10 Considerations to Shape Your Cloud Email Security Strategy

This list is designed to help you prioritize your biggest email security concerns and solutions requirements. Knowing these details throughout the selection process will ensure you get the information you need to select the right cloud email security platform.

1. Identify which email-based threats concern you the most and understand how the solution stops them.

□ Does the solution block traditional attacks, such as spam and simple phishing?

□ Can it detect and stop advanced, socially-engineered attacks such as business email compromise and account takeover attacks?

□ Can the platform connect with your cloud email provider to block the full spectrum of email attacks, including malware and invoice fraud?

2. Determine which detection signals you want the solution to use.

□ Does the technology detect known indicators of compromise?

□ Can it analyze email content and account for contextual signals such as the relationship between sender and recipient?

□ Can the platform consider user identity and behavior data including sign-in activity, typical location, and normal devices?

3. Verify how end users are able to access their email accounts.

□ Are users required to follow legacy protocols and basic authentication to log in?

□ Does accessing an email account require modern multi-factor authentication?

4. Establish how you prefer to remediate malicious mail.

□ Is malicious email automatically triaged and remediated?

□ Will the SOC team be required to manually triage and remediate all user-reported attacks?

□ Does the solution display native banners that warn end users of potentially malicious content?

Abnormal

5. Decide how many email security solutions you're willing (or able) to operate.

□ Can the technology be integrated into your existing email infrastructure?

□ Can it connect directly to your cloud email provider to enhance native security capabilities?

□ Does it offer additional protection beyond what you currently have?

6. Identify which management tasks are consuming the most time and effort.

□ Will the platform eliminate the need to manually review user-reported threats?

□ Does it make it easy for security teams to quickly find and redirect misdelivered messages?

□ Does the solution offer comprehensive dashboards that centralize important data and reports?

7. How much time will your security team save on investigation and reporting after implementation?

□ How much time will your security team save on investigation and reporting after implementation?

□ Will the solution provide visibility into the number of malicious emails remediated?

□ Does the technology account for time saved through increases in email productivity?

8. Decide what types of insights you need.

□ Does the platform offer basic insights, such as the number of attacks blocked?

□ Can analysts view detailed assessments, including attack types and indicators of compromise?

□ Does the technology enable tenant posture analysis?

9. Establish how you want to address time-wasting email like graymail.

□ Does the solution rely on rule-based detection, spam digests, and quarantine portals?

□ Can it offer a native user experience within your Microsoft or Google environment?

□ Does the technology provide personalized, adaptable protection for various use cases?

10. Know with which third-party technologies the platform must integrate.

□ Will analysts be able to log into the solution via an SSO tool?

□ Can it integrate with your SOAR platform to trigger playbooks when users engage with malicious emails or compromised accounts?

□ Can the solution augment your SIEM with metadata and risk scores for better attack correlation?