



Trend Micro™ CLOUD APP SECURITY

Advanced threat detection and DLP for Microsoft Office 365

As you move to cloud-based enterprise applications like Office 365, you need to be extra vigilant about security. While Office 365 includes built-in security features, many organizations are looking to supplement the platform with advanced controls to detect hidden and targeted threats which could ultimately result in a costly data breach. Email is the primary method of attacks but collaboration tools like OneDrive and SharePoint can also be used to spread malware. In fact, the Verizon 2015 data breach study found that 75% of attacks spread to a 2nd victim within 24 hours! This risk is compounded as users work remotely and files are shared between partners and customers using devices outside of security policy enforcement. Moreover, network breach detection systems employed to detect advanced threats miss traffic between remote users and Office365.

Trend Micro™ Cloud App Security enhances Office 365 with advanced threat protection controls to help you communicate and collaborate more confidently in the cloud. The solution extends Office 365 built-in security with document exploit detection and sandbox malware analysis to detect zero-day malware and malicious code hidden in PDF or Office documents. Plus, it improves your visibility into compliance with data loss prevention. Cloud App Security also keeps threats from migrating over OneDrive or SharePoint Online from mobile workers or trusted partners.

Cloud App Security integrates directly with Office 365. There is no need to re-route email traffic and you can expand protection beyond email to include collaborations over SharePoint and OneDrive.

KEY ADVANTAGES

Reduce risk of spear-phishing emails and file sharing

- Safeguards Exchange Online, SharePoint Online, and OneDrive for Business against the 12,500 new threats seen every hour
- Detects threats using an aggressive scanner, document exploit detection, web reputation, and cloud-based intelligence
- Uses dynamic sandbox analysis to investigate the behavior of suspect files, not just static pattern matching, and quarantines harmful files and email
- Leverages proven Deep Discovery sandbox technology rated #1 by NSS Labs²

Block zero-day and hidden malware

- Employs patternless sandbox malware detection to lower your risk of breach
- Monitors the actual behavior of suspect files in virtual sandbox environments using multiple versions of operating systems and applications
- Uses document exploit detection to find hidden malware inside common office file formats like Word, PowerPoint, and Excel as was seen in 60% of targeted attacks in 2014³

Seamlessly extend Office 365 security

- Empowers users to continue to access email and work in a way that is familiar to them on any device
- Preserves full Office 365 user and administrator functionality
- Direct cloud-to-cloud integration via Microsoft API's enables high performance and scalability
- Minimizes latency impact by assessing the risk of files before sandbox malware analysis

Key Benefits

- Protects Office 365 email and file sharing
- Enhances built-in security with sandbox malware analysis
- Detects advanced malware hidden in office or PDF documents
- Eliminates the need to re-route email traffic
- Integrates directly with Office 365 to preserve user and administrative functionality

“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 Christians,
IDC

1. Verizon 2015 Data Breach Investigations report
2. 2014 NSS Labs Breach Detection Systems Report
3. Targeted Attack Trends, 2014 Annual Report, March 2015



“Sixty percent of malware in targeted attacks is hidden inside Office file formats like Word, PowerPoint, and Excel.”

Trend Micro Targeted Attack Trends,
2014 Annual Report, March 2015

Simple to deploy with no software or device changes

Cloud-to-cloud integration doesn't rely on redirecting email

- Adds security without burdening IT with changing devices, user settings, installing software, or changing its MX record to re-route email
- Delivered as a cloud service with no software to deploy
- Automatic provisioning enables setup in minutes

Scalable and high performance architecture

API integration eliminates the need for an MX record change to re-route email traffic

- Provides robust functionality resulting from over 15 years experience integrating with Microsoft Exchange and SharePoint
- Assess the risk of email attachments and files before sandbox to avoid unnecessary latency

Controls sensitive data for compliance

Real-time visibility and optional blocking of compliance data for Office 365 communications

- Get visibility of sensitive data use in Exchange, SharePoint, and OneDrive for Business
- Simplifies setup with over 200 built-in and customizable templates
- Employs real-time monitoring to block, quarantine, or report on compliance policies

System Requirements:

- Office 365 plans: all plans that include Microsoft "business-class email"
- Web browser for administration: current or previous version of Microsoft Internet Explorer, Google Chrome, or Mozilla Firefox



Securing Your Journey to the Cloud

©2015 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro T-ball logo, and OfficeScan 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. [DS03_Cloud_App_Security_150528US]