Trend Micro™

CLOUD APP SECURITY

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

As you adopt cloud-based enterprise applications, such as Microsoft Office 365, Google Workspace, Salesforce®, Box™, and Dropbox™, you need to be more vigilant about security than ever. While these applications are delivered in a safe manner, you share the responsibility to secure the content that passes through them.

What are the risks?

- Ninety-six percent of social engineering attacks start with email[1].
- According to the FBI, BEC scams amounted to **US$1.7 billion in losses** in 2019—half of the year's total losses due to cybercrime—with an average of US $75,000 per incident[2].
- Remote workers, partners, and customers may unknowingly share malicious files using cloud file-sharing services.
- The security included with Office 365 (E3 and below) is designed to detect known malware but over 95% of malware is *unknown*.

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 Office 365 and Gmail against advanced malware and other threats, and enforces compliance on other cloud file-sharing and collaboration services, including Box, Dropbox, Salesforce, Google Drive™, Microsoft® SharePoint® online, Microsoft® OneDrive® for business, and Microsoft® Teams.

Cloud App Security integrates directly with Office 365, Google Workspace, and other services using application programming interfaces (APIs), maintaining all user functionality without rerouting email traffic or setting up a web proxy. This second layer of defense caught threats beyond those detected by the cloud email services' built-in security.

KEY ADVANTAGES

Protects Office 365 and Gmail email from phishing and advanced malware

- Discovers unknown malware using multiple patternless techniques, including pre-execution machine learning and sandbox analysis.
- Uses multiple operating systems and extensive anti-evasion technology on our sandboxing technology.
- 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 Writing Style DNA. This unique technology detects impersonations of high-profile users (such as the CEO, VP, GM) 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 Office file formats and PDF documents with the unique document exploit detection engine.
- Protects internal email and allows manual scan to uncover attacks already in progress.
- Prevents credential phishing by blocking URLs which disguise as a legitimate logon website.

Enforces compliance for cloud file-sharing and collaboration services

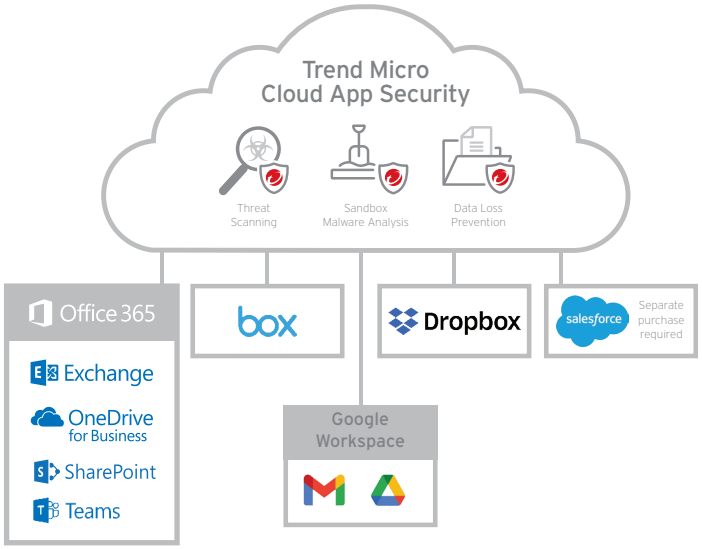
- Provides Trend Micro™ Integrated Data Loss Prevention (DLP) and advanced malware protection for Box, Dropbox, Salesforce*, Google Drive, SharePoint, OneDrive, and Teams.
- Enables consistent DLP policies across multiple cloud-based applications.
- Discovers compliance data in existing stored files and email by scanning databases.
- Simplifies setup with 240+ pre-built compliance templates, user/group policies, and support for Microsoft® Rights Management services.

*Salesforce protection requires a separate purchase outside of protection for other cloud services

KEY BENEFITS

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

> "In 2019, Trend Micro Cloud App Security blocked 12.7 million high-risk threats that passed through Office 365 and Google Workspace built-in security."
>
> **Trend Micro Cloud App Security Report 2018**



Optimized for minimum impact to administrators and users

- Preserves all user and administrator functionality.
- Provides direct cloud-to-cloud integration for high performance and scalability.
- Minimizes latency impact by assessing the risk of files and URLs before sandbox analysis.
- Supports hybrid Office 365 and on-premises Microsoft® Exchange™ architectures in conjunction with Trend Micro™ ScanMail™.
- Integrates with Trend Micro Apex Central™ for central visibility of DLP and threat events across your organization's endpoints, servers, and web traffic.
- Provides programmatic access through Cloud App Security automation and integration to Representational State Transfer (REST) APIs, allowing the security team of your organization to investigate, detect, and respond to security issues.

Deploys automatically with no software or device changes

Cloud App Security's cloud-to-cloud API integration doesn't rely on redirecting email or web proxies. As a result, it:

- Adds security without burdening IT with changing devices or user settings, installing software, setting up a web proxy, or changing the MX record to reroute email.
- Integrates quickly and automatically with Office 365, Google Workspace, and other cloud services.
- Extends the capabilities of your Cloud App Security with advanced Trend Micro™ XDR functionality, providing investigation, detection, and response across your endpoints, email, and servers.

Detection and response for email and beyond

One hundred percent detection is the goal, but in reality, no security can prevent 100% of attacks 100% of the time. When malware is found on an endpoint, chances are it came from an email. You want to know who else received the email and if this malicious attachment is in any other mailboxes. You then need to take action by quarantining the emails and possibly resetting passwords on the affected email accounts. The XDR capabilities of Trend Micro Vision One™ combines detection and response for email, endpoints, cloud server workloads, and/or network to give you a single console to investigate and respond to complex attacks. Access to the Vision One threat defense platform with advanced email XDR capabilities are automatically included in Cloud App Security purchases, outside of any Trend Micro™ Worry-Free™ bundles.

Trend Micro™ Managed XDR

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

SYSTEM REQUIREMENTS

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

[1] 2020 Verizon Data Breach Investigations Report
[2] FBI, 2020

COMPLETE USER PROTECTION

Cloud App Security is part of the **Trend Micro™ Smart Protection™ Complete Suite**, powered by XGen™ security. It combines the broadest range of endpoint and mobile threat protection capabilities with multiple layers of email, collaboration, and gateway security. It also enables you to manage users across multiple threat vectors from a single management console that gives you complete user-based visibility into the security of your environment.

Cloud App Security is also part of **Trend Micro Smart Protection for Office 365**, which provides complete threat protection for Office 365 against phishing, BEC, ransomware, internal email risks, and file sharing risks. Powered by XGen™ security, it combines a software as a service (SaaS) email gateway with Cloud App Security and uses the optimum blend of cross-generational threat defense techniques.

POWERED BY XGen™ SECURITY

> "Cloud App Security reliably catches even unknown threats that are difficult to detect with Office 365. It reminds us of the power of multilayered defense."
>
> **Hironori Araya,**
> Head of PR and Information Group,
> Tohoku Electrical Safety Inspection Association

TREND MICRO™

Securing Your Connected World