

# Trend Micro™ CLOUD APP SECURITY™

Fortschrittlicher Schutz vor Bedrohungen und Datenverlust für Office 365 und Cloud-Services für den Dateiaustausch

Beim Einsatz von cloudbasierten Unternehmensanwendungen wie Microsoft® Office 365™, Box, Dropbox und Google Drive müssen Unternehmen in puncto Sicherheit noch wachsamer sein als je zuvor. Diese Anwendungen werden zwar in einer sicheren Umgebung bereitgestellt, aber Unternehmen tragen gemeinsam die Verantwortung für den Schutz der Inhalte der Anwendungen.

## Welche Risiken gibt es?

- 94 % aller Ransomware-Angriffe<sup>1</sup> und über 90 % aller zielgerichteten Angriffe beginnen mit einer Email.
- Die weltweiten Verluste infolge von BEC-Angriffen (Business Email Compromise) betragen 2018 mehr als 12 Mrd. US-Dollar<sup>2</sup>, und die Attacken verursachen Kosten von durchschnittlich 160.000 US-Dollar pro Vorfall<sup>2</sup>.
- Externe Mitarbeiter, Partner und Kunden nutzen möglicherweise unwissentlich bösartige Dateien über Cloud-Services für den Dateiaustausch.
- Die in Office 365 integrierten Sicherheitsmechanismen (E3 und niedriger) sind darauf zugeschnitten, bekannte Malware zu erkennen. Doch mehr als 90 % der heutigen Malware ist unbekannt.

Die potenziellen Kosten eines Sicherheitsvorfalls sind zu hoch, als dass man sich allein auf einen Basisschutz verlassen könnte, der nur vor einem geringen Teil aller Bedrohungen schützt.

Mit **Trend Micro Cloud App Security** haben Unternehmen die Möglichkeit, die Effizienzvorteile von Cloud-Services zu nutzen und gleichzeitig hohe Sicherheitsstandards aufrechtzuerhalten. Die Lösung schützt eingehende und interne Office 365 Emails vor komplexer Malware und anderen Bedrohungen und setzt darüber hinaus die Compliance zu anderen Cloud-Services für den Dateiaustausch durch, wie z. B. Box, Dropbox, Google Drive, SharePoint® Online und OneDrive® for Business.

Cloud App Security lässt sich über APIs direkt in Office 365 und andere Services integrieren, wobei der gesamte Funktionsumfang für Benutzer ohne Umleitung des Email-Verkehrs und ohne Einrichtung eines Web-Proxys erhalten bleibt.

## ENTSCHEIDENDE VORTEILE

### Schützt Office 365 Emails vor Phishing und komplexer Malware

- Entdeckt unbekannte Malware mithilfe mehrerer patternloser Methoden, einschließlich maschinellem Lernen vor der Ausführung (Pre-Execution) und Sandbox-Analysen.
- Verwendet in der preisgekrönten<sup>3</sup> Sandboxing-Technologie von Trend Micro mehrere Betriebssysteme und extensive Anti-Evasion-Technologien.
- Erkennt BEC-Angriffe mithilfe künstlicher Intelligenz, einschließlich von Expertensystemen und maschinellem Lernen, die dafür eingesetzt werden, um Email-Header, Inhalte und Urhebererschaft zu analysieren und gleichzeitig wichtige Nutzer besser zu schützen.
- Verhindert Spoofing-Betrug auf Führungsebene durch den Einsatz von Writing Style DNA. Diese einzigartige Technologie erkennt Nachahmung von wichtigen Anwender (wie CEO, VP, GM) durch die Analyse des Schreibstils einer verdächtigen Email und dem Abgleich mit einem KI-Modell des Schreibstils dieses Anwenders.
- Findet mithilfe der einzigartigen Engine für die Entdeckung von Dokumenten-Exploits in beliebigen Office-Dateiformaten und PDF-Dokumenten versteckte Malware.
- Schützt interne Email und ermöglicht manuelle Scans, um bereits laufende Angriffe aufzudecken.
- Verhindert Phishing von Anmeldeinformationen, indem sie URLs blockiert, die sich als legitime Office 365 Anmelde-Website tarnen.

### Setzt die Compliance für Cloud-Services für den Dateiaustausch durch

- Stellt DLP-Lösungen und Schutz vor komplexer Malware für Box, Dropbox, Google Drive, SharePoint Online und OneDrive for Business zur Verfügung.
- Ermöglicht anwendungsübergreifende, einheitliche DLP-Richtlinien für die Cloud.
- Erkennt durch das Scannen von Datenbanken Compliance-Daten in vorhandenen gespeicherten Dateien und Emails.
- Erleichtert das Aufsetzen durch mehr als 240 vordefinierte Vorlagen zur Compliance, Benutzer-/Gruppenrichtlinien und Unterstützung für Microsoft Rights Management Services.

## ENTSCHEIDENDE VORTEILE

- Schützt Emails in Office 365 und andere Cloud-Services für den Dateiaustausch
- Erkennt Ransomware und anderen Schadcode in Office 365- oder PDF-Dokumenten
- Identifiziert BEC-Angriffe (Business Email Compromise) mithilfe von Künstlicher Intelligenz
- Schützt interne Email und ermöglicht nach Bedarf Scans über Email Postfächer
- Bietet Transparenz bei der Nutzung sensibler Daten in Cloud-Services für den Dateiaustausch
- Durch einfache API-Integration keinerlei Einschränkung auf den Geräten

„Trend Micro App Security blockierte 2017 3,4 Mio. hochriskante Bedrohungen, die Office 365 nicht erkannt hatte.“

Trend Micro  
Cloud App Security 2017 Report

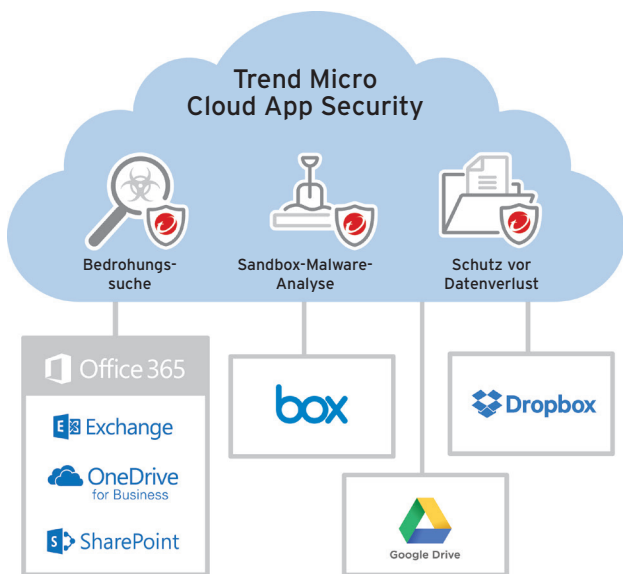
## Minimale Beeinträchtigungen für Administratoren und Anwender

- Gesamter Funktionsumfang für Anwender und Administratoren bleibt unberührt
- Bietet hohe Leistung und Skalierbarkeit durch direkte Cloud-to-Cloud-Integration
- Minimiert Latenzzeiten durch eine Risikobewertung der Dateien und URLs vor der Sandbox-Analyse
- Unterstützt in Kombination mit Trend Micro™ ScanMail™ hybride Architekturen aus Office 365 und lokalen Exchange-Anwendungen
- Bietet die zentrale Übersicht über DLP- und Bedrohungsereignisse über alle Endpunkte, Server und den Internet-Verkehr des Unternehmens hinweg durch die Integration in Trend Micro™ Control Manager™

## Automatische Bereitstellung ohne Änderungen an Software oder Geräten

Dank der Cloud-to-Cloud-Integration von Cloud App Security ist die Umleitung von Emails oder die Nutzung von Web-Proxys nicht notwendig. Daraus folgt:

- Mehr Sicherheit, ohne dass die IT-Mitarbeiter sich um den Austausch von Geräten, neue Benutzereinstellungen, die Installation von Software, die Einrichtung eines Web-Proxys oder die Änderung des MX-Records zur Umleitung von Emails kümmern müssen
- Eine schnelle und automatische Integration in Office 365 und andere Cloud-Services



## SYSTEMVORAUSSETZUNGEN

Weitere Informationen und die neueste unterstützte Version finden Sie unter:

<http://www.trendmicro.de/produkte/cloud-app-security/>

CLOUD-ANWENDUNGEN	DETAILS
Office 365	Office 365 Education, Business, Enterprise und Nonprofit. Office 365 Enterprise K1 (nur E-Mail). Eigenständige Pläne: Exchange Online, OneDrive for Business, SharePoint Online Plan.
Box	Box Business und Enterprise
Dropbox	Dropbox Business
Google Apps for Work	Unterstützung für Google Drive in Google Apps for Work (zusätzlicher E-Mail-Schutz durch Trend Micro™ Hosted Email Security möglich)

**Webbrowser zur Verwaltung:** aktuelle oder frühere Version von Microsoft Internet Explorer®, Google Chrome oder Mozilla Firefox

<sup>1</sup> TrendLabs 2017 Security Roundup, March 2018

<sup>2</sup> FBI, 2018

<sup>3</sup> 2017 NSS Labs Breach Detection Systems Report

## COMPLETE USER PROTECTION

Cloud App Security ist Bestandteil der Trend Micro™ Smart Protection Complete Suite – unterstützt durch XGen™ Security. Sie kombiniert eine breite Vielfalt von Fähigkeiten zum Schutz vor Endpoint- und mobilen Bedrohungen mit mehreren Schichten von Email-, Collaboration- und Gateway-Sicherheit. Und darüber hinaus können Anwender unabhängig vom Übertragungsweg der Bedrohungen von einer zentralen Management-Konsole aus verwaltet werden. So hat der Admin den Sicherheitsstatus jedes einzelnen Anwenders in der Umgebung jederzeit vollständig im Blick.



„Cloud App Security entdeckt zuverlässig auch unbekannte Bedrohungen, die für Office 365 nur schwer zu erkennen sind. Die Lösung erinnert an die Stärken einer mehrschichtigen Verteidigung.“

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



© 2019 Trend Micro Incorporated. Alle Rechte vorbehalten. Als einer der weltweit führenden Anbieter von IT-Sicherheitslösungen verfolgt Trend Micro das Ziel, eine sichere Welt für den digitalen Datenaustausch zu schaffen. Die innovativen Lösungen für Privatanwender, Unternehmen und Behörden bieten mehrschichtigen Schutz für Rechenzentren, Cloud-Workloads, Netzwerke und Endpunkte. Weitere Informationen: [www.trendmicro.com](http://www.trendmicro.com) [DS08\_Cloud\_App\_Security\_Datasheet\_180720DE]