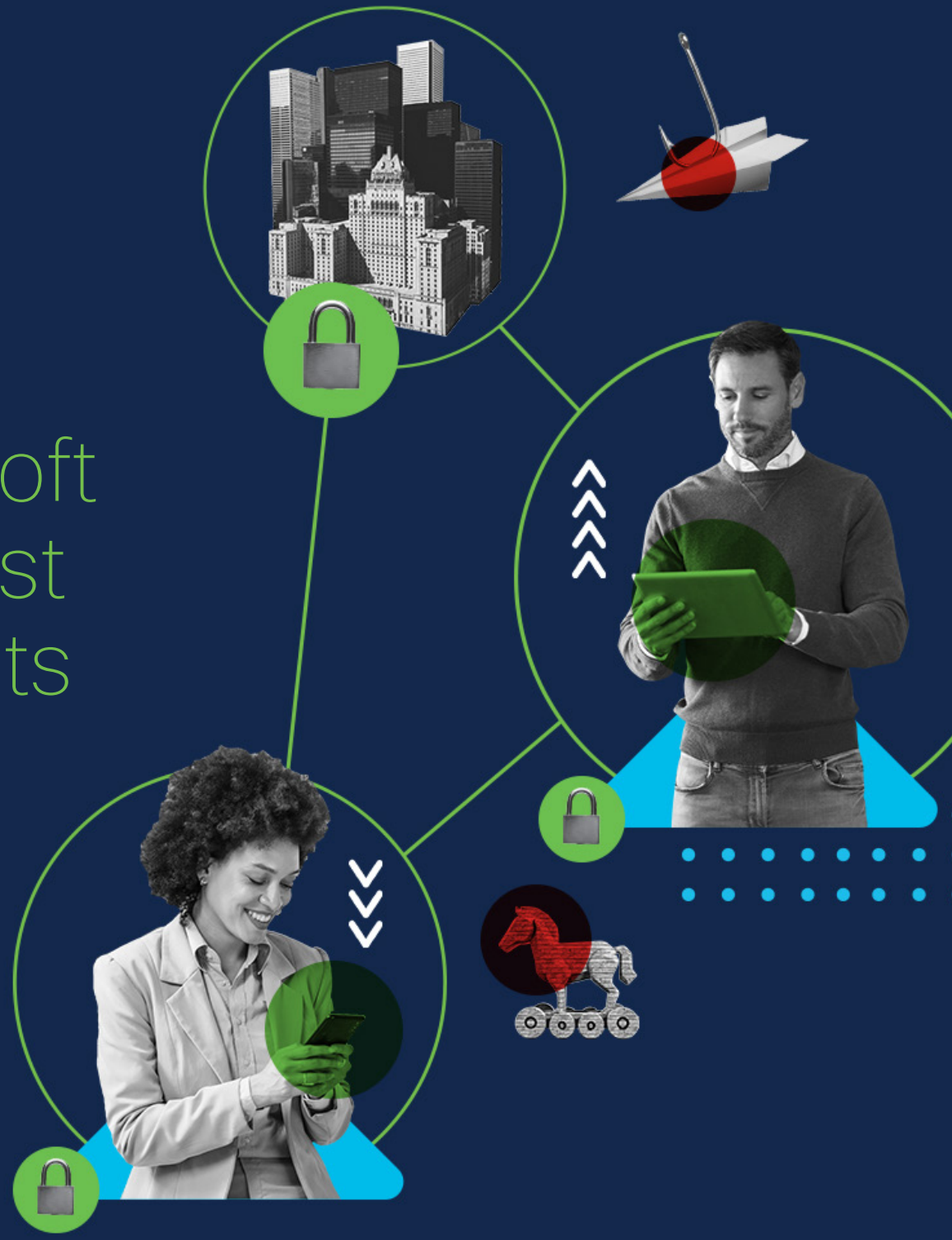
CISCO
SECURE

E-book

Securing Microsoft 365 Email Against Advanced Threats



cisco The bridge to possible

In this e-book:

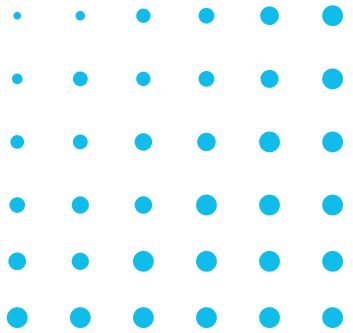
The rise of cloud email

Email continues to be the most common form of communication across businesses, but how and where we use email has changed. Businesses are increasingly migrating to cloud email platforms for improved productivity, the ability to work from anywhere on any device, and continual access to the latest tools and features.

Microsoft 365 phishing takeover is **1 of the 3** most common email threats.[1]

By 2020, **50% of organizations** using Microsoft 365 will rely on non-Microsoft tools to maintain consistent security.[2]

But, despite all these benefits, there's a catch — cloud-based email has left users and devices open to new threats and vulnerabilities. Let's explore these risks — particularly in the context of Microsoft 365 — and what you can do to secure every mailbox across your organization.



Email remains vulnerable to breaches

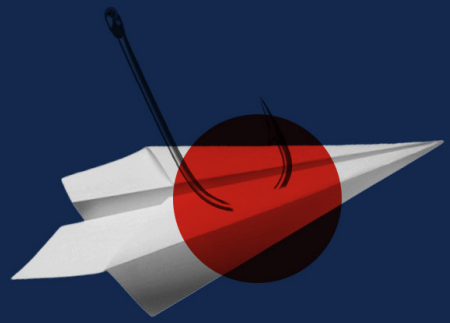
As the cornerstone of business communication, email remains the #1 vector for internet-based threats.[3] More than 3.4 billion email scams or phishing emails are sent every day, and more than 90% of breaches begin with email.[4,5]

And it's no wonder – email is also the most lucrative way for cybercriminals to attack organizations. Business email compromise (BEC) in particular is one of the fastest-growing security threats; over the past several years, BEC attacks have doubled, and the amount stolen has tripled, with estimated losses between 2016 and 2020 totaling $26 billion.[6]

And that's just the beginning. Cloud email in particular has become a major target for attacks, with substantial gaps in security leaving users, devices, and data vulnerable to threats.

Attackers also attempt to breach email using a variety of other methods, including:

Ransomware
Phishing
Malware
Spam
Domain Compromise
Account Takeover
Internal Threats
Spoofing



Securing against advanced threats

While it's true that every email provider offers some degree of protection, email isn't as secure as you might think, and native security can't be fully relied on to mitigate every threat. So, while Microsoft 365 provides a basic level of security, it's often not enough – particularly when it comes to ransomware and phishing. To truly secure your organization's mailboxes, you need additional layers of protection.

Gartner, considering these recent challenges, recommends "a strategic approach to security that layers inbound, outbound, and internal detection and remediation."[1] Its *2019 Market Guide for Email Security* suggests a growing need for Cloud Email Security Supplements that address gaps in your existing email security posture.[1]

Offering comprehensive, cloud-delivered security for services like Microsoft 365, this supplemental security leverages diversified intelligence to protect against threats that come from both outside and inside your organization. In this way, you can have greater confidence that every email, everywhere, has the protection it needs.

~40%

of Microsoft 365 customers will supplement their security with a third-party solution by 2023.[1]

What should a supplemental security solution deliver?

Cloud email security supplements are defined by a number of key components, including:

Multiple security services to assess each of an 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 – including threats from within the organization

Automated detection and remediation tools to quickly mitigate the spread of email-borne threats

In addition to these capabilities, this solution should provide cybersecurity teams with:

Visibility

into all emails – inbound, outbound, and internal

Simplicity

of deployment, configuration, and management

Integration

with Microsoft 365 and other email security solutions

Intelligence

with diversified, up-to-date info on threats

With quick and easy deployment, Cisco Cloud Mailbox Defense is a supplemental security solution that ensures your team, your email, and your organization have the robust protection they need.

Cloud Mailbox Defense

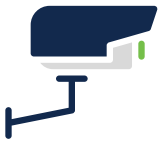
Simplify your email administration with easy search and remediation.

Enrich your incident response investigations with conversation tracking and trajectory.

Empower your security operations with triage and open APIs.

Supplement your secure email gateway with internal visibility.

Administration



Operations

Incident Response

The Cisco Cloud Mailbox Defense advantage

Today, Cisco offers businesses a comprehensive email security solution called Cloud Mailbox Defense. Cloud Mailbox Defense uses proven Cisco Email Security technologies to address security gaps in Microsoft 365 cloud email, blocking advanced threats like ransomware, phishing, BEC, spoofing, and spam.

Fully integrated with Microsoft 365, Cloud Mailbox Defense provides complete visibility and protection for inbound, outbound, and internal email messages. Organizations can automatically stop threats before they reach the user – and quickly mitigate the impact of breaches if they do occur – all without interrupting the regular delivery of messages.

Ideal for businesses of all sizes, Cloud Mailbox Defense offers simple deployment, superior visibility, easy attack remediation, and best-in-class threat intelligence from Cisco Talos.

To provide even greater visibility, automation, and protection, Cloud Mailbox Defense can be integrated with Cisco SecureX. SecureX connects all of Cisco's integrated security portfolio with your entire security infrastructure to deliver a consistent experience that strengthens security across your network, endpoints, applications, and the cloud.

Cloud Mailbox Defense, powered by Talos Threat Intelligence

One of the largest and most trusted security research organizations, Talos continually scans the globe for new attacks, dangerous URLs, malware, and spoofs. Delivering rapid, actionable threat intelligence that's shared across every Cisco product, Talos ensures your security services are better equipped to take action: once a threat is discovered anywhere in the Cisco ecosystem, it's instantly blocked everywhere.

Simplicity

- ✓ Deployment
- ✓ Configuration
- ✓ Management

Visibility

- ✓ Messages
- ✓ Search/Triage
- ✓ Open APIs

Integration

- ✓ Talos Intelligence
- ✓ MS APIs
- ✓ SecureX Threat Response (Winter 2020)

Superior protection for Microsoft 365 email

The increased use of cloud email platforms can make it challenging for organizations to effectively protect every mailbox. That's where Cisco Cloud Mailbox Defense can help. Building upon leading Cisco Email Security technology, Cloud Mailbox Defense secures Microsoft 365 email with a unique combination of visibility, simplicity, integration, and intelligence – so your organization can feel confident that it's fully protected.

Protect cloud email with Cisco Cloud Mailbox Defense:

Start your free trial

"With Cisco Cloud Mailbox Defense, I'm able to quickly identify, track, tag, and categorize internal emails."

– Director of IT Security

Sources:
1. Gartner, *Market Guide for Email Security*, Peter Firstbrook, Neil Wynne, June 6, 2019.
2. Gartner, *How to Enhance the Security of Office 365*, 2017.
3. FBI IDC Report, 2019.
4. Valimail, *Email Fraud Landscape*, Spring 2019.
5. Verizon 2019 Data Breach Investigations Report.
6. *Business Email Compromise: The $26 Billion Scam*, Federal Bureau of Investigation, September 10, 2020.

cisco SECURE