Microsoft 365 Security Features Protect Business Data from Evolving Threats

Microsoft 365 includes a set of integrated tools designed to prevent, detect, and respond to attacks. By addressing endpoint security, identity and access management, email threats and cloud access security, Microsoft 365 security features deliver a unified approach to cyber security.

Microsoft security offerings continually evolve to keep pace with the threat landscape. Consequently, product naming and packaging changes from time to time. This post provides a basic outline of several key Microsoft 365 security offerings. To choose and implement the right tools for your business, we recommend working with a security services provider.

Microsoft Defender for Endpoint

With remote work and the ability to conduct business on a multitude of devices, the attack surface has broadened exponentially. Microsoft Defender for Endpoint empowers organizations to detect and protect each endpoint connecting to the network.

Previously called Defender Advanced Threat Protection, Microsoft Defender for Endpoint delivers a full-fledged endpoint detection and response (EDR) tool. Using machine learning, it inventories each endpoint, as well as the software and processes running on each device.

This helps to protect the network from attack through a breached endpoint. It also reduces the ability of threats to travel from one endpoint to another.

Microsoft Defender for Identity

Typically, attackers will attempt to compromise user accounts and then move laterally through the network. Once they elevate privileges to admin level, they can take over a domain and wreak havoc. Formerly known as Azure Advanced Threat Detection, Microsoft Defender for Identity helps to protect against both outside attacks and insider threats.

Like Microsoft Defender for Endpoint, Microsoft Defender for Identity uses machine learning to identify normal behavior for users and devices. With the baseline in place, it then monitors active directory (AD) accounts for suspicious activity.

Microsoft Defender for Office 365

Microsoft Defender for Office 365 addresses threats that arise through email and collaboration. Because email remains the delivery method of choice for malware, Microsoft Defender for Office 365 includes Safe Attachment and Safe Links protections. Additionally, it uses machine learning to identify phishing emails.

These tools provide protection over and above the Exchange Online Protection (EOP) that applies to all Exchange users. EOP includes spam and malware filtering, as well as the ability to quarantine suspicious emails.

Microsoft Cloud App Security

As a cloud access security broker (CASB), Microsoft Cloud App Security essentially acts as a firewall in the cloud. It identifies each cloud app and service being used in the organization, assigning a risk score to each. Additionally, using automated policies and processes, it detects and addresses risky behavior.

Start with These 5 Microsoft 365 Security Features

Microsoft 365 offers an array of security features, and organizations need to identify the right features and settings for their business needs. If your organization has not already done so, consider implementing these security controls available in Microsoft 365

- **Encryption** – Microsoft 365 includes multiple layers and types of data encryption. For instance, organizations can ensure encryption for files on a device, as well as files and emails in transit. Encryption for Teams protects chats and instant messages. And double key encryption capabilities offer additional protection for highly sensitive data.
- **Multi-factor authentication** – Most data breaches involve a compromised user account. Thus, implementing multi-factor authentication (MFA) provides essential protection. When organizations combine MFA with conditional access policies, they can implement granularity, meaning that users do not need to double authenticate every time.

- **Safe Attachments and Safe Links policies** – Safe attachments and safe links tools use a virtual environment to check attachments and links in real time. Policies allow organizations to apply these protections specifically to certain groups, users, or domains. They can be used in email, Microsoft Teams, and Office 365 apps.
- **Strengthen password policies** – Azure Active Directory provides the ability to implement core password protections. When a user changes their password, Azure AD checks the new password against a global banned password list. Additionally, organizations can define a custom list of banned passwords to add additional protection.

- **Content classification** – Using sensitivity labels and policies, organizations can apply appropriate protections to sensitive data. For instance, based on defined policies, they can enforce encryption or block certain types of data from being shared.

Microsoft 365 security features, while powerful, are best applied with expert cyber security experience. The cyber security experts at eMazzanti will help your organization choose and implement the right solutions for your business needs.