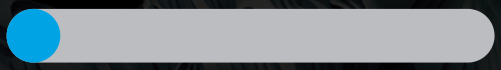
MSP's Guide to **Cloud App Security & Ransomware Prevention**

TREND MICRO™

Cloud apps require more than baseline security

Digital transformation has accelerated in 2021, and with the reality of a distributed workforce, cyber-criminals see your clients' rapid adoption of cloud and SaaS services, such as Microsoft Office 365, Google Workspace, Salesforce, Box™, and Dropbox™, as lucrative targets for exploitation. While these services offer baseline security, MSPs share the responsibility to secure their clients' digital assets that pass through them.

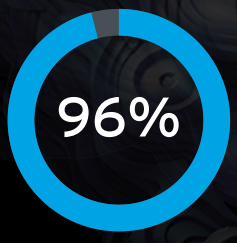


5%

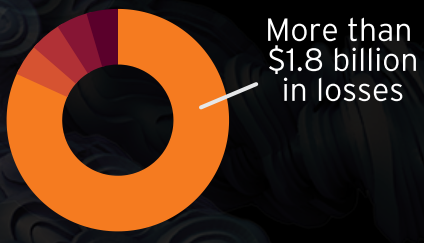
The baseline security included with those services is designed to protect against known malware, which only accounts for 5 percent of malware.[1]

What are the risks?

BEC (Business Email Compromise)



Ninety-six percent of social engineering attacks start with email.[2]



According to the FBI, BEC scams were responsible for the largest victim loss by crime type in 2020.[3]

- Users unknowingly share malicious files using cloud file-sharing services
- Account takeover and credential theft
- Ransomware attacks
- Confidential corporate data loss

Enhance baseline security

Remote working has made phishing emails even more common. According to Trend Micro's 2020 Annual Cybersecurity Report, most employees believed relying on their IT departments, or utilizing a VPN, would help diminish phishing attacks, but the truth is, workers are still getting phished.

Elevate your clients' protection by considering technologies such as:

AI-based BEC Detection

Authorship analysis compares a suspected impersonation to an AI model of a high-profile user's writing style.

Document Exploit Detection

Parses files to look for known and potential exploits in the intended office application.

Sandbox Analysis

Behavioral analysis using thousands of file features and machine learning models better improves detection of unknown malware.

Data-Loss Prevention

Implement policies across email, cloud storage, and teams to simply compliance initiatives and prevent the unauthorized sharing of client's corporate assets.

Computer Vision

Leverages AI models to analyze branding elements, login forms, and other site content of suspected websites used in credential stealing schemes.

Connecting the dots: XDR working hand-in-hand with cloud app security

While securing and getting visibility into your client's cloud apps is important, it's only a portion of the security picture.

XDR (extended detection & response) seeks to combine and correlate information across multiple sources such as email, endpoints and network, enabling faster detection and response to multi-faceted attacks.

When malware is found on an endpoint, chances are it came from an email. XDR can help you answer these questions for a faster and more efficient response:

Detection

Are there compromised accounts sending internal phishing emails?

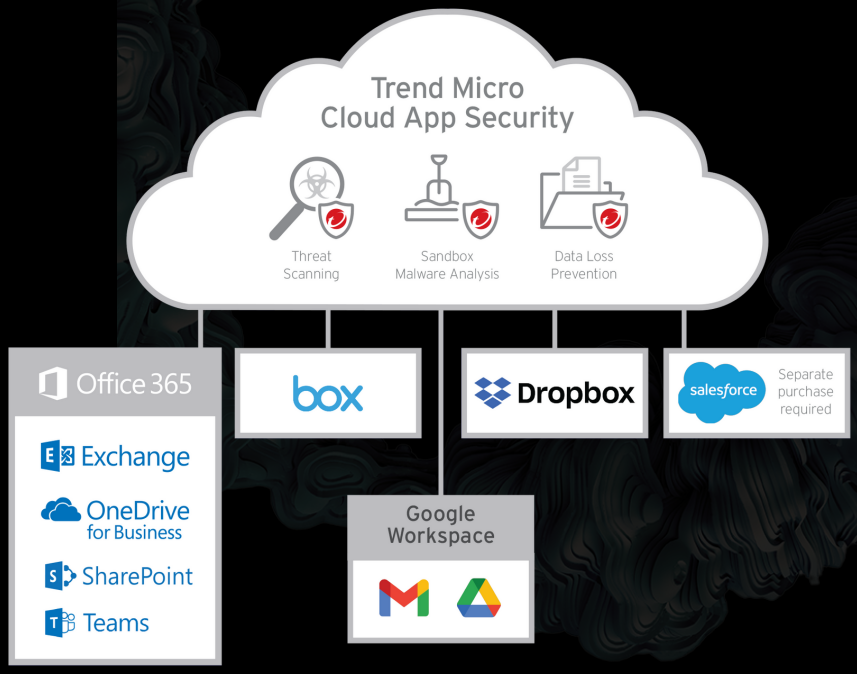
Investigation

Who else received this email / threat? Who is the sender? Are there any attachments or links? Did other clients receive the same compromised email?

Response

Quarantine email, delete email, block sender, block URLs/files

What to consider when evaluating a cloud app security solution:



- Can this solution be set up quickly with automatic provisioning to Microsoft or Google APIs?
- Is there software to install or email to re-route?
- Does this solution combat credential phishing attacks using technology to analyze branded elements, login forms, other site content to catch fake login sites?
- Does this solution enforce 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?
- Does it integrate 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?
- Can it analyze the writing style of a suspicious email and compare it to an AI model of that user's writing to prevent executive spoofing scams?

Ransomware is persistent and evolving

Ransomware is relentless, and attacks that can devastate your clients' businesses are on the rise. It's a type of malware that locks, encrypts, or otherwise prevents data and systems from being accessed by their owners, and requires victims to pay a ransom to the criminal responsible for the attack in order to regain access.

Ransomware is primarily distributed via exploit kits, social engineering schemes, and spam mails that are sent to a large number of email addresses. When a recipient opens a malicious attachment or clicks a compromised link, the malware is downloaded on to the user's system. The fear of losing priceless data can push users to pay the ransom—and while they may opt to pay, having their files unlocked or decrypted is never a guarantee.

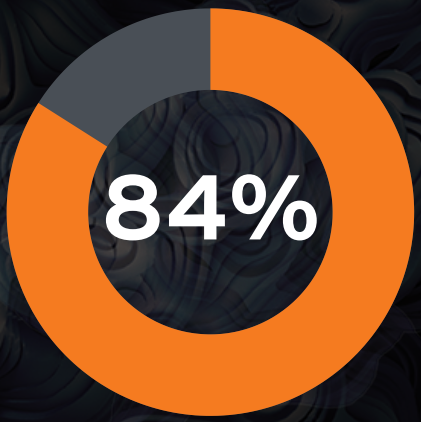
Protect your clients from ransomware

- Leverage automated back-up and restore processes
- Apply software patches as soon as they become available
- Educate clients on prevention of email phishing
- Limit access to business critical information
- Bolster clients' security posture with layered ransomware protection

It all starts with your clients' users. They're the most vulnerable when it comes to ransomware – whether it's falling for a phishing email or clicking on a malicious web link.

What does a modern ransomware attack look like?

Modern ransomware actors identify and target valuable data, often exfiltrating it from a victim's network organization rather than simply encrypting it. This gives them another avenue for extortion: if a victim does not pay the ransom, the attacker can threaten to publicize the private data. For organizations holding intellectual property data, proprietary information, private employee data, and customer data, this is a serious concern. Any data leak will come with regulatory penalties, lawsuits, and reputational damage.



Percentage of organizations that have reported security incident types related to phishing and ransomware in the past 12 months[4]

Another significant feature of modern ransomware is that the actors are more precise and involved in the attack. They take over networks in multiple human-supervised stages, veering away from click-on-the-link automatic events. They also spend significant time conquering different parts of the victim's network (a process that may take weeks or months) before they execute the ransomware payload, making such attacks look more like nation-state advanced persistent threat (APT) attacks instead of traditional ransomware incidents.[5]

Minimize the risk of ransomware on endpoints across your customer base

When ransomware infects your clients, it can access whatever data a compromised user in their business can access. It can consume several man hours as you try to recover lost files through email threads, with little hope of recovery.

Ensure your solution has:

- High-fidelity Machine Learning, which analyzes files not only before execution but also during runtime for more accurate detection, with noise cancellation like census and whitelist checking to reduce false positives.

- Behavior monitoring for suspicious behavior associated with ransomware, such as the rapid encryption of multiple files, so that the encryption process can be automatically stopped and the endpoint isolated, before ransomware can spread and cause more damage to your data.

- Real-time web reputation to determine if a URL is a known delivery vehicle for ransomware

[1] Trend Micro Research, Feb 2019
[2] 2020 Verizon Data Breach Investigations Report
[3] 2020 IC3 report
[4] Osterman Research White Paper, Mar 2021
[5] Modern Ransomware Report, Jun 2021

FREE tools to help assess & secure your clients' security posture

FREE email and endpoint security assessment service

We invite you to utilize our free email and endpoint security assessment service with your clients to see if they are effectively protected against the advanced threats that are impacting organizations today.

Secure the human layer by leveraging Phish Insight

Phish Insight, powered by Trend Micro, provides you with a free, easy-to-use platform to conduct effective real-world phishing simulations and customized training campaigns across your customer base. Phish Insight has been developed to strengthen your last line of defense, the human.

Contact Us


www.trendmicro.com/msp


msp@trendmicro.com


888.977.4200

Threats Detected and Automatically Blocked Globally in 2018.

Created with real data by artist Daniel Beauchamp.