Security Guide for Microsoft 365 Outlook

5 Criteria to Consider When Evaluating Email Security

Email is just one facet of a broad, complex enterprise technology ecosystem, but it's a critical one: With the average employee sending over 10,000 emails every year, email remains the backbone of corporate communication.

If your organization uses Microsoft 365 Outlook, you likely need an additional layer of email security, particularly if you are in a highly regulated industry subject to regulations like HIPAA, ITAR, GDPR, CJIS, or others.

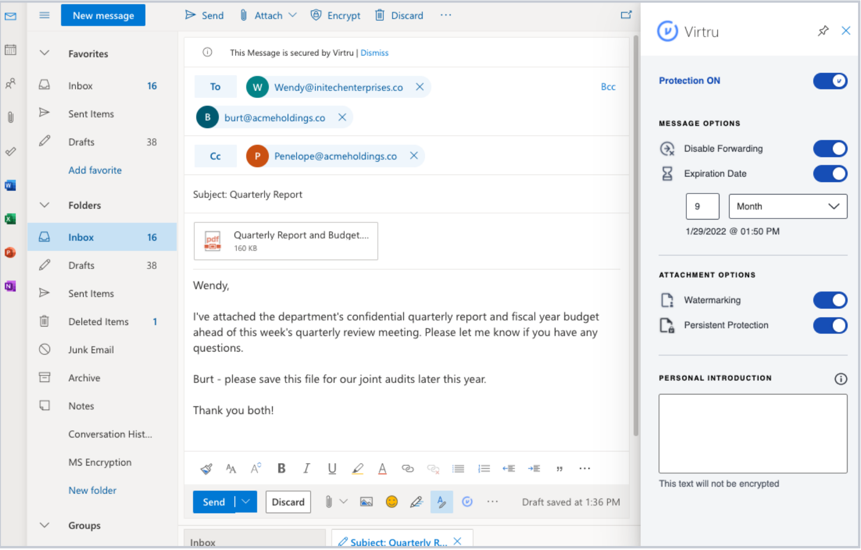
When evaluating an email security solution to augment Microsoft 365 Outlook, there are five criteria to consider to ensure you choose a solution that will equip you and your users to share data freely and securely — both today and in the future.

1. Implement strong security across devices and platforms

The enterprise technology ecosystem is complex, with hundreds of interconnected software applications, security tools, and networks facilitating data sharing. If your organization is operating in any kind of hybrid environment — Microsoft Outlook and Gmail, PC and Mac, cloud and on-prem, in-office and work-from-home, mobile and desktop — ensuring data is protected across environments can be a challenge at best, and a security nightmare at worst.

Your top priority is ensuring that you're safeguarding your organization's most vital data in motion, in use, and at rest. With email representing a massive flow of data in and out of your organization, it's a smart place to start.

For organizations using Microsoft 365 Outlook, look for an additional layer of protection to supplement Microsoft's native email security features as Microsoft 365 may not deliver the same data protection that might be needed, especially for highly regulated industries. Also look for a solution that integrates within the browser, desktop, and mobile Outlook experiences, equipping your users to secure the data they're sharing from any device, and within any instance of Outlook.



This Message is secured by Virtru | Dismiss

To: Wendy@initechenterprises.co, burt@acmeholdings.co   Bcc

Cc: Penelope@acmeholdings.co

Subject: Quarterly Report

Quarterly Report and Budget.... 160 KB

Wendy,

I've attached the department's confidential quarterly report and fiscal year budget ahead of this week's quarterly review meeting. Please let me know if you have any questions.

Burt - please save this file for our joint audits later this year.

Thank you both!

Draft saved at 1:36 PM

Virtru

Protection ON

MESSAGE OPTIONS

Disable Forwarding

Expiration Date

9 Month

1/29/2022 @ 01:50 PM

ATTACHMENT OPTIONS

Watermarking

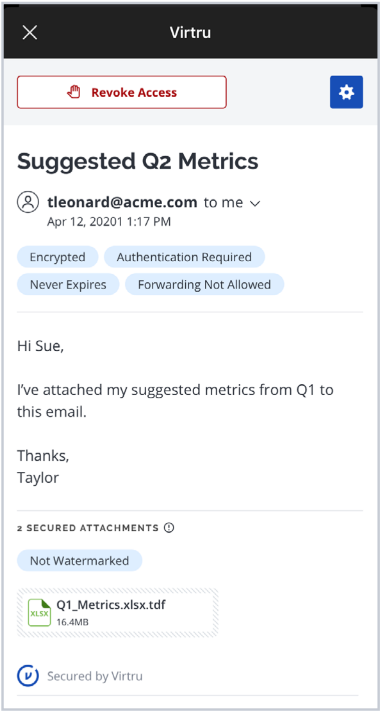
Persistent Protection

PERSONAL INTRODUCTION

This text will not be encrypted

Interoperability should also be a key focus for tech leaders: You don't want gaps in your data protection due to incompatibility, especially when you have some users on Mac, some on PC, and some primarily using mobile.

A recent study from Okta showed that 36% of its Microsoft 365 customers also deploy Google Workspace[1] so for organizations with different email configurations for different users, ensure your Gmail and Outlook users have consistent experiences and your users are able to send and receive encrypted data across platforms, seamlessly. More importantly, ensure that when sharing encrypting emails you are able to secure data inside and outside your organization. In a recent Virtru study, we saw that 82% of organizations share data externally every day, with over four in 10 doing so on a continuous basis.[2]



Suggested Q2 Metrics

tleonard@acme.com to me

Apr 12, 20201 1:17 PM

Encrypted | Authentication Required | Never Expires | Forwarding Not Allowed

Hi Sue,

I've attached my suggested metrics from Q1 to this email.

Thanks,
Taylor

2 SECURED ATTACHMENTS

Not Watermarked

Q1_Metrics.xlsx.tdf 16.4MB

Secured by Virtru

[1] Okta Businesses at Work 2021 Report

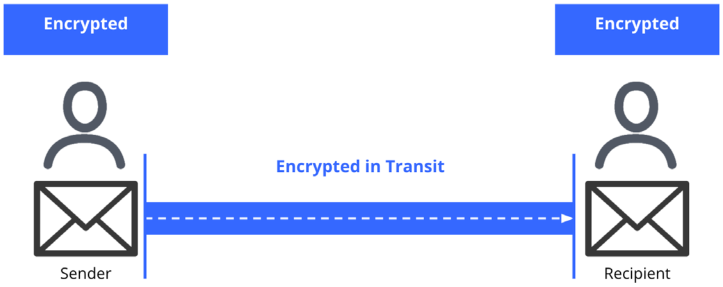
[2] Virtru Securing the Digital Workplace Report

2. Equip your team with a solution that aligns with your business goals

Your email security solutions should support your organization’s strategy — not just for technology, but for the business overall. Increasingly, technology has come to the forefront as a predictor of business success: Your products, offerings, and services are only as seamless and competitive as the technology infrastructure supporting them.

The tech partners and vendors that you select become an integral part of your business strategy. Examine whether they are providing you with the flexibility and scalability you need today, as well as in the future. A large Virtru retail customer has shared that they are no longer investing in traditional infrastructure and are now looking to grow and invest in ecommerce. By adding end-to-end encryption and an added layer of security, they are helping to mitigate risk, drive business alignment, and drive innovation in a secure fashion.

For those looking to achieve a Zero Trust security strategy, examine whether your data security tools equip you to achieve the level of granularity and data-centric protection you want to achieve. Are your tools moving you forward in terms of securing the data your teams share, or are they holding you back from being more agile and targeted with your data protection strategy?



End-to-End Encryption with Virtru

- Encrypted at all times
- Data stays protected, throughout the lifecycle
- Zero Trust, split knowledge key architecture further prevents unauthorized access
- Use existing accounts
- No new usernames or passwords

With a data-centric approach to security, you can set your organization up for greater flexibility in the future. As the threat landscape escalates, and as regulations like GDPR, CJIS, HIPAA, and others continue to evolve, flexibility is key for ensuring that organizations can adapt to these changes. In terms of both effort and cost, having a framework optimized for information security will pay off in the long run.

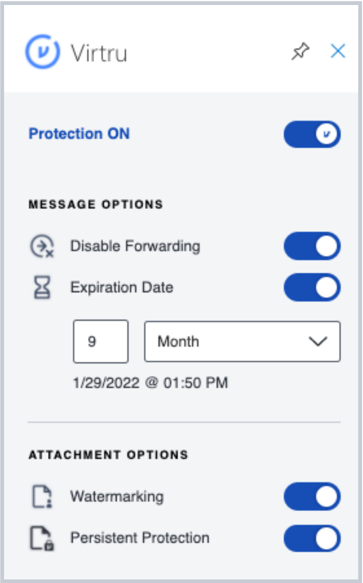
Ensure you look for a data-centric email protection for Microsoft Outlook that gives you full control of your data, across the entire data lifecycle. Look for self-hosted encryption key options, so that neither Microsoft nor any other provider can access encrypted information. Additionally, should a data breach or other incident occur, you can immediately rotate your encryption key to mitigate any data loss.

3. Ensure your teams can collaborate freely

Data is only valuable when it's accessible. It's not useful to anyone if it's locked away: It needs to be used, analyzed, and shared.

With the prevalence of work-from-home and distributed workforces, the surface area of risk for an organization is wider than ever. Employees need to collaborate and share information more broadly. It's critical that employees have the tools they need to share information freely while still protecting it. In other words, ensure that sensitive data can flow between senders and recipients seamlessly, while remaining under your control even after it's been sent and opened. The spectrum of sensitive data is nuanced, so look for email encryption that gives users several options for how they want to safeguard their data, including:

- Disabling forwarding
- Setting an expiration date
- Applying watermarking
- Enforcing persistent protection, which requires the recipient to authenticate every time they access the shared information, even if it's been downloaded to a computer
- Securely authenticating recipients without any hassle, enabling secure and seamless collaboration and data sharing



Protection ON

MESSAGE OPTIONS

Disable Forwarding

Expiration Date

9 Month

1/29/2022 @ 01:50 PM

ATTACHMENT OPTIONS

Watermarking

Persistent Protection

This way, administrators also gain visibility into their users' data sharing, and can determine which external domains are receiving shared data, who is sending protected data, and what kinds of data they're sharing. If they see something that doesn't look right, make sure that they also have the authority to revoke access to data at any time—either at an individual level or at an organization-wide level.

4. Implement granular controls to protect business data

Once a standard email leaves your organization, you lose visibility into where it goes from there: Where it's forwarded, who downloads attachments, and how long that information is being circulated.

This makes it nearly impossible to fully understand or mitigate data loss if a sensitive file is shared. When evaluating an email protection solution for Outlook, examine whether it covers the entire life cycle of the data, from creation to sharing and beyond, and that you are able to audit the data flow at any time.

Admins and users should be able to see exactly who has accessed and shared information, and revoke access at any time, including disabling forwarding, and setting an expiration date for access to data — even after the email has been sent and even opened. In the event of a breach admins can recall information and stay in control.

This visibility into the full data lifecycle puts IT leaders and administrators at ease, knowing that they have persistent control over their organization's sensitive data at all times.

5. Deploy quickly and easily across your organization to ensure you are getting the most value

Email security tools are only effective when employees actually use them, so they need to be straightforward to implement, easy to use, and seamless for recipients to access.

A lot of email security solutions are portal-based—requiring recipients to create a username and password to access encrypted information. This creates hurdles for recipients and, as a result, employees may hesitate to use these solutions. This is especially true for executives, sales teams, or teams that collaborate with high-value external partners. They want to put their best foot forward with clients and colleagues, without introducing friction into the data sharing process. In a recent Virtru study we saw that over one-third of users are within sales, support, and marketing, and that over half of encryption policies are created by users in HR and Finance.

You want to think through the user experience for everyone who interacts with your email security tools—not just for your administrators, but also for your end users and their networks of recipients, whether those are consumers, clients, partners, or investors.

In addition, you want to ensure that you are able to deploy email encryption quickly and easily and that it integrates directly within all instances of Outlook. The total cost of ownership is important to evaluate any time you are adding new tools, and the cost of deployment needs to be considered together with the cost of the new security tool. Selecting a solution that takes months to deploy can be frustrating and unproductive, not to mention resource intensive, taking away from other projects you can be working on.

About Virtru

Virtru is a global leader in data security and privacy. Virtru's email encryption for Microsoft 365 Outlook complements and enhances your Microsoft experience with the secure, data-centric protection you need. Whether you're in a highly regulated industry like healthcare, manufacturing, or government that requires meeting compliance needs—or you want to safeguard customer and company data from the escalating number and frequency of data breaches, Virtru can help you ensure your data is protected everywhere it's shared.

Learn how Virtru can help you share sensitive data in Microsoft 365 Outlook.
Contact us to schedule a demo. virtru.com/contact-us

virtru

At Virtru, we empower organizations to unlock the power of data while maintaining control, everywhere it's stored and shared. Our portfolio of solutions and tools—built on our open data protection platform—governs data throughout its lifecycle. More than 6,000 customers trust Virtru for data security and privacy protection.