cisco SECURE

Five tips for choosing cloud-based email security

1. Be cloud confident

Having the best defense for the number one attack vector—email—is vital to keeping your people productive and your organization protected. But doing so can be time consuming for your team given the increasingly complex landscape. More people work remotely on many devices and often use cloud email, which has opened up new vulnerabilities. Not to mention, attacks just keep getting more sophisticated.

The good news is cloud-based email security can simplify and take much of that workload off your team's plate so they can focus on more strategic security initiatives. But to make the move, you need to be confident that:

- Your data will have the right protection and you can meet your government and industry regulations.
- You can quickly and easily migrate your email security policies to the cloud.
- You'll get the best-of-breed protection you need for the ever-evolving email threat environment.

Find out how you can be cloud confident with Cisco Secure Email.

Get the eBook

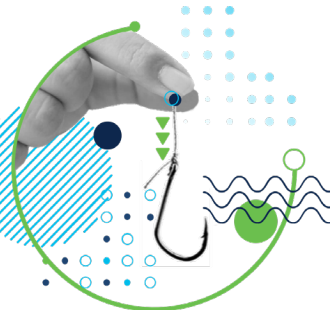
2. Cover your bases with comprehensive protection

Cybercriminals weaponize email in many ways, whether it's to introduce malware into an organization's systems, steal data, or extort money—to name just a few examples. So you want to ensure that when you move to cloud email security, you have comprehensive, proven email protection you can rely on from a trusted, industry leader.

You need capabilities that can quickly detect, block, and remediate advanced threats in incoming mail such as Business Email Compromise (BEC), ransomware, advanced malware, phishing, and spam. Not only that, it's important to protect your brand and data in outgoing email.

Learn how you can get the best protection for your email.

Read the Cisco Secure Email At-A-Glance



3. Secure Microsoft 365 against advanced threats

Cloud email in particular has become a major target for attacks. Microsoft 365 provides a basic level of security but often it's not enough—especially when it comes to ransomware and phishing.

Microsoft 365 account takeover through credential phishing is one of the top three most common email threats.[1]

You need supplemental email security for Microsoft 365 that automatically stops advanced threats before they reach the user—and quickly mitigates the impact of breaches if they do occur—all without interrupting the regular delivery of messages.

That's where Cisco Cloud Mailbox comes in.

Learn more

[1] 2020 SonicWall Cyber Threat Report

4. Power it with industry-leading threat intelligence

To detect and prevent not just known but emerging email threats, your cloud email security must be backed by industry-leading, comprehensive threat intelligence that's rapid and actionable.

One of the largest and most trusted security research organizations, Cisco Talos continually scans the globe for new attacks, dangerous URLs, malware, and spoofs. Once a threat is discovered anywhere in the Cisco ecosystem, it's instantly blocked everywhere.

Meet Cisco Talos

5. Simplify and increase visibility and efficiency across your security ecosystem

Email security is just one part of the security infrastructure your team has to stay on top of. You want it to be easy to manage as part of your security big picture. And you want to expedite the time to detect threats across multiple components and enable a fast, synchronized response. That way your team not only saves time but gets more out of your cloud email security and the rest of your security portfolio—and all of your business functions are more secure.

See how the built-in capabilities of the SecureX platform provide unified visibility, enhanced automation, and stronger protection within Cisco Secure Email and across all your security solutions—Cisco and otherwise.

Watch the video

Next steps

Learn more about Cisco Secure Email

Request a 45-day trial of Secure Email

Start your 30-day free trial of Cloud Mailbox