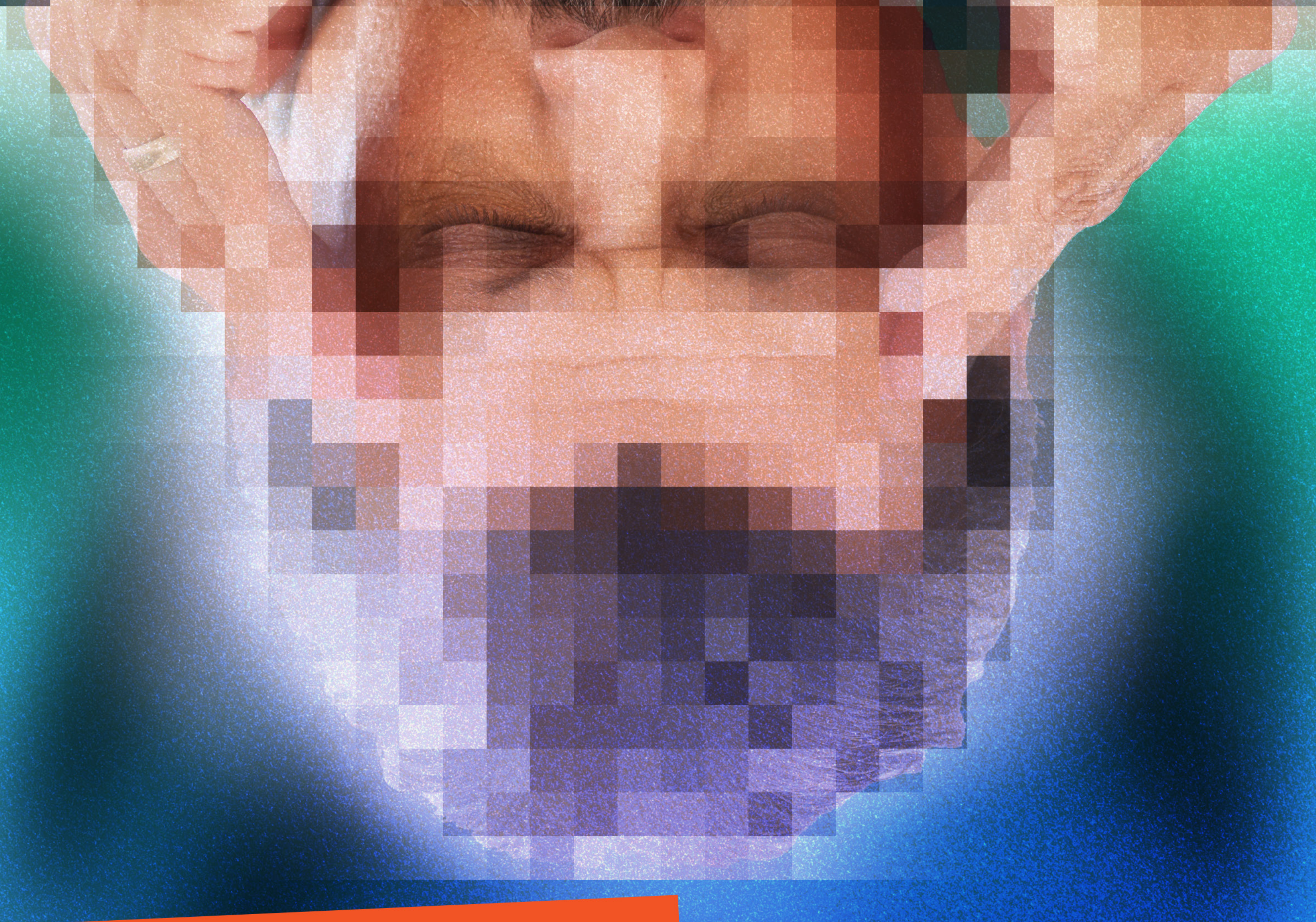


SIX WAYS TO CURE EMAIL ENCRYPTION HEADACHES IN MICROSOFT 365

A free eBook by mailprotector

About This Guide

Welcome to "**Six Ways to Cure Email Encryption Headaches in Microsoft 365**," an eBook designed to help Managed Service Providers (MSPs) navigate the often complex and confusing world of email encryption.

As organizations increasingly rely on Microsoft 365 for email communications, ensuring that sensitive data remains protected has never been more critical. Yet, while Microsoft 365 offers three types of email encryption, many MSPs struggle with gaps, complexity, and challenges that could expose their clients to risk.

This eBook will guide you through six key strategies to overcome these email encryption headaches, empowering you to offer better security solutions to your customers. From understanding Microsoft's built-in limitations to discovering what features to prioritize in an email encryption solution, we've got you covered with actionable insights and practical advice.

No need to grab the Advil, just keep reading.

With the cost of data breaches hitting a record high and the email encryption market expanding rapidly, industry insights reveal a pressing need for solutions that address complexity, user experience, and key management challenges.

The global average cost of a data breach in 2024 is $4.88M USD—a 10% increase over the previous year and the highest total ever.

IBM

Source: https://www.ibm.com/reports/data-breach

65% of organizations cite complexity and poor user experience as major barriers to adopting email encryption solutions widely.

FORRESTER®

Source: https://www.forrester.com/report/the-state-of-encryption-2023/RES179959

59% of respondents cite key management as the top encryption challenge.

ENTRUST

Source: https://www.entrust.com/resources/reports/global-encryption-trends-study

The global email encryption market size is projected to grow from $6.2B USD in 2023 to $16.3B by 2028.

MARKETSANDMARKETS™

Source: https://www.marketsandmarkets.com/Market-Reports/email-encryption-market-182623205.html

Microsoft 365's Built-in Email Encryption: A Critical Analysis

To effectively provide the right email encryption tools to the right clients at the right time, MSPs must understand the core functionality of Microsoft 365's three primary email encryption methods first:

Office Message Encryption (OME)

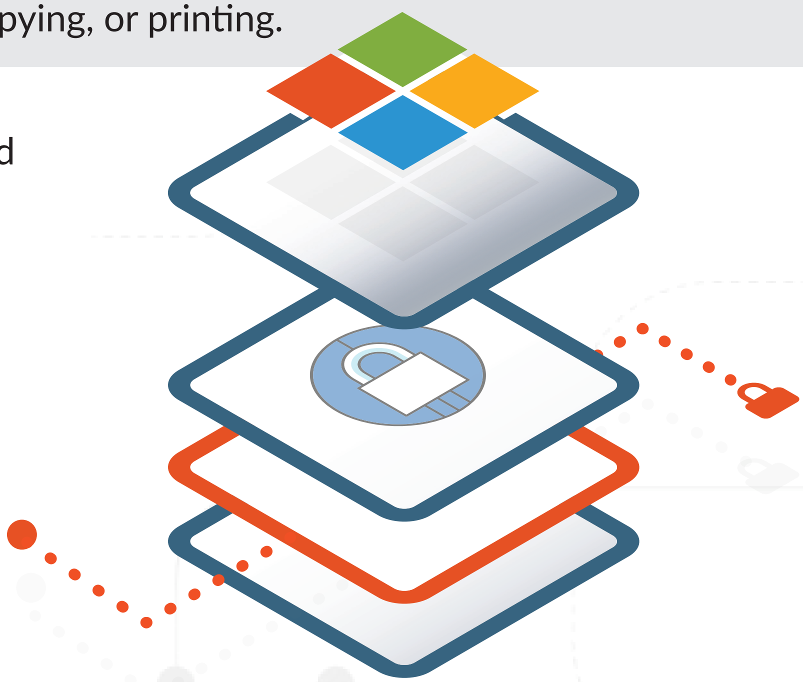
Server-side encryption with web portal access. Allows sending encrypted emails to any recipient, regardless of their email provider.

Secure/Multipurpose Internet Mail Extensions (S/MIME)

End-to-end encryption using public/private key pairs. Requires both sender and recipient to have S/MIME certificates installed.

Information Rights Management (IRM)

Content control and encryption for emails. Enables senders to restrict recipient actions like forwarding, copying, or printing.



Each method has its own strengths and limitations regarding ease of use, key management, and compatibility with different email clients and systems.

Let’s dive in.

OME

Office Message Encryption (OME)

OME is Microsoft 365's built-in solution for email security, offering a balance between protection and usability.

This cloud-based service encrypts emails on Microsoft's servers before transmission, making it compatible with any email service. Outlook users have a seamless experience, while other recipients access encrypted messages through a web portal.

OME's key advantages include easy implementation and integration with other Microsoft 365 services. However, OME does have limitations. Senders have limited control over encrypted messages once sent, and the extra steps for non-Outlook users can create friction. Additionally, it may not meet some organizations' advanced security or compliance needs.

MSPs should carefully evaluate OME's suitability based on their client's specific security requirements, budget constraints, and regulatory obligations before recommending it as part of a comprehensive email security strategy.

- 👍 **Integrated**
- 👍 **Easy to use**
- 👎 **Limited control**
- 👎 **Recipient friction**
- 👎 **Compliance gaps**

Top 4 Pain Points of OME Encryption

Recipient Friction

Non-Outlook users must navigate to a separate web portal to access encrypted messages, potentially discouraging consistent use and slowing communication. This extra step can lead to frustration and reduced adoption of secure email practices, especially when dealing with external partners or clients.

Limited Control

Once an encrypted email is sent, senders have minimal control over the message. They can't easily revoke access or track who has viewed the content. This lack of granular control can be problematic for sensitive communications that require ongoing management or in situations where message recall is necessary.

Key Management Concerns

With encryption keys managed by Microsoft, organizations lose some control over their data security, raising concerns about potential unauthorized access or compelled disclosure. This centralized key management approach may not align with organizations' security policies that require complete control over their encryption keys or have strict data sovereignty requirements.

Compliance Gaps

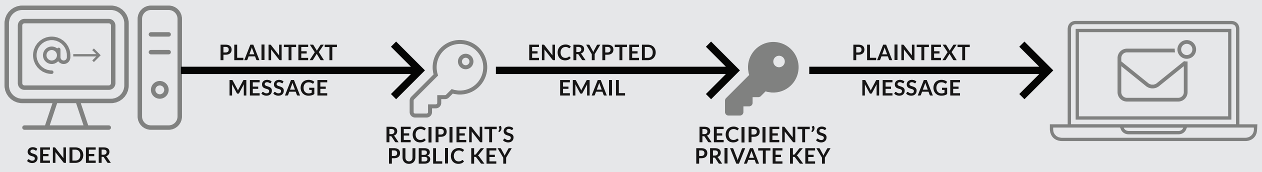
OME may not meet all regulatory requirements for certain industries, leaving potential compliance gaps that could expose organizations to risk. Organizations in heavily regulated sectors like healthcare or finance may find that OME's features fall short of the specific encryption and data protection standards mandated by regulations such as HIPAA or GDPR.

S/MIME

Secure/Multipurpose Internet Mail Extensions (S/MIME)

S/MIME is an end-to-end email encryption standard supported by Microsoft 365, offering high security for email communications. It uses public-key cryptography, where each user has a pair of keys: a public key for encryption and a private key for decryption. This ensures only the intended recipient can read the message.

S/MIME's main advantages include strong security, message integrity verification, and non-repudiation. However, it comes with significant complexity in implementation and management. Another notable limitation of S/MIME is that it prevents Microsoft 365 from scanning encrypted emails for malware and viruses. This creates a blind spot in the organization's email security infrastructure, shifting the burden of threat detection to the endpoint level.



MSPs should consider S/MIME for clients with high-security needs and the technical resources to manage the complexities. It's best suited for organizations where the benefits of end-to-end encryption outweigh the implementation challenges.

- 👍 Strong security
- 👍 End-to-end encryption
- 👎 Complex setup
- 👎 Key management challenges
- 👎 Limits malware scanning

Top 4 Pain Points of S/MIME Encryption

Key Management Concerns

Managing cryptographic keys in S/MIME presents significant challenges. If a private key is lost, all previously encrypted emails become inaccessible, potentially resulting in critical data loss. Conversely, if a private key is compromised, all past and future communications are at risk. Implementing secure processes for key storage, backup, and rotation can be complex and resource-intensive.

Complex Setup and Certificate Management

S/MIME requires each user to have a digital certificate, which can be complicated to obtain, install, and manage. This complexity extends to certificate distribution, especially when communicating with external parties.

Limited Compatibility

Not all email clients and services support S/MIME, which can create barriers to communication. Users may find themselves unable to send encrypted emails to certain recipients or struggle to read encrypted messages on mobile devices, leading to frustration and potential security breaches.

Interference with Malware Scanning

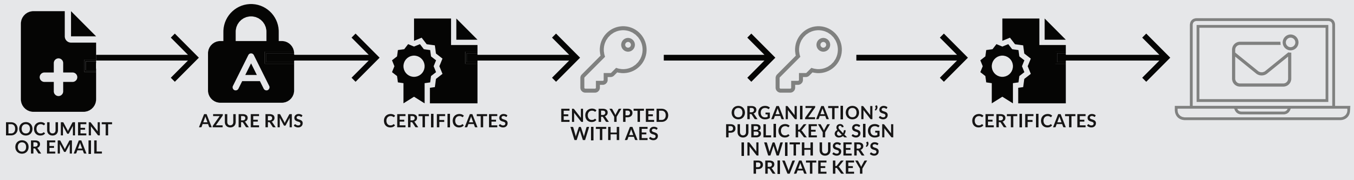
S/MIME encryption prevents Microsoft 365 from scanning the content of encrypted emails for malware and viruses. While some security measures can still be applied based on unencrypted metadata, organizations using S/MIME need to place greater emphasis on endpoint protection and user education to guard against malware. This limitation could potentially increase an organization's vulnerability to email-borne threats.

IRM

Information Rights Management (IRM)

IRM is a technology supported by Microsoft 365 that helps protect sensitive information from unauthorized access. Unlike traditional encryption methods, IRM focuses on controlling what recipients can do with the information after they access it.

IRM works by applying usage rights and restrictions to email messages and attachments. These controls can prevent actions such as forwarding, copying, printing, or taking screenshots of protected content. The protection travels with the document, even when it leaves the organization's boundary.



A key advantage of IRM is its granular control over document usage. It allows organizations to implement detailed policies based on user roles or document sensitivity. However, IRM has challenges, including complex setup and potential user friction. Another notable limitation is that it may not provide true end-to-end encryption like S/MIME.

MSPs should consider IRM for clients who must control sensitive information beyond their organizational boundaries. It's particularly suitable for industries dealing with confidential information that requires persistent protection. However, MSPs should be prepared to assist with the complex setup and ongoing management that IRM requires.

- 👍 Granular access control
- 👍 Persistent protection
- 👎 Complex setup
- 👎 Potential user friction
- 👎 Not true end-to-end encryption

Top 4 Pain Points of IRM Encryption

Complex Setup and Management

Implementing IRM requires careful planning and configuration. Organizations need to define and maintain detailed rights management policies, which can be time-consuming and complex.

Lack of True End-to-End Encryption

Unlike some other encryption methods, IRM does not provide true end-to-end encryption. While IRM protects content and controls its usage, the information may still be accessible to Microsoft or other intermediaries under certain circumstances. This limitation can be significant for organizations dealing with highly sensitive data or those in strictly regulated industries that require complete control over their information.

User Experience Challenges

While IRM offers strong protection, it can create friction in user workflows. Protected documents may require additional steps to access, and users might face restrictions on common actions like copying, printing, or forwarding. This can lead to frustration and potential workarounds that might compromise security.

Dependency on Azure RMS

IRM in Microsoft 365 relies on Azure Rights Management (Azure RMS) for key management and policy enforcement. This dependency on cloud services may not align with organizations' security policies that require complete on-premises control over their data protection mechanisms.

SIX STRATEGIES TO OVERCOME EMAIL ENCRYPTION HEADACHES

After exploring the limitations of Microsoft 365's email encryption options, you might wonder, "So what now?" Don't worry, we've got you covered. Let's dive into six practical strategies that will not only solve the email encryption headaches we've discussed but also elevate your email security game.

#01

Keep It Simple, Keep It Secure

Let's face it: if email encryption is a hassle, people won't use it. Look for tools that make email encryption as easy as clicking "send." You want robust security without the headache of complicated setups or extra software. The best solutions will encrypt messages automatically so your team doesn't accidentally send sensitive data in the clear. Remember, the easier it is to use, the more likely your clients will actually use it!

#02

Make Life Easy for Recipients

Ever tried to open an encrypted email and felt like you needed a Ph.D. in computer science? Yeah, not fun. Your encryption solution should be a breeze for recipients, whether they're in your organization or not. Think secure access without the friction – even for that not-so-tech-savvy client. After all, secure communication shouldn't mean putting the brakes on business.

SIX STRATEGIES TO OVERCOME EMAIL ENCRYPTION HEADACHES

#03

Spread Out Those Keys

Putting all your eggs in one basket is risky, especially when it comes to encryption keys. Instead of centralized key management (aka a hacker's dream), look for solutions that use a decentralized or session-based approach. It's like giving each conversation its own unique lock. This way, even if one key is compromised, the rest of your data stays safe and sound.

#04

Keep an Eye on Your Data

Wouldn't it be great if you could track your encrypted emails like a package? Look for solutions that offer end-to-end visibility. You should always know where your data is, how it's protected, and who's accessing it.

SIX STRATEGIES TO OVERCOME EMAIL ENCRYPTION HEADACHES

#05

Stay Ahead of the Compliance Game

With new data protection regulations popping up like whack-a-mole, your email encryption solution needs to keep up. Look for tools with built-in compliance features for standards like HIPAA. The best solutions will help you manage and prove compliance without manual headaches.

#06

Serve Up the Whole Email Security Enchilada

Let's face it: focusing solely on email encryption is like ordering an enchilada with just the tortilla. Sure, it's a start, but it's just one ingredient in the recipe that'll make cyber threats say, "No gracias!"

What you really need is a fully loaded dish of encryption, threat detection and remediation, compliance, continuity, and more.

And just like you wouldn't want different chefs preparing each part of your enchilada, you'll want one trusted vendor to whip up this email security fiesta. That way, you'll get a perfectly balanced blend of protection, consistent flavoring (aka policies), and a single number to call when you need extra salsa (or support).

SIX WAYS TO CURE EMAIL ENCRYPTION HEADACHES IN MICROSOFT 365

Closing Thoughts

By implementing these six strategies, you're not just solving the email encryption headaches caused by Microsoft 365's limitations – you're setting up an email security posture to combat today's threats and tomorrow's challenges.

When you're ready to experience the peace of mind that comes with comprehensive email security, we invite you to explore what Mailprotector has to offer. Whether you're looking to enhance your current email security measures or completely revamp your approach, we're here to help you serve up the whole enchilada – minimal assembly required.

Thanks for reading!

m mailprotector®

Mailprotector designs, builds, and supports products that help organizations secure and optimize email. Our mission is to unleash email as the revolutionary communication tool it was meant to be, so people can focus on using their talents to move the world forward.

LEARN MORE

mailprotector.com/demo