Prevention First

Cloud security: Native app protection is not an end but rather a beginning

Digital Security
Progress. Protected.

IT admins are certain to be counted among the 3 billion users of Google Workspace, or the 320 million users of the Microsoft Teams collaboration app. After successful deployment and the setup of some security rules, in an ideal world, they can free up time to do other critical tasks while corporate teams are working within secure collaboration environments.

Those tech giants have incorporated high-tech security directly into their cloud applications, so there is nothing to worry about, right? Well, these widely used cloud applications are protected and regularly updated, but that does not mean that they are immune to any and all threats out there.

There are numerous cases of **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.

Growing appetite

Companies around the world are constantly seeking ways to operate more efficiently, and independently of location, the revenue in the public cloud market more than doubled between 2019 and 2023 and is projected to reach $690.3 billion in 2024.

However, as the market grows, so does the appetite of threat actors. Between June 2021 and July 2023, **ESET detected and blocked millions of threats that would have otherwise bypassed the native protection** of Microsoft 365 and Google Workspace cloud office suites.

The majority of those blocked threats were phishing and spam messages; the latest data show that there is no end to this trend. According to the ESET H2 2023 Threat Report, spam has increased by 6 percent, and malicious HTML files sending victims to phishing websites (HTML/Phishing.Agent trojan) are still by far the most detected email threat.

Overall, these email attacks comprise almost a quarter (23.4 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.

ESET DETECTIONS IN NUMBERS

Scanning takes place after the native cloud office products mark the email or file as "safe". Without ESET Cloud Office Security, these emails and files would likely make their way into users' inboxes and online collaboration tools.

1M+
malware threats

500k+
phishing emails

30M+
spam emails

1000+
never-before-seen detections by ESET LiveGuard Advanced

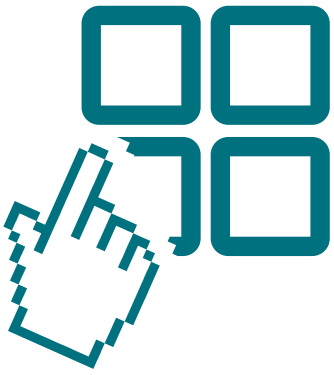
Your apps are not so secure

Real-life examples show that legitimate cloud apps and services can be abused to deliver malware, obfuscation of malicious processes, remote access to corporate devices — you name it.

In H2 2023, ESET researchers noticed new phishing email campaigns of an unknown threat actor targeting businesses in European countries. **Emails contained malicious attachments** enhanced by AceCryptor, a cryptor-as-a-service malware that is designed to hide other malware from cybersecurity tools. If successful, attackers could deploy Rescoms' (also known as Remcos) remote access tool and spy upon their victims.

Throughout 2022, a cyberespionage group, OilRig, actively developed and used a series of downloaders that abused the Application Programming Interface (API) of legitimate cloud services such as Microsoft Graph OneDrive, Microsoft Graph Outlook, and Microsoft Office EWS to hide its malicious communication. For example, **they abused email accounts to create draft messages with hidden commands for malware** already infesting devices, notes another ESET research blog.

Luckily, sometimes cybersecurity professionals find vulnerabilities sooner than threat actors. In June 2023, UK-based security services provider Jumpsec's Red Team discovered an easy way to deliver malware using Microsoft Teams via an account outside the target organization. Red Team's members **bypassed built-in protection and were able to fool the system** into thinking that an external user was, in fact, an internal account.



Additional security

Via the cases described above, it is clear that native security in cloud applications is not enough. To minimize this growing attack surface, **companies can enhance Microsoft or Google's built-in controls** with additional layers of protection for cloud-hosted email, collaboration, and storage. This extra protection should also aim for prevention, mitigating attacks before they can do any harm.

How to improve cloud defenses:

- **Spam filtering** – Spam messages accounted for over 45 percent of 333 billion emails sent and received daily around the world in 2022. With the right filtering solution, companies can save a lot of employees' time and avoid troubles with malicious spam.
- **Anti-phishing** – One in four U.S. companies that faced a cyberattack in 2022 noticed that the initial vector was phishing. Having an automated tool that recognizes phishing links attached to emails could come in handy.
- **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** – In the fast-evolving world of IT, new threats emerge constantly, and 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.

Single platform

Having so many tools at your disposal may look like another challenge – how can you manage such a robust security system?

In fact, the number of alerts coming to IT teams daily already plays on admins' nerves. Security Operation Center (SOC) team members are only getting to half of the alerts that they're supposed to review within a typical workday, according to March 2023 study commissioned by IBM and completed by Morning Consult.

However, a proper solution can actually **reduce the complexity of businesses' cybersecurity if some processes are automated**. Here are some examples:

- 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 be immediately notified about new alerts instead of constantly checking the situation in a dashboard.
- Suspicious quarantined files can be easily managed in one place with a possibility to release/delete them or further investigate them separately if needed.
- Solutions allow multi-tenant management with tens of thousands of users covering accounts created within the two most used platforms, Microsoft 365 and Google Workspace.

How ESET helps

Additional security doesn't necessarily have to increase the complexity of an IT admin's job. As a global leader in digital security for more than 30 years, ESET recognizes the needs of IT admins and managers using cloud services.

ESET Cloud Office Security provides advanced protection for Microsoft 365 and Google Workspace apps with all the above-mentioned features. Businesses can thus adopt a prevention-first strategy and minimize cloud-related attack surfaces while easing theburden on IT admins with a user-friendly cloud management console.

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 researcher**s. ESET protects your business so it can unlock the full potential of technology.

EXPLORE

ESET®

Digital Security
Progress. Protected.