10 Must-Ask Questions for Choosing the Best Cloud Email Security Solution

Choosing an email security platform isn't just about ticking boxes. It's about ensuring the technology can address the ever-shifting realities of today's threat environment. In addition to our list of most important challenges, we've designed these 10 questions to support a more informed evaluation: to uncover meaningful differences between vendors, move beyond surface-level claims, and focus on what truly matters—detection accuracy, behavioral context, automation, and user impact. Use this checklist to ensure you pick the email security platform best suited for your organization.

1. Can the solution detect attacks that don't include payloads or known indicators?

Legacy tools rely on scanning for malware, bad links, or known domains. Today's threats often include no payload at all—just persuasive language and human trust.

- ☐ Does the platform use behavioral AI to analyze tone, content, and sender context?
- ☐ Can it detect payload-free BEC, impersonation, and VIP fraud?
- ☐ Will it identify threats that look normal but act abnormally?

2. Does the platform natively understand your employees, vendors, and their behavior?

Effective detection starts with knowing what's normal. A modern platform should go beyond mere scanning of anomalies in content; it should build consistent baselines across internal and external communications.

- ☐ Can the solution profile users, vendors, and communication history?
- ☐ Does it understand invoice frequency, typical recipients, and message style?
- ☐ Does it adapt to organizational changes over time?

3. Can it detect internal threats like lateral phishing or insider compromise?

Once an attacker gains access to a legitimate account, they can launch phishing campaigns from inside your environment, bypassing external defenses and abusing trust.

- ☐ Does the solution monitor east-west (internal) traffic, not just inbound?
- ☐ Can it detect abnormal behavior from real employee accounts?
- ☐ Does it use consistent but flexible behavioral baselines to flag internal misuse?

4. Is threat remediation instantaneous, or delayed by manual workflows?

Even a short delay increases the chance that an employee clicks, replies, or forwards a malicious email. The longer threats linger, the higher the risk—and the heavier the burden on SOC teams. Manual triage and investigation consume valuable analyst hours, especially when dealing with user-reported phishing and abuse mailbox traffic.

- ☐ Does the platform remediate threats in milliseconds, not minutes or hours?
- ☐ Can it remove messages from every affected inbox automatically?
- ☐ Does it reduce SOC workload by automating triage and surfacing only high-risk messages?

5. Can it automatically detect and stop account takeovers—before internal attacks happen?

Attackers easily exploit legacy authorization, MFA fatigue, and malicious apps to compromise accounts without detection.

- ☐ Does it monitor sign-in activity, device type, and login patterns?
- ☐ Will it flag MFA bypass or risky app installs in real time?
- ☐ Can it take action before compromised accounts are used for lateral phishing?

6. Does the platform give visibility into configuration risks and cloud app permissions?

Misconfigurations, overly permissive apps, and tenant-level changes are some of the easiest ways for attackers to gain footholds. Yet, many email security tools don't properly monitor them.

- ☐ Can the platform surface risky changes in Microsoft 365 or Google Workspace?
- ☐ Does it detect over-permissioned or suspicious third-party apps?
- ☐ Will it alert on tenant posture drift before leading to exposure?

7. How much value does the solution deliver from AI—vs. using it for trendy marketing?

AI is everywhere now, but not every implementation is meaningful. Bolted-on AI rarely delivers the depth or precision needed to detect modern threats.

- ☐ Is AI central to how threats are detected, scored, and remediated?
- ☐ Does the platform learn from user and organization-specific behavior?
- ☐ Can it explain its decisions in a way analysts can trust?

8. Does it reduce end-user noise while keeping employees productive?

Too many alerts, irrelevant emails, and digest fatigue erode attention and hide real threats. Email security should clean up the inbox, not clutter it.

- ☐ Can the solution suppress graymail based on behavior and engagement?
- ☐ Does it reduce time spent managing quarantines and digests?
- ☐ Can it quantify productivity gains for different user groups?

9. Does the platform provide relevant, real-time security awareness training?

Security awareness training matters—but too often, programs rely on static, one-size-fits-all content that fails to reflect modern threats. Many simulations are outdated, disconnected from real attack patterns, and time-consuming to manage. The result: low impact, high effort, and limited improvement in user behavior.

- ☐ Is the training customized to reflect the specific risks each employee faces, rather than relying on outdated, one-size-fits-all content?
- ☐ Can the platform convert real attacks into timely simulations that deliver training when it's most impactful?
- ☐ Can security teams measure impact without spending hours managing content and campaigns?

10. Is it built for the future—or just retrofitted for today?

Some solutions claim to be cloud-native but were originally built for a different era. Ask how deeply the architecture supports modern workflows, with an eye toward future re-configurations and threat vectors.

- ☐ Was the platform built API-first, or adapted from SEG infrastructure?
- ☐ Can it deploy quickly and integrate deeply with cloud providers and pre-existing security tools?
- ☐ Does it protect communication platforms across the SaaS environment, beyond email?