Security and Information Protection for Multi-Region Organizations with a Single Microsoft 365 Tenant

Overview

Using a single Microsoft 365 tenant for your global organization is the best choice and experience for many reasons. However, many architects wrestle with how to meet security and information protection objectives across different regions. This set of topics provides recommendations.

Two approaches for multi-national organizations

Apply security and information protection globally (recommended)

Security and information protection are applied consistently across the entire global organization

- Apply multi-factor authentication to all users, regardless of region.
- Establish a baseline of security, including conditional access and related policies, and apply these to all users.
- Apply information protection policies consistently across the organization, regardless of regional requirements.
- Instead of exempting locations from information protection policies, focus on tuning sensitive information types and policies to reduce false positives. Also configure overrides that inform users and give them the option to take the right action for the flagged data.

This approach provides the most comprehensive security and information protection and leaves hackers with less opportunity to accomplish their goals by traversing laterally.

Create custom policies and isolate these to specific regions (not recommended)

Use security and information protection boundaries to craft policies that apply to specific regions

- Evaluate the requirements for each region. Craft specific security policies for each region and use security groups and other boundaries to isolate these to the targeted region.
- Apply information protection policies only to the regions with these requirements.
- Customize sensitive information types for each region to reduce false positives within that region. Do not use these across other regions.
- Isolate sites and data to specific regions and limit access from outside the region.

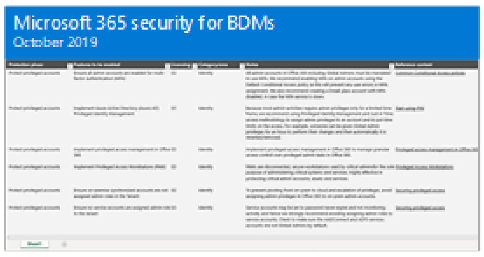
This approach is not recommended. Isolating data and policies leaves security and information protection gaps and reduces the opportunity for collaboration. Hackers can accomplish their goals by traversing laterally, where less restrictive security is applied to accounts and then target data across the organization.

Approaching security and information protection systematically

A recommended systematic approach for implementing security and information protection includes these phases:

- Protect privileged accounts
- Reduce the surface of attack
- Protect against known threats
- Protect against unknown threats
- Assume breach
- Continuous monitoring and auditing

For more information, including a spreadsheet for tracking your progress, see Microsoft 365 Security for Business Decision Makers (BDMs).



Microsoft 365 security for BDMs
October 2019

To send feedback about this documentation, please write to us at CloudAdopt@microsoft.com.

Apply protection consistently across regions

Security

- Define and apply the same security policies across the entire organization.
- Configure a baseline level of security through conditional access policies and apply these to all users.
- Some users might warrant increased security, such as senior leaders or researchers who have access to classified data. For these users, established a set of contindional access policies that are appropriate and apply these consistently across your organization.
- Don't configure unique policies for specific regions or countries.
- Apply Microsoft threat protection capabilities globally using the recommended roadmap (later in this guide) as a guide.

Information protection

- Create policies to protect specific types of data and then apply these policies uniformly across the entire organization.
- Craft policies to target data, not specific regions or countries.
- Instead of creating policies for specific regions, tune the organization-wide policies to reduce false positives and use overrides appropriately.

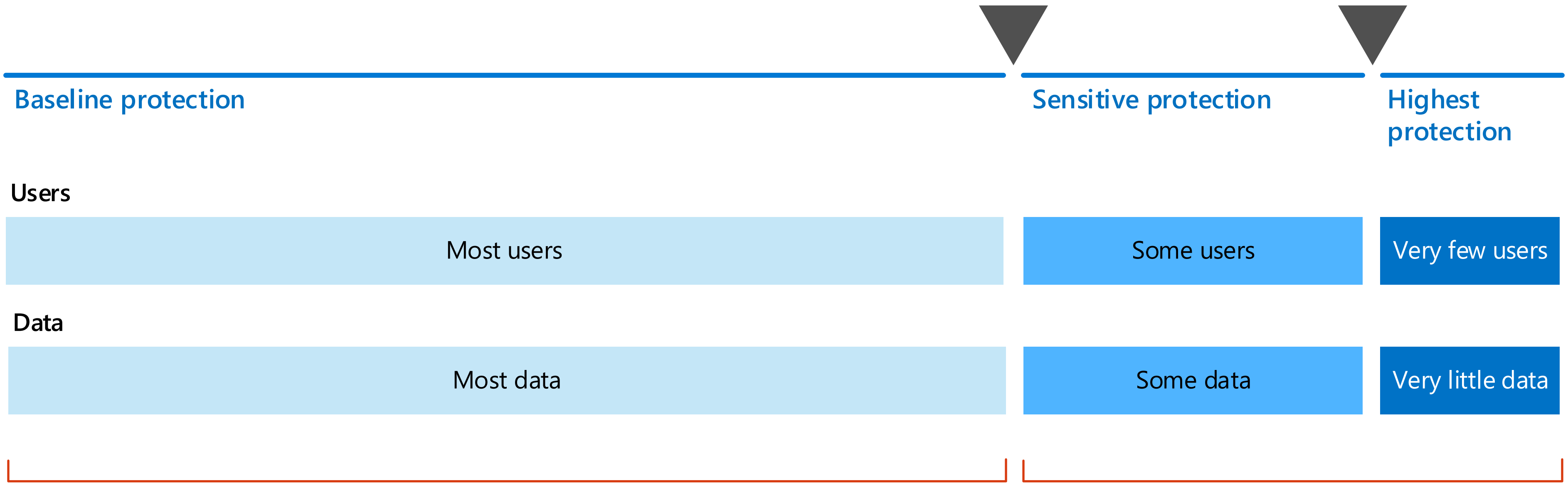
Not recommended:

- Trying to craft geo-specific policies.
- Allowing admins of different regions to craft different policies.

Define tiers of protection and apply these uniformly

Rather than defining region-specific policies, Microsoft recommends defining a small number of tiers of protection for your organization and applying these protections consistently everywhere. For example, protect sensitive users and content in Japan with the same protections that are applied to sensitive users and content in Europe.

Tiers of protection work well for protecting user accounts, sites and libraries, and Microsoft Teams in uniform ways, depending on their sensitivity. Additionally, sensitivity labels, retention labels, and data loss prevention policies target and protect data regardless of where it resides.



	Baseline protection	Sensitive protection	Highest protection
Users	Most users	Some users	Very few users
Data	Most data	Some data	Very little data

Apply a consistent baseline of protection across your entire organization

Establish a baseline for your entire organization and apply it uniformly.

Resources:

Recommended identity and device access policies
Recommended conditional access policies for baseline, sensitive, and highly regulated protection.

Secure SharePoint Online sites and files
Recommended protection for SharePoint Online sites and files for baseline, sensitive, and highly regulated protection.

Teams for highly regulated data
Protect highly regulated data in Teams.

Some user accounts and data require higher levels of protection

Define higher tiers of protection for your organization and apply these uniformly to the user accounts and data that warrant this protection.

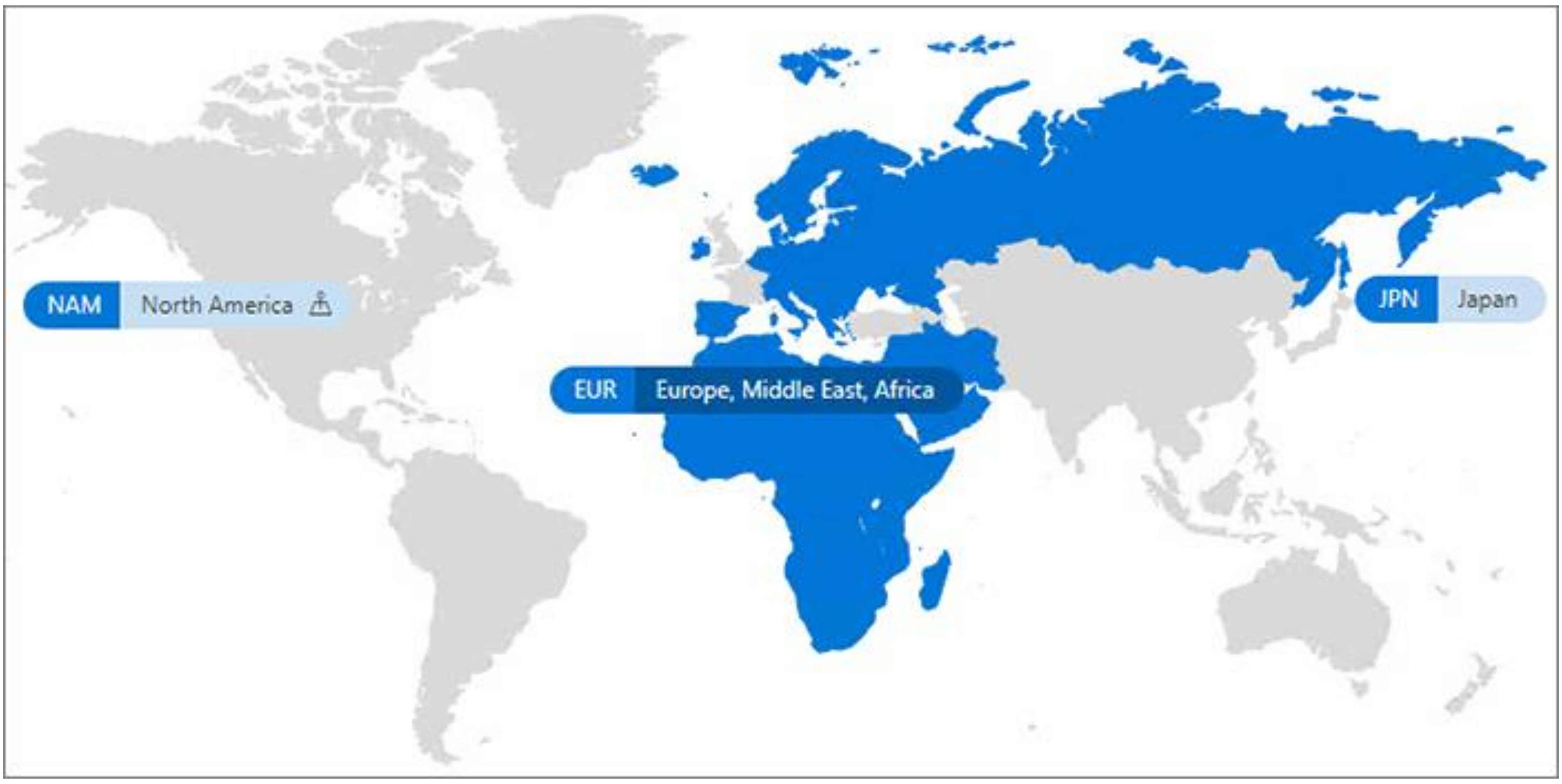
Admins at regional sites might be better positioned to identify the user accounts and Microsoft Teams or SharePoint sites that fit these categories. However, The protection applied for each of these categories should be consistent across the organization. For example, policies for sensitive protection in Japan should be the same as those applied in for sensitive protection in Europe.

Does my organization need Office 365 Multi-Geo?

Office 365 Multi-Geo is an add on capability that gives an organization the ability to select multiple geographic regions and/or countries within the existing tenant for data at rest locations. Multi-Geo provisions and stores data at rest in the geo locations that you've chosen to meet data residency requirements. Some organizations require this to roll out modern productivity experiences to their global workforce.

If your organization does not need to meet data residency requirements, you do not need Multi-Geo. If you do need this capability, reach out to your Microsoft Account Team to sign up.

- Office 365 Multi-Geo locates user mailboxes, OneDrive, and user-created sites at the location of the user.
- Teams is Multi-Geo aware. If a user in Europe creates a Team, then the site and group associated with this team resides in Europe.
- Collaboration across multiple geographical locations is not affected.
- Multi-Geo is intended for data residency requirements, not for performance.
- Office 365 Multi-Geo does not affect Azure AD. All identities remain at the location of the tenant.



How Office 365 Multi-Geo affects security and information protection

Security	Information protection
Office 365 Multi-Geo doesn’t change the recommendation for security, which is to apply the same policies across the entire organization.	Office 365 Multi-Geo doesn’t change the recommended approach for information protection, which is to create policies to protect specific types of data and then apply these policies uniformly across the entire organization.

Additional resources:

Office 365 Multi-Geo overview

Teams experience in an Office 365 OneDrive and SharePoint Online Multi-Geo-enabled tenancy

Where your customer data is stored (aka.ms/dcmaps)

Administering an Office 365 Multi-Geo environment

Administration with a single tenant

Follow recommendations to limit the number of administrators and to secure accounts and access used for administration. Establish a baseline of security tenant-wide. Multi-national organizations can use regional administrators to help identify accounts and data that should be protected at higher levels.

Resources:

About Office 365 admin roles
Available roles and recommendations.

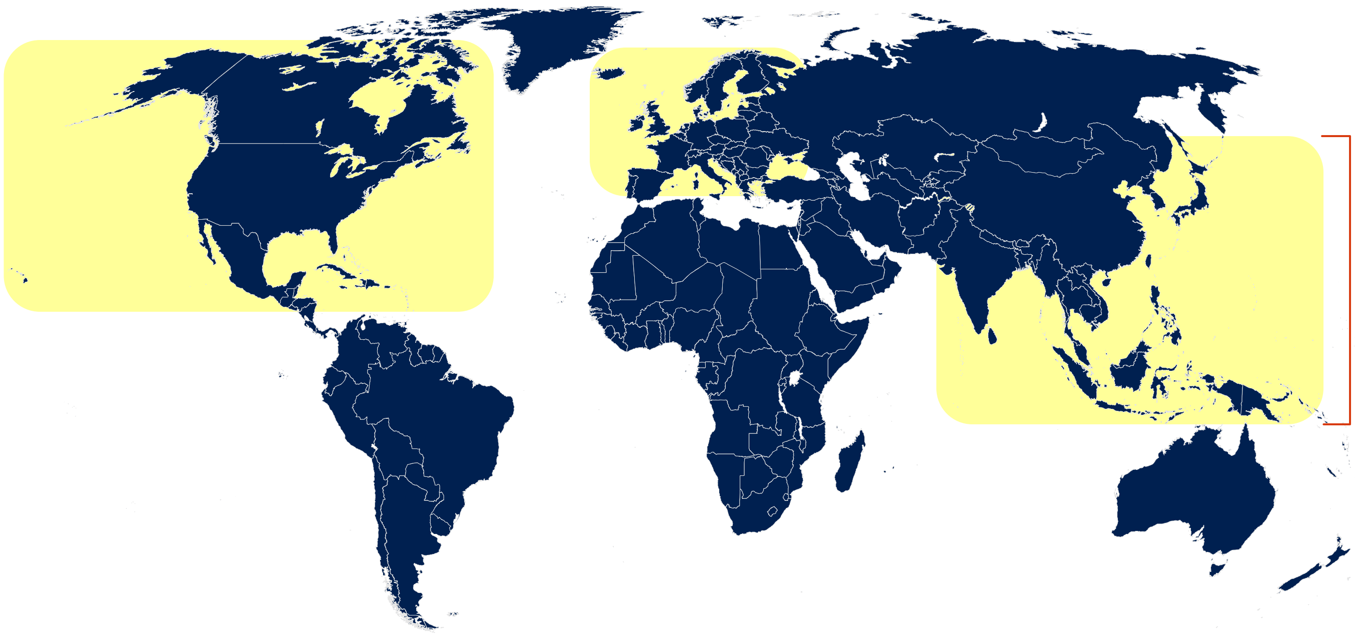
Protect privileged accounts
Top recommended capabilities for securing privileged accounts.

Securing privileged access
In-depth guidance, including how to configure a Privileged Access Workstation (PAW).

Administering an Office 365 Multi-Geo environment
Describes how Office 365 service administration works in a multi-geo environment.

Global admins
Establish a baseline of protection that applies to the entire tenant.

Service admins (Exchange, SharePoint, Microsoft Teams, etc.)
Service admins configure tenant-wide protection for their service.



Regional admins

Admins at regional locations are more familiar with their users and data and can recommend and/or apply higher tiers of protection where appropriate.

Regional admins should be limited to a specific service. Some services provide the option to limit the scope of access through Roll-based Access Control (RBAC) or user groups, or specific SharePoint sites.

Azure Active Directory

Use RBAC with Azure Active Directory to customize scopes of administration.

Assign administrator and non-administrator roles to users with Azure Active Directory

What is role-based access control (RBAC) for Azure resources?

Add or remove role assignments using Azure RBAC and the Azure portal

Exchange Online

Create role groups and assign these groups to manage specific mailboxes.

Permissions in Exchange Online

Manage role groups

SharePoint Online

Assign admins at the site level.

Manage site admins

Microsoft Teams

Options are limited to admin roles only.

Use Microsoft Teams administrator roles to manage Teams

Office 365 Security & Compliance Center

Options are limited to admin roles only.

Permissions in the Office 365 Security & Compliance Center

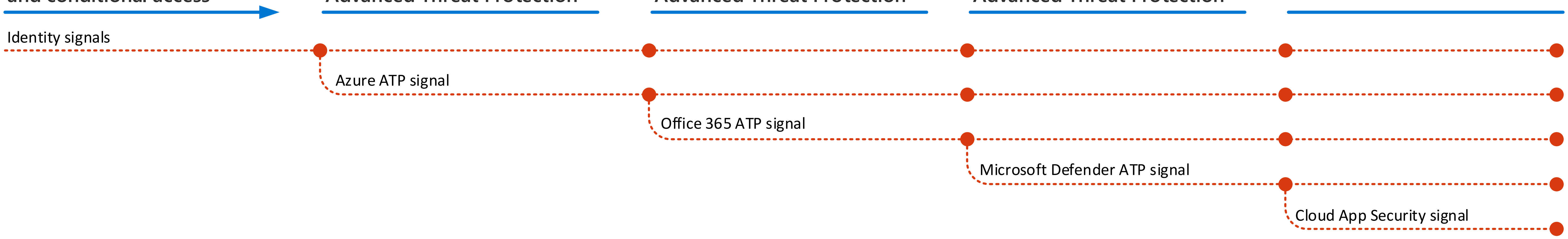
Threat protection

This topic recommends a roadmap for implementing threat protection capabilities. Microsoft threat protection capabilities are integrated by default and signals from each capability add strength to the overall ability to detect and respond to threats.

The combined set of capabilities offer the best protection for organizations, especially multi-national organizations, compared to running non-Microsoft products. Organizations with multiple security teams can implement these capabilities in parallel.

Regional considerations — Internal governance between regional teams is Important. Try to use the same policies for all regions.

Start here



Identity signals

Azure ATP signal

Office 365 ATP signal

Microsoft Defender ATP signal

Cloud App Security signal

Multi-factor authentication and conditional access

Protect against compromised identities

Begin with this protection because it's foundational.

User impact

Some.

Admin work

Minimal.

Recommended identity and device access policies

Azure Advanced Threat Protection

A cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

Focus on this next because It protects your on-prem and your cloud infrastructure, has no dependencies or prerequisites, and can provide immediate benefit.

User impact

None.

Admin work

If all domain controllers meet pre-requisites, just install it and go.

Office 365 Advanced Threat Protection

Safeguards your organization against malicious threats posed by email messages, links (URLs) and collaboration tools. Protections for malware, phishing, spoofing, and other attack types.

This is recommended next because change control, migrating settings from incumbent system, and other considerations can take longer to deploy.

User impact

Minimal if using Office 365 ProPlus.

Admin work

As little as an hour to configure, perhaps a bit more to update user training and documentation. Migrating settings from incumbent system may take longer.

Note: Be sure you also configure the threat protection capabilities included in all Office 365 subscriptions (Exchange Online Protection).

Microsoft Defender Advanced Threat Protection

An endpoint security solution that helps prevent, detect, investigate, and respond to advanced threats. Provides both indicator-based and behavioral detection and response capabilities.

This takes longer to deploy, but can be done in parallel with the other capabilities if other admins are responsible.

User impact

If application whitelisting is used, impact can be significant. Otherwise, any impact is far preferable to the alternative.

Admin work

Scope of work depends on the number of endpoints and available deployment methods.

Microsoft Cloud App Security

A cloud access security broker for discovery, investigation, and governance.

You can enable this early to begin collecting data and insights. Implementing information and other targeted protection across your SaaS apps involves planning and can take more time.

User impact

Only if you are using it to block unsanctioned applications.

Admin work

For discovery and investigation, very little for Office 365 and Azure. For governance, depends on the type and number of apps, policies, and other considerations.

March 2020

Information protection

Use compliance features consistently across geographies.

1. Label content with a consistent set of cross-geography sensitivity labels

2. For content with retention or deletion requirements, use a set of cross-geography retention labels.

3. Use cross-geography data loss prevention policies to protect sensitive information.

Sensitivity labels

Use sensitivity labels to designate the sensitivity of files and emails and enable business rules and workflows based on the label. Use labels consistently across geographies where possible.

Use a small number of labels
Use a small number of well-defined labels across departments and geographies. Large numbers of labels can be hard to manage and can lead to user confusion and content misclassification.

Use auto-classification where possible
Auto-classifying documents or emails by using sensitive information types or other business rules reduces the risk of sensitive content not getting properly classified.

Allow override with business justification
Sometimes the most appropriate classification is best known by the users most closely connected to the content. Allowing users to reclassify content and provide a business justification can help make sure the best label is applied.

Use additional labels for highly sensitive data
For highly sensitive data, use label-based encryption and secure a site or team with a custom label for that purpose.

Retention labels

With retention labels, you can define how long documents and emails must be retained and when they can or must be deleted.

Set retention to the longest required time
For content that has different retention requirements across geographies, set your retention policy to the longest period required for all locations. This simplifies retention management.

Auto-apply labels
Auto-apply labels where possible. Sites can auto-apply retention labels to all documents in the site.

Create labels by department
Create labels by department rather than by geo location. Create geo-specific labels only when needed for specific compliance requirements (such as deletion of files as soon as possible).

Data loss prevention

With data loss prevention, you can configure a wide range of conditions, exceptions, and actions that can be applied to Exchange email, Teams chats and channel messages and OneDrive and SharePoint documents.

Use sensitive information types
Use sensitive information types with DLP to prevent exfiltration of sensitive information across geographies. Sensitive information types can be used by data loss prevention and Microsoft Cloud App Security policies to limit access to sensitive information.

Use DLP policies
Use DLP policies to restrict access to content based on conditional matches across documents and email.

Avoid user overrides
Allowing users to overrides a DLP policy can increase your risk of data exfiltration if the user's account is compromised. Avoid allowing user overrides when dealing with sensitive data.

Use geo-specific policies to address false positives.

4. Identify false positives that cannot be addressed with cross-geography labels and policies and address those with geo-specific policies.

Options for geo-specific issues

In some cases, even using the recommended information protection options, you may still have enough false positives to cause problems with productivity. This can happen if you have different information types that are very similar. The options below can help you work around these issues. In some cases, using these options may increase your risk of data exfiltration. Weigh that risk against the risk of users bypassing your governance practices in order to remain productive.

Use exact data matches
Use exact data matches to white-list or black-list specific data where possible.

Update built-in sensitive information types
Recreate built-in sensitive information types to customize pattern matching and sensitivity. Make adjustments to minimize false positives while still catching actual sensitive information.

Use geography-specific DLP policies
For areas where data in some geographies is more likely to produce false positives than others, consider using multiple DLP policies for the same information type with different tuning for each geography.

Limit overrides
If overrides are needed, limit them to the groups or geographies most prone to false positives. This reduces possible avenues for data exfiltration.

Use an approval workflow
Instead of overrides, send DLP-flagged emails through an approval workflow by using mail flow rules.

Resources:

Customize or create a new sensitive information type
Describes how to optimize these, including reducing false positives.