sublime

Email Security **Buyer's Guide**

What to know before buying an email security solution.

Contents

Email is ubiquitous.

Email has been the de facto standard of business communication for decades. News, requests, invoices... almost everything gets sent via email. So much information passes over email that you can get a clear picture of a business just by looking in its inboxes.

Email is reliable.

Email works consistently and expectedly. Everyone has an email address and if a message fails, a clear message is returned to the sender. Email doesn't accidentally get dropped between seats.

While email's ubiquity has driven adoption and increased surface area, it has also driven increases in attack volume, velocity, and technique evolution. This has led to a game of cat and mouse that, while a constant within security, is especially noticeable within the email domain.

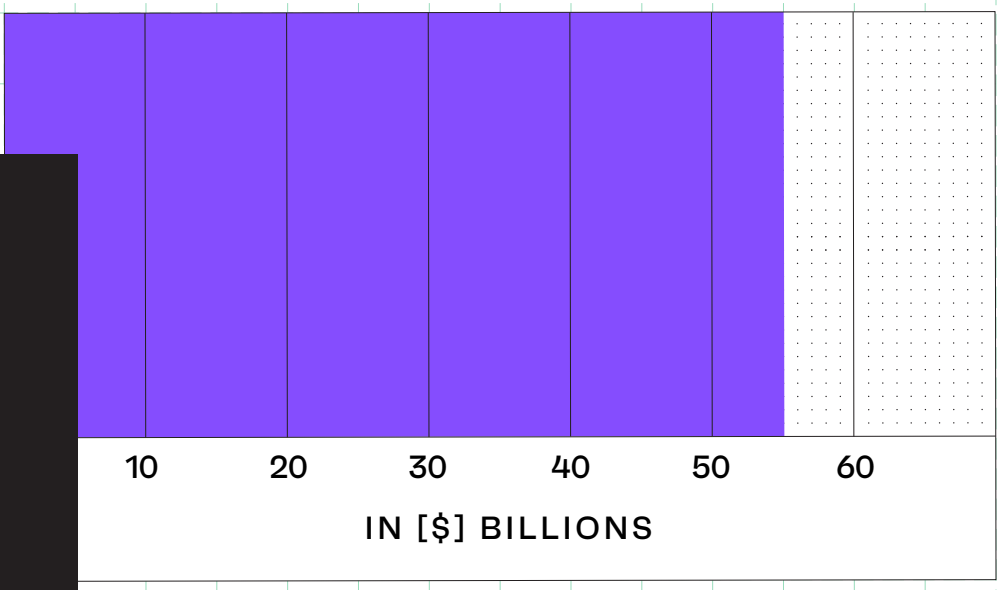
The cost of running an email scam is near zero, meaning bad actors can always be testing new variants and attack types with very little overhead. With the recent proliferation of LLMs, they can quickly research a target and then automatically create realistic scams that can easily pass as authentic to a busy employee.

But you know this. You're familiar with the stats.

$55 BILLION

in business email compromise (BEC) fraud losses between 2013-2023.

Source: https://www.ic3.gov/PSA/2024/



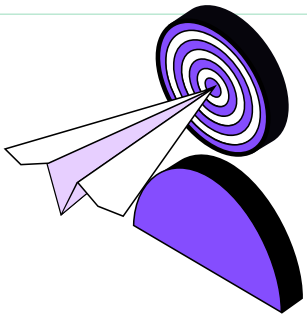
You're looking for a solution that keeps you secure against the full range of attack types.

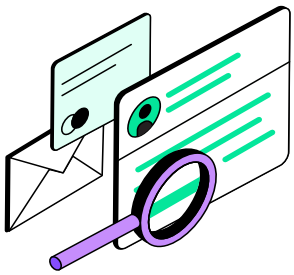
BEC/FRAUD

Social engineering-based attacks impersonating employees, VIPs, vendors, or other trusted entities to trick targets into transferring funds or sharing sensitive data.

CREDENTIAL PHISHING

Attacks that trick victims into providing their login credentials, often through deceptive email messages and websites that mimic legitimate platforms.





CALLBACK PHISHING

Messages impersonating reputable sources in order to persuade victims into calling a phone number, enabling bad actors to bypass traditional security.

MALWARE/ RANSOMWARE

Messages that deliver malicious payloads hidden within innocuous-seeming files, some of which can autoload.

EXTORTION

Attacks that coerce victims by holding sensitive information or assets hostage while demanding payment or concessions. These can be real or convincingly faked.

RECON

Messages that test the security perimeter of a target. The information gathered from these attacks is used to tailor further attacks like BEC and phishing to increase chances of success.

SPAM

While considered a nuisance more than an attack, spam can be used as a smokescreen to hide malicious attacks within a noisy inbox.

In this guide, we'll cover what to consider and your options for keeping your inboxes secure.

IMPLEMENTATION TYPES

Inline vs API

The main cloud email providers are Google Workspace and Microsoft 365. Each of these come with their own security protocols that act as a first line of defense. But these defenses are hurdles, not walls, with attackers devising novel ways to bypass them every day. This layer of email security is foundational for businesses, but not complete.

When deciding on supplemental email security, the first thing to consider is whether you want an inline or API solution. Each has its own pros and cons.

While most organizations choose one option, it's important to note that these two solutions are not mutually exclusive and can be applied on top of each other. **No two companies are the same, so the final approach is up to you.**

	Inline	API
Order of operation	The security solution sits in front of the user inboxes applying security before delivery.	Security is applied directly after a message reaches the inbox. Some solutions process in seconds, others may take minutes.
Mail delivery flow	Messages are only delivered after they're scanned.	Messages are delivered first and then scanned directly after.
Implementation	Routing rules must be updated to route mail through the inline mail server. For email gateways, MX records must be	The security service connects to the mail provider via API.
Service downtime	The service provider becomes a single point of failure for mail deliverability. A disaster recovery plan must be in place to mitigate disruption to business.	If the security service is down, emails are delivered without security screening. The business must be notified promptly that the messages haven't been scanned.
Header manipulation	Email headers are manipulated to pass email authentication, but can also be updated to inject scores/verdicts directly into headers.	Headers can be modified post-delivery.
DNS discovery	For email gateways, attackers can look at DNS records to see who your security provider is.	n/a
API Rate limiting	n/a	Depending on the email service provider and tier, API limits can be reached, so retries must be implemented to handle gracefully.
Deployment options	Talk to the vendor about cloud and tenancy options.	Talk to the vendor about cloud and tenancy options.

REQUIREMENTS

Time, Money, Coverage

Implementation type does not have to be a requirement of your selection process, just a detail. Most often, teams will create a list of potential solutions that include both inline and API-based solutions.

To narrow this list down to a few solutions to test head-to-head, we recommend considering the following three table stake items: **time, money, and coverage.**

REQUIREMENT 01	**Time** **COVERS:** How time intensive is implementation? How much time is saved once implemented?
REQUIREMENT 02	**Money** **COVERS:** How much will implementation cost? How much will the solution help you save?
REQUIREMENT 03	**Coverage** **COVERS:** Does the solution meet all of your coverage needs? Does it surpass them?

REQUIREMENT 01: TIME

Time

Time has a direct correlation to team satisfaction, as they'll want the tool to make their life easier in the long run. A longer ramp up can be justified with longer term gains, so be sure to consider both the front and back ends.

01
How long does it take to implement?

Depending on the type of solution you choose, implementation can be as simple as configuring API connections or as involved as setting up a duplicate of your environment as a sandbox.

02
How long will it take to configure your POC?

How many days/weeks/months of historical data are required for a POC?

How long does that ingest take?

03
How long will you be testing for?

Depending on the solution you're testing, there will be different date ranges to prove efficacy. In some cases, they may not even allow you to remediate during POC, giving you a shorter POC, but more time configuring the live environment.

04
How long does it take to ramp up your team?

Does the vendor offer training?

Is their documentation extensive and intuitive?

Do they provide a support or service offering for the first few months?

05
How intuitive and transparent is the platform?

When a false positive or false negative occurs, how easy is it for your team to perform a root cause analysis and apply a fix?

06
How much time does your team spend within the tool?

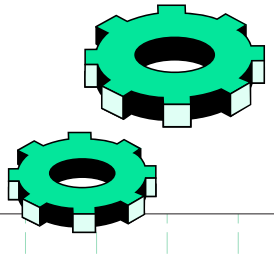
How much direct usage is required once the tool is running?

Can noise be easily filtered for your environment?

Does usage decrease over time, indicating a front loaded usage model?

07
How much of the usage can be automated?

Can your instance be tuned to maximize automations to decrease reliance on human intervention?



REQUIREMENT 02: MONEY

Money

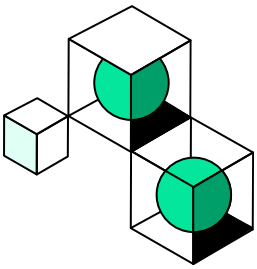
You have a budget and your tool will need to fit within that budget. Not just on the date of purchase, but every quarter after.

01

What is the licensing model?

As users are added, how much will the costs inflate?

Are group and shared mailboxes an additional charge?



02

What features come with each tier level?

Is the POC testing at a higher cost tier and will you have to give up features to stay within budget?

Are there others features that may impact the total cost down the road?

Are all of the things you saw in the demo included in the quote?

03

What sort of FTE hours are you looking at to be operational at scale?

Use the Time section above to determine what operating costs you'll be looking at.

04

How many other tools are required to run the platform?

Will you need to invest in any integration or automation tools?

Are there costs (ex: API call fees) for integrating with other tools?

REQUIREMENT 03: COVERAGE

Coverage

At a minimum, the tool you choose needs to detect and prevent email-based attacks and scams. But beyond that, you could have minimum requirements for threat hunting, attack surface reduction, customizable detections, and more.

01
Does it cover all of the attack types your company is facing?

The tool needs to be able to cover all the types of email attacks you're facing without being supplemented.

02
Are detections static, dynamic, or a combination of the two?

Is security built on lists and rules or does it use machine learning/AI for threat recognition?

03
Does it offer an abuse mailbox?

Does the tool provide an abuse mailbox for end users to send potentially malicious messages to?

04
Does it offer quarantine?

Does the tool provide a quarantine that's inaccessible to end users?

05
Can you understand what the tool is doing in your environment?

If somebody comes to you in two weeks asking if a message was/wasn't blocked, do you have the context you need to answer the question?

06
Can you adjust/add rules to your needs?

Can you adjust rules to your environment? To your business? To how your teams work?

Are the rules static or do they allow you to leverage AI, machine learning, and user behavior?

07
Does it allow for threat hunting?

Are you able to use the tool's detection capabilities to run custom hunts for proactive detection?

08
No tool is 100% perfect. What is the turnaround time for getting coverage updated?

What's the process for getting a rule or model updated? What's the SLA on rule updates per tier? How do you confirm coverage was actually updated?

DIFFERENTIATORS

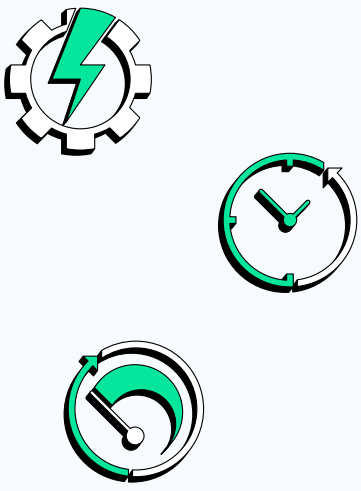
Efficacy, Transparency, Control

Once you've used your implementation and requirements criteria to narrow down your list of potential solutions, it's time to put them into a POC to see how they perform specific to your environment.

While testing, there are three interrelated attributes that you need to focus on: **efficacy, transparency, and control.**

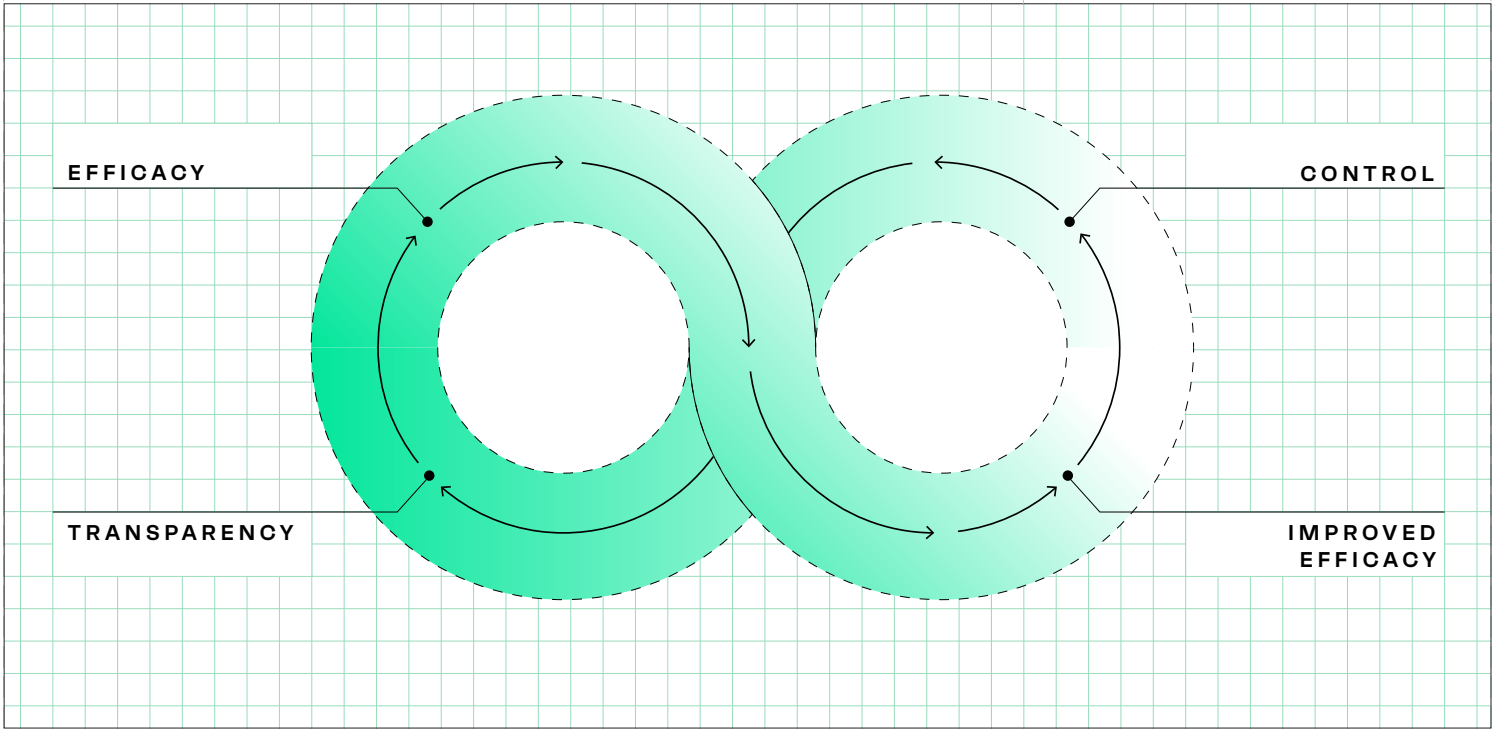
Let's look at the interconnectedness of these three in a highly-effective system.

The Email Security Efficacy Cycle



No two companies are the same, so there is no way for a vendor to precisely tell you how effective they are in your environment without a POC. Additionally, effectiveness should go up as the system is tailored to your company, starting during POC and continuing in production.

Efficacy can be maximized by being able to clearly identify shortcomings/failures and implementing fixes using this cycle:



Efficacy

When you start a POC, you'll have a baseline of efficacy that should already be close to your expectations. If efficacy is very low OOTB, it may not be worth your time to continue the POC.

Transparency

Once initial efficacy is determined, your solution needs to have the visibility to allow you to see what isn't working. You need to be able to see what detections are causing false positives and what is unique about the messages that are handled as false negatives.

Control

After gaining an understanding of efficacy failures, your solution needs to be able to be adjusted for your environment. AI models must learn and detections need to be able to be modified quickly to boost efficacy without flagging false positives.

Improved Efficacy

After learning the unique patterns of behavior to your company, efficacy should be higher.

The result? Efficacy never stops improving.

DIFFERENTIATOR 01: EFFICACY

Efficacy

Other facets of efficacy should be considered beyond the simple count of malicious emails identified.

Efficacy considerations should also include:

01

How are false negatives managed?

Every false negative is a chance for an attack to succeed. Your tool needs to be able to be adjusted quickly and verifiably as false negatives are identified.

02

How are false positives managed?

False positives can negatively impact business by keeping important communications out of inboxes. The tool needs to be able to be adjusted quickly and verifiably when messages are incorrectly flagged.

03

How many parts of an email can be used during detection?

Every part of an email (header, body, attachments, etc.) should be scanned for detection purposes, including optical character recognition of images (embedded and attached).

Additionally, the detection logic should be able to combine all the parts (ex: the content of the email with the contents of the attachment).

04

How many layers deep can links and attachments be scanned?

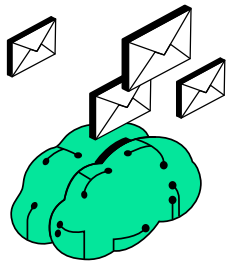
Attackers use URL shorteners and nested attachments to hide attacks. Your solution needs to be able to get through as many redirects and subdirectories as it takes to understand the attack.

05

How many different verdicts does the tool offer?

Email security isn't binary (malicious or non-malicious). Your security solution should offer a variety of verdicts to cover the spectrum of emails from malicious to unwanted to safe, with options in between.

DIFFERENTIATOR 01: EFFICACY



06

Are historical data and user behavior taken into account when identifying threats?

Your tool needs to recognize what's normal behavior for your company, departments, and users based on past interactions and behaviors.

07

How are AI and machine learning applied?

Tools that leverage Natural Language Understanding (NLU) and Named Entity Recognition (NER) have a better understanding of the tone and intent of a message. Tools that leverage computer vision are able to recognize and operationalize images and text within images Optical Character Recognition (OCR) for use with detections.

08

Is your tool too reliant on dynamic lists, rules, regex, and filters?

Solutions need adaptive detections powered by machine learning/AI to understand the intent of a message even if wording is varied.

09

How hard is it to manage an attack campaign?

Your tool needs to be able to group large scale attacks for easy triage across inboxes.

10

Can rules be adjusted for different teams or individuals within your company?

Different departments in your business may have different tolerance levels.

For more insight into this, see the Example Use Cases to Consider section later in this guide.

11

Are you allowed to test all functionality during POC?

Some vendors disable functionality during a POC, like remediation. Is that acceptable for your testing?

DIFFERENTIATOR 02: TRANSPARENCY

Transparency

Email is key to your business, and the tool you choose will be making automated, real-time decisions on email traffic. You will need to be able to understand what happened, why it happened, and how to alter the outcome for future messages if need be.

01

Do you get clear explanations of why a label was applied?

You should be able to open an email that's been flagged as malicious and easily understand why.

02

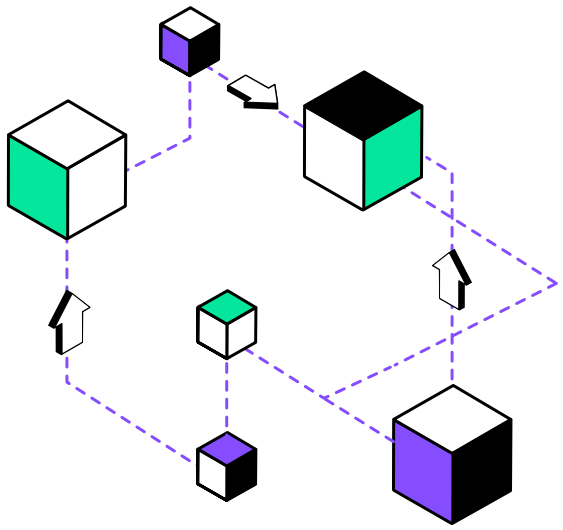
Is detection logic easy to understand?

When a detection fails or is overly sensitive, you need to be able to see why so you can adjust it.

03

How many methods of detection are in use?

You need to have insight into the rules, lists, filters, machine learning, and AI used in your solution.



04

How is detection logic adjusted or created?

Do you have to open a ticket with the vendor or can you apply updates directly to your system?

05

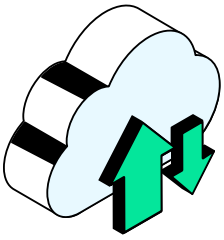
Will the solution be training its AI on your emails?

Most teams do not want their private corporate communications to be used as training material for LLMs.

DIFFERENTIATOR 03: CONTROL

Control

No two companies are alike, and yours can't be treated as an outlier by your security provider.



01

Can you enrich the solution with your own data?

Your email security solution should be able to operationalize your other threat intel.

02

Can it be deployed exactly the way you need?

If you need a self-hosted solution but the provider only does SaaS, you'll need to keep looking.

03

Is there a REST API?

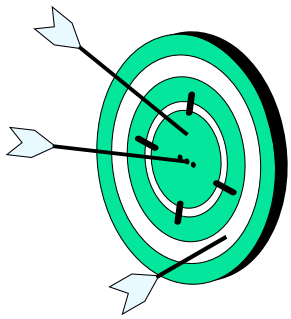
Your tool should have a REST API that allows response actions so you're able to build out custom integrations and automations.

04

Does it integrate easily with your existing SOAR/SIEM solutions?

Your email security needs to be able to easily push data into broader security ecosystems.

DIFFERENTIATOR 03: CONTROL



05

Can threat hunt logic be easily transitioned into rules?

After performing a threat hunt within a selection of messages, the logic from the hunt should be easily moved into a detection.

06

Can rules be configured for attack surface reduction along with threat detection?

You need to be able to put guardrails in place that clearly indicate risk without automatically flagging an email as malicious.

07

How granular does your control get?

Determine if you have the ability to make modifications you'll need to boost efficacy or if those rules are governed by the solution provider.

08

How easily can you adjust your system for updated needs?

You need to be able to apply updates globally as your company grows and evolves.

09

How quickly can your solution adapt to novel threats?

New attacks are invented every day. Your solution needs to show that it can stay up to date with the most novel attacks.

Example Use Cases to Consider

Flexibility is a key tenet of a best-in-class email security solution. Some email security best practices just don't apply to your organization.

Here are a few examples to help you start thinking about your own.

Finance teams want HTML attachments

While HTML attachments are a common vector for attack, finance teams legitimately use them for secure messaging with banking partners.

Recruiters want attachments from freemail

Unsolicited PDF from first time senders? Recruitment teams need those to get through.

Suppliers want invoices from freemail

Supply companies often work with small companies that don't have their own custom-domain email addresses. These need to be allowed.

VC firms want financial requests from new domains

A commonly blocked email is one that has a financial request from a new domain. If you're a VC, your success hinges on funding unknowns–unknowns that likely just spun up their new website. Their security solution can't blanket reject these types of emails.

Insider security

InfoSec teams like to be able to apply attachment rules in both directions. Your solution should be able to use the same rules for outbound as it does for inbound.

Executive-level personal mail habits

Your CEO has the tendency to get into business threads with their personal email address. An exception needs to be made instantly to keep them happy.

DFIR teams want ransomware requests

If you're on a security team either catching or negotiating with bad actors, your email security solution needs some exceptions for emails that are clearly malicious.

Email Security From Sublime

Sublime gives every team–from analysts to executives–the tools they need to be successful.

sublime

Get a demo to see our full range of Enterprise features:

https://sublime.security/demo/

SOC ANALYSTS

Make fast, accurate risk assessments and take the right actions with automatic quarantine, agentic AI triage, webhooks, alerting, and more.

INCIDENT RESPONSE

IR teams can unleash the full power of Sublime to close incidents quickly, including threat hunting, detection engineering, contextualized workflows, and integrations into SIEMs/SOARs.

SECURITY LEADERS & EXECUTIVES

Sublime gives you the context and reporting you need to be confident in your email security, as well as the AI and automations you need to maintain operational efficiency. Know the types of threats being faced, as well as who is being targeted, to keep your organization safe.

THREAT INTELLIGENCE

Sublime uses an industry-leading Core Feed from the start, but you can connect any third-party, private, OSINT, YARA, or or other threat intel feed to the platform to boost detections and retro-hunt.

DETECTION ENGINEERS

Give teams a full detection workbench for fast iteration and 30 days of backtesting, as well as threat hunting tools that leverage the same MQL and machine learning enrichments as detections.