zivver

How to fix the security flaws in secure email gateways

A comprehensive guide to today's email security challenges

Introduction

The rise of digital transformation has led to a significant increase in email traffic and, as a result, the number of threats posed to our business emails. Many organisations rely on a secure email gateway (SEG) as a main line of defence against these threats. However, while SEGs do offer protection against inbound threats, they leave organizations at risk to one of the leading vectors for data incidents.

This report investigates why an increasing number of organisations, are recognizing the need to complement SEGs with an email data protection (EDP) supplement to ensure complete email security, and how, through a combination of both, organizations can reduce the leading causes of data leaks.

How important is email security?

Email remains a primary communication tool for the majority of organisations, across all sectors. Research shows that **88%** of employees and **97%** of managers believe email is essential for their business. In 2021, there were an estimated **319.6 billion** emails sent and received daily around the world. This figure is projected to increase to **376.4 billion** by 2025.

In order to build an effective data loss prevention strategy, organization leaders must first identify where the primary risks lie – that is, understanding the leading causes of data leaks.

It is common knowledge that the risk of data loss or data breaches via email is already high and is continuing to increase. As such, IT and data governance leaders realise the importance of equipping employees with tools to protect the sensitive data they share via email every day. At the same time, organizations must ensure compliance with evolving data protection legislation including the GDPR to avoid substantial reputational damage, financial losses, and legal consequences.

According to the ICO, **80%** of data leaks are 'non cyber related' incidents; incidents which are not caused by SPAM, malware, ransomware and phishing, but accidental data loss.

In fact, the leading causes of data incidents are often the simplest mistakes with the biggest consequences – sending information to the wrong person (misaddressed email), mistakenly sending the wrong information (failure to redact), adding recipients in the 'To' field rather than using Cc or Bcc (Failure to use BCC), and/or not using the right label or tool. Unauthorised access, often due to a lack of two factor authentication (2FA/MFA) protection, is also a leading cause of data leaks.

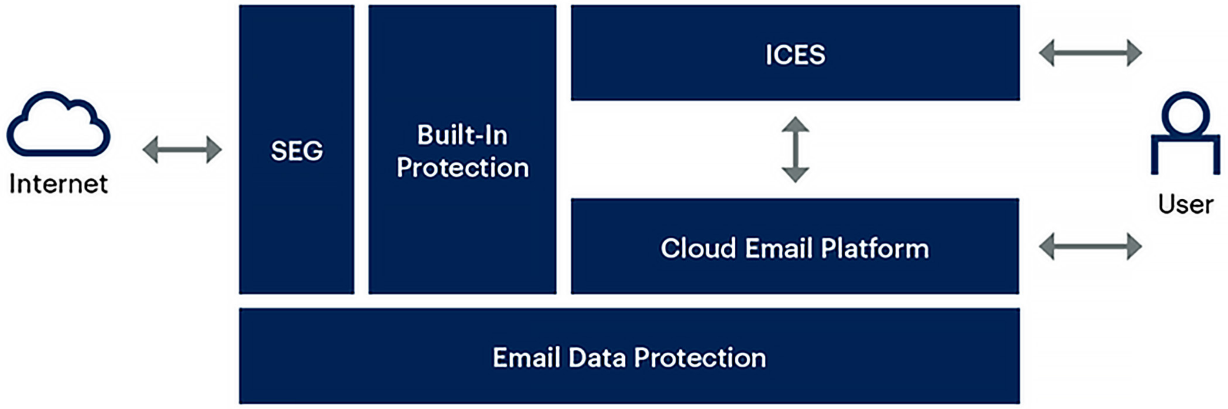
Employees cannot be trained to avoid making mistakes. While education is important (indeed, security training does play an important role in protecting an organization against security incidents), it is also essential to implement tools that definitively address the main causes of data leaks.

A combination of technology and training is the silver bullet to preventing data leaks today. Ensuring said technology prevents both inbound and outbound threats – malicious and non-cyber related attacks – is integral to preventing costly data incidents.

Limitations of SEGs

According to 2023 Gartner® Market Guide for Email Security, there are three main types of email security solutions (see Figure 1):

Email Security Submarket



Source: Gartner
SEG: Secure email gateway; ICES: Integrated cloud email security
735200_C

Gartner.

As per Gartner "Secure email gateway (SEG) – Email security for both inbound and outbound email has traditionally been provided by SEG solutions either as an on-premises appliance, a virtual appliance or a cloud service. SEGs process and filter SMTP traffic, and require organizations to change their Mail Exchange (MX) record to point to the SEG.

Integrated cloud email security (ICES) – The adoption of cloud email providers that provide built-in email security hygiene capabilities is growing. Advanced email security capabilities to supplement these native capabilities are increasingly being deployed as integrated cloud email security solutions rather than as a gateway. These solutions use API access to the cloud email provider to analyze email content without the need to change the MX record. Integrated solutions go beyond simply blocking known bad content and provide in-line prompts to users that can help reinforce security awareness training, as well as providing detection of compromised internal accounts. Initially, these solutions are deployed as a supplement to existing gateway solutions, but increasingly the combination of the cloud email providers' native capabilities and an ICES is replacing the traditional SEG.

Email data protection (EDP) – Email data protection solutions add encryption to track and prevent unauthorized access to email content before or after it has been sent. EDP can also help prevent accidental data loss due to misdirected recipients."

The first line of defence between an organization and external threats, SEGs are designed to protect against what are traditionally considered to be the most prominent security threats: SPAM, viruses, malware and ransomware. These solutions are built to be invisible to end-users and typically block or quarantine messages classed as dangerous.

However, targeting non-cyber related security threats requires a different approach. These solutions must empower busy, well-meaning employees to send sensitive information securely, with the appropriate security measures applied. Employees must be enabled to work securely and efficiently.

This requires outbound email security measures to not only empower best practice with every email and file sent, but they must also not hinder workflows. In addition, recipients to secure emails must also enjoy a user-friendly experience.

While most SEG suppliers understand the need to also address outbound risks, their operating models and technologies often constitute very basic solutions, resulting in poor user experience and unsophisticated functionality.

End to end email security

EDP supplements are designed to complement cloud email platforms such as Microsoft 365 and SEGs. They provide comprehensive protection against outbound risks with the following functionality:

Right sized security and best practice: Employees are notified when to encrypt emails before sending.

Intelligent algorithms: Machine learning powered business rules, tailored to the specific needs of the organization, identify and alert employees to the presence of sensitive data in their emails and attachments, empowering users to encrypt emails or review the contents of their messages before sending.

Zero-access encryption: Ensuring only the intended recipient can access sensitive data at rest with zero access, zero knowledge encryption.

Multi-factor authentication: The ability to configure multi-factor authentication controls, per the recipient's preferred method of authentication.

Large file sharing: Email clients limit file sizes to 25MB typically; file transfer sites often fail to meet data protection requirements and fall short on preventing non-cyber related causes of data incidents. EDPs integrate with email clients to enable employees to send large files securely.

Tracing capabilities: Legal proof of delivery and audit logs enable data security professionals to report and manage incidents with the relevant authorities, supporting compliance with data protection legislation.

Email revocation: Efficient email recall, without time limits, enables incidents to be controlled and even avoided in the instance that an email is yet to be opened.

Not all EDP solutions deliver all of these functionalities. User experience for both the user and recipient also varies across different providers.

The solution to email security

Zivver has been recognized as a Representative Vendor for Email Data Protection for three consecutive times in the Gartner Market Guide for Email Security report.

Zivver Secure Email and Secure File Transfer lead a new generation of secure digital communications, providing effortless, smart, secure technology to safeguard sensitive information while ensuring regulatory compliance. Zivver empowers employees to work with minimal disruption through seamless integration with Outlook, Microsoft 365, and Gmail, adding a security and privacy layer to existing platforms.

By operating silently in the background of your email client, employees can share sensitive data and large files without jumping through hoops, securing sensitive data:

- **Before sending,** with prompts to encrypt emails and act on potential errors
- **During transit,** with advanced encryption and zero knowledge, zero access methodology (because we don't hold your encryption keys)
- **After sending,** with the ability to recall emails, configure MFA, manage access controls, and data logging

Trusted by over 8,000 organizations globally, Zivver empowers organizations across all sectors including central and local government, healthcare, legal, education, accountancy and finance.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Conclusion

Email security is complex and SEGs alone cannot deliver comprehensive email security. By complementing SEGs with an EDP supplement, organisations can ensure end-to-end email security that protects against both inbound and outbound risks.

With an effective EDP supplement, organizations can significantly reduce data leaks while increasing productivity business-wide, ensuring that sensitive information is protected in accordance with data protection laws and regulations.

Zivver Secure Email delivers human error prevention, email encryption, and legal proof of delivery tools, empowering users to manage their sensitive data securely, effortlessly.

Learn more about how Zivver can support your organization.

zivver

London

5 New Street Square
EC4A 3TW London
United Kingdom

+44 (0) 203 285 6300

Amsterdam

Spaklerweg 52
1114AE Amsterdam
The Netherlands

+31 (0) 85 01 60 555

linkedin.com/company/zivver facebook.com/zivver @zivver_en

zivver.com