Prevention First

# Prevent Email Threats

## Why Microsoft 365 and Google Workspace Native Protection is Not Enough

ESET®

Digital Security
**Progress. Protected.**

# Email Protection Gaps

Organizations are certain to be counted among the 3 billion users of Google Workspace (including 1.8 billion active Gmail users), 400 million Outlook users, or the 320 million users of the Microsoft Teams collaboration app, all of which are essential digital business tools.

After their successful deployment and setup of some security rules, in an ideal world, corporate teams could focus on business-critical tasks while working within secure collaboration environments.

That isn't necessarily the case. There are **numerous threat actors abusing legitimate cloud apps**, but this problem has a solution. IT managers need to implement additional layers of security.

With the right tools, admins can minimize the attack surface vectoring from their cloud services, taking a prevention-first approach that protects their corporate collaboration apps and email from threats before they execute.

Among the biggest challenges businesses face in the cloud application security space are mostly email related threats:

### PHISHING AND SPEAR-PHISHING

Attackers use innovative methods such as using QR codes or homoglyphs to trick people into scanning and/or clicking on seemingly legitimate links.

### IMPERSONATION AND EMAIL SPOOFING / BUSINESS EMAIL COMPROMISE

Emails trying to trick people into believing that a legitimate sender is communicating with them are getting better every day especially with the increasing use of AI technologies.

### HUMAN FACTOR

Employees make mistakes, rendering email gateways especially attractive to attackers. Cybersecurity trainings are still relevant as the human factor remains the weakest link in the chain and no technology can work 100% if it is not used correctly.

### ZERO-DAY THREATS

AI is also making it easier for adversaries to create new or never-before-seen threats.

# Email: Cybercriminals' Favorite Playground

Email remains the leading vector for cyber threats. Over the past several years, ESET has detected and blocked millions of threats that bypassed the native protection of both Microsoft 365 and the Google Workspace cloud office suit.

**The majority of those blocked threats were phishing and spam messages**. According to Verizon, the median time for users to fall for phishing emails was less than 60 seconds. Their 2024 Data Breach Investigations Report claims that Pretexting is one of the most used attack techniques. Its numbers almost doubled from 2022 to 2023 and now Pretexting is involved in around 20% of all financially motivated attacks. The majority of Pretexting incidents resulted in Business Email Compromise (BEC) with the median transaction amount around $50,000, according to FBI IC3 dataset. The latest data show that there is no end to this trend.

According to the ESET H2 2024 Threat Report, spam detection increased by 19 percent, and malicious HTML files sending victims to phishing websites (HTML/Phishing.Agent trojan) are still by far the most prevalent email threat. Overall, these **email attacks comprise almost a quarter (23.8 percent) of all cyber-threats** detected by ESET. Other cloud threats detected by ESET telemetry include various types of malware, such as backdoors, spyware, infostealers, and downloaders.

# Not as Safe as You Think

Although both Microsoft and Google have incorporated high-tech security directly into their cloud applications, both of which are protected and regularly updated, it does not mean that they are immune to any and all threats out there.

Real-life examples show that legitimate cloud apps and services can be abused to deliver malware, obfuscate malicious processes, and enable remote access to corporate devices:

- ESET researchers noticed new phishing email campaigns by an unknown threat actor targeting businesses in European countries in recent years. The emails contained malicious attachments enhanced by AceCryptor, a cryptor-as-a-service malware designed to hide other malware from cybersecurity tools. If successful, attackers could deploy Rescoms' (also known as Remcos) remote access tool and spy on their victims.

- In the latter half of 2024, **Formbook, an infostealer** first discovered in 2016, saw a significant resurgence, with detections increasing by over 200%. This malware collects, among other things, clipboard data, keystrokes, screenshots, and cached browser data. It is a malware-as-a-service (MaaS) solution, sold on underground forums, that spreads via malicious attachments in phishing emails. ESET products protected nearly 34,000 users from this malware primarily in Eastern and Central Europe, as well as Japan, Canada, and Spain.

- Fortunately, in most cases, cybersecurity professionals discover vulnerabilities sooner than threat actors. In June 2023, UK-based security services provider Jumpsec's Red Team discovered and then demonstrated a way to deliver malware using Microsoft Teams via an account outside the target organization. Jumpsec's team **bypassed built-in protection** and was able to fool the system into thinking that an external user was, in fact, an internal account.

ESET, a leading cybersecurity provider, employs ESET Cloud Office Security to secure cloud-based collaboration environments.

This advanced solution enhances the built-in security features of Microsoft 365 and Google Workspace by performing scans after the native cloud office products have marked emails or files as "safe".

**The following data* from ESET show how many threats made it through the native defenses**.

**920,000**

email threats detected

**813,000**

phishing emails blocked

**110,000**

non-email threats originated from OneDrive, SharePoint, and Google Drive

**75,820,000**

spam emails captured

*2024 data

# How to Improve Cloud Defenses

It's clear that alone, native security in cloud applications isn't enough. To minimize this growing attack surface, and prevent and mitigate attacks before they can do any harm, companies should consider enhancing Microsoft or Google's built-in controls with **additional layers of protection:**

### Spam filtering

Spam messages accounted for over 46.8 percent of the 362 billion emails sent and received daily around the world in 2024. With the right filtering solution, companies can save significant employee time and avoid troubles with malicious spam.

### Anti-phishing

In 2024, phishing was identified as the initial attack vector in 22% of cyberattacks faced by U.S. companies. Having an automated tool that recognizes phishing links attached to emails is absolutely critical.

### Anti-malware scanning

A good cloud security solution should automatically scan for any new and changed files in shared storage to prevent malware from executing or spreading.

### Behavioral analysis and sandbox environment

As new threats constantly emerge, automated cybersecurity tools need to be prepared for never-before-seen attacks. This can be done with in-depth behavioral analysis of suspicious samples in a secure isolated sandbox environment.

### Anti-spoofing and rule engine

Adverse emails masking their own identity and impersonating a legitimate sender must be stopped. With this control, only emails appearing to come from trusted sources are actually legitimate and allowed.

### Homoglyph protection

Attackers use look-alike characters to create deceptive email addresses or domains that appear legitimate. Detecting and blocking these homoglyph attacks helps prevent spear-phishing and other malicious activities, ensuring your organization's communications remain secure.

### Email Clawback

This feature enhances security by allowing admins to quarantine emails directly from the scan log. By doing so, the email moves out of the recipient's inbox, enabling immediate action in case of a suspected attack like spear-phishing.

# How ESET Helps

Having so many tools at your disposal and managing a robust security system may look like any other challenge, however, fielding additional security doesn't necessarily have to increase the complexity of an IT admin's job.

**ESET Cloud Office Security provides advanced preventive protection for Microsoft 365 and Google Workspace apps** with all the above-mentioned features. It improves an organization's security posture with advanced threat protection, as well as visibility and control of cloud-based email, file sharing, and both data and collaboration tools. In addition to streamlined operations and enhanced security, ESET Cloud Office Security contributes to **reducing complexity by centralizing and automating routine processes** such as:

- New users within the business environment do not need to be added manually by an IT admin in a console but are automatically protected after their account is created.
- IT admins can set up notification intervals to avoid alert fatigue while also ensuring that they receive the most important warnings.
- Suspicious files can be easily managed in one centralized quarantine with the possibility to release/delete them or further investigate them separately if needed.
- The solution allows multi-tenant management for tens of thousands of users covering accounts created within the two most used platforms, Microsoft 365 and Google Workspace.

With a focus on prevention and the protection of end users and their devices, ESET Cloud Office Security ensures increased levels of an organization's threat protection by minimizing cloud related attack surfaces, thus easing the burden on IT admins with a user-friendly cloud management console.

As a stand-alone solution, or as part of the ESET PROTECT Platform, ESET Cloud Office Security helps protect organizations against infections, minimizes work disruptions due to unsolicited messages, and helps prevent targeted attacks as well as never-before-seen types or threats, especially ransomware.

## INTEGRATION

Lastly, ESET Cloud Office Security boasts free integration with **ESET LiveGuard Advanced**, a cloud-based technology that uses advanced scanning, cutting-edge AI, cloud sandboxing, and in-depth behavioral analysis to prevent targeted attacks as well as new or unknown threats, including ransomware.

# This is ESET

## **Proactive defense.** Our business is to minimize the attack surface.

Stay one step ahead of known and emerging cyber threats with our **prevention-first approach**, **powered by AI and human expertise**.

Experience best-in-class protection, thanks to our in-house global **cyber threat intelligence**, compiled and examined for over 30 years, which drives our extensive R&D network, led by **industry-acclaimed researchers**. ESET protects your business so it can unlock the full potential of technology.

**BOOK A DEMO**

**Multilayered, prevention-first**

**Cutting-edge AI meets human expertise**

**World-renowned threat intelligence**

**Hyperlocal, personalized support**

Digital Security
**Progress. Protected.**