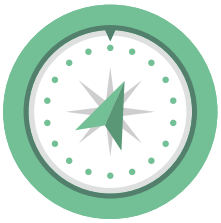


The Buyer's Guide to Email Security

LIBRAESVA

CONTENTS

INTRODUCTION

Choosing the right security and vendor is crucial in today's dynamic threat landscape. A secure email environment is an organization's first step to keeping your business safe from threats. But how do you know where to start?

There are several things to consider when evaluating potential email security providers, including comprehensive protection against evolving threats, integration capabilities, reliable performance, and strong support services.

In this guide, we've compiled a checklist to aid you in selecting your new vendor. By focusing on the attributes outlined here, you can identify an email security provider that aligns with your organization's needs. Let's explore the steps to take and areas you should consider so your organization can focus on what it does best–and leave the email security to the experts.

Phishing is the most prevalent threat in the US, up 34% year-over-year.

The United States Federal Bureau of Investigation's recent Internet Crime Report found that phishing is the most prevalent threat in the US — up 34% compared to the previous year.

PART 1: When to Make a Change

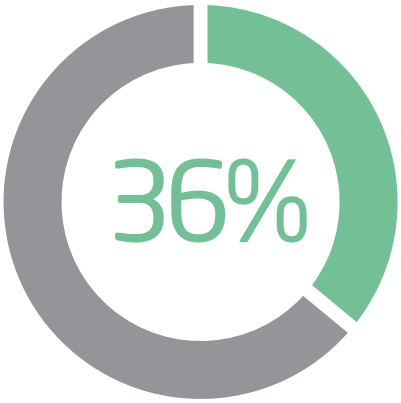
There could be many reasons why your organization is on the hunt for a new email security vendor. Here are a few that may be driving you to make a change.

Inadequate Protection
If your current email security vendor fails to provide sufficient protection against evolving threats, such as phishing attacks, malware, or data breaches, it may be time to explore alternative options. Regular security assessments and monitoring can help identify any vulnerabilities or gaps in your existing solution.

Poor Performance or Reliability
If your email security solution consistently underperforms, experiences frequent downtime, or causes delays in email delivery, it can negatively impact productivity and security. Unresolved technical issues or a lack of responsiveness from the vendor's support team may indicate a need for a change.

Changing Business Needs
Your email security requirements may change as your organization evolves. This can result from business growth, expansion into new markets, regulatory compliance updates, or technological infrastructure shifts.

Lack of Integration and Compatibility
If your email security does not integrate well with other critical systems or platforms in your organization, it can create inefficiencies and complexities. Seamless integration with your existing email infrastructure, directory services, cloud platforms, and other security solutions is essential.



...of all security breaches begin with a phishing attack

Inadequate Support and Vendor Relationship
Strong vendor support is crucial regarding email security. If you are consistently dissatisfied with the level of support, responsiveness, or expertise you receive, it may be a sign to consider switching. Effective communication, timely updates, and collaboration are essential for maintaining a successful vendor relationship.

Cost-Effectiveness
Regularly reassess the cost-effectiveness of your email security solution. If your email security's pricing structure no longer aligns with your budget or the value provided does not justify the cost, it may be worth exploring alternative options.

These are just a few of the reasons you may be considering making the switch. Now, let's look at how to start planning your search.

PART 2: Planning Your Search

To kick off your search, you'll want to consider some key questions and planning steps. Here are a few to get you started.

Identify Security Needs
Begin by assessing your organization's specific email security needs and priorities. Consider the threats you commonly encounter, regulatory compliance requirements, scalability requirements, and integration with existing infrastructure.

Define Requirements and Objectives
Clearly define your requirements and objectives. Determine essential features, such as anti-spam filtering, malware detection, malicious URL and attachment protection, phishing, remediation, encryption, data loss prevention (DLP), and user authentication. Prioritize these requirements based on their significance to your organization.

Identify stakeholders
The decision-making process for selecting an email security provider usually involves multiple stakeholders. While the specific individuals affected may vary depending on your organization's structure and size, the following roles commonly play a role in choosing an email security provider:

IT Security team
IT Security teams, including information security officers, IT managers, and cybersecurity professionals, typically play a critical role in evaluating and selecting an email security provider. They are responsible for assessing the organization's security needs, identifying potential threats, and ensuring that the chosen solution aligns with the overall security strategy and requirements.

IT Operations Team
IT Operations teams may be involved in the selection process, including system administrators and network administrators. They provide insights into the organization's existing IT infrastructure, email systems, and network architecture.

IT Procurement or Vendor Management
IT procurement or vendor management teams evaluate vendor proposals, negotiate contracts, and ensure that the selected email security provider offers favorable pricing, licensing terms, and service-level agreements.

Determine C-Suite involvement
Executives and management stakeholders, such as CIOs (Chief Information Officers), CISOs (Chief Information Security Officers), and other senior decision-makers, provide strategic direction, assess the potential impact on the organization's operations and budget, and align the selection process with broader business goals and risk management strategies.

Continued on next page >>

PART 2: Planning Your Search

Choose some user representatives
Involving representatives from user groups, such as department heads or end-users, can provide valuable insights regarding user experience and ease of use that contribute to selecting a solution that effectively addresses user needs while maintaining a high level of security.

It is essential to have cross-functional involvement from stakeholders to ensure that the selected provider meets the organization's security requirements, aligns with IT infrastructure, considers budgetary constraints, and addresses user concerns. This collaborative approach helps make a well-rounded decision that meets the entire organization's needs.

PLANNING CHECKLIST	✓
Identify Security Needs	
Consider your threat landscape	
Determine compliance requirements	
Define Objectives	
Outline your security objectives	
Prioritize your list	
Identify Stakeholders	
IT Security team	
IT Operations Team	
IT Procurement or Vendor Management	
C-Suite	
User representatives	

PART 3: What to Look for in an Email Security Provider

Now that you have your plan and you've answered some key questions, you can dive into your vendor selection process. Here are the areas you'll want to consider when evaluating your next email security vendor.

AI-ENABLED

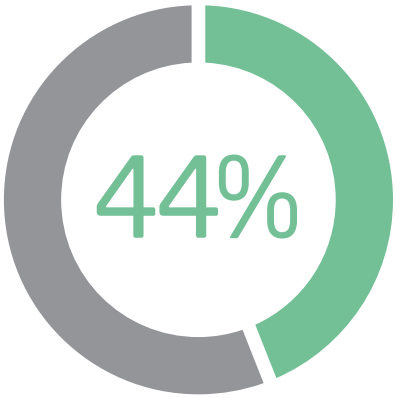
Email security solutions incorporating artificial intelligence (AI) can offer significant benefits.

Advanced Threat Detection

AI-powered algorithms can analyze and identify complex patterns and anomalies in email content, attachments, and user behavior. This allows the system to detect sophisticated and evolving threats - such as targeted phishing attacks, spear-phishing, or advanced malware - that traditional rule-based systems may struggle to recognize.

Real-time Behavioral Analysis

AI algorithms can analyze and learn from historical data, to establish baseline behavior for individual users or across the organization. By continuously monitoring email communication patterns and user behavior, AI can identify unusual or suspicious activities indicative of a potential security threat.



44% of organizations reported success rates over 80% for their AI-powered cybersecurity tools. (Gitnux)

Most modern email security solutions predominantly operate in the cloud; however, on-premises and hybrid deployments are also common.

PART 3: What to Look for in an Email Security Provider

Dynamic Risk Scoring
AI can assign risk scores to incoming emails based on various parameters, including content, sender reputation, attachments, and context. This provides a more accurate assessment so organizations can quickly prioritize and respond to high-risk emails.

Adaptive and Self-Learning Capabilities
AI systems can adapt and learn from new email security trends and attack techniques. They continuously update their knowledge and models based on evolving threat landscapes, allowing them to stay ahead of emerging threats.

Reduced False Positives
Traditional rule-based email security systems often generate false positives, flagging legitimate emails as potential threats. AI-based solutions can significantly reduce false positives by leveraging machine learning that learns from data patterns and user feedback.

Incorporating AI into email security solutions helps organizations stay ahead of the constantly evolving threat landscape, improving threat detection accuracy, reducing response time, and enhancing overall security effectiveness. AI's adaptive, self-learning nature ensures that the email security system remains robust and proactive in the face of emerging threats.

PART 3: What to Look for in an Email Security Provider

EASE OF USE

Consider how important it is for your users to have a straightforward solution that makes security easy, without affecting the quality of their daily inbox experience. Here are usability questions and considerations you'll want to explore.

Customizable

Is customization sufficient to enhance the solution's user-friendliness? Is the solution designed with ease of use in mind? Can administrators envision themselves effectively working with the solution?

Unobtrusive behavior

Is it easy to integrate with other solutions? Ideally, a cloud-based email security solution should seamlessly integrate into users' workflows, operating discreetly in the background. End-users should primarily notice a reduction in bothersome emails without being burdened by cybersecurity concerns.

Spam visibility

Can users easily see spam emails? Accessing emails marked as spam should be a straightforward and intuitive process. If the solution mistakenly flags a legitimate email as spam, the user should be able to recover it quickly. However, differentiating between confirmed "safe" emails and spam should require a separate process to prevent accidental network vulnerabilities.

Automated summaries

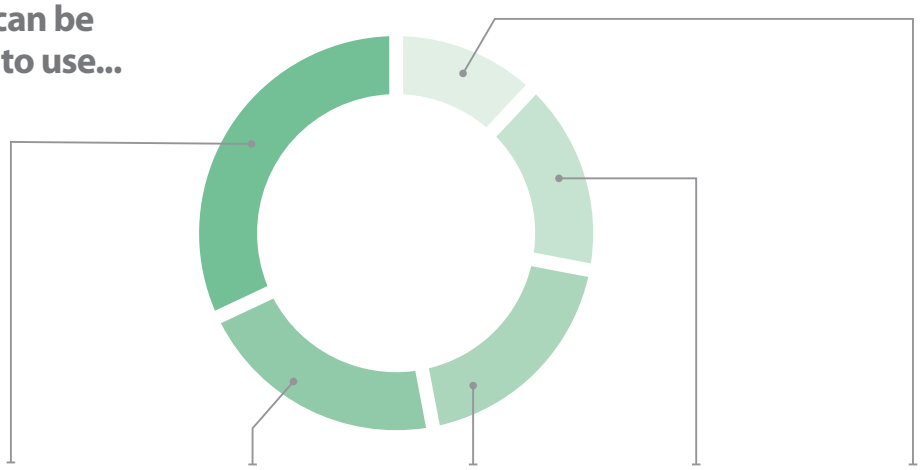
Are users notified when emails are sent to the spam folder via automated "wrap-up" notifications daily or weekly? This type of notification empowers users to identify any misclassified legitimate emails. The user or administrator should be able to personalize the frequency of these updates.

Suspicious email reporting

How effortless is it to identify suspicious emails and flag them? Can domains or addresses be easily blocked from sending emails to your accounts? Is it easy to retrieve information related to blocked emails?

A SaaS solution can be considered easy to use...

Source: Map My Growth



32%	21%	19%	16%	12%
If our non-technical employees can easily learn how to use it	If the interface is modern and intuitive	If many things are automated (little maintenance required)	If it doesn't take much time to get from beginner to advanced	If the onboarding is smooth/guided

PART 3: What to Look for in an Email Security Provider

PRICING & FEES

Consider the overall value provided by each email security provider you're considering, weighing the cost against the features, performance, and level of protection offered. Evaluate pricing models, such as per-user or per-domain, to align with your organization's needs.

Understanding the pricing and licensing structure of the solution you're exploring is crucial to ensure it aligns with your organization's needs.

There are other questions you'll want to answer regarding ownership and licensing. For instance, if a team member leaves the company, can their mailbox be transferred to another user without requiring an additional license? What happens to emails sent to an inactive user? Different providers have varying policies regarding shared mailboxes. Some may charge an extra fee for this service, while others offer it free.

Remember soft costs, such as integration services, support packages, add-ons, and more, should be included when you're making your selection.

You'll also want to consider if the vendor has budget-friendly complementary solutions, such as email security user training and email archiving. This way, you can get all of your key email security solutions from one vendor, with one contract.

Typically, plans are priced based on the number of protected mailboxes or the volume of email traffic. It is important to inquire about the consequences if these limits are exceeded. Will there be an additional fee for surpassing the specified thresholds? Similarly, if your usage falls significantly below capacity, can you downgrade your plan accordingly? Is it easy to upgrade your plan as your organization scales?

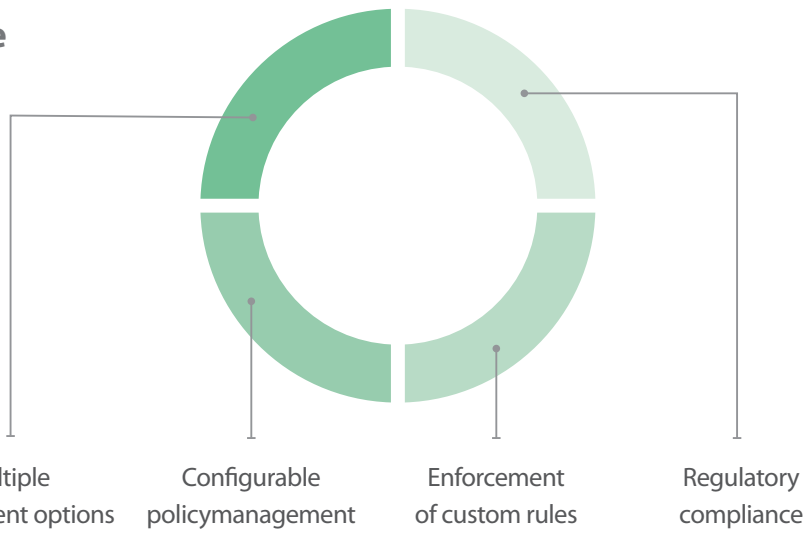
PART 3: What to Look for in an Email Security Provider

PLATFORM CONFIGURABILITY & FLEXIBILITY
Consider how easy it is to configure and customize the solution you're considering. Think about policies, as well as the presentation of information and data. Your admins need to be able to tailor policies to meet your industry's and your company's specific needs.

You should also investigate your deployment options. Whether your business wants to host, in the Cloud, on-premises, or using another option, ensure that the vendor can meet these needs.

Finally, check there are flexible policy management capabilities, allowing your admins to define and enforce custom rules for email filtering, whitelisting, blacklisting, data loss prevention (DLP), and regulatory compliance.

Your vendor should offer the ability to perform the following functions:



PART 3: What to Look for in an Email Security Provider

INTEGRATIONS
Integrations ensure the success and adoption of your email security solution. The specific integrations required may vary depending on your organization's needs and existing infrastructure. Here are a few common ones:

Email Clients
Seamless integration with popular email clients such as Microsoft Outlook, Gmail, or Thunderbird ensures that the email security solution can efficiently scan and protect emails within the client interface.

Email Gateways
Does the solution include or integrate with an email gateway? Email gateways allow for centralized management and enforcement of security policies, including spam filtering, malware detection, and data loss prevention (DLP). This ensures that all incoming and outgoing emails pass through the security solution.

Cloud Services
Integration with cloud-based platforms, such as Microsoft Office 365 or Google Workspace, is essential for organizations using cloud-based email services. It enables the security solution to monitor and protect email traffic within the cloud environment.

Active Directory or LDAP
Integration with directory services like Active Directory or LDAP (Lightweight Directory Access Protocol) facilitates streamlined user management and authentication. This integration simplifies user provisioning and ensures your solution aligns with existing user directories and access controls.

Incident Response Systems
Integration with incident response systems or ticketing systems allows for the automatic generation of security incidents and alerts facilitating efficient incident response and remediation processes.

API and Webhooks
An email security solution with well-documented APIs and webhooks enables custom integrations with other internal or third-party systems. This flexibility allows organizations to tailor the solution to their specific requirements and workflows.

PART 3: What to Look for in an Email Security Provider

LAYERED SECURITY
Multi-layered protection is vital for businesses of all sizes, regardless of industry. Threats are everywhere, and organizations need to implement a comprehensive defense strategy. This may be the most important requirement of your new email security solution.

The first layer of email security often involves an Email Security Gateway, a long-standing technology that has evolved over time. The second layer focuses on post-delivery protection, targeting advanced threats like Business Email Compromise. This layer may include features like inbox detection platforms where users can report suspicious messages for analysis and quarantine. The final layer is the incident response component, which helps identify and remove harmful emails based on user reports.

While gateways play a crucial role, incident response is also important, especially for addressing phishing attacks. Gateways can detect phishing attempts with malicious URLs or attachments, but may struggle with plain-text phishing messages. Incident response components provide an additional layer of defense in such cases.

In addition, you'll want to ensure the following are in place:

Strong Data Encryption
The security provider should offer robust encryption protocols to safeguard the confidentiality and integrity of email communications. Encryption ensures that sensitive information remains secure in transit and at rest.

Advanced Threat Intelligence and Updates
Regular updates and real-time threat intelligence are crucial to stay ahead of emerging email threats. The provider should actively monitor and respond to new attack vectors, continuously improving their security measures.

Automation and Quick Response Times
Automation and Quick Response Times allow for efficient handling of email submissions and timely notification of users

PART 3: What to Look for in an Email Security Provider

COMPLIANCE & REPORTING
Security, compliance, and reporting expectations and requirements can vary depending on the sector in which organizations operate.

Some of these standards may be legally binding. Some cloud email security solutions automatically log activities for auditing purposes, enabling organizations to demonstrate their adherence to best practices during audits.

Organizations can address the requirements of common regulatory frameworks such as GDPR, HIPAA, and FINRA by demonstrating their policies for preventing data mismanagement. If your organization falls under the oversight of any of these frameworks you should ask your provider about their ability to prove and enforce compliance.

When considering an email security solution, ask yourself: How efficient are the reporting and auditing functions? Are logs automatically generated, and how can they be accessed? Does the solution provide predefined Data Loss Prevention (DLP) policies that align with specific regulatory frameworks?

You'll also want to invest in robust reporting and auditing capabilities if required by your industry. Look for comprehensive insights into email security events, threat detection, and user behavior. Detailed audit logs and analytics help in identifying potential vulnerabilities and maintaining compliance.

Your Email Security Solution Should Address:

- **Phishing**
- **Malware distribution**
- **Ransomware**
- **Data loss prevention**
- **Spoofed Emails** using DKIM, SPF, and DMARC
- **Anti-Spam**
- **Compliance**
- **Security testing/training**
- **And more!**

PART 3: What to Look for in an Email Security Provider

SCALABILITY & PERFORMANCE

Consider the provider's ability to handle email traffic volume and accommodate your organization's growth. Ensure that their infrastructure can deliver high performance and low latency, even during peak usage periods.

API-backed email protection scans incoming emails once they have arrived in your inbox. While this scanning process is often more advanced than the default spam filters provided by your email host, it may result in a slightly longer delay. Since the email has already reached the user's inbox, there is a potential risk if they open a malicious link before the email has been scanned.

The duration of these scanning checks can impact user productivity. For example, when waiting for an email containing an OTP (One-Time Password), it is undesirable to experience even a brief delay in receiving that email.

Investigating how the cloud email security solution operates and the timeframe required for email scanning is essential. Is the scanning time consistently quick, or are there factors that could potentially cause delays? How long does the scanning process typically take if sandboxing or CDR (Content Disarm and Reconstruction) techniques are employed?

In addition, you'll want to ask about downtime. You want an email security system you can trust. Check for SLAs that guarantee service reliability and uptime, ensuring minimal disruptions to your email infrastructure. If a SaaS-based solution often fails or SLAs aren't up to par, you may want to move on to another vendor.

Make sure the solution your organization chooses meets the

99% uptime standard.

PART 3: What to Look for in an Email Security Provider

REPUTATION & SUPPORT
Reputation and support may be last on this list, but it's crucial. Exceptional support can make a vendor stand out, while subpar support can lead to regret over the contract agreement.

Consider the provider's support offerings, including availability, response times, and expertise, and assess the provider's reputation, customer reviews, and industry recognition. Look for certifications or partnerships demonstrating their commitment to security standards and best practices.

During the implementation process, support can be significant, and it's vital to understand the available resources and the required involvement from your side. Will you need to allocate your IT employees' time, or will the vendor handle the majority of the implementation work?

Assess the vendor's ongoing support and resource allocation throughout your entire customer journey. Will you have a dedicated account manager who can address your immediate concerns and ensure your long-term success, or will you be directed to a ticketing system for any requests?

Observe the involvement of the vendor product team. Are they receptive to customer feedback and responsive in addressing concerns and implementing customer-driven enhancements? A vendor with engaged product and support teams indicates a positive future customer experience.

Assess your email security providers reputation

- **Expertise**
- **Customer reviews**
- **Response times**
- **Industry recognition**

CONCLUSION

Choosing the right email security and vendor is paramount in today's ever-evolving threat landscape. With many organizations anticipating severe email-borne cyber-attacks within the next year, securing your email environment is a critical step to safeguard your business.

Remember to carefully consider deployment options, AI-driven capabilities, ease of use, pricing structures, platform configurability, and integrations when evaluating potential vendors. Multi-layered protection, compliance and reporting features, scalability, and reputation and support should also be key factors in making your decision.

With this guide you can confidently choose the right email security solution and ensure the safety of your organization's communication channels against emerging risks. Stay vigilant, proactive, and well-informed in the ever-changing landscape of cybersecurity threats.

PART 4: Vendor Checklist

Use this checklist to help you build your shortlist or make your final decision.

CHECKLIST FOR SELECTING AN EMAIL SECURITY PROVIDER	/LIBRAESVA	Vendor 1	Vendor 2
Comprehensive Protection			
Extensive protection from evolving threats (phishing, malware, data breaches)	✓		
Advanced AI capabilities for threat detection and analysis	✓		
Layered security measures against a wide range of threats	✓		
Customization and flexibility in policy management	✓		
Seamless integration with popular email clients and services	✓		
Performance & reliability			
Consistent performance, reliability, and minimal downtime	✓		
Scalability and efficiency in handling email traffic	✓		
Ease of use			
User-friendly interface and intuitive management features	✓		
Adaptability to changing business needs	✓		
Flexible deployment options (on-premises, cloud-based, etc.)	✓		
Compliance			
Meets regulatory and compliance requirements	✓		
Robust reporting and auditing capabilities	✓		
Pricing & Fees			
Transparent pricing and licensing options	✓		
Cost-effective solution(s)	✓		
Support			
Ongoing support and training	✓		
Excellent technical support and reliable service	✓		
Positive reputation and industry recognition	✓		

ABOUT LIBRAESVA

If you're looking for a vendor that checks all the boxes and will work with you to protect your business and your people, look no further.

At Libraesva, we believe enterprise email security should be made easy, so that every organization can eliminate email borne threats, preserve email data and provide an environment for their people to communicate safely. We are 100% focused on creating simple to manage, all-inclusive email security solutions.

Libraesva has won many awards, is named as Category Leader for 2023 in Email Security by GetApp, a Gartner company, is consistently certified by Virus Bulletin as one of the best email security systems, and is trusted by leading brands around the world.

Libraesva.com