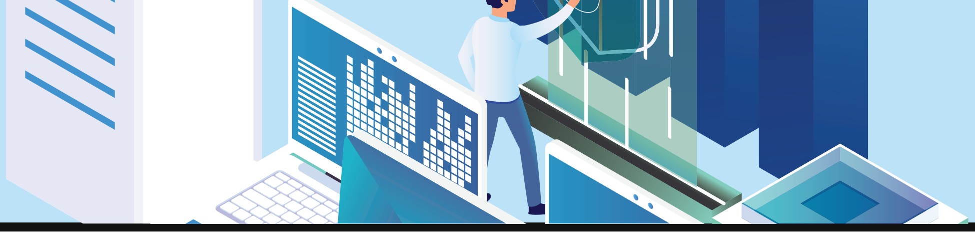
eFax Corporate®

White Paper

Why Cloud Fax Is Better for Secure Data Exchange Than Email (Yes, Even Encrypted Email)



When a reporter asked the prolific American bank robber Willie Sutton why he robbed banks, Sutton replied, “Because that’s where the money is.” 1

America’s FBI, which chased Sutton for years and even placed him on the agency’s Ten Most Wanted Fugitives list, described the career criminal’s methods as innovative and creative. He often disguised himself as a police officer or maintenance person—and this was decades before TV and movies depicted these strategies. He found unusual ways to breach banks, including dropping in through skylights in the ceiling. Sutton even escaped from prison several times.

Which brings us to the main argument of this paper.

The ever-evolving email encryption landscape only underscores email’s risks. Email service providers and encryption software makers need to continually up their game because they know organisations use email to transmit their most sensitive content—a fact that also attracts the sharpest cybercriminals. As Willie Sutton might have reasoned, yes, encrypted email is a challenging target, but it’s fortified precisely because it often carries the most valuable data.

In this paper, we’ll explore several technical and behavioural reasons that email—even encrypted email—is not sufficiently secure for transmitting your sensitive and government-regulated data. But the primary reason is also the simplest: Hackers’ favorite target for organisations’ data is their email—because that’s where the money is.

Now let’s discuss a few other key reasons you might want to choose a transmission platform other than encrypted email for sending and receiving highly sensitive materials.

7 Drawbacks of Encrypted Email

1. Email encryption isn’t hackproof.

Of all the arguments were going to make against using encrypted email to transmit confidential data, this one is the weakest, which is why we’re getting it out of the way first. Still, though, even this point should make you think twice about just how safe your company’s encrypted emails will be.

In 2018, a group of applied-science researchers working for universities in Germany and Belgium ran tests on the two most popular email encryption schemes: PGP and S/MIME. They discovered serious vulnerabilities in both.

In 28 tests of PGP-protected email clients, the researchers found their decryption attempts successful 10 times—a better-than-30% success rate. The story was worse for S/MIME encryption. In those cases, researchers were able to successfully convert the encrypted messages into readable plaintext 25 times out of 35.2

So, why is this the weakest argument against email encryption? Because, as many technology experts have since explained, exploiting the vulnerabilities that these researchers uncovered (which they collectively called “eFail”) would be very difficult. But as we’ve witnessed in the years since 2018, cybercriminals are fast learners, and they’re increasing their skills every day.

Also, as of 2021, Microsoft Outlook—the most popular business email programme in the world—still offers S/MIME as one of its two primary encryption options.3

2. Your emails are only as secure as the keys encrypting their contents.

Here, we begin to see the real weaknesses inherent in email encryption. Let’s use a real-world example.

In 2020, hackers breached the United States Treasury Department’s email servers and stole the messages of many of the department’s highest-ranking officials. And yes, these messages were all encrypted—likely using the most advanced encryption software available.

But as The Guardian reported, the cybercriminals were able to decrypt and read those messages because they also stole the email accounts' encryption keys.4

You can invest the time and budget to deploy the most sophisticated email encryption on the market. You can configure your corporate email such that no employee may send or receive a message without first using keys to establish a trusted connection with the other party.

But if hackers can access any of those keys because an employee failed to store them securely, you might as well be leaving hackers the plaintext versions of every message and attached file on that employee's account.

3. Even encrypted email can be stolen.

As a TechRadar article points out, encrypting your email serves only one purpose: It stops unauthorised third parties (anyone without the required decryption key) from reading the contents of your messages.5

But it won't stop a determined cybercriminal from grabbing an email message in transit, at one of the many nodes the message passes through on its journey to the recipient's inbox. Once hackers intercept an email in-flight, they can apply their skills and resources to converting it from ciphertext to plaintext.

And remember, as we saw above with the US Treasury breach, smart hackers' preferred option is to steal an email user's decryption key. Then, they can intercept encrypted messages sent or received by that account and read them in plaintext.

4. Your encrypted email won't necessarily remain encrypted for its entire journey.

Just because your company sends an email with encryption doesn't mean the message will arrive at its recipient's account in encrypted format, or that it will remain encrypted at rest on that recipient's email server.

Even Google—which proudly highlights the security and encryption features of its Gmail service for businesses—admits that unless both parties to an email transmitted over Google's system use the same encryption protocol, Gmail doesn't promise encryption all the way through to the recipient's inbox. Here's the relevant statement on Google's Email Encryption FAQ's page:

Question: Why isn't all email sent to or from Gmail encrypted in transit?

Answer: For decades, the default has been for email to travel across the Internet unencrypted—as if it was written on a postcard. Gmail is capable of encrypting the email it sends and receives, but only when the other email provider supports TLS encryption. In other words, **encrypting 100% of all email on the Internet requires the cooperation of all online mail providers.6**

5. Encryption won't keep out emails with malware.

Unless you are augmenting your email encryption with other cybersecurity measures—including antimalware apps, firewalls, and employee training—you won't stop a malicious email containing ransomware or some other nefarious programme from landing on your company's network. All your encryption software will do is encrypt the malware contained in the email message or attachment.

In fact, here's an infuriating irony: Your encryption programme could prevent your malware-detection app from spotting and isolating a malicious email before it reaches your employee's computer.

Then, theoretically, the hackers could access your employee's entire email inbox. Among the many horrible things that could happen next, the hackers could steal your employee's decryption key (if the file is stored or copied in an email), then decrypt and steal all messages and file attachments stored on that account.

6. Encryption can't stop the most popular hacking technique of all: phishing.

A 2021 ZDNet story revealed that email phishing remains cybercriminals' most common technique to hack into organisations' networks to launch attacks such as ransomware. (Actually, the report notes, email phishing is tied for first place with brute-force attacks against companies' remote desktop protocol services, each one accounting for 42% of all hacks.)7

As you know, one of the greatest threats to any company's digital assets is employee error.

7. Your employees might not always use it.

This might be the most important reason to think twice about allowing a company culture where employees regularly send and receive confidential or legally regulated data by email. And here's a recent real-world example of the dangers.

In 2021, cybercriminals hacked the email accounts of more than 100 top officials of the Polish government, including several Members of Parliament.

Were these officials' government email accounts protected by encryption? Yes, of course. But as Reuters reported, the documents stolen and eventually leaked from this breach—many of them confidential—were sent and received on these officials' personal email accounts.8

In fact, one major source of leaked government data, the story points out, was the personal email account of the top aide to Poland's Prime Minister.

Now, if federal government officials are at times using their non-work email accounts to transmit sensitive data—likely for convenience—what are the chances your employees won't do the same?

You can set up encryption for your corporate email environment and require all company documents sent only after engaging the encryption programme. Your employees will undoubtedly make a best effort to comply whenever possible. But inevitably, there will be times when an employee is out, does not have access to the corporate email client, and needs to send or receive a confidential document.

For example, if you're a law firm, say one of your associates is out and receives an urgent request from a client for certain legal documents. Your employees can access those documents from her phone, using your firm's file-sharing app. But on her phone, she has access only to her personal Gmail account—her unencrypted Gmail account.

Or, if a client asks the associate to sign and return a doc ASAP—and she has only her Gmail account—that scenario presents the same problem. For the sake of expediency, and being a responsive solicitor, your associate might give the client her personal email address, sign the doc electronically, and send it right back over Gmail.

If you've established the difficult rule that every inbound and outbound message requires encryption keys, you might find your employees using these workarounds on a regular basis.

Let's say you're using an email encryption programme. Your employee receives a message, decrypts it, and reads the contents. If the message contains a link to a malicious site, or has malware embedded, your employee erroneously taking whatever action the message asks could trigger the malicious code.

And at that point, sophisticated hackers could gain access to your decryption keys, launch a ransomware attack locking the entire company out of your networks and email programmes—or simply steal the emails in encrypted format and save stealing the decryption keys for another day. Now let's review a few key reasons that secure cloud faxing is the better option for transmitting your company's most sensitive data.

3 Reasons You Should Instead Use Cloud Fax for Secure Data Exchange

1. Cloud fax has been providing enterprise-caliber secure document exchange for decades.

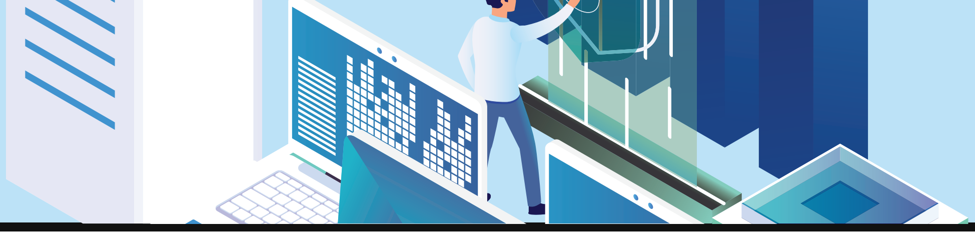
Digital cloud fax technology is decades ahead of email in terms of secure data transmission for a very logical reason. While email messages run the gamut from exchanging confidential data to asking coworkers where to go for lunch, most businesses use fax only to share important—and often highly sensitive—documents. Nobody faxes a colleague about where to go for lunch.

As a result, cloud fax providers have had to develop an infrastructure that guarantees business users the most secure, private, and legally compliant way to transmit their confidential data to clients, vendors, partners, and other third parties.

At the same time, email encryption programmes are constantly playing catchup with the ever-evolving techniques and resources available to cybercriminals.

Let's not forget what even Google says on its encryption FAQ page:

"For decades, the default has been for email to travel across the Internet unencrypted—as if it was written on a postcard."



Moreover, it's worth pointing out a Microsoft announcement that the company is beginning to phase out older encryption-in-transit protocols TLS 1.0 and 1.1 for its Outlook emails—and defaulting to the newer TLS 1.2 standard. Here's Microsoft's statement:

"To provide the best-in-class encryption to our customers, **Microsoft plans to deprecate Transport Layer Security (TLS) versions 1.0 and 1.1 in Office 365** and Office 365 GCC. We understand that the security of your data is important, and we're committed to transparency about changes that may affect your use of the TLS service." 9

While that's great news for the 100,000 organisations around the world using Outlook today, Microsoft only posted this announcement in December 2021. Meanwhile, TLS 1.2 has been the default protocol for all of eFax Corporate's cloud faxes for more than a decade.

Indeed, many of the world's most heavily regulated organisations have been relying on the eFax Corporate platform to transmit their most heavily regulated documents for a quarter-century.

Bottom line: Businesses around the world were sending and receiving highly sensitive data over eFax Corporate's secure cloud-fax network for decades while, as Google puts it, the "default" for email was still to "travel across the Internet unencrypted—as if it was written on a postcard."

2. Cloud fax is far less vulnerable to social engineering attacks.

Corroborating that ZDNet story we mentioned earlier, a 2021 report from the European Union Agency for Cybersecurity also found that social engineering remains the most prevalent attack technique for cybercriminals.10

This is another reason that it makes more sense to transmit your company's sensitive and government-regulated data by cloud fax instead of email.

When your employees receive a cloud fax from a partner or client, chances are that fax isn't going to ask them to take any action in the document itself.

In nearly all cases, inbound faxes contain common, familiar documents central to employees' everyday workflows. These could be court documents for law firms, signed contracts for financial and real estate companies, or updated patient records for healthcare organisations.

It would make little sense for an inbound fax ask to an employee to "click on this link"—and even less sense for that employee to comply.

As such, exchanging sensitive documents with partners, vendors, and other third parties will be much safer by cloud fax than by email—because employees don't tend to fall for phishing attempts in a fax.

3. Cloud fax just isn't on hackers' radar.

It's worth returning once more to our original point: Hackers target corporate email for the same reason Willie Sutton targeted banks: Because that's where the money is.

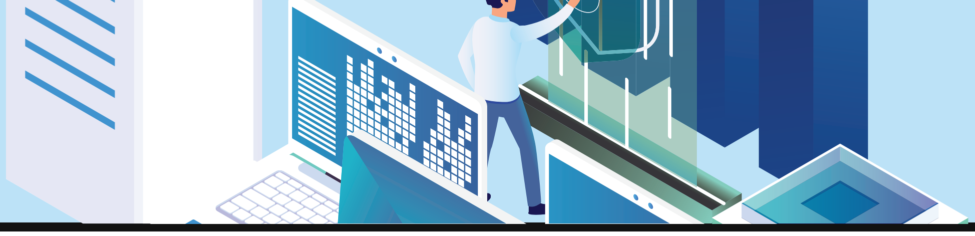
No matter how much effort you put into encrypting every email message, cybercriminals will always be looking for new and clever ways of breaching your email environment and stealing the messages' contents—either to blackmail you with them, or to sell the data on the dark web.

As we've outlined above, there are simply too many reasons—both technical and behavioural—that even the best encryption programme might not always hold up across your organisation. And, as we've also noted repeatedly, your email environment remains a favorite target for the most sophisticated hackers.

Obviously, your organisation is always going to need email service. And we highly recommend you deploy as advanced an encryption solution as you can find and afford.

But to the extent that your employees regularly send and receive confidential documents and data regulated your industry's privacy laws, your best bet is to keep those communications outside of your email environment altogether—and handle them all over the most proven and trusted cloud-fax solution on the market.

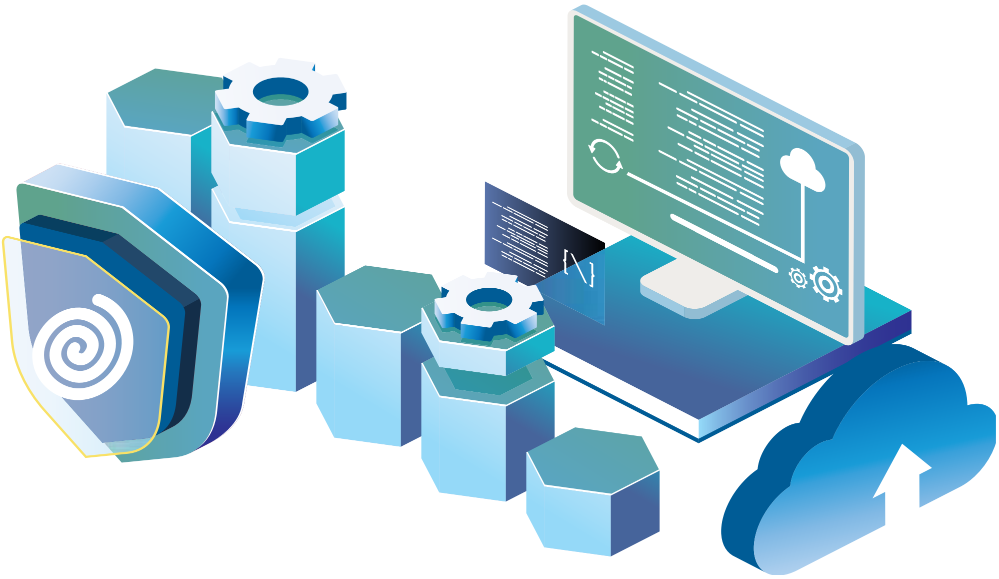
Why? Because, among its many other advantages for securely and confidentially transmitting documents, cloud fax also has the virtue of flying under the radar of cybercriminals—who are too busy trying to breach email.

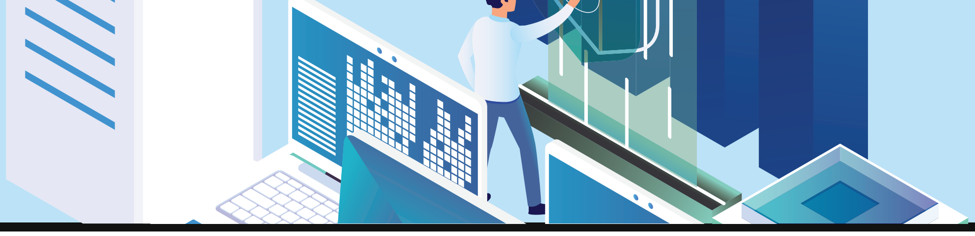


A Side-by-Side Comparison

Finally, let’s take a brief look at the relative strengths and weaknesses of cloud fax vs. encrypted email programmes for secure data exchange.

	eFax Corporate	Encyrpted Email
Common breach point for cybercriminals?	No	Yes
Common target for ransomware attacks?	No	Yes
Common target for social engineering attacks?	No	Yes
Sends message content to your inbox?	No	Sometimes
Can guarantee end-to-end encryption in all transmissions?		
A history of being hacked and compromised?	No	Yes
Uses TLS 1.2 encryption for all data in transit?	No	Sometimes
Uses AES 256-bit encryption for all data at rest?	No	Sometimes
Can guarantee end-to-end encryption in all transmissions?	No	No





References

1. FBI: Famous Cases and Criminals—Willie Sutton
2. Wired: Encrypted Email Has a Major, Divisive Flaw
3. Microsoft: Encrypt Email Messages for Outlook for Microsoft 365 and Outlook 2021
4. The Guardian: US Government Hack Compromised Dozens of Treasury Email Accounts
5. TechRadar: Why Choose a Secure Email Provider for Your Business—and Why You Might Not
6. Google: Email Encryption FAQs for Gmail
7. ZDNet: Ransomware: These Are the Two Most Common Ways Hackers Get Inside Your Network
8. Reuters: Hackers Breached Several MPs' Email Accounts, Poland Says
9. Microsoft: Preparing for TLS 1.2 in Office 365 (December 2021!)
10. ENISA: The European Union Agency for Cybersecurity Threat Landscape 2021

About eFax

eFax is the leading HITRUST CSF® certified digital cloud-faxing solution, trusted by five of the top 10 global enterprises and four of the top 10 Fortune 500 healthcare companies. The eFax Corporate product transmits billions of documents annually and is widely used in the USA, Canada, Europe, and Asia-Pacific. Its appeal and success are built around three key features: the widest selection of phone numbers; an easy way to send and receive faxes and voicemail by email; and a fast, reliable and secure communications network. As a core product of Consensus Cloud Solutions' leading interoperability suite, it creates operational efficiencies and enhances communications for paper-reliant industries such as healthcare, legal, manufacturing, finance and real-estate.

European Headquarters

eFax
European Headquarters
Unit 3, Woodford Business Park
Santry, Dublin 17, Ireland

Contact Sales
UK 0800 689 0588
Rest of Europe +353 (1) 656-4950

Web:
efaxcorporate.com

Follow Us