# ENHANCING EMAIL SECURITY IN MICROSOFT 365: OVERCOMING LIMITATIONS.

When it comes to cybersecurity, businesses relying solely on the built-in security tools in Microsoft 365 may be exposing themselves to significant risks. While Microsoft's cloud-based email and collaboration platform offers native cybersecurity capabilities, experts warn that these tools may not be sufficient in safeguarding against sophisticated attacks. In this article, we will explore the key reasons why enhancing email security in Microsoft 365 is overcoming these limitations and protecting your business from cyber threats.

## Popular Target for Cyber Criminals.

Given the extensive adoption of Microsoft 365 worldwide, it comes as no surprise that cyber criminals frequently target this platform. Numerous successful companies, including global enterprises, rely on Microsoft 365 for their daily operations. In fact, Microsoft had 300 million monthly active users on its messaging app Teams alone in March 2023. Unfortunately, this popularity makes Microsoft 365 an attractive target for malicious actors seeking to exploit security vulnerabilities.

Research from Proofpoint's State of the Phish report reveals the extent of cyber criminals' focus on Microsoft. In 2022, Microsoft topped the list as the most abused brand, with over 30 million messages utilizing Microsoft branding or featuring Microsoft products. Attackers can create their own Microsoft 365 tenant to test and refine malicious emails, potentially compromising organizations that rely on the same native security controls.

## Evolving Sophistication of Cyber Threats.

As the cybersecurity industry evolves, cyber criminals continuously refine their tactics to stay one step ahead. The ever-changing threat landscape poses significant challenges, with threats becoming increasingly sophisticated and difficult to detect.

Advanced phishing attacks, for example, have surpassed traditional methods and now employ intricate techniques to bypass security measures. Cyber criminals may gain access to multi-factor authentication (MFA) tokens, putting the entire Microsoft 365 cloud environment at risk. Moreover, business email compromise (BEC) attacks exploit social engineering, making them challenging to identify

through native Microsoft email controls. Telephone-Oriented Attack Delivery (TOAD) attacks, relying on human vulnerability, pose further complications due to their text-based nature.

## Addressing Cybersecurity Gaps.

While Microsoft 365 offers email hygiene capabilities through Exchange Online Protection, certain security aspects remain unaddressed. Outbound brand protection, for instance, is not included in the default package. Microsoft provides additional security upgrades like Microsoft Defender for Office 365, but relying solely on these tools may not suffice in today's threat landscape.

Augmenting Microsoft native security is essential to fill critical gaps. Three key areas that require attention include:

a) Security awareness: Educating employees to recognize and report fraud is crucial. Simplified reporting tools that work across all devices can empower users to alert the security team promptly.
b) Automated remediation tools: Responding to threats swiftly is vital in a breach situation. Automated remediation enables quick investigation and eliminates time-consuming manual tasks, enhancing the efficiency of security teams.
c) Supplier account compromise: Often, security teams lack visibility into the third-party accounts their organization interacts with. Proactively detecting compromised supplier accounts is crucial to maintaining a secure environment.

In today's increasingly complex threat landscape, relying solely on Microsoft 365 native email security may not be enough to combat against cyber-attacks. Attackers frequently target Microsoft 365 due to its widespread adoption. Additionally, the evolving sophistication of cyber threats necessitates a proactive approach to address vulnerabilities and gaps in native security. By adopting a layered and integrated security strategy, businesses can enhance their protection and mitigate the risks associated with relying solely on Microsoft 365 native email security.

Source