techworld FROM IDG Insights

Issue: **April 2019**

THE COMPLETE GUIDE TO ENTERPRISE EMAIL

Credit: iStock

Produced by IDG

Credit: iStock

You’ve got mail

Despite the emergence of a whole raft of ‘email killers’ over the past few years, such as Slack and Microsoft Teams, email remains the de facto mode of office communication, bringing with it purchasing decisions, management headaches and a whole bunch of security risks.

Front, the hot San Francisco-based start-up which creates software to simplify the management of shared inboxes, found that the average person spends half their workday in their inbox. Research from The Radicati Group found that people sent and received more than 120 billion work emails every single day in 2017.

What we are saying is that even if it’s not everyone’s favourite communication channel, email is far from dead, meaning if you run an IT department, it should still be front of mind.

In this month's Complete Guide we run through everything you need to know about the state of enterprise email today, including which vendor to choose, how best to manage your organization's email and protect against threats. Scott Carey

Contents

Credit: iStock

Best email provider for business 2019

We look at some of the things you should be considering when choosing an email service for your business

It's a huge part of office life, but most of our working lives will see our email client dictated by the company we have joined, with little room to change. However, for those of us going it alone and setting up independent businesses, or those now managing major IT decisions, choosing or deciding to switch to a new email provider isn't something that can be decided on overnight.

Most of us will have used Microsoft's email offering, Outlook, or Google's Gmail. Both offer a great business email service, with loads of storage and integrated calendars. However, while these are good options, they are not the only ones out there. Here, we look at both well- and lesser-known email platforms, and provide advice on hosted or self-hosted options.

As with picking any new software, there are plenty of things to consider before taking the plunge. Usability, for example, is extremely important, especially if you're going to have a large amount of staff transitioning onto the new platform. Ask your potential service provider questions like: Does the platform have a steep learning curve? Will it provide online training? What online resources are available to users?

You should also take note of the extras you'll get. Many of the firms here also offer document editing suites, advanced email security, and business add-ons such as accounts and invoicing management.

If you don't need any additional features, you could save some money by just going for a standalone email.

One decision you will face, though, is whether to go for webmail or desktop.

Webmail

Emails are stored on an online server mailbox, meaning an Internet connection is required to access mail. Some businesses prefer this over on-premise email hosts as it offers flexibility and doesn't take up any physical storage.

Webmail usually provides greater storage space, and in most cases unlimited storage is still pretty cost-effective. However, because webmail services do not work offline, reliability can sometimes be an issue.

Desktop email

Emails are stored on-premise, so you don’t need an Internet connection to access your emails. For some businesses this is a big plus because it means multiple email accounts can be open at the same time without signing in and out of accounts. As desktop email doesn’t require an Internet connection it won’t fail in times of poor bandwidth, gaining a point for reliability. On the downside syncing devices is more time-consuming than webmail, data is stored in one place so is potentially vulnerable, the server will require maintenance, and you are linked to an operating system that is restrictive if your business runs both PCs and Macs.

Microsoft Outlook and Google Gmail

Outlook and Gmail are the two most popular email services, and likely to be the most recommended for both business and personal use. Although they offer similar functionalities, both have their promoters and detractors. Here we examine some of the important deciding factors between the two.

Note that we are looking at Outlook as part of Microsoft’s cloud Office 365 suite rather than as a standalone Exchange product, and Gmail as part of the broader G Suite set of business software.

User experience

In 2018, Microsoft Outlook added a new Simplified Ribbon feature that better aligns with other Office software and reduces clutter at the top of your inbox. Users can now personalize or remove commands to suit their individual requirements. The inbox message list was also improved, so users can more easily identify important messages. This includes the ability to colour code or flag messages for clear visual markers. Another area to receive an update was the folder pane, which now features favourites, personal folders and group icons. Overall, the user experience is now simpler to navigate and customize to individual needs.

Gmail has always prided itself on providing a clean, simple inbox view and has long offered customizable features. The main feature that tends to grab users' interest is the conversation view of emails, which makes sending messages faster and easier. Gmail also includes filters and labels for email management, with the ability to filter messages in groups of 'from', 'to', and whether messages are with or without attachments.

Its latest update in 2018 delivered a brand-new user interface, with calendar and tasks embedded within the inbox. New features include the ability to snooze an email, push reminders, use automatic responses, plus offline functionality was improved. Gmail is also increasingly leveraging Google's machine learning expertise to make email 'smarter', with the option of ordering emails by importance, for example.

Storage

Microsoft and Google both offer 15GB of free storage. However, Gmail's storage offering is spread across Google Drive and Google Photos. It's unlikely that any business user would opt for the free service, though.

Google offers unlimited cloud storage on both its business and enterprise plans, or up to 1TB for businesses with fewer than five users.

Microsoft Office 365 Business subscribers are provided with 50- to 100GB of mailbox space, depending on which plan they are on, and 1TB of total storage as standard.

Integrations and add-ons

Both Gmail and Outlook come as part of a broader office suite, housing file storage, word processor, spreadsheet, and presentation tools.

Google Docs, Sheets and Slides users can invite others to edit documents and collaborate in real time, either suggesting edits, making tracked changes or reviewing the document's full edit history. Plus, with Gmail, you'll be able to open an email attachment and it will launch in the relevant integration, ready for you to review, edit, and so on.

Similarly, Outlook also offers easy access to Word, Excel, PowerPoint and OneNote from the email client.

Both services come with seamlessly integrated calendars and contacts, as well as email scheduling, filters, flags and smart searches. Outlook also houses a variety of add-ons (or add-ins as Microsoft calls them), such as online payment platforms like PayPal. Other add-ons include GitHub, Twitter and Trello.

Email sizes

Typically, business users are able to exceed the default file size limit if the mail server allows it. This includes file compression or saving files to a cloud storage service, such as OneDrive, Dropbox, iCloud or Google Drive, and sharing a link. The stated maximum file size limit for email attachments in Outlook is 20MB for business email. Gmail offers a size limit of up to 25MB, and if attachments pass this limit then Gmail automatically adds a Google Drive link for the recipient to open.

Videoconferencing

Both clients offer solid videoconferencing capabilities. Users of Gmail Business can create a Google Hangouts videoconference with up to 25 participants. This number goes up to 50 for Gmail Enterprise users.

Outlook provides access to Skype as standard. Subscribers to Office 365's Business Premium plan also get access to Microsoft Teams, where they can create videoconferences with up to 250 people. Not all video screens will be able to show at the same time, though.

Both Outlook and Gmail make it easy to send a videoconferencing request, whether it be through Hangouts or Teams, via email. All the recipient has to do is click on the link and follow the instructions.

Security

There are few differences between Outlook and Gmail's security features. Both provide two-step authentication, AI-powered spam filters, and a 'verified' sender option, to make sure only trusted addresses can contact you.

Interestingly, Google has been working with machine learning algorithms to reduce the amount of phishing attacks its users receive. It will now label an email with a colour coded warning system. If a message is deemed malicious it is marked red, while lesser risks are marked yellow.

Price

Currently, Gmail can be bought as part of G Suite for £6.60 per user/month for standard business users or £20 per user/month for enterprise customers. Both plans come with unlimited cloud storage, business email, shared calendars, videoconferencing and secure instant messaging, as well as access to Google's entire productivity suite. Note that on 2 April 2019 G Suite Basic and Business Additions will increase in price – the former by $1 (around 75p) and the latter by $2 (around £1.50).

Outlook, as part of Office 365, is available on two different business plans: Office 365 Business is £7.90 per user/month, while Office 365 Business Premium is £9.40. This includes access to Microsoft's entire online productivity suite, plus OneDrive. Microsoft Teams is, however, available on Business Premium only. For enterprise customers there are three payment tiers: E1, E3, and E5. Outlook is not available on E1, but is on E3 (£17.60 per user/month) and E5 (£30.80 per user/month). Enterprise customers will get access to Outlook, the whole productivity suite, Exchange, SharePoint, Stream, Yammer, and Power BI Pro for E5 customers.

Mailbird Pro

Mailbird Pro (£15 per user/year) is a desktop email client designed for Windows 7, 8 and 10 users. It's available for both personal and business use, though, the most recent release is more clearly adapted to business purposes. One of the platform's main selling points is its integration with a range of apps such as WhatsApp, Twitter and Slack. Employers can remove third-party app integration in order to minimize possible distractions for their employees, though.

Zoho Workplace

Like G Suite, Zoho Workplace (Zoho Mail) offers a range of business-focused apps, including Zoho Docs and Office Suite. Zoho Mail promises an ad-free, simple and reliable mail service with a guaranteed uptime of 99.9

percent. And while it does offer a Standard package for £2.40 per user/month, its Professional plan, which provides 100GB of combined storage and 40MB of email attachments, costs just £4.80 per user/month.

Atmail

Offering both cloud and on-premise mailboxes, by choosing Atmail cloud mail hosting, you will receive between 100GB storage and 1TB of storage (depending on your price plan), maintenance and security updates, built-in antivirus and a custom domain, not to mention a user interface similar to Google Apps. It offers good customization features, with custom branding, logos and themes integration coming as standard when opting for its cloud email server. For those wanting an on-premise email service, you can expect to pay around £295 per year for 50 users.

FastMail

It's easy to get carried away with email and pay for a lot more than you actually need. If you can manage on a smaller inbox and file storage, then cheaper options such as FastMail are great. The company's professional package comes in at $9 (around £6.75) per user/month, and offers 100GB of storage, no ads or tracking, and the ability to sync with mobile devices. Users will receive fast web and mobile apps, access to multiple domains and email filtering, making organizing, storing and archiving much easier. You can also add on more storage as and when you need it, to scale with your businesses. FastMail doesn't tie you into a contract either, so you can change service if this isn't the one for you.

Yahoo Mail

If you're a small business or start-up, Yahoo Mail offers a solid free email provider with great filtering capabilities. Often a downside of free email platforms is the number of ads served. However, its responsiveness, cloud storage integration (Dropbox and Google Drive) and massive 1TB of free storage make it worth considering. It also includes a translator, which is a nice touch for a free email service. The record-breaking data breach suffered by Yahoo, which could have affected as many as three billion users, is worth taking into account. Away from its free version, its business plan offers unlimited mail storage capacity, and very good address book and filtering capabilities. Plus, it is ad-free. You can get this from $1.19 (around 91p) per user/month.

Verdict

As always, selecting the right email provider depends on your business needs. For many, Microsoft Outlook provides the gold standard of business email suites. It can provide the best option if you're looking for an on-premise email provider, particularly for companies interested in using other Microsoft services.

For companies with a strong social presence, Mailbird Pro provides an excellent option for integrating a range of social apps within the email service, eliminating the need to switch between numerous tabs.

While for media companies, Google's email offering is frequently used in conjunction with the excellent G Suite, which allows seamless sharing and editing of content.

For smaller start-ups, picking a low-cost provider like Yahoo Mail or Zoho Workplace (for companies with under 25 users) could be the best option. Techworld Staff

Credit: iStock

Work email management

Five email tips businesses should know

According to technology research firm Radicati, by Q4 2019, the amount of worldwide email users will increase to over 2.9 billion with the total number of worldwide emails sent and received daily increasing by 5 percent by 2019. With such a large volume of emails circulating, businesses need to ensure absolute control over their email management systems.

Managing director of Cryoserver Robin Bingeman sheds some light on tackling common problems associated with business email management.

Think about storage

How a business stores mass emails is an important issue to address when looking to cut costs. A lot of businesses will either use a mail server/cloud, delete old emails or archive them, and while all of these options have their benefits, they are dependent on the organization's size and monthly outgoing email allowance.

"Keeping emails on the mail server will slow down inboxes and will cost the business money, but deleting emails straight away might mean you fail to comply with industry regulations," explains Bingeman. "By taking emails off the mail server and archiving them elsewhere you will speed up day-to-day processes, save money and still be compliant. This means that emails can be stored for as long as they are needed without upsetting the smooth running of the business."

Make sure emails can be accessed quickly

Data privacy is an important issue, so creating a best practice for your email should be high on any businesses' list of priorities.

Bingeman tells us: "It is important that emails can be accessed quickly and easily, but it is equally important to limit access to sensitive information. Choose an email management solution that allows you to restrict access to certain data."

Encryption

Businesses should make sure they not only encrypt sensitive data but also provide some level of encryption for standard emails as a precaution.

"Restricting access is crucial, but in order to properly secure data your solution should provide encryption," urges Bingeman. “This makes it more difficult for emails to be hacked, tampered with or leaked, protecting your business and your sensitive data.”

Have a searchable archive

Creating a searchable email database saves time and is just a small thing to make life a lot easier.

According to Bingeman: “Make sure that your archive is really easy to search. We know that looking for emails wastes time, so implement a solution that makes it easier for your colleagues to retrieve emails. This is especially important for colleagues who work in HR or compliance who will have to find lots of different emails to resolve disputes or meet regulations every day.”

Good email management equals productivity

Productivity can be boosted when a good email management system is put in place as employees are left to focus on other (probably more important) tasks.

Bingeman says: “Recognize the link between productivity and email management. According to Radicati, we receive and send, on average, 122 emails a day – they take up a large portion of our time. By giving employees an email solution that is easy to use, search and manage you will free up time across the business.” Christina Mercer

Credit: iStock

Email security

Keep your messages safe by following our tips

Email is an indispensable tool for every business, which makes it a tempting target for cybercriminals. To bolster your defences against them, follow our top tips on how to keep your email secure.

Encrypt your email

Email encryption protects sensitive information by scrambling the data for anyone who doesn't have a key to decrypt it. This makes it extremely difficult for hackers to intercept and read your communications. Leading email providers often offer built-in encryption features, but these can come with limitations. For example, Gmail's encryption only works if the recipient is also using Google apps. If you want a more comprehensive form of protection, you can download additional specialist encryption software or use web-based encryption email services such as Sendinc.

Invest in security software

An antivirus program can help protect you from phishing attacks and other malicious threats. Additional software, such as network security systems and specialist filtering services, can help address specific needs. Keep all of your security software and your operating system up to date to ensure new threats are eliminated.

Think before you click

Humans remain the weakest link in the cybersecurity chain, and phishing is their biggest threat (see **page 19**). To avoid adding your name to the long list of victims, tread carefully around any emails that ask you to click a link or download an attachment. Be suspicious of any messages that arrive with no clear context and are sent from someone you don't know. Ensure your firm's email security policies are thorough and up to date, and that staff are trained in best practices for email use.

Use a password manager

Strong passwords can be tricky to remember, particularly as they should be changed periodically. A password manager such as LastPass or Dashlane can generate and manage all your secure passwords to keep your emails safe and your memory clear.

Delete unnecessary web accounts

Every account you own is another vulnerability that hackers can exploit. Reduce the number of access points to your information by closing all web accounts you no longer need or use, for example, a long-forgotten Yahoo email account.

Consider a specialist secure email service

Encrypted email accounts will add an extra level of protection. Services such as ProtonMail and Tutanota automatically encrypt your email data to keep both the messages and contacts private. The end-to-end encryption makes it impossible for anyone to decrypt your messages without your password.

Be careful with public Wi-Fi networks

Public Wi-Fi networks are notorious targets for cybercriminals. Take extra precautions by only using sites that don't use your sensitive information and by using a VPN.

Reduce third-party access to your inbox

Review the add-ons connected to your inbox to find out which third-party programs can access your email account. Decide whether their value outweighs the risk of their ability to view, manage, delete and send email from your account and remove any of the services that you don't need or recognize. Tom Macaulay

Credit: iStock

Spot phishing emails

Advice on recognizing a malicious email

Email is an effective gateway for hackers and cybercriminals. A 2017 study from Keepnet Labs found that a staggering 48.2 percent of phishing messages were opened by the target across all campaigns, up from 30 percent in 2016. Here are our top tips for detecting a phishing email.

Incorrect spelling and grammar

Organizations and brand marketers take their communication very seriously and often have emails proofread before being sent out. It is highly unlikely the email came from the original source if it is packed with spelling and grammatical errors.

Strange URLs

A phishing email is likely to include links that direct you to a site asking for login details, where would-be attackers can then steal your account details.

Often, the URL will appear valid. To check it simply hover your mouse over the link. This will display the real hyperlink – if it looks unfamiliar, then it's not safe to click.

The domain name may also be different to the organization or brand it claims to be from. Check the sender's address and look back at how domain addresses usually appear in previous, legitimate emails you have received from that organization.

Personal information

If the email begins with 'Dear Customer' as opposed to being addressed by your name, it is unlikely that it came from the organization itself. If it is from a company that has your personal details on file, then it is more likely to address the email to you.

Also, a bank would never ask for personal information, such as account details, via email. This is a clear way to spot a phishing email.

Requests for urgent action

Emails that claim 'urgent action' is required are generally phishing scams. If you do receive such an email, it is best to give the organization a direct call before taking any action. Usually, if it is legitimate, the company will either write a letter or call you.

What to do if you've been a victim?

Phishing scams can be reported as suspicious communications via an online form on the Action Fraud website (**fave.co/2U0gEjY**). There is also more information on what to do in the case of phishing scams on the government website (**fave.co/2X8MoVU**).

Hannah Williams

Credit: iStock

How to encrypt emails

With data hacks on the rise, email encryption is a must

Methods for end-to-end email encryption have been around for many years, but they are still used only to a limited extent across businesses. However, with cyberattacks on the rise, particularly within SMBs, companies are taking high risks if they neglect email protection. If you don't use encryption yet, you should do so as soon as possible. Our tips will help you find the right solution for your needs.

Rely on standards

There are two groups of standards for email encryption. One is transport encryption using 'Transport Layer Security' (TLS), the other is its predecessor 'Secure

Socket Layer' (SSL), where the sender and recipient set up an encrypted tunnel for email communication.

To ensure data is secure for both the sender and the recipient, two protocols could be used: S/MIME (Secure / Multipurpose Internet Mail Extensions) and OpenPGP (Pretty Good Privacy).

Another possibility of content encryption is provided by Microsoft Rights Management Services (RMS). Although it is not a standard, but instead used by some companies to encrypt emails, RMS is available in two versions: as Active Directory RMS (AD RMS) for on-premise use; and as Azure RMS in conjunction with the Microsoft cloud.

However, not all transmitted information is made illegible to third parties during encryption. The so-called metadata such as sender, recipient and subject line are transmitted in plain text, which can pose a security risk. The combination of transport and content encryption, therefore, offers the greatest possible security.

Standards guarantee you the greatest possible compatibility with the email software used by your customers and business partners. Encryption standards are also typically integrated into many email solutions.

Alternative methods

Although technologies such as Pretty Good Privacy (PGP) have been on the market for more than 25 years, they are still relatively underused. This is probably because certificates and keys are a prerequisite for use. This, in turn, requires an appropriate infrastructure or at least technical know-how.

So, you can't necessarily assume that all your email recipients can also communicate on the basis of PGP or

S/MIME. That's why you should offer them alternatives. In principle, there are two ways to do this, pull or push.

In 'pull procedures', the recipient logs on to the sender's system and receives the messages after they have authenticated themselves. Typical examples are secure webmail portals. With the 'push method', however, the email is converted, encrypted and sent to the recipient as an attachment to a carrier email. Formats such as Zip, PDF or HTML are particularly suitable here.

Secure your internal communications

The methods previously mentioned are primarily designed for communication with external partners. However, you should also rely on maximum security in internal communication. We recommend you support the encryption of email messages within your company – ideally using standards that already exist in your email client. This saves you the installation and maintenance of additional plug-ins and add-ons.

Data flow and content control

End-to-end encryption of email communication poses a challenge. Security systems such as virus scanners, anti-spam software or DLP (Data Leakage Protection) solutions can no longer analyse the content of messages and thus, no longer work correctly. You should use a solution that provides interfaces for these central data flow and content control systems or ones that can even filter out malicious code from encrypted emails.

Keep emails private as well as secure

Although detection of malware, spam and other harmful or unwanted content is important, it can interfere with your email privacy. It is still important for the senders and recipients to be aware of the content of an email. This is where end-to-end encryption can help, because the central data flow and content control is not possible.

Think about automated emails

Automated emails can also hold sensitive data that is worth protecting, such as payslips, delivery notes or invoices. Therefore, you should use a service for these that also supports encryption since most applications themselves are not designed for this.

Another point to consider is email archiving. If messages are stored in encrypted form, they are very difficult to find, since information can only be extracted via metadata. An encryption solution should also provide interfaces for archives and journal systems.

What about attachments?

Email is often used as a medium for sending files, although it was not originally intended for this purpose. This leads to considerable problems, especially with large attachments, for example, if the recipient's system does not accept the attachment. To get around this you should choose an encryption tool that also supports sending emails with large attachments without overloading and clogging the mail servers.

In such solutions, these attachments are not physically transported via the mail server, but via systems that are designed for this purpose.

Mobile security

Of course, secure email communication must also work with all mobile devices. The encryption solution of your choice should support the methods that are already available in the native mail clients of the device platforms or the mail clients of your Mobile Device Management (MDM) system.

Don’t commit to just one tool

To remain future-proof and flexible, you should rely on a system that can run on a wide variety of operating systems and platforms. It should also give you the choice of operating the system internally, or in a hybrid environment. Of course, all current email clients and servers on all platforms should also be supported.

Think about usability

Every project stands and falls with user-friendliness. If you use an encryption solution that is difficult and laborious to use, users will not use it. Therefore, the used one should neither hinder nor restrict the user in his daily work. Christina Mercer

Credit: iStock

Recover deleted emails

We've all experienced that sinking feeling of accidentally clicking the 'delete' button. Here's what to do next

When you delete an email, it's immediately transferred into your 'trash'. You then have a 30-day window to recover these emails before they are deleted forever.

Upon realizing an accidental deletion, head quickly over to the 'trash', locate the email in question and use the right-click function to pull up your options. Then, click 'move to' and the location you would like to place the email in – whether that's back into your inbox or a different folder.

Beyond the trash folder?

However, of course, in some cases it may be over the crucial 30-day deadline before you realize you actually do want to recover that important email. What are your options in this case?

Bad news: there is a good chance your email has been irrevocably deleted. However, you do have a recourse of action available to you. You can email Google's support team to ask whether there is a possibility of getting the email back. Although this service is aimed more at emails that have gone missing as a result of your account being compromised, if in need, you can try Gmail's missing email page. Here, you need to fill in a form providing information. Do this as soon as you realize the email is MIA – the longer you wait the less likely the possibility of retrieving it.

Recover deleted emails in Outlook

Similarly to Gmail, in Outlook you also need to head over to the 'deleted items' box, in the case of a deleted email, or other item like a contact or calendar event. Once you've located the deleted email in the folder, simply click restore to recover it. This folder may also be labelled the 'trash' folder, depending on which version of Outlook you're using.

If you can't locate the email in the deleted items folder, the next place to head is the Recoverable Items folder. This folder is generally hidden, and is where emails are directed when either delete an item from the deleted items folder, empty the deleted items folder, or permanently delete an item by pressing Shift+Delete.

Before attempting to access the recoverable items folder, it has to be noted that if you are using a version of Outlook where you have a ‘trash’ instead of a ‘deleted items’ folder, this folder doesn’t exist, and you won’t be able to recover emails beyond your Trash folder.

For users of the version that supports the recoverable items folder, once you’ve clicked on the ‘Deleted items’ folder, make sure the ‘Home’ tab at the top of the page is selected, and you should see the option ‘Recover deleted items from server’. If you don’t see this option, then unfortunately your version of Outlook doesn’t support this option.

Once you’ve clicked this, you should see a list of all the emails that you can recover. Simply select the one of your choice, click ‘Restore Selected Items’ and then ‘OK’. From here, the email will be placed back into your ‘Deleted Items’ folder, from where you move it to a folder of your choice.

If the email isn’t here, all hope is not lost – just yet. As most email servers will make backup copies from time to time where they are kept for a short while, it might still be possible to restore it by contacting support here. **Laurie Clarke**

IDG