Trend Micro™

Cloud App Security

Advanced threat and data protection for Microsoft 365, Google Workspace™, and other cloud services

Today, email and collaboration tools are becoming more widely used and even the preferred method when communicating within and outside an organization. As you adopt cloud-based enterprise applications, such as Microsoft 365, Google Workspace™, Box™, and Dropbox™, you need to be more vigilant about security than ever before. While these applications are secured by the provider, you share the responsibility to secure the content that passes through them.

What are the risks?

- 96% of social engineering attacks start with email.
- According to the FBI , BEC scams were responsible for billions of dollars in losses as the largest victim loss by crime type in 2021.
- Remote workers, partners, and customers may unknowingly share malicious files using cloud file-sharing services.
- The security included with Microsoft 365 (E3 and below) is designed to detect known malware but over 88% of malware is unknown, according to Trend Micro™ Research.

The potential costs are too high to accept baseline security that only protects against a small portion of threats.

Trend Micro™ Cloud App Security enables you to embrace the efficiency of cloud services while maintaining security. It protects incoming and internal emails from Microsoft 365 and Gmail™ against advanced malware and other threats. It also enforces compliance on other cloud file-sharing and collaboration services, including Box, Dropbox, Google Drive™, Microsoft SharePoint online, Microsoft OneDrive for business, and Microsoft Teams.

Cloud App Security integrates directly with Microsoft 365, Google Workspace, and other services using APIs, maintaining all user functionality without changing the MX record to reroute email traffic or setting up a web proxy. This second layer of defense caught 39.9 million high-risk threats beyond those detected by the cloud email services' built-in security.

Key Advantages

Protects Microsoft 365 and Gmail email from phishing and advanced malware

- Discovers unknown malware using multiple patternless techniques, including **pre-execution machine learning** and **sandbox analysis**.
- See risk insights for internal users, top targeted employees, and users with high-risk events.
- Identifies **BEC** attacks by using artificial intelligence (AI), including expert system and **machine learning**, to examine email header, content, and authorship, while applying more stringent protection for high-profile users.
- Prevents executive spoofing scams using **Trend Micro™ Writing Style DNA**. This unique technology detects impersonations of high-profile users by analyzing the writing style of a suspicious email and comparing it to an AI model of that user's writing.
- Finds malware hidden in common Microsoft 365 file formats and PDF documents with the unique **document exploit detection** engine.
- Protects internal email and allows auto or manual **retro-scan** to uncover attacks already in progress.
- Prevents **credential phishing** by blocking URLs which disguise as legitimate logon website.

Enforces compliance for cloud file-sharing and collaboration services

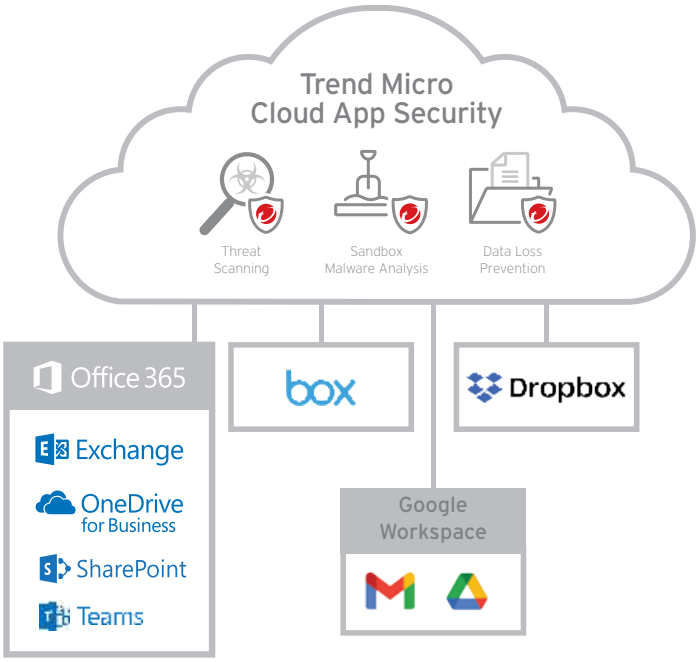
- Provides Trend Micro Data Loss Prevention™ (DLP) and advanced malware protection for Box, Dropbox, Google Drive, SharePoint, OneDrive, and Teams.
- Discovers compliance data in existing stored files and email by scanning databases.
- Simplifies setup with more than 240 pre-built compliance templates and user/group policies
- Support for Microsoft Information Rights Management (IRM)
- Supports action based on Microsoft Information Labels

Key Benefits

- Protects Microsoft 365 email and Gmail, along with other cloud file-sharing and collaboration services.
- Detects ransomware and other malware hidden in Microsoft 365 file formats or PDF documents.
- Identifies BEC attacks using artificial intelligence.
- Protects internal email and allows on-demand retro-scanning for mailboxes.
- Gives visibility into sensitive data use with cloud file-sharing services.
- Preserves all user functionality on any device with simple API integration.

> In 2022, Trend Micro Cloud App Security blocked 39.9 million high-risk threats that passed through Microsoft 365 and Gmail built-in security.

Trend Micro Cloud App Security Report 2022



Cloud App Security Advanced

Cloud App Security Advanced adds additional capability to protect emails before they arrive at the mailbox with both Advanced Threat Protection and Data Loss Prevention.

Benefits include:

- Protect emails before they arrive at Microsoft 365 or Gmail, without changing MX records
- Protect outbound emails with DLP rules, preventing unwanted data loss
- Reduce the risk of threats such as malicious emails, phishing, BEC, or ransomware entering your mailbox

Detection and response for email and beyond

When malware is found on an endpoint, most of the time it came from an email. You need to know who else received the email and if this malicious attachment is in any other mailboxes, i.e., where else the attack chain is inside your organization. Unlike other products that just provide logs for visibility of data, XDR for Cloud App Security has automated response actions as well as a powerful workbench to allow an analyst to investigate the incident from multiple layers, including email, endpoint, network, and more. With the power to respond from batch quarantining or removing emails, to account-based management like changing passwords or disabling the account when necessary. We correlate against attack surface, detection models, observed attack techniques, and protection layer detection logs, which allows us to automate response actions using security playbooks.

The industry-leading XDR capabilities of Trend Vision One™ combines detection and response for email, endpoints, cloud server workloads, and/or network, providing a single console to investigate and respond to complex attacks.

Trend Micro™ Managed XDR

Trend provides 24/7 alert monitoring, alert prioritization, investigation, and threat hunting as a managed service. Managed XDR offers standard or advanced service packages on Trend's security layers across email, endpoints, servers, cloud workloads, and network. With Managed XDR, you can benefit from detailed threat investigations and hunting without extensive in-house resources.

System Requirements

For more details and the latest supported version visit: docs.trendmicro.com/en- us/enterprise/ cloud-app-security-online-help/about-cloud-app-secu/introduction/requirements.aspx

> Cloud App Security reliably catches even unknown threats that are difficult to detect with Microsoft 365. It reminds us of the power of multi-layered defense.

Hironori Araya,
Head of PR and Information Group,
Tohoku Electrical Safety Inspection Association

NEW Inline Mode for double-layer protection

Dual-Layer Email Protection Package

Cloud App Security Advanced is also part of **Trend Micro™ Smart Protection for Microsoft 365**, which provides complete threat protection against phishing, BEC, ransomware, internal email risks, and file sharing risks. It combines the advantages of Cloud App Security Advanced with a software as a service (SaaS) email gateway to add pre-delivery filtering for spam and phishing emails along with outbound DLP and email encryption controls.

For more information, please visit trendmicro.com