Microsoft

Maintain compliance with controls and visibility that adhere to global standards

Introduction

Employees need to access, generate, and share organizational information ranging from extremely confidential to informal. You must ensure that all information and the movement of that information comply with industry standards without inhibiting workflow. Microsoft 365 security solutions can help you know what's happening with your data, set permissions and classifications, discover and prevent leaks, and more. Customized and clear solutions can help you reach your organization's compliance standards.

How can I ensure only authorized people can view sensitive information?

Microsoft Azure Information Protection

Azure Information Protection allows you to put standards in place that make it easy for you and your employees to know what data is public or confidential, and then enforce permissions that allow only the right eyes on the right information. To classify documents you must first configure your company's classification policy. Configure the Azure Information Protection policy by signing in to the Azure portal as an administrator, selecting Azure Information Protection in the apps list. All Azure Information Protection users start with a default policy that you can then configure to suit your needs. Once you have created the policy that works best, publish your changes to deploy that policy to all managed apps and devices.

Risk-based conditional access

Risk-based conditional access means that only authorized people can see sensitive information and they will be subject to scrutiny in questionable scenarios. Risk-based conditional access in Azure Active Directory (Azure AD) adds machine learning informed by the Microsoft Intelligent Security Graph to monitor sign-ins and identify accounts that may be compromised, even if the account credentials are accurate. Conditional access lets you define policies that provide contextual controls at various levels, such as the user, location, device, and app level, while taking risk information into consideration. To set risk-based conditional access policies, select "conditional access policies" in the Azure portal. There you assign conditional access policies in Azure AD to enable multi-factor authentication (deny all access from this location, etc.) Microsoft Intune enrollment is required to use this application.

How can I make sure compliance concerns don't affect my employees' productivity?

Microsoft 365 Security and Compliance Center

The Microsoft 365 Security and Compliance Center allows you to assign roles and groups of roles to specific employees. This way you can designate employees to manage common tasks and functions, freeing up IT time. The Microsoft 365 Security and Compliance Center lets you grant permissions to people who perform compliance tasks, such as device management, data loss prevention, eDiscovery, and retention.

The Microsoft 365 Security and Compliance Center includes the Service Assurance dashboard, which offers details on how Microsoft 365 implements security, privacy, and compliance controls; insights into implementation of encryption, incident management, tenant isolation, and data resiliency; and information on how you can leverage Microsoft 365 security controls and configurations to protect your data. To access the Service Assurance dashboard, go to the Microsoft 365 Security and Compliance Center, sign in with your Microsoft 365 account, and select Service Assurance on the left panel (see Figure 1).

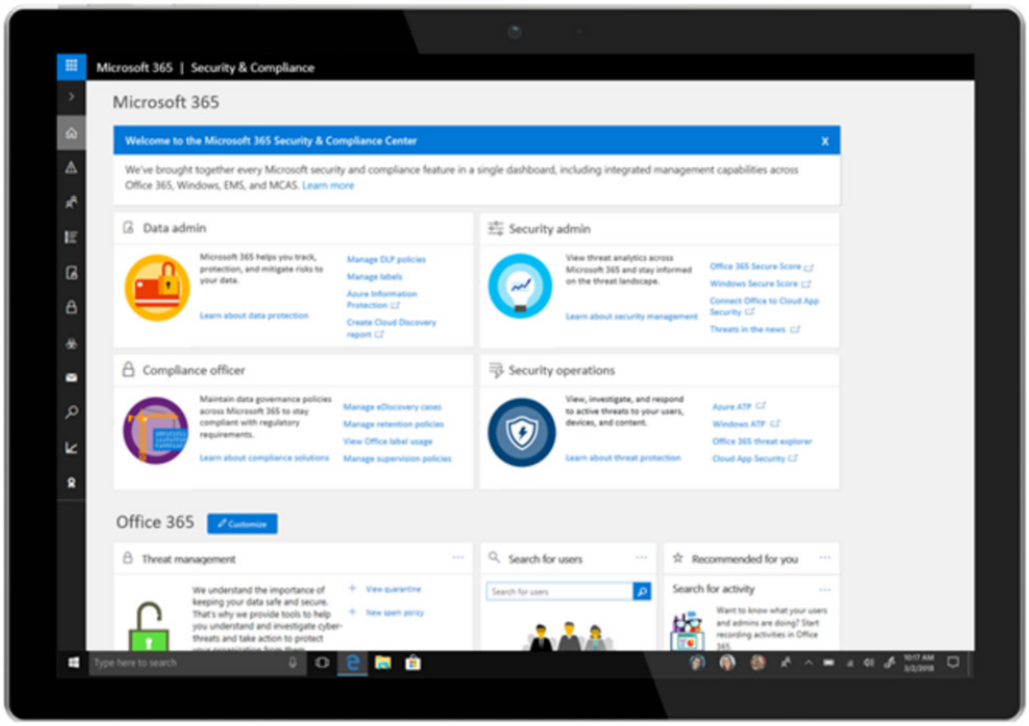

Figure 1. The Microsoft 365 Security and Compliance Center Service Assurance dashboard.

Advanced compliance and advanced data governance

Microsoft Advanced Data Governance offers proactive policy recommendations and automatic data classifications that help you take actions on data, such as retention and deletion, throughout the data lifecycle. You can enable default system alerts to identify data governance risks; for example, you could detect an employee deleting a massive volume of files.

You can create custom alerts by specifying alert-matching conditions and threshold. You also have the ability to apply compliance controls to on-premises data by filtering and migrating that data to Microsoft Office 365 using Microsoft Advanced Compliance plans.

How can I maintain my company compliance policy across all documents and devices?

Maintaining compliance and security at an organization in which employees bring their own devices (BYOD), use company-owned devices, or a combination of both is increasingly common. You must be able to apply both universal and specific policies to all devices that contain or create company data.

Microsoft Intune

Intune mobile device management (MDM) allows administrators to configure devices according to their company compliance standards. A device's compliance status is then used by conditional access policies to block or allow access to email and other corporate resources.

Mobile application management (MAM) through Intune App Protection allows administrators to enforce app-based compliance settings on apps that support application management, such as Office 365 apps.

Microsoft Cloud App Security

Microsoft Cloud App Security identifies which third-party cloud-based apps your employees are using. By monitoring for the risk inherent in unsanctioned apps at your organization, it allows you to restrict access from unsecured apps to your organization's network.

Microsoft 365 Security and Compliance Center

Microsoft 365 also offers MDM. By managing devices through the Microsoft 365 Security and Compliance Center, you can control iOS, Android, and Windows devices through Office 365 MDM, and specify a number of security and encryption settings.

Deployment tips from the experts

Start by enabling conditional access policies

Define risk policies by enabling conditional access in Azure AD to ensure that only authorized people see sensitive information and secure identities.

Use the Microsoft 365 Security and Compliance Center

Access the Service Assurance dashboard through the Microsoft 365 Security and Compliance Center, to manage Microsoft 365 security, privacy, and compliance controls, and devices.

Invoke confidentiality standards

Classify documents, invoke confidentiality standards, and enforce permissions with Azure Information Protection.

Plan for success with Microsoft FastTrack

FastTrack comes with your subscription at no additional charge. Whether you're planning your initial rollout, needing to onboard your product, or driving end-user adoption, FastTrack is your benefit service that is ready to assist you.

Get started at FastTrack for Microsoft 365.

Microsoft