

Trend Micro™ CLOUD APP SECURITY™

Advanced threat and data protection for Office 365 and cloud file-sharing services

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

What are the risks?

- 79% of ransomware attacks¹ and over 90% of targeted attacks start with email
- Ransomware families grew 752%¹ and cost businesses \$1 billion in 2016²
- Business Email Compromise (BEC) attacks cost an average of \$132,000 per incident³
- 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 90% 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 Office 365 email from advanced malware and other threats, and enforces compliance on other cloud file-sharing services, including Box, Dropbox, Google Drive, SharePoint® Online, and OneDrive® for Business.

Cloud App Security integrates directly with Office 365 and other services using APIs, maintaining all user functionality without rerouting email traffic or setting up a web proxy.

KEY ADVANTAGES

Protects Office 365 email from phishing and advanced malware

- Uses multiple patternless techniques, including sandbox analysis to find unknown threats.
- Uses artificial intelligence to examine email intention and attack indicators to identify Business Email Compromise (BEC) attacks. More stringent protection can be set up for high-profile users.
- Finds malware hidden in common Office file formats and PDF documents with the unique document-exploit detection engine.
- Blocks emails with malicious URLs before delivery and re-analyzes URLs in real time when a user clicks on one.
- Combines pre-execution machine learning, anti-malware, heuristics, and dynamic analysis using award winning⁴ sandboxing to detect ransomware and other zero-day malware. Sandbox analysis uses multiple operating systems and extensive anti-evasion technology.
- Protects internal email and allows manual scan to uncover attacks already in progress.

Enforces compliance for cloud file-sharing services

- Provides DLP and advanced malware protection for Box, Dropbox, Google Drive, SharePoint Online, and OneDrive for Business.
- Enables consistent DLP policies across multiple cloud-based applications.
- Discovers compliance data in existing stored files and email by scanning databases.
- Simplifies setup with more than 240 pre-built compliance templates, user/group policies, and support for Microsoft Rights Management services.

KEY BENEFITS

- Protects Office 365 email and other cloud file-sharing services
- In the last two years, stopped six million high-risk threats that weren't caught by Microsoft
- Detects ransomware and other malware hidden in Office file formats or PDF documents
- Identifies Business Email Compromise attacks using artificial intelligence
- Protects internal email and allows on-demand scan for mailstore
- Gives visibility into sensitive data use with cloud file-sharing services
- Preserves all user functionality, on any device, with simple API integration

“Trend Micro has a proven track record in endpoint and cloud security, and it is the one of the first leading vendors to offer a combination of advanced security solutions for Office 365.”

Chris Christiansen
IDC

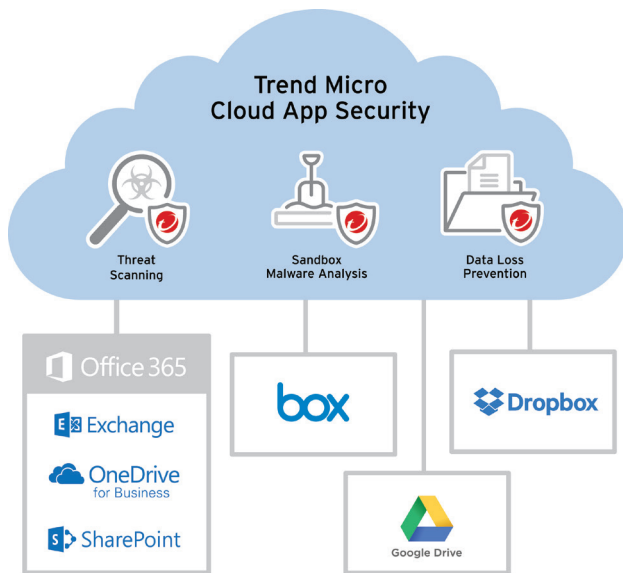
Optimized for minimum impact to administrators and users

- 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 Exchange architectures in conjunction with Trend Micro™ ScanMail™.
- Integrates with Trend Micro™ Control Manager™ for central visibility of DLP and threat events across your organization's endpoints, servers, and web traffic.

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 and other cloud services



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>

CLOUD APPLICATIONS	DETAILS
Office 365	Office 365 Education, Business, Enterprise, Nonprofit, and U.S. Government plans. Office 365 Enterprise K1 (email only). Standalone plans: Exchange Online, OneDrive for Business, SharePoint Online Plan.
Box	Box Business and Enterprise
Dropbox	Dropbox Business
Google Apps for Work	Supports Google Drive within Google Apps for Work (Trend Micro™ Hosted Email Security can provide additional email protection)

Web browser for administration: current or previous version of Microsoft Internet Explorer®, Google Chrome, or Mozilla Firefox.

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. And it 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—the only third-party solution that provides complete threat protection for Office 365 against phishing, Business Email Compromise (BEC), ransomware, internal email risks, and file sharing risks. Powered by XGen™ security, it uses the optimum blend of cross-generational threat defense techniques including machine learning, sandbox analysis, and more.



“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



Securing Your Journey to the Cloud



For more information contact
800.656.7702 or
info@smstechsolutions.com

¹ TrendLabs 2016 Security Roundup, February 2017

² CSO, Ransomware took in \$1 billion in 2016—improved defenses may not be enough to stem the tide, Jan 2017

³ Trend Micro Enterprise Network Protection Against Cyberattacks Primer: Business Email Compromise

⁴ 2016 NSS Labs Breach Detection Systems Report

© 2017 Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro logo and the t-ball logo, Trend Micro Cloud App Security, Trend Micro Deep Discovery, Trend Micro ScanMail, and Trend Micro Control Manager are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. [DS07_Cloud_App_Security_170912US]