MICROSOFT 365 & TOPSEC

Why additional security layers are vital when you have moved or are thinking about moving your email to the cloud.

M365 is the most adopted cloud email and office application solution available on the market today. Most IT admins say the reason they made the move to Office 365 is because "they no longer have the time to spend administering their on-premises exchange" However, most overestimate the security capabilities of MS365.

MS365 security threats

From within MS365

It's a well-known fact within the cyber security industry that a lot of threats originate from email accounts within MS365's own environment.

Inbound email

MS365 defaults for connection time checks such as SPF, DKIM and DMARC are non-secure. It has other insecure default behaviors for legacy compatibility reasons and because they must take a one size fits all approach. For example, MS365 will accept emails from non-existent domain names and domains which do not represent an FQDN.

Configuration

Configuration can be a big issue when the person responsible for setting up MS365 fails to configure it correctly, failure of correct provisioning can leave you vulnerable to many major security threats.

One size fits all approach

MS365 is commonly described as a one size fits all type of solution with regards to security. This is a multi-tenant environment whose features do not allow for flexibility when it comes to unique targeted email borne threats against end users.

Source Links

URLs that are found to be bad on arrival (first Topsec scan): 20% of total caught. URLs that are found to be bad on Topsec rescans: 80% of total caught.

What this means is that MS is missing up to 80% of these malicious links and with something like our Inbox Protect Service this serious threat is ameliorated as we rescan for up to 5 days.

- ## Redirect Links:

Bad redirects on first Topsec scan: 31% of total caught. Bad redirects on Topsec rescans: 69% of total caught.

This demonstrates the need to have checks performed after the email arrives. Rescans can occur the day the email arrives and up to 5 days after delivery.

- ## The accessibility of MS365 presents another problem.

  - Predictable circumvention. Any hacker in the world can create an MS365 account to figure out how to circumvent their security.
  - ATP is Version 1. Introduced in 2015, its features and functionality are relatively immature when compared to solutions established security companies like Topsec have been honing for decades.
  - Opaque reporting and forensics functionality. Visibility and control in the Microsoft security interface is limited. This makes it difficult to deep-dive into a specific incident, find the root cause, which users are impacted, if a user account was compromised, if data was lost, etc. At the same time, ATP limits reporting based on time constraints. For example, it takes a few hours to return a mail protection detail reports for messages older than 7 days. For data older than 90 days, reports are inaccessible.
  - Co-Pilot has recently opened a new raft of targeted AI based Spear Phishing scenarios because of its ability to analyse and 'understand' copious amounts of email and again MS has no defense against itself.

- ## It's not a security license

MS365's E3 and E5 etc. licenses are Office suite licenses that include security elements but are not fully focused on email security and threat prevention.

Why do you need additional layer of security?

Protection from hackers

MS365 is commonly used by hackers to simulate their attacks, so it is easy for attackers to test their methods until they can bypass MS365's security filters.

Security focus

Our mission statement is to fully focus on protecting the communication of our end users. MS365 is a multifunctional product with no particular focus on email security.

Prevents human errors – Outbound Monitoring

Outbound email is limited to policy checks and rules (if they are setup) and DKIM signing. The main reason for outbound use is to take advantage of our IP reputation. We do not scan, spam check, or look for trends on outbound email.

What TOPSEC do for you?

Queue your emails

In the event of an MS365 outage Topsec will queue your company's emails, meaning emails will not be bounced or lost during the outage. We will then resend the emails once a connection to MS365 can be re- established.

Unique rules

MS365 must implement common rule sets to cater to everyone on their cloud solution. Topsec can apply a unique and dynamic rule set depending on the client's requirement.

Support

Topsec will provide monitored and personalized support 365/24/7. We will support, monitor, inform and advise your company personally about any changes to your user accounts.

Every email goes through the same checks

Topsec treats all emails from MS365 as aggressively as they would any other email, MS365 treats emails from their own platform more favorably.

With the world's most talented engineers and an infinite budget, why does Microsoft fall victim to phishing attacks that get past ATP and Exchange Online Protection (EOP) for Office 365? (25% of all Phishing Attacks get through MS 365) and 80% of malicious links are poisoned post-delivery.

The reasons have nothing to do with any specific failure by Microsoft, but much to do with the widespread adoption of MS365 as an enterprise collaboration suite. Because MS365 is the most used platform, it is also the most attacked. This creates strengths and weaknesses in ATP.

Organizations should use a third-party email security layer sitting in front of and inside of MS365 that has more tailored AI, security that is invisible to hackers, real-time retrospective remediation and flexible and responsive reporting, control, and support.

A layered security module is imperative when moving your email to a multi-tenant cloud environment like MS365.