CISCO
SECURE

Brief

How to Secure Microsoft 365 Email Against Advanced Threats

Enhance your business email defenses with Cisco Secure Email Cloud Mailbox

CISCO The bridge to possible

Malware and malicious spam come in as the 1st and 2nd most common causes of downtime.[1]

The rise and risk of cloud email

Email is the primary method of communication in business – and the number one threat vector for cyberattacks. Because remote and hybrid work models are pushing more people to do tasks on their own devices, cloud-based email is quickly becoming the standard.

But your cloud mailbox can host much more than messages and attachments: Malware and other threats can often linger undetected in cloud mailboxes, costing organizations massive amounts of money, data, time, and trust. (There's a reason behind the surge in compliance and regulation requirements!)

Microsoft 365's cloud email in particular is highly vulnerable to the widespread threats. Unfortunately, Microsoft's own solution, Advanced Threat Protection (ATP), doesn't effectively cover Microsoft 365's security gaps. We're uncovering the risks associated with cloud email – specifically those associated with Microsoft 365 – as well as how to find a comprehensive security solution that protects your organization.

Top threats and impacts

Did you know that 90% of cyberattacks begin with an email? It's the most prevalent way to gain a foothold in a business network.[2] The top threats to cloud email today include Business Email Compromise (BEC), malware, phishing, spam, spoofing, and blended threats combining multiple vectors, such as social engineering.

The consequences of these threats vary in category – but a successful attack can be catastrophic across the board.

Top threats defined

Business Email Compromise

Email that appears from a legitimate-looking sender or email address to trick the recipient into sharing something confidential or valuable. The email accounts of corporate executives or wire transfer staff are often spoofed.

Malware/ Ransomware

Intrusive software designed to damage and destroy computer systems. Common malware includes viruses, spyware, and ransomware, which blocks people from accessing their computer files, systems, or networks until they pay a ransom.

Phishing

Fraudulent communication designed to lure a victim. The message looks to be from a trusted sender and coaxes the victim to take the bait (like clicking a link) and provide confidential information.

Spam

Unsolicited and unwanted junk email sent out in bulk to an indiscriminate recipient list. It can include malicious links that infect your computer with malware.

Spoofing

A disguised email address, sender name, or website URL made to convince targets that they're interacting with a trusted source. The aim is to have the recipient download malware, send money, or disclose sensitive information.

The catastrophic consequences

$26B

Estimated losses between 2016 and 2020. Over the past several years, BEC attacks have doubled and the amount stolen has tripled.[3]

$125,439

Average amount lost in fraudulent transactions stemming from a BEC attack.[4]

5–48

Hours of downtime reported by the majority of companies after a severe breach.[1]

36%

CISOs who reported impacted operations due to a breach. Operations was the top area of impact, followed by brand reputation (33%) and finances (28%).[1]

Microsoft 365: Security gaps and attacks

The convenience and scalability of Microsoft 365 is great. The same can’t be said about its native security. While Microsoft ATP provides basic security, it’s not enough to protect against common threats or Microsoft 365’s security gaps.

1 of 3

Most common email threats: Microsoft 365 phishing.[5]

~40%

Microsoft 365 customers who will supplement their security with a third-party solution by 2023.[5]

31%

Cases where bad actors initiated a Microsoft 365 account takeover after the initial breach, out of the 950 reviewed in BakerHostetler’s 2020 report.[6]

What makes Microsoft 365 the first target? According to the leader of BakerHostetler’s digital risk advisory and cybersecurity team, Microsoft 365 accounts store contacts and email addresses that offer hackers a treasure trove of information for their next phishing or scam targets.

The call for integrated cloud email security

The dramatic migration to cloud email and increase in both volume and success of phishing attacks demand a reevaluation of email security. If your organization uses cloud email, you need a solution that is both comprehensive and cloud-native to protect the business and employees.

What to look for when supplementing cloud email security:

- **Multiple security services** to assess each email's potentially harmful vectors (attachments, links, and the message itself)
- **Continual analysis** that scans every mail entering or leaving every mailbox for proactive protection anywhere and everywhere
- **Automated detection and remediation** tools to quickly mitigate the spread of email-borne threats

Superior protection for Microsoft 365

With simple configuration and quick deployment, Cisco Secure Email Cloud Mailbox is a supplemental security solution that ensures that you have the robust protection you need to protect every inbox. Cloud Mailbox uses proven Cisco technologies to address the security gaps in Microsoft 365, blocking advanced threats like BEC, malware and ransomware, phishing, spam, and spoofing.

Not only do you get robust protection, you also get valuable hours back – as well as fewer headaches. Thanks to Cloud Mailbox's ease of use, IT teams are free to focus on more business-critical tasks.

Cisco Secure Email Cloud Mailbox was named one of 10 hottest new cloud security tools by CRN in 2020.[7]

Cloud Mailbox features and benefits

By using Cloud Mailbox for Office 365, you gain:

Simple scalability, search, and remediation

Set up and deploy in five minutes and scale to any company. Experience the ease of fast, automated detection and remediation tools that enable you to spot and address threats in hours or even minutes – much faster than it would take using Microsoft 365's native controls.

Triage and open APIs

Get full integration into Microsoft 365 and leading APIs and keep email security as close to the mailbox as possible with direct integration with Azure. That means messages and attachments stay in Microsoft's cloud, no MX record changes required, and metadata is sent to Cisco for reporting and remediation.

Security-reinforcing threat intelligence

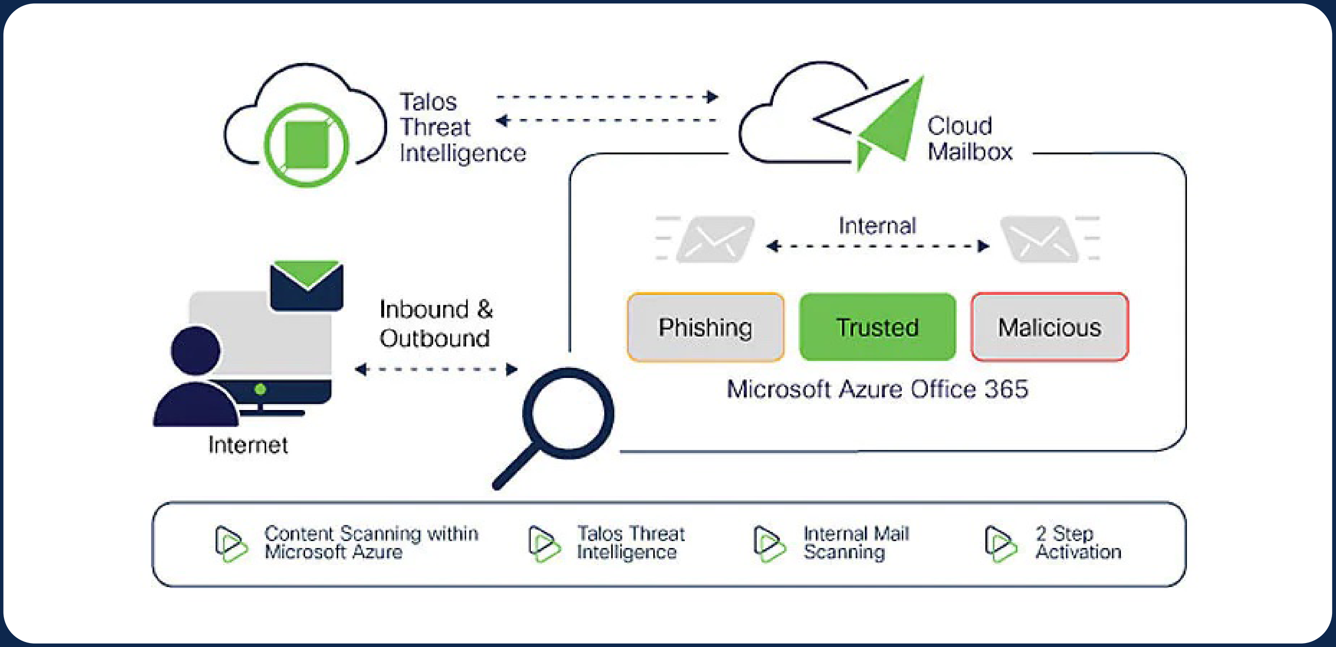
When you implement Cloud Mailbox, you implement a solution powered by Cisco Talos, a globally recognized threat research team. Talos delivers diversified, up-to-date threat intelligence so you're equipped to take action before attacks occur.

Conversation tracking and trajectory for incident response

Unlock visibility into all emails – inbound, outbound, and internal – for easy and proactive threat detection anywhere and everywhere. You can stop threats without interrupting the regular flow of messages.

> "Cloud Mailbox is the first solution that is as easy as it claims to be."
> – Anthony Gates, EVP/GM, Rhino Networks

How it works


Talos Threat Intelligence
Cloud Mailbox
Internal
Inbound & Outbound
Phishing
Trusted
Malicious
Microsoft Azure Office 365
Internet
Content Scanning within Microsoft Azure
Talos Threat Intelligence
Internal Mail Scanning
2 Step Activation

Experience Cloud Mailbox

Ideal for businesses of all sizes, Cloud Mailbox offers simple deployment, fast remediation, and peace of mind. Ready to experience simple, effective cloud email security for Microsoft 365?

Start your free trial

Sources:

1. Cisco Secure. *Cisco Cybersecurity Report Series 2020: CISO Benchmark Study.* February 2020.
2. Verizon. *Data Breach Investigations Report.* 2018.
3. Federal Bureau of Investigation. *Business Email Compromise: The $26 Billion Scam.* September 10, 2020.
4. HIPAA Journal. *$301 Million Lost to BEC Attacks Each Month.* July 25, 2019.
5. Gartner. *Market Guide for Email Security.* Peter Firstbrook and Neil Wynne. June 6, 2019.
6. BakerHostetler. *2020 Data Security Incident.* 2020.
7. CRN. *The 10 Hottest New Cloud Security Tools of 2020.* Michael Novinson. December 16, 2020.

cisco SECURE