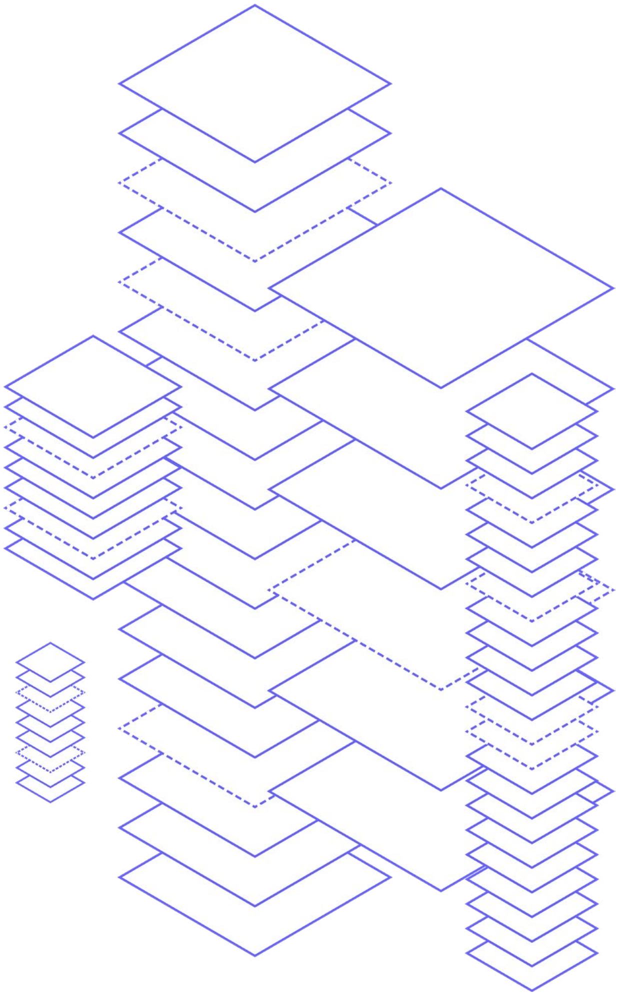
Abnormal

The Essential Guide to Cloud Email Security

7 Best Practices for Protecting Your Email Environment



The Need for Cloud Email Security

As organizations have migrated to cloud-based infrastructure and office platforms like Microsoft 365 and Google Workspace, they've seen clear benefits: easier collaboration, greater agility, and lower costs and maintenance related to infrastructure. But for most organizations, the challenge of determining how to keep data protected and employees safe from attacks in a cloud-based environment remains unsolved.

Still today, email remains the primary attack vector utilized by attackers to infiltrate a business. This is partially due to its ease of access and because modern threat actors can utilize tactics that enable them to bypass traditional security solutions like secure email gateways. For the last seven years, socially-engineered attacks including business email compromise (BEC) have been the leading cause of cybercrime losses, and that trend is only expected to continue.

$2.4B
Losses due to BEC in 2021.

35%
Percent of all cybercrime losses attributable to BEC.

65%
Increase in exposed losses from BEC.

Most organizations recognize that their existing solutions aren't providing an adequate level of protection against email-based threats. And while they may want to improve their security posture, it can be difficult to find the right solution.

In a recent survey of 300 security leaders:

- **92%** of respondents had experienced at least one email-related security incident within the past year.
- **78%** of stakeholders believe that secure email gateways (SEGs) are largely incapable of protecting modern cloud email environments.
- **79%** of respondents think the native security capabilities of cloud email solutions like Microsoft 365 offer insufficient protection on their own.

Knowing that attacks are increasing both in volume and severity and that current solutions cannot stop them, many organizations are looking for new approaches to cloud email security. But before making any changes, you first need to define your unique email security challenges and their impact on your organization. Understanding where your current processes and technology solutions are falling short will help you determine how to move forward.

7 Common Email Security Challenges

Organizations that rely on legacy email security solutions or even the newest generation of API-based products encounter various challenges due to shortcomings within the technology itself. Below are seven common challenges security teams face when they rely upon inadequate email security solutions.

Challenge #1:

Detection approach lacks internal organizational context.

- Not built to analyze internal East-West email traffic between employees.
- Cannot ingest signals across users' identity and behavior, such as device, sign-on location, or authentication method to inform detection approach.
- Cannot build an organizational baseline of normal business behavior to precisely detect anomalies.

Outcome:

When email security solutions cannot develop an organization-specific context for detection, security teams miss sophisticated lateral attacks that exploit trusted relationships between employees.

Challenge #2:

Security team lacks visibility into supply chain risks.

- Has no understanding of the nature of business relationships between vendors and employees and no knowledge of communication frequency, invoice cadence, invoice format, or primary contacts.
- Cannot alert security teams to signals about vendor account compromises that have impacted other organizations.
- Effectively treats all communications with vendors the same, regardless of risk level.

Outcome:

Attackers infiltrate enterprises via weak links in the security posture of their vendors, defrauding employees into sharing sensitive data or paying fraudulent invoices.

Challenge #3:

Threat detection approach is reactive rather than proactive.

- Focused only on detecting known bad indicators of compromise in email, such as malicious attachments, suspicious links, and untrusted domains.
- Unable to prevent text-based and payloadless attacks that come from known IP addresses or senders.
- Cannot detect email-based attacks that leverage novel techniques lacking known attack signatures.

Outcome:

SOC teams remain in a reactive posture against evolving email-borne threats, and fail to prevent attacks that lack known signatures.

Challenge #4:

Email threats linger in employee mailboxes for too long.

- Warns employees of threats by adding banners to risky emails, but relies on end users to take the right action.
- Sends potential threats to an analysis queue, where they await manual triage by a skilled analyst.
- Solution is slow to analyze inbound emails and make detection decisions because of reliance on a slower journaling approach; post-remediates messages in minutes or hours.

Outcome:

Attacks dwell in inboxes while waiting for review by the security operations team, allowing more time for employees to engage.

Challenge #5:

Limited ability to detect compromised internal email accounts.

- Focused on detecting anomalies strictly within email content and not on user behavior.
- Limited visibility to user identity and behavior attributes, such as impossible travel, new devices, new browsers, or new authentication methods that can indicate a potentially hijacked email account.
- Exposes risk of costly human error because of reliance on manual review or intervention.

Outcome:

Attackers use hijacked email accounts as the tip of the spear to initiate additional attacks across the enterprise or move laterally across systems.

Challenge #6:
Legacy technology unable to limit time-wasting graymail effectively.

- Impacts productivity as employees spend hours each week sorting through promotional emails and newsletters.
- Forces employees to use quarantines and spam digests in a separate user interface to view relevant emails.
- Burdens IT teams who must manually review and address user-reported issues.

Outcome:

Employees, and particularly executives, lose days of productivity each year sorting through promotional mail.

Challenge #7:
Cloud email platform is exposed to unauthorized access and abuse.

- Solution addresses a narrow approach to email security focused only on inbound email attacks.
- Employees can access email using legacy authentication protocols, bypassing MFA.
- Security teams have limited visibility into tenant settings and third-party application integrations that may expose the organization to risk.

Outcome:

Attackers may gain access to corporate infrastructure through exposed entry points in cloud email platforms.

7 Critical Capabilities for Cloud Email Security

Cloud email security platforms utilize a novel approach to detecting and remediating email attacks. The right platform provides advanced inbound email attack protection, offers tools to improve end-user productivity, and tackles the need to secure email infrastructure across each of its various entry points.

Because many vendors claim to offer this cloud email security functionality, it can be challenging to distinguish marketing language from reality. To address the seven challenges that plague traditional email security programs, cloud email security platforms should include seven key capabilities.

Capability #1:
An API-based approach to integrating with the cloud office.

- Full East-West and North-South visibility to analyze anomalies within email content.
- Ability to ingest large sets of data from multiple products and services.
- Enhances visibility into identity and relationship data to drive detection efficacy.

✓ **Why It Matters:**

Allows cloud email security solution to develop an internal organizational understanding of known good by utilizing a vast amount of data broader than email message content.

Capability #2:
The ability to proactively detect and mitigate supply chain risks.

- Builds an understanding of how vendors interact with an organization—including invoicing cadence, communication frequency, key contacts, years of relationship, and more.
- Uses knowledge engines to query and organize information about vendors and build behavioral profiles for each organization.
- Utilizes federated risk signals from hundreds of organizations to help defend against vendor account compromise.

✓ **Why It Matters:**

Prevents financial supply chain compromise by detecting behavioral anomalies in vendor communications.

Capability #3:
A risk-adaptive approach to detection.

- Combines NLP and NLU analysis of inbound email content with tens of thousands of signals about user identity and behavior for a risk-adaptive approach to threat detection.
- Analyzes sequences of events against context to detect never-before-seen threats.
- Remediates inbound email attacks in milliseconds when anomalies are detected.

Why It Matters:

Helps security teams adopt a proactive posture against evolving threats with a solution that is constantly learning and adapting.

Capability #4:
Allows for automated and instantaneous remediation.

- Removes threats from user inboxes with automated remediation—no rules, policies, or configuration needed.
- Provides instantaneous remediation, eliminating dwell time and the reliance on security awareness training for end users.
- Reduces SOC team burden by automating the review and response to user-reported phishing emails.

Why It Matters:

Removes the possibility of employees engaging with malicious emails.

Capability #5:
Ability to automatically detect and mitigate employee account takeovers.

- Baselines normal behavior for every end user by analyzing signals including login frequency, authentication methods, locations, devices, operating systems, browsers, and more.
- Uncovers subtle anomalies to precisely detect compromised accounts.
- Remediates messages sent from compromised accounts and disarms compromised users before attackers can do further damage.

Why It Matters:

Stops attackers from abusing compromised accounts to carry out lateral phishing campaigns.

Capability #6:

The ability to improve employee productivity with smart filtering of spam and graymail.

- Applies the same advanced behavioral AI, NLP, and NLU that helps detect and remediate the most sophisticated email-borne attacks to the challenge of time-wasting email.
- Utilizes an API-based approach to surface unique productivity insights on user engagement, open rates, folder movements, and the productivity and time impact of limiting graymail on the business.
- Maintains a native experience, eliminating the need for end-user quarantines or digest summaries.

Why It Matters:

Improves executive and employee productivity by removing unwanted promotional mail from the inbox.

Capability #7:

The ability to protect the cloud email platform from unauthorized access.

- Offers visibility into the configuration of the cloud email platform and any potential risk exposures.
- Monitors for configuration drift in the email environment.
- Acknowledges posture changes, whether positive or negative, and notifies administrators of risk.

Why It Matters:

Secures the enterprise from emerging side-channel attacks targeting cloud email platforms.

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?

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?

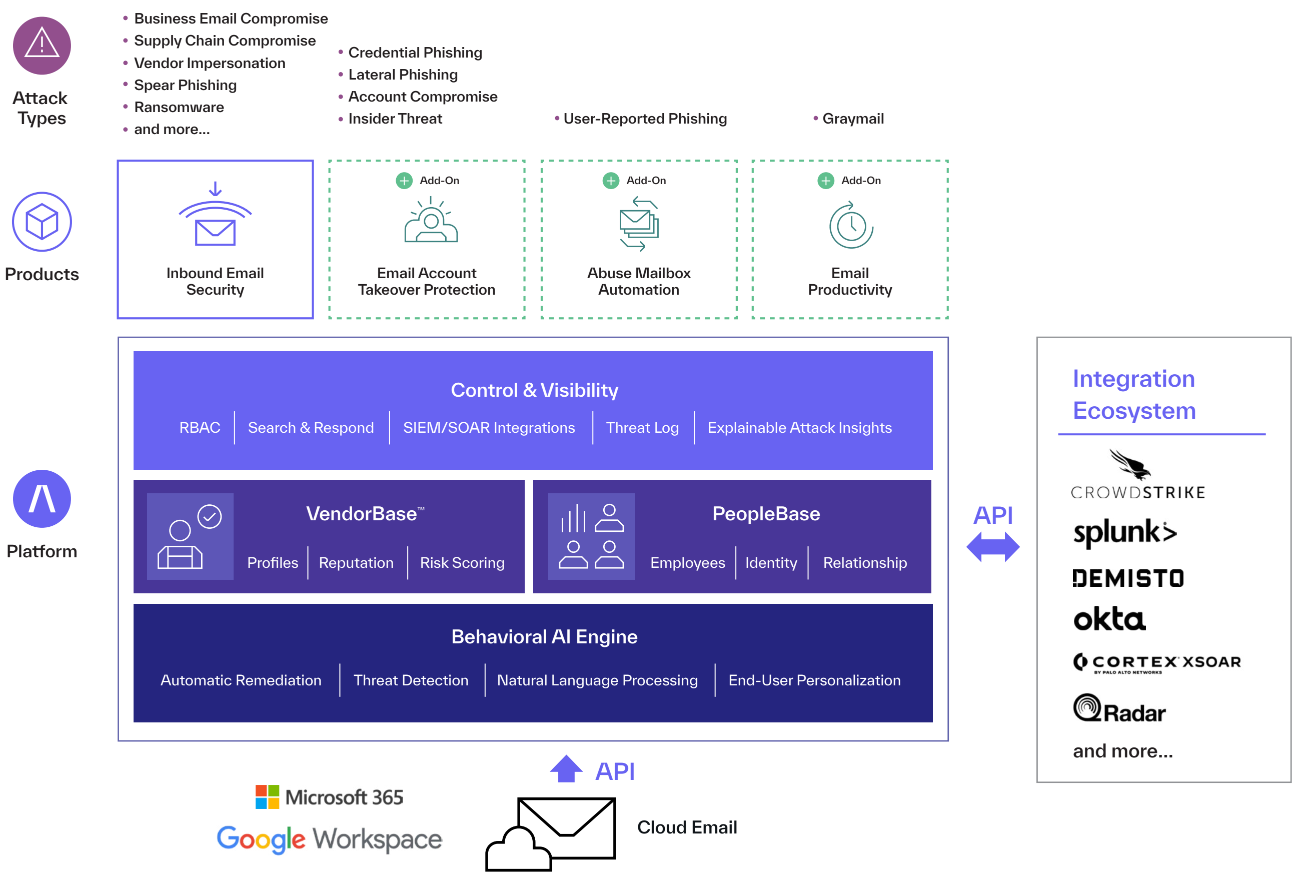
□ Can the solution augment your SIEM with metadata and risk scores for better attack correlation?

An Abnormal Solution to Cloud Email Security

As a cloud-native email security platform, Abnormal leverages behavioral data science to stop the never-before-seen attacks that evade traditional security tools. Where legacy email security solutions rely on rules and policies to identify attacks, Abnormal delivers a fundamentally different approach that precisely detects and then automatically remediates email threats.

The Abnormal platform delivers inbound email security, internal and external account takeover protection, and abuse mailbox automation, as well as productivity-focused promotional mail filtering and insights.

Abnormal Behavioral AI Platform



Attack Types

- Business Email Compromise
- Supply Chain Compromise
- Vendor Impersonation
- Spear Phishing
- Ransomware
- and more...

- Credential Phishing
- Lateral Phishing
- Account Compromise
- Insider Threat

- User-Reported Phishing

- Graymail

Products

- Inbound Email Security
- Add-On: Email Account Takeover Protection
- Add-On: Abuse Mailbox Automation
- Add-On: Email Productivity

Platform

Control & Visibility: RBAC | Search & Respond | SIEM/SOAR Integrations | Threat Log | Explainable Attack Insights

VendorBase™: Profiles | Reputation | Risk Scoring

PeopleBase: Employees | Identity | Relationship

Behavioral AI Engine: Automatic Remediation | Threat Detection | Natural Language Processing | End-User Personalization

API

Integration Ecosystem

CROWDSTRIKE
splunk>
DEMISTO
okta
CORTEX XSOAR
Radar
and more...

API

Microsoft 365
Google Workspace

Cloud Email

Unlike traditional email security solutions, Abnormal requires no rules or policies to detect attacks. Instead, security teams integrate Abnormal with Microsoft 365 or Google Workspace in minutes via API, and Abnormal starts working immediately to develop an organizational baseline of known-good behavior. Any email message that deviates from that baseline is automatically addressed and remediated.

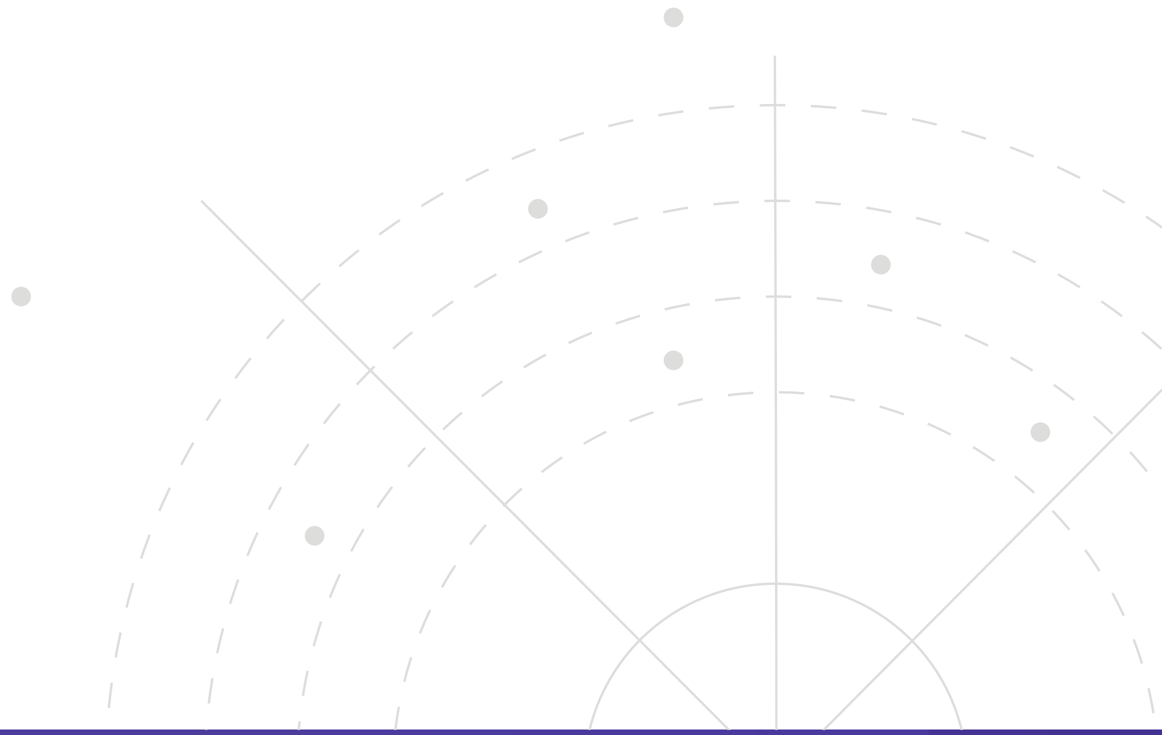
Abnormal also provides VendorBase, which automatically identifies all vendors in your ecosystem to understand their individual risk level. By recognizing when a vendor may have a high risk of fraud, Abnormal knows when an email should be more heavily scrutinized for malicious activity.

Selecting the Right Security Solution

While every organization has different requirements when it comes to cloud email security, there is little denying that there is a need for a solution to block the increasing threat of socially-engineered attacks and other malicious emails that bypass legacy solutions.

To maximize the impact of your email security platform, ensure that it offers superior protection against all types of email attacks, provides opportunities to improve end-user productivity, and can secure email infrastructure across all entry points. When combined with the ability to detect and automatically remediate compromised accounts, as well as abuse mailbox automation, the right solution will both protect your organization and save time for your security team.

Cloud email needs cloud email security. Be sure that the solution you choose provides what you need to protect your employees, environment, and organization.



Interested in Discovering Cloud Email Security?

Request a Demo:

abnormalsecurity.com →

Follow Us on Twitter:

@AbnormalSec