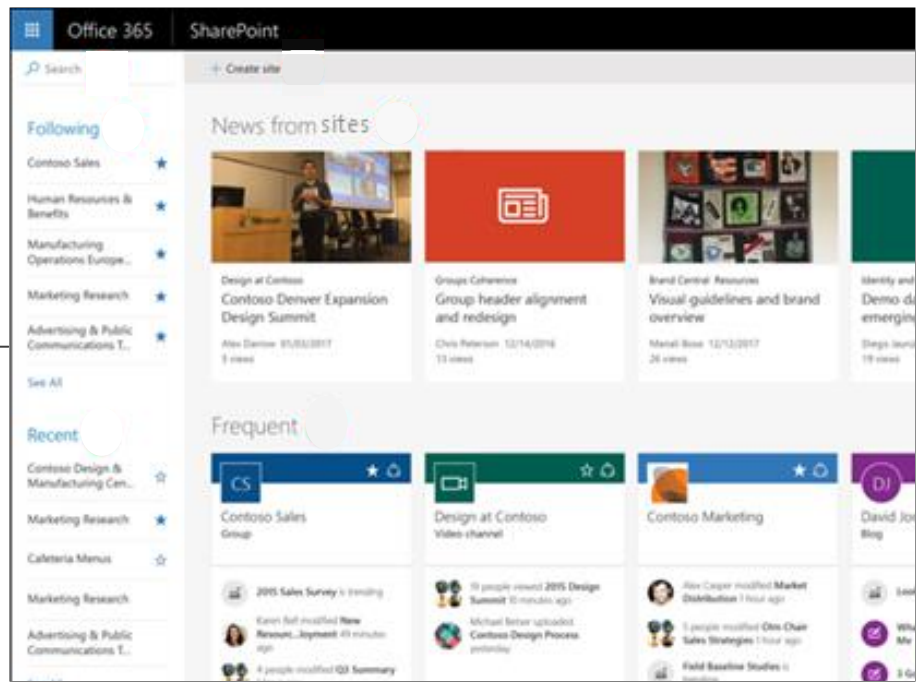
SharePoint Online team sites

SharePoint Online team sites provide an engaging collaboration experience and can be configured for the appropriate level of protection for your projects and files. Default settings allow open collaboration and easy sharing, but you can protect sites at various levels up to the maximum protection for highly confidential files and controlled membership.



Users can see and access their sites from:

- SharePoint homepage in Office 365
- Outlook client (below the Inbox)
- Microsoft Teams (from the Teams web app on Office 365 or the Microsoft Teams desktop application)



What is a SharePoint team site?

Find news, sites, and portals in Office 365

Tenant-wide settings for SharePoint Online and OneDrive for Business

SharePoint and OneDrive for business include tenant-wide settings that affect all sites and users. Some of these settings can also be adjusted at the site level to be more restrictive (but not less).

Sharing

Tenant-wide sharing policies are configured during tenant setup in this guide. For this solution we recommend keeping the default sharing policy that allows all sharing with all account types, including anonymous sharing. Set anonymous links to expire, if desired. Also change the default link type for sharing to Internal. See the **Tenant setup and configuration** topic (6) in this guide for more information.

While it might seem counterintuitive to allow external sharing, this approach provides more control over file sharing compared to sending files in email. SharePoint and Outlook work together to provide secure collaboration on files.

- By default, Outlook shares a link to a file instead of sending the file in email.
- SharePoint and OneDrive for Business make it easy to share links to files with contributors who are both inside and outside your organization.

You also have controls to help govern external sharing. For example, you can:

- Disable an anonymous guest link.
- Revoke user access to a site.
- See who has access to a specific site or document.
- Set anonymous sharing links to expire (tenant setting).
- Limit who can share outside your organization (tenant setting).

SharePoint sites and libraries can be configured with more protection, as needed. This topic includes recommended configurations for more secure SharePoint sites.

Share sites or documents with people outside your organization

Use external sharing together with data loss prevention (DLP)

If you don't allow external sharing, users with a business need will find alternate tools and methods. Microsoft recommends you combine external sharing with DLP rules to protect sensitive files.

Device access settings

Device access settings for SharePoint Online and OneDrive for Business let you determine whether access is limited to browser only (files can't be downloaded) or if access is blocked. These settings are currently in First Release and apply tenant-wide. Coming soon is the ability to configure device access policies at the site level. For this solution, we recommend not using device access settings that apply tenant-wide.

To use device access settings while these are in first release:
Set up the Standard or First Release options in Office 365

OneDrive for Business

Visit these settings to decide if you want to change the default settings for OneDrive for Business sites. Currently, the sharing and device access settings are duplicated from the SharePoint admin center and apply to both environments.

Continued on next page (page 1 of 4 in this topic)

Team site collaboration and security recommendations

Create and configure team sites with the right balance of security and ease of collaboration. This topic includes recommendations for four different configurations, starting with a public site within your organization with the most open sharing policies. Each additional configuration represents a meaningful step up in protection, but makes it more difficult to collaborate.

Public sites and private sites

Public site	Private site
Anyone in the organization can discover and access this site	Only members can discover and access this site

SharePoint team site configurations recommended to protect data at different tiers

	Baseline protection		Sensitive protection	Highly confidential
	Open discovery and collaboration within the organization.	Private site and group with sharing allowed outside the group.	Isolated site. Sharing only allowed to members of the site. DLP used to protect files.	Isolated site + file encryption with Azure Information Protection.
Public/private	Public	Private	Private	Private
Who has access?	Everybody in the organization, including B2B users.	Members only. Others can request access.	Members only. Others can request to access.	Members only. Others *cannot* request access.
Site-level sharing controls	Sharing allowed with anybody. Default settings.	Sharing allowed with anybody. Default settings.	Only members of the site can access contents of the site. Members can grant non-members access to specific content on the site, but the site admin needs to approve these actions.	Only group members can access contents of this site. Sharing is limited to members of the site. Other users cannot request access to the site or contents.
Site-level device access controls			Site-level controls coming soon. Prevent users from downloading files to non-compliant or non-domain joined devices. This allows browser-only access from all other devices.	Site-level controls coming soon. Block download of files to non-compliant or non-domain joined devices.
Office 365 labels	Internal Public	Private	Sensitive	Highly Confidential
DLP rules			Warn users when sending files that are labeled as sensitive outside the organization. Add a policy tip to describe how to share the file by encrypting the file with a password. To block external sharing of sensitive data types, such as credit card numbers or other personal data, use DLP rules for these data types (including custom data types you configure).	Block users from sending files outside organization. Allow users to override this by providing justification, including who they are sharing the file with. Add policy tip to describe how to share the file by changing the label and re-encrypting the file with a password.
Azure Information Protection				Use Azure Information Protection to automatically encrypt and grant permissions to files. Protection travels with files in case they leak. Office 365 cannot read into files encrypted with Azure Information Protection. So be aware that DLP rules can only work with the metadata (including labels) but not the contents of these files (such as credit card numbers within files).
Example project sites	Event planning site Shared calendar	Video production & approval team Speech writing team Research and communications	Analytics team site Finance team site	Strategic planning site Trade secret files

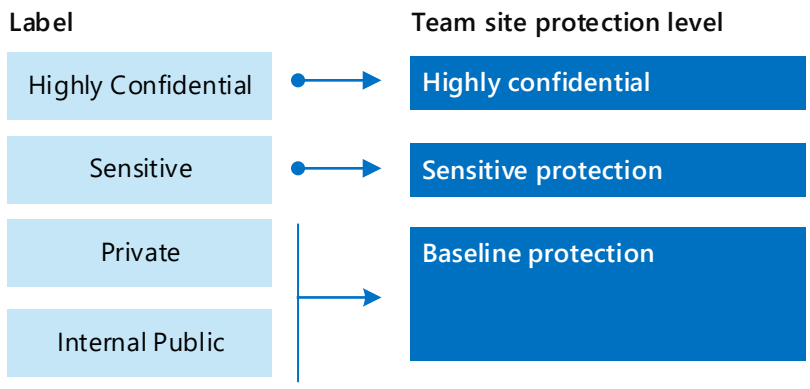
Continued on next page (page 2 of 4 in this topic)

Setup classification and labeling

Using Office 365 labels is recommended for environments with sensitive data. After you setup and deploy labels:

- You can apply a default label to a document library in SharePoint and Office 365 group sites, so that all documents in that library get the default label.
- You can apply labels to content automatically if it matches specific conditions.
- You can apply protection using data loss protection (DLP) capabilities.
- People in your organization can apply a label manually to content in Outlook on the web, Outlook 2010 and later, OneDrive, SharePoint, and Office 365 groups. Users often know best what type of content they're working with, so they can classify it and have the appropriate policy applied.

For this solution, the following are examples of labels that support the four different types of sites. These can be used to automatically label files in document libraries. Or, users can manually apply the appropriate level. This solution includes suggestions for configuring data loss protection rules to protect data classified as sensitive and highly sensitive.



To learn about labels, including where to configure these, see Overview of labels.

Deploying team sites

Secure SharePoint Online sites in a dev/test environment
Create these team sites in a dev/test environment

Baseline protection

Open discovery and collaboration within the organization.

1. Create the team site. In the Privacy settings section, choose **Public**.
   Create a team site in SharePoint Online
2. Edit the document library for the team site to automatically assign the Internal **Public** label.
   Applying a default label to all content in a SharePoint library

Private site and group with sharing allowed outside the group.

1. Create the team site. In the Privacy settings section, choose **Private**.
   Create a team site in SharePoint Online
2. Edit the document library for the team site to automatically assign the **Private** label.
   Applying a default label to all content in a SharePoint library

Sensitive protection

Isolated site. Sharing only allowed to members of the site. DLP used to protect files.

1. Create the team site. In the Privacy settings section, choose **Private**.
   Create a team site in SharePoint Online
2. Configure site permissions using Azure AD group membership.
   Design an isolated SharePoint Online team site
   Deploy an isolated SharePoint Online team site
3. In Advanced permissions settings, go to Access Request Settings and clear these check boxes:
   - Allow members to share the site and individual files and folders.
   - Allow members to invite others to the site members group
4. Edit the document library for the team site to automatically assign the **Sensitive** label.
   Applying a default label to all content in a SharePoint library
5. Create a DLP policy to *warn* users when they send sensitive files in email. (This capability is currently in First Release.) Add a policy tip on how to safely share files. The policy tip character limit is 250.

Example policy tip:
To share with a user outside the organization, download the file and open it. Click File > Protect Document > Encrypt with Password, and then specify a strong password. Send the password in a separate email or other means of communication.

Highly confidential

Isolated site + file encryption with Azure Information Protection.

1. Create a sensitive protection site following steps 1-3 above.
   When configuring Access Request Settings, also clear this check box:
   - Allow access requests
4. Edit the document library for the team site to automatically assign the **Highly Confidential** label.
   Applying a default label to all content in a SharePoint library
5. Setup a DLP policy to *block* users from sending sensitive files in email. Allow users to override this by providing justification. Add a policy tip.

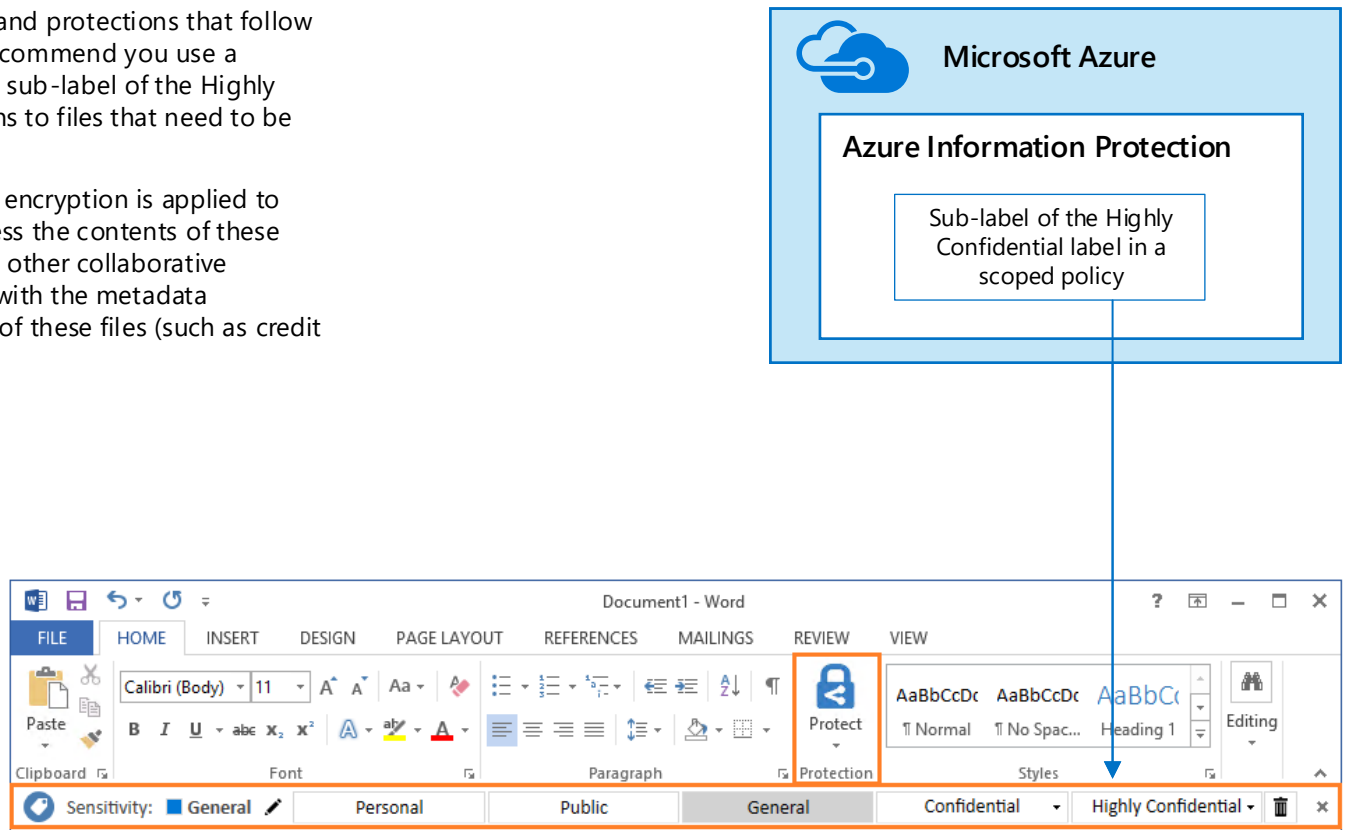
Example policy tip:
If the user does not have permissions to read the file, change the label from Highly Confidential to Confidential and then document the justification for the change.
To share with a user outside the organization, first download the file and then encrypt it with a strong password.

Continued on next page (page 3 of 4 in this topic)

Use Azure Information Protection to protect highly confidential files

Use Azure Information Protection to apply labels and protections that follow the files wherever they go. For this solution, we recommend you use a scoped Azure Information Protection policy and a sub-label of the Highly Confidential label to encrypt and grant permissions to files that need to be protected with the highest level of security.

Be aware that when Azure Information Protection encryption is applied to files stored in Office 365, the service cannot process the contents of these files. Co-authoring, eDiscovery, search, Delve, and other collaborative features do not work. DLP policies can only work with the metadata (including Office 365 labels) but not the contents of these files (such as credit card numbers within files).



Deployment

1. **Activate Azure Rights Management**
   [Activating Azure Rights Management]

2. **Configure a scoped policy with protection and publish the policy**
   Select users and groups the scoped policy will apply to. Recommended protection includes disabling ability to print, copy and extract content, and forward.
   [How to configure the Azure Information Protection policy for specific users by using scoped policies]

Using the solution

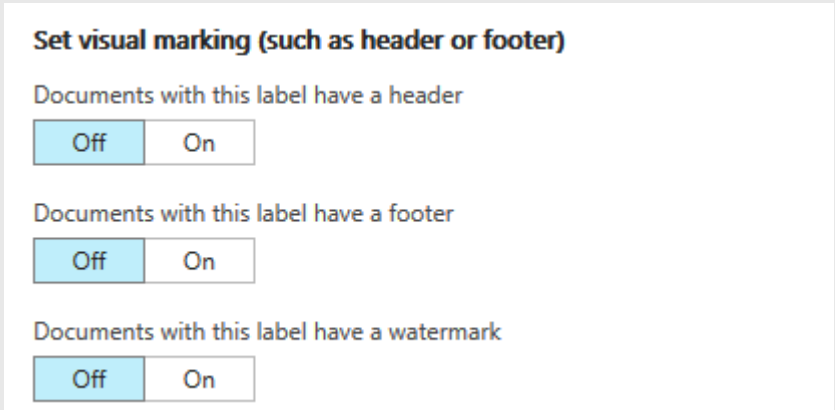
1. **Install the Information Protection client**
   You can script and automate the installation, or users can install the client manually.
   [The client side of Azure Information Protection]
   [Installing the Azure Information Protection client]
   [Download page for manual installation]

2. **Use the client toolbar to apply labels**
   Users outside your organization who are included in permissions do not need to be involved in labeling. Their permissions will allow them to access the contents of files.

3. **Upload files to the SharePoint library**
   Be sure users know which SharePoint library to use for your highly confidential files.

Adding visual markings

You can configure protection for a label to add visual markings. This helps ensure users understand the sensitivity of files and protects against accidental data leakage.



Adding permissions for external users

There are two ways you can grant external users access to files protected with Azure Information Protection. In both these cases, external users must have an Azure AD account. If external users aren't members of an organization that uses Azure AD, they can obtain an Azure AD account as an individual by using this signup page: [https://aka.ms/aip-signup].

- Add external users to an Azure AD group that is used to configure protection for a label — You'll need to first add the account as a B2B user in your directory. It can take a couple of hours for [group membership caching by Azure Rights Management].
- Add external users directly to the label protection — You can add all users from an organization (e.g. Fabrikam.com), an Azure AD group (such as a finance group within an organization), or user. For example, you can add an external team of regulators to the protection for a label.

Microsoft Security Guidance for Nonprofits

Planning and implementation guidance for fast-moving organizations that have an increased threat profile

Adding users to your environment

After setting up your tenant and configuring it for protection, you're ready to add users and enable them for multi-factor authentication.

Add user accounts and manage group membership

If you've setup Azure AD groups with group-based licensing, users will be provisioned with the cloud services they need.

1 Add new users to Azure Active Directory

These are your tenant domain users.

[Add new users to Azure Active Directory]

2 Add B2B collaboration users

These are users who do not belong directly to your organization.

[Add B2B collaboration users to your organization]

3 Add users to the intended Azure AD groups

These are the groups you created during tenant setup.

[Manage group membership for users in your Azure Active Directory tenant]

Setup multi-factor authentication (MFA)

The conditional access rules you setup prevent users from accessing cloud services until they are setup for MFA. You can use MFA in Office 365 or Azure AD. For this solution we recommend Azure AD so you can use it with other SaaS apps in your environment. The first time users sign in, they'll be asked to enroll their account for two-step verification.

1 Enable users for MFA

To start requiring MFA for a user, change the user's state from disabled to enabled.

[Getting started with Azure Multi-Factor Authentication in the cloud]

2 Setup MFA for B2B collaboration users

Learn how MFA works with B2B accounts.

[Conditional access for B2B collaboration users]

Microsoft

Microsoft Security Guidance for Nonprofits

Planning and implementation guidance for fast-moving organizations that have an increased threat profile

Azure analytics

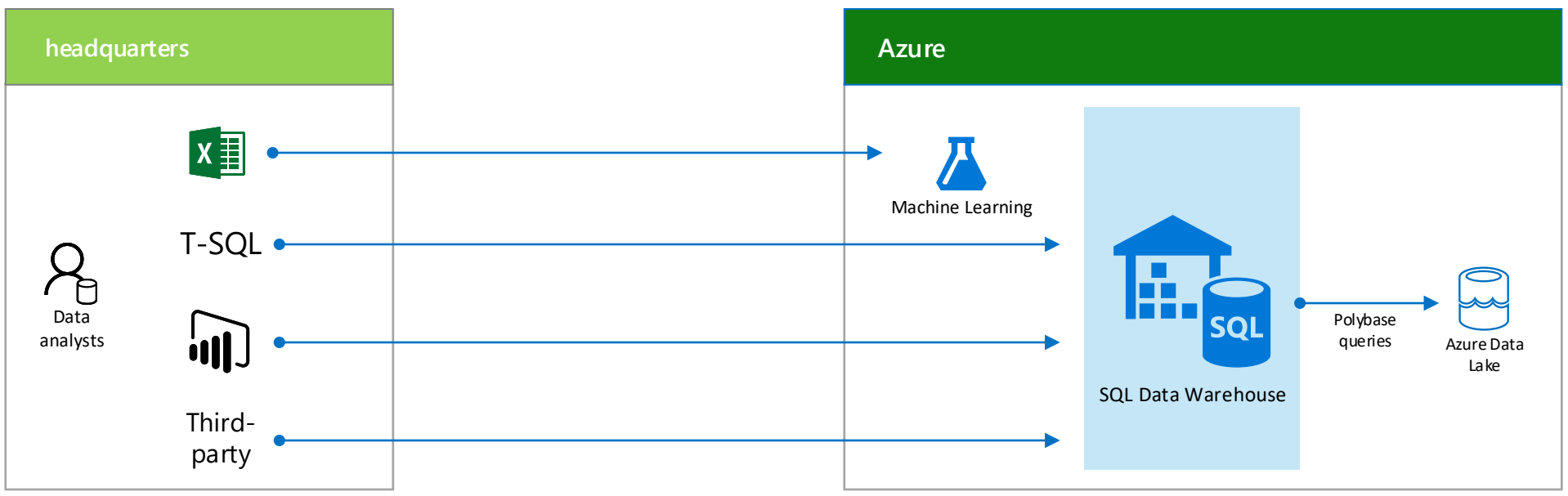
Data analysis and business intelligence is a very important element of a successful organization. The ability to analyze data on beneficiaries, donors, historical information, and current trends can help the candidate and senior staff make informed decisions about program development and direction.

To address these needs, Microsoft recommends the combination of Azure SQL Data Warehouse and Azure Data Lake.

The analytics environment for an organization should be:

Secure	Permissions to access the data and perform analysis should be confined to data analysis staff.	With Data Warehouse and Data Lake, permissions can be managed with Azure AD groups that are part of your identity infrastructure.
Single source	Although there are a variety of database storage formats, technologies, and applications for analytics, for simplicity and a common tool set, you should store all of your data for analysis in the same place.	With Data Warehouse and Data Lake, all of your data can be stored, accessed, and analyzed from a single location.
Scalable	You need an analytics environment that can scale for incoming data.	SQL Data Warehouse can scale to essentially unlimited data sets.
Cost-effective	Programs on donors. Therefore, your analytics environment should balance functionality with ongoing costs.	By separating storage from compute resources, SQL Data Warehouse allows you to only pay for what you store and when you analyze it.

Here is the Azure analytics environment for your campaign:



Once your data is stored in SQL Data Warehouse and Azure Data Lake, your data analysts can use a variety of SQL-based tools to access and perform BI.

- SQL and structured data is stored in SQL Data Warehouse
- Unstructured data is stored in Azure Data Lake, but is accessible for analysis by Polybase queries sent to SQL Data Warehouse

Continued on next page (page 1 of 2 in this topic)

Secure your data in SQL Data Warehouse

Connection security

With firewall rules, you can specify the set of IP addresses from which connections must be initiated. For example, you could whitelist the public IP addresses of your organizational headquarters.

Encryption

Traffic to and from your SQL Data Warehouse is always encrypted. Additionally, you can encrypt the data stored at rest with Transparent Data Encryption (TDE).

Authentication

You can use SQL Server Authentication accounts or Azure AD accounts. For example, you can specify that the only Azure AD accounts that can authenticate are those in your Analytics staff Azure AD group.

Authorization

You can use SQL Server Authentication accounts or Azure AD accounts. For example, you can specify that the only Azure AD accounts that can authenticate are those in your Analytics staff Azure AD group.

If you use all of these security methods, the only people with access to the SQL Data Warehouse are those in your Analytics staff Azure AD group, with specific permissions or database roles, and are connecting from your campaign headquarters. At all times, the data is encrypted at rest and when sent over the Internet.

More information

Threat detection for SQL Data Warehouse

You can use Azure SQL Data Warehouse Auditing to detect anomalous database activity that could be a potential security threat and send you an email notification.

More information

Migrate your data to Azure analytics

Here are the steps to migrate your existing databases and data sources to SQL Data Warehouse and Azure Data Lake:

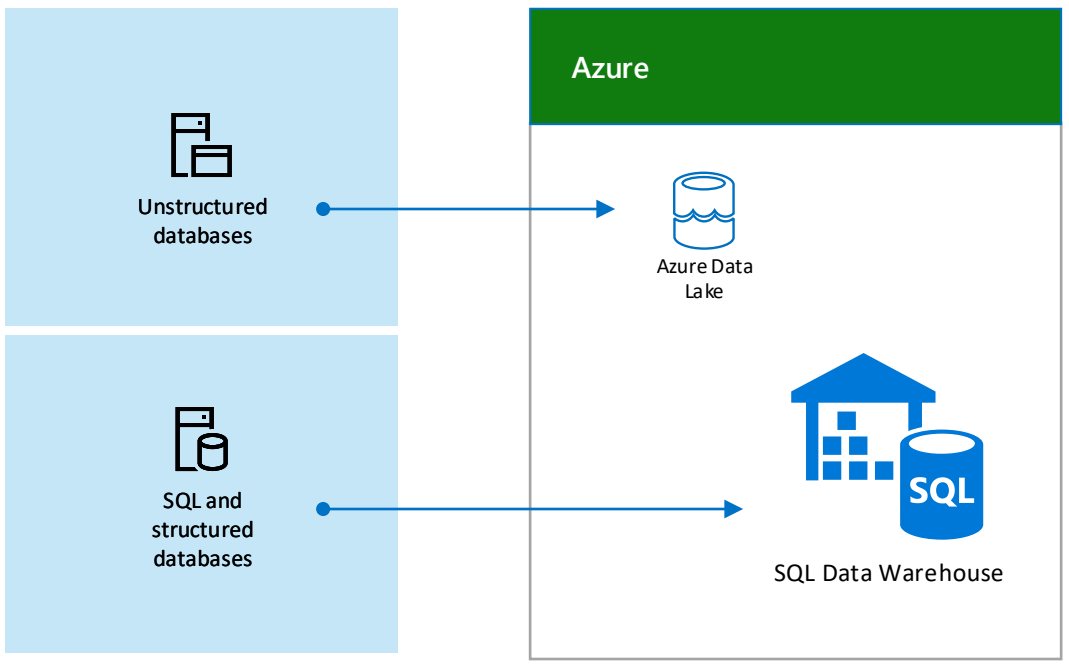
1. Migrate existing SQL data and additional third-party structured databases into SQL Data Warehouse.

2. Configure existing SQL server and additional third-party structured data sources to feed new data directly into SQL Data Warehouse.

3. Migrate unstructured data to an Azure Data Lake store.

4. Configure unstructured data sources to feed new data directly into the Azure Data Lake store.

More information



Microsoft