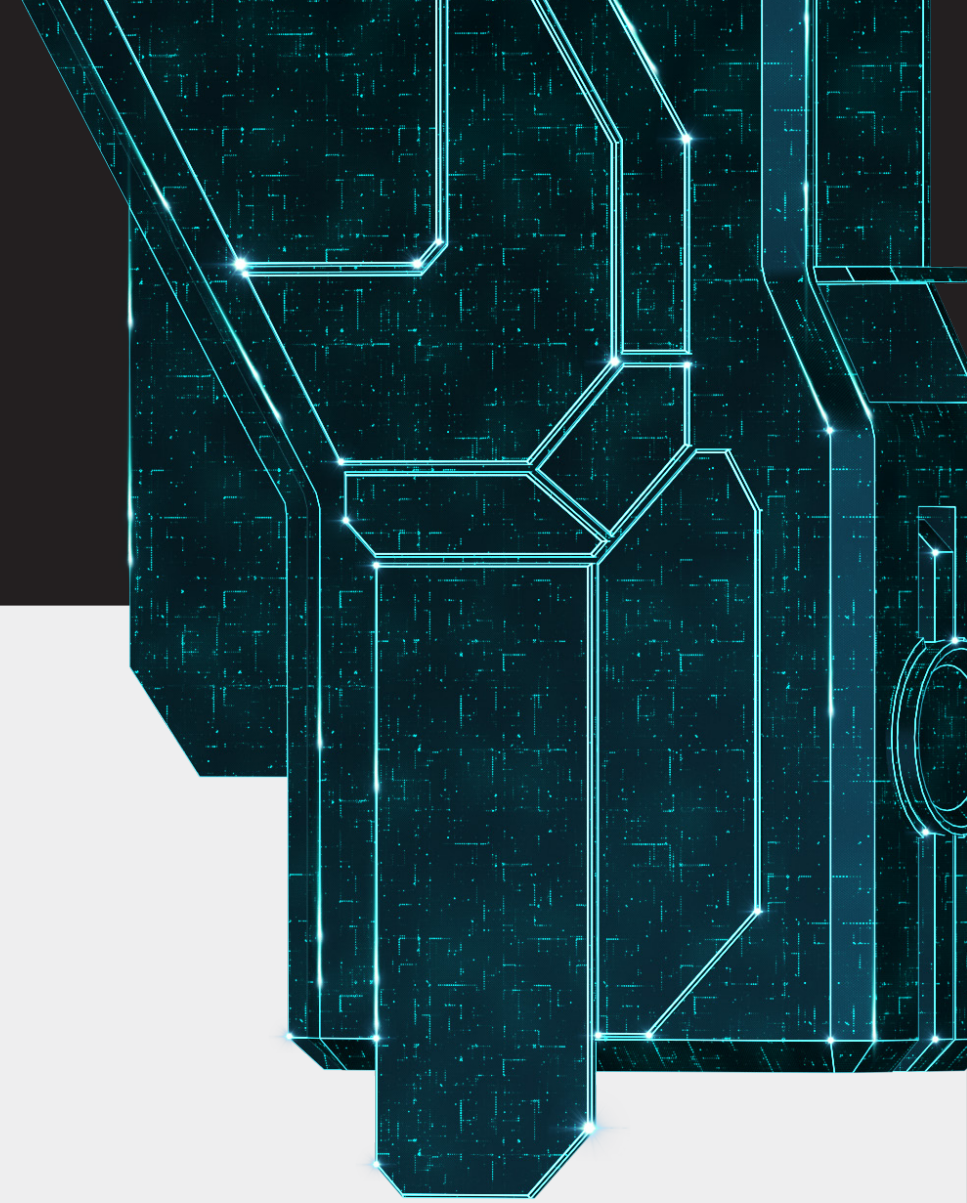
CYBERSECURITY
EXPERTS ON YOUR SIDE



CLOUD OFFICE SECURITY

An elevated security approach for Microsoft 365 applications

Organizations using Microsoft 365 need an added layer of cost-effective, risk-mitigating protection beyond Microsoft's native security capabilities for spam filtering, anti-malware and anti-phishing.

Challenges for Microsoft 365 security

With over 250 million daily users, Microsoft 365 is one of the largest collaboration tools in use today. This also makes its applications some of the most targetable for cyberattacks like spam, malware and phishing.

Protecting email communication, file sharing and collaboration is crucial for businesses. Microsoft 365's combination of email, file storage and popular applications including OneDrive, SharePoint, Exchange Online and Teams carries a wealth of business data making it a top target for cybercriminals.

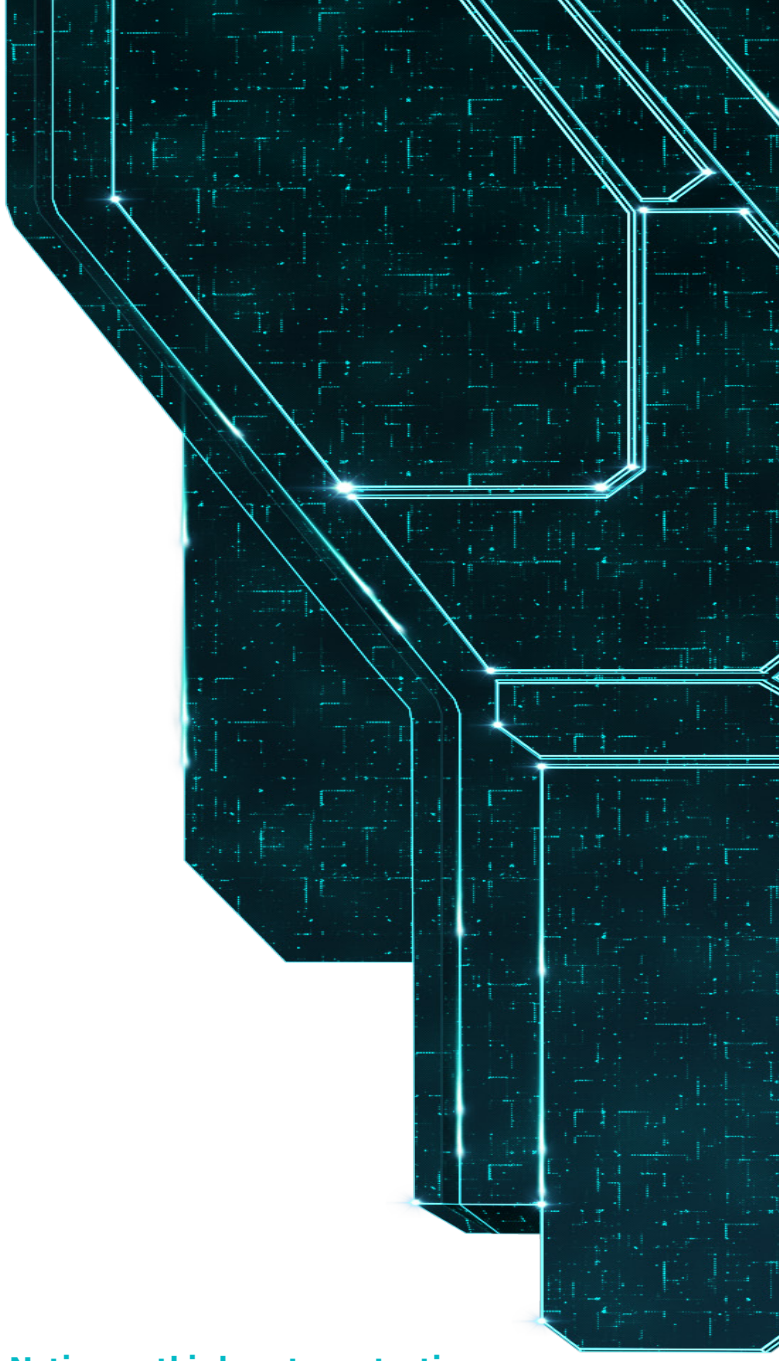
Cyberattacks on Microsoft 365 applications are constant and becoming increasingly sophisticated to exploit vulnerabilities and identify weaknesses.

While Microsoft 365 does offer some security, it might not be enough to ensure your organization's overall protection from spam, malware and phishing. A recent SE Labs report indicates that Microsoft Office 365 Advanced Threat Protection only offers 23% protection on phishing emails and a total protection rating of 62%. Gartner projected in 2020 over 50% of organizations adopting Microsoft 365 will rely on third-party tools to fill gaps in security (How to Enhance the Security of Office 365). As remote workforces continue to operate outside of traditional office spaces, this percentage is sure to increase.

IT organizations concerned about security, compliance and data privacy with Microsoft 365 applications require advanced protection features like anti-spam, anti-malware and anti-phishing for better security and end-user experience in Exchange Online, OneDrive, SharePoint and Teams.

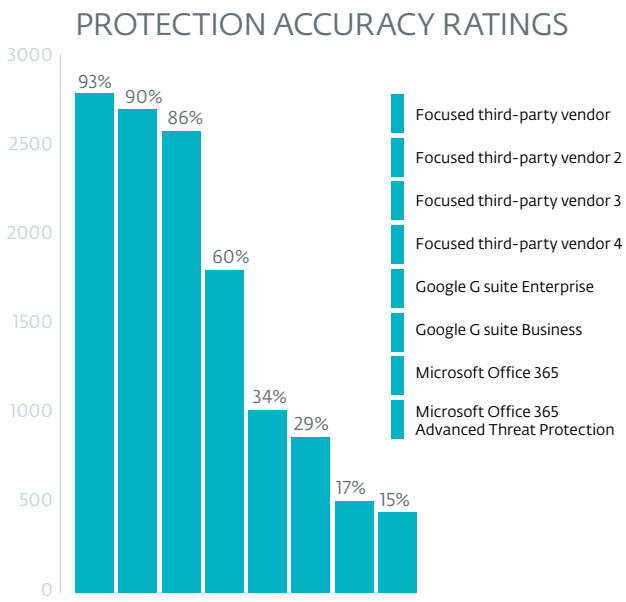
What to consider while evaluating solutions

Determining the cost-effectiveness of added protection for Microsoft 365 applications and focusing on flexibility for licensing options is well worth your time. Identifying solutions that are delivered as a service and provide a dedicated, cloud-based management console you can access from anywhere will help ensure you're getting a good value. A dashboard that provides complete control and visibility, includes automated notification features, and works seamlessly across devices using Microsoft 365 will reduce time demands on IT admins and effectively reduce overall costs.



Native vs. third-party protection

- Third-party protection of Office 365 is commonly requested and offered
- Native Microsoft protection is often not sufficient



Source: SE Labs report: "Email security services protection Jan-Mar 2020"

ESET Cloud Office Security provides elevated protection

Advanced preventive protection from ESET Cloud Office Security (ECOS) offers multiple enhancements compared to Microsoft's native security capabilities. ECOS improves an organization's security framework with advanced threat protection, as well as visibility and control of cloud-based email, file sharing, data and collaboration tools. With a focus on protecting end users and their devices, ESET Cloud Office Security ensures increased levels of threat protection for your organization—whether users are on-premises or working remotely.

By utilizing an enhanced anti-spam engine as an essential component, you can filter all spam emails and keep user mailboxes free of unsolicited or undesired messages, mitigating the adverse effects of unsolicited emails and helping prevent external emails that lead to targeted attacks.

With robust anti-malware scanning on all incoming emails and attachments, as well as all new and changed files in OneDrive, you can keep users' mailboxes free from malware and prevent any spread through cloud storage across multiple devices.

Advanced anti-phishing protection for Exchange Online searches messages to identify links (URLs) and analyzes them against a constantly updated database of known phishing links to prevent users from accessing sites and email messages containing links that lead to these web pages.

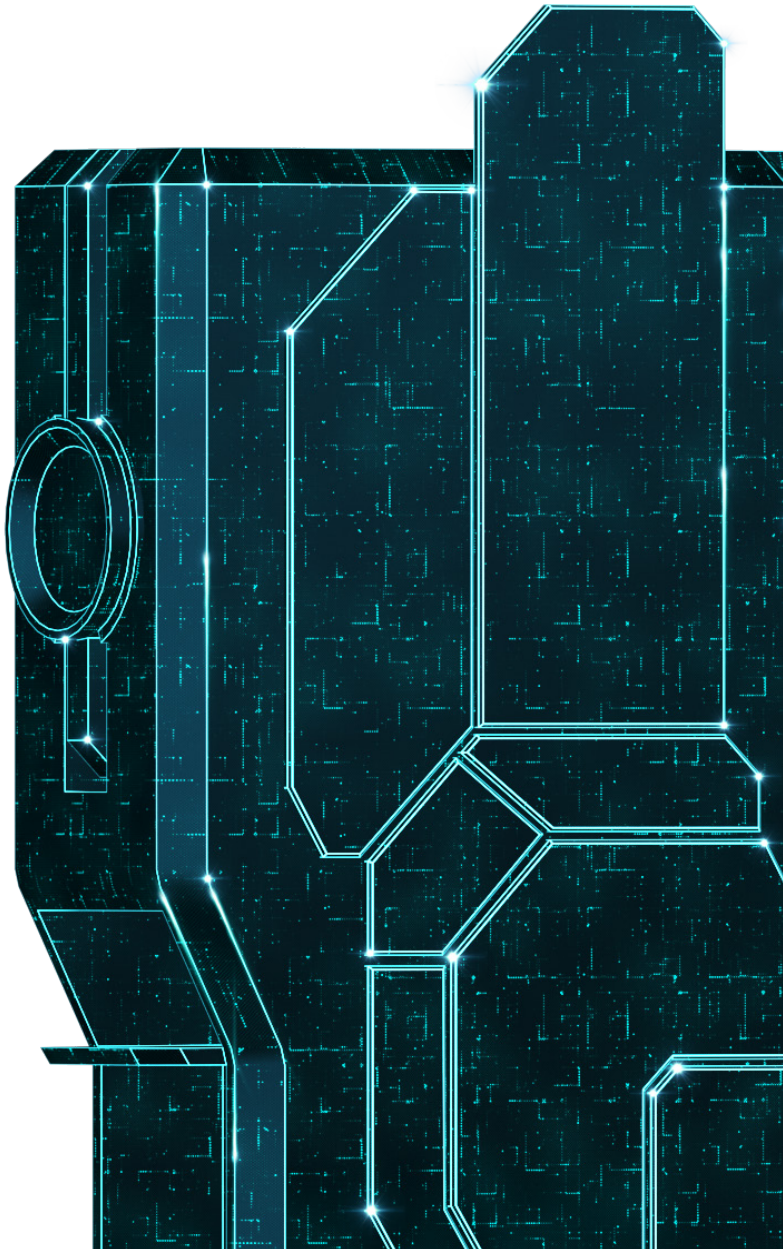
Better security for the remote workforce

The need for advanced protection goes beyond mail and storage, especially with the increase in remote workforces. Hybrid offices are becoming ubiquitous, and many businesses are relying primarily on collaboration tools such as Microsoft Teams for day-to-day activities, communication and internal or external meetings. With ESET Cloud Office Security's advanced protection for Microsoft Teams, you'll have better peace of mind and ensure your organization's daily collaboration is safe and secure.

Using ECOS protection features ensures that every file that is in a user's OneDrive, shared via SharePoint, or transferred via Teams is checked using a powerful anti-malware engine that leverages the same security technology as ESET's award-winning endpoint solutions.

An easy-to-use cloud management console allows for setup and deployment in minutes with a dashboard that provides value-added information and automated notifications to improve an admin's efficiency. The need to continuously check the dashboard is removed with automated notifications sent to admins or users to immediately bring awareness of any potential threats, saving time (and therefore, money).

Enabling automatic protection ensures that any new users created within Microsoft 365 will be protected without the need to add them individually. Admins can also further investigate emails and files from the console with ease, using quarantine manager to decide whether to delete or release objects that have been quarantined by the security solution.



The key takeaway

The increased adoption of Microsoft 365 applications, the shift to remote workforces and a rapidly evolving threat landscape are driving the need for more advanced, preventive protection for cloud applications. ESET Cloud Office Security delivers a cost-effective, scalable way to provide value-added protection that enables increased security through a powerful combination of spam filtering, anti-malware scanning and anti-phishing capabilities.

LEARN MORE

20210609