Barracuda
Your business, secured.

Is Microsoft email security good enough?

The top 7 gaps in Microsoft 365 email security

Many organizations ask themselves if native email security in Exchange Online Protection or Microsoft Defender for Office 365 provides adequate protections to safeguard their users, data, and communications. Unfortunately, protection varies depending on each user's license, and although Microsoft is continuously improving its email security capabilities, gaps remain. As a result, IT security professionals must determine if Microsoft's native security meets their business requirements. We have identified seven capabilities where Microsoft security may fall short and be insufficient.

01 | Threat detection efficacy

Microsoft 365 alone does not provide adequate protection against advanced email attacks blocked by AI-powered Barracuda Impersonation Protection. To measure Barracuda's detection efficacy compared to Microsoft, we have processed more than 10 billion emails delivered to Microsoft accounts across all license types.

Microsoft limitations

Microsoft 365 has an average miss rate of 47% across advanced email attacks, such as conversation hijacking, phishing, and impersonations. For more sophisticated attacks, such as conversation hijacking attacks, Microsoft's miss rate jumps to 88%. Microsoft 365's native security features are insufficient for organizations to protect their users from today's complex threats.

4.2M
ATTACKS BARRACUDA BLOCKED

1.99M
ATTACKS MICROSOFT MISSED

47%
MICROSOFT MISS RATE

How Barracuda can help

Barracuda delivers comprehensive security for Microsoft 365 with effective AI-enabled protection against phishing, business email compromise, and account takeover. With a powerful AI engine that uses the metadata of historical emails from internal and external senders combined with natural language processing, Barracuda's Impersonation Protection enhances the security of Microsoft 365 users with superior detection efficacy.

02 | Microsoft 365 data backup

Microsoft has taken extensive measures to reduce the risk of data loss due to a fault on its behalf. However, they cannot protect you from your users' actions or threats beyond their control. These risks represent the majority of typical data loss events. Therefore, Microsoft recommends you regularly back up your data or use third-party backup apps and services.

Microsoft limitations

According to Microsoft's Shared Responsibility Model, your organization remains ultimately responsible for your data protection. Determining if a file, folder, email, or SharePoint site is natively recoverable can be challenging. Different assets have different limitations like file type restrictions; recovery point options; retention periods; default settings or configurable maximums; recovery from folder navigation or e-discovery search; or if the user, administrator, or Microsoft themselves must perform the recovery.

How Barracuda can help

Barracuda Cloud-to-Cloud Backup allows customers to back up critical data daily within Exchange Online, OneDrive, Teams, OneNote, and SharePoint directly from the cloud to the cloud, giving you instant scalability and nothing to manage. In addition, backups are inherently isolated from Microsoft's production networks, and multiple secure copies of the data are maintained in different locations.

03 | Zero-day attachment sandboxing

Microsoft Safe Attachments provides an additional layer of protection for email attachments that have already been scanned by the anti-malware protection in EOP and is included in MSDO Plan 1 and 2, Business Premium, and E5. Specifically, Safe Attachments detonates attachments in a virtual environment to detect zero-day threats.

Microsoft limitations

Safe Attachments is not included with EOP, meaning it is not included with Business Basic, Business Standard, E1, or E3. It is included in Business Premium and E5. Shared mailboxes require a license to take advantage of Safe Attachments. Microsoft uses a virtualized environment based on MS hypervisor technology to scan attachments, which some types of malware can evade.

How Barracuda can help

Barracuda Email Gateway Defense leverages multiple antivirus engines to block known malware. Unknown (zero-day/zero-hour) malware is identified by multilayered Advanced Threat Protection that leverages AI, heuristics, behavioral analysis, and a dynamic sandbox. Unlike traditional sandboxes that rely on a hypervisor infrastructure, Barracuda dynamically emulates different platforms at every execution. Shared mailboxes do not require a license to take advantage of Advanced Threat Protection.

04 | Time-of-click URL sandboxing

Microsoft Safe Links helps protect against malicious phishing links and other attacks and is included with MSDO Plan 1 and 2, Business Premium, and E5. Links without a valid reputation are detonated asynchronously in the background. It also adds time-of-click protection from malicious URLs by providing URL scanning and rewriting for inbound messages. When enabled, URLs are scanned before delivery, regardless of if the URLs are rewritten.

Microsoft limitations

Safe Links is not included with EOP, meaning it is not included with Business Basic, Business Standard, E1, or E3. It is included in Business Premium and E5 but is disabled by default. There are several limitations in Safe Links as it relates to hypervisor-aware malware, end-user override, unsupported transport protocols, unsupported public folders, and lack of "in the moment" security awareness training.

How Barracuda can help

Barracuda Link Protection is included with all Email Protection plans, is enabled by default, and requires minimal to no configuration. End users cannot override the Link Protection warning screen, and they are directed to security awareness training through integration with Barracuda Security Awareness Training. Hypervisor-aware malware is also less likely to evade Barracuda's dynamic sandbox, and FTP/S is supported in addition to FTP. Mail-enabled public folders are supported, and shared mailboxes do not require Barracuda Link Protection licenses.

05 | Impersonation Protection

Impersonation Protection in MS Defender for Office 365 (MSDO) Plan 1 and 2, Business Premium (BP), and E5 is artificial intelligence (AI) that determines email patterns with users' frequent contacts to distinguish between messages from legitimate and impersonated senders.

Microsoft limitations

Impersonation Protection (IP) is not included with Exchange Online Protection (EOP), meaning it is not included with Business Basic, Business Standard, E1, or E3. It is included in Business Premium and E5 but disabled by default. There are several limitations related to IP depending on whether the sender and recipient have or haven't communicated previously, and it cannot protect more than 350 users or 50 domains from being impersonated. False positives frequently result from senders with common names, personal accounts, internal vendor and partner accounts, and former employees.

How Barracuda can help

Barracuda Impersonation Protection is included in all plans and works out of the box with no rules or policies to specify, enable, or configure and without limiting the number of sender addresses, users, or domains.

06 | Email archiving

A Microsoft Archive is a specialized mailbox that appears alongside the user's primary mailbox in Outlook. Retention policies can automatically move items to the archive to shrink the mailbox and improve its performance.

Microsoft limitations

Archives for all standard and shared mailboxes are limited to 50GB for Business Basic, Standard, and E1. Archives start at 100GB for Business Premium and E3/E5. By default, the archive's content is not

immutable, and only mailboxes licensed and enabled for Litigation Hold can retain deleted messages beyond a 14-day window. Unlicensed user archives exceeding 50GB or those placed in Litigation Hold require a paid Exchange Online Plan 1 license and Archiving add-on license or Exchange Online Plan 2. 100GB archives are sometimes still advertised as “unlimited “ but actually cannot exceed 1.5TB after enabling expansion.

For 100GB mailboxes, the auto-expansion option enables an artificial maximum of 1.5TB. Microsoft Purview automatically determines which archive folders get moved to each new 100GB increment, how many subfolders to create, and which items are distributed to these folders to synthetically overcome the 100GB initial maximum. There are many limitations, including a maximum daily growth rate, import size and file type restrictions, search restrictions, appropriate use restrictions, when the archive can be increased, the time delay for each increase, if the folders can be deleted after an expansion, if folders can be recovered after deletion, read/unread inaccuracy, and other limitations with hybrid on-premises/cloud environments.

How Barracuda can help

Barracuda Cloud Archive Service provides true unlimited storage on a simple and predictable per-user basis. Archive data is immutable and stored outside of production data. There are no intermediate storage segments to be created at 100GB intervals. Growth is not throttled. There are no charges to retain data in inactive mailboxes, regardless of size or the requirement for a Litigation Hold.

07 | Conditional Access

Microsoft offers user-based Conditional Access in Azure Active Directory Premium P1 and P2. Conditional Access brings together various identity-driven signals to make decisions and enforce organizational policies.

Microsoft limitations

Conditional Access is only included in Business Premium and Microsoft 365 E3 and E5; it’s not included in Business Basic, Standard, and Office E1/E3/E5. Native passwordless certificate-based authentication is unavailable. Conditional Access policies are enforced after first-factor authentication is successful. Organizations must use Intune to check device identity and security posture during authentication, but end users (especially BYOD) and contractors don’t want to enroll in mobile device management (MDM) systems like Intune.

How Barracuda can help

Barracuda Zero Trust Access enhances your multifactor authentication (MFA) implementation using certificate-based authentication in Barracuda CloudGen Access. CloudGen Access checks the user and device identity pair before the user authenticates or obtains authorization for apps or internal resources.

Overcome native Microsoft 365 email security limitations by using Barracuda Email Protection.

Barracuda
Your business, secured.