An Essential Guide to End-to-End Encryption
End-to-End (E2E) Encryption is a system of secure communication, protecting data so that only the sender and the receiver can read the message. If the message is intercepted, no third party would be able to decipher or alter the message, securing it from any bad actors.

Data encryption is necessary to help protect your enterprise’s valuable data. It’s also important when you need to keep your company’s communications secure. For this reason, you need to consider updating your company’s communications solutions to ensure the strongest possible security – which typically includes encrypted messaging.

Many apps boast of their encryption technology, but is all E2E security the same?

Is All End-to-End Security the Same?

You can liken the definition of E2E security to reading the labels on food at the supermarket. There is a difference between what is organic vs. homegrown, non-GMO vs local, etc. All of these are on the packages of food you buy and all are supposed to mean something very specific, but there is very little oversight into the practical usage of these terms by food providers, leaving it up to the consumer to really read the labels and determine what is most important to them. Simply buying something off the shelf because the food producer says it’s healthy is not enough.

It’s the same with E2E security. There are many definitions of E2E encryption which can be found from a number of reputable sources. Most of them will allude to a method of communication where only the communicating users can see messages or be included on a call. Some will use other related terms such as at-rest/in-transit, cryptography, safe from hacks and eavesdropping, or third parties. Figuring out what works best for your business can be very complicated, like trying to figure out which granola is healthier: natural or organic.
What's the Difference Between End-to-End Encryption and Client-to-Server Encryption?

The single most important security differentiator between communication platforms is whether they offer end-to-end encryption (E2E) rather than client-to-server encryption (C2S). Modern products, including Wickr networks, built exclusively with end-to-end encryption provide a new level of data and communication security. However, many other tools described as “secure” use antiquated client-to-server encryption. The use of client-to-server architecture is especially prevalent in products that offer video communication. Prominent examples would include Zoom, Slack, WebEx, Skype for Business, Telegram (in its default setting) and many others.

The distinction between end-to-end encryption vs client-to-server encryption is so important that it's fair to say the two types of platforms are fundamentally different.

Many Small Baskets or One Huge One?

So, what's the difference? Invariably, in any such platform all traffic is routed through a single central server. The difference between E2E and C2S platforms is that an E2E server is of little to no value to an attacker trying to steal secrets on an E2E platform. Whereas, for C2S platforms the central server contains a vast trove of highly sensitive data making it one of the single most valuable targets in your entire organization's infrastructure.

Gaining access to a C2S messaging server means gaining access to all communication on your entire network in one fell swoop! Nor is this just about ongoing communication. When you log in to your account on a new device do you see your conversation history? If so, then so can anyone with access to that server. A compromised server can listen in and record any and all calls, see (and manipulate) all files being transferred, and read all messages being exchanged and stored as conversation histories. Compromising a single server in a C2S platform simultaneously gives the attacker access to, say, all private communication with your clients and contractors, trade secrets and operational data exchanged by your employees, legal strategies discussed with lawyers, business strategies discussed amongst the executives, negotiation tactics discussed amongst sales and so much more.
The risk of exposure of a C2S server comes not just from external attackers but often from simple negligence or accident. A recent survey found nearly 200 organizations vulnerable due to their miss-configured Amazon S3 buckets alone. For example, 300 million Wechat and QQ private messages were recently leaked due to a mis-configured database.

But regardless of how carefully we defend against those threats, a C2S server inevitably remains vulnerable to various insider attacks (e.g. Snowden, Manning, Winner, Shulte). In fact, insider attacks are, by far, the most dominant type of threat to the cybersecurity of organizations across the board making such attacks a particularly important threat to defend against. Yet, any administrator with (digital or physical) access to a C2S server also has unfettered access to all comms data on the platform. Worse, many C2S platforms actually come equipped with features which (essentially, by design) trivialize precisely such low-effort/low-skill/high-impact insider attacks. Slack, for example, offers the “Export Data” feature which lets a (rogue) administrator download the entire communication history of a Workspace in a single operation. Just as for server administrators, access to such features again means having access to a single point of failure for the security of all communication on the platform.

In contrast, on an E2E platform, all comms data is only available at the end points involved in the individual conversations. (Technically, traffic is encrypted by its sender in a way that only the intended receivers can decrypt it. The middleman, or the central server, has no ability to decrypt the message or data). So, in an E2E platform, the server does little more than blindly route encrypted traffic between clients. Thus, compromising the server leaks nothing at all about what is being said, sent or talked about in the network; neither past nor present.

**But it uses “TLS”. Isn’t that good enough?**

To be secure, both web traffic and messaging platforms must use cryptographic channels to secure communication between their applications’ end points. In a web browser, TLS is the industry standard protocol for building those channels.

A critical difference between browser and messaging security is where those endpoints lie. For the web, servers (along with clients) are endpoints. Servers host, maintain, process and filter web applications’ data. In contrast, in messaging applications the sever is no more than a middleman transparently forwarding data between endpoints. In other words, while web applications naturally reflect a C2S channel structure, messaging is instead fundamentally an E2E application.

Despite its success in the web space, relying only on TLS between clients and the server is just not the right tool for securing a messaging platform. Simply put, the approach does nothing at all to avoid the huge risk of letting a single server have access to your entire organization’s communication.
What Are the Enterprise Data Encryption Best Practices?

Enterprises employ data encryption to protect valuable data from unauthorized access. To ensure the strongest protection against data breaches and theft, organizations must follow best practices in choosing which data to encrypt, how to encrypt it, and who has access to that data.

Identify Valuable Data

A large organization may have sensitive data stored in multiple physical and virtual locations. It is necessary to take an inventory of where the most valuable data is located at all levels of the organization. This includes both data at rest and data in transit across the network.

Once these locations are pinpointed, you need to prioritize the most valuable data assets and storage repositories. This will help you develop the best strategy for encrypting the data.

Protect Data at Rest

Data at rest includes all data stored on physical media, whether magnetic, optical, or solid-state devices. The most effective way to protect data at rest is through strong encryption controlled by cryptographic keys.

Protect Data in Transit

Data in transit refers to data transferred between locations or components, typically over the network or to/from cloud storage. Data in transit is vulnerable to various types of attacks, including session hijacking and man-in-the-middle attacks, that can gain access to all manner of confidential data and communications. To protect data in transit, use SSL/TLS protocols, virtual private networks (VPNs), and end-to-end encryption.

Choose an Appropriate Encryption Algorithm

There are multiple encryption algorithms in use today. Best practices dictate embracing state-of-the-art encryption that has been properly tested in real-world situations. Consider factors such as memory usage, encryption speed, and cost. You should also make sure the encryption you choose adheres to relevant international and industry standards, including those set by the National Institute of Standards and Technology (NIST).

Manage Cryptographic Keys

Protecting your cryptographic keys is imperative to protecting your organization's sensitive data, especially any data stored in the cloud. The best secure containers, known as key vaults, help you maintain secure control of the keys used to encrypt and access your data. Key vaults also control and log access to any items stored within, such as certificates.
Your organization’s IT security staff should manage key permissions as necessary. Best practice is to grant access to groups, users, and applications at a specific scope, such as a resource group or subscription.

In addition, you should establish a secure location, separate from your company’s data, to store your cryptographic keys. You should also create backup keys and store them in different locations. Key management should be centralized to avoid isolation vulnerabilities. Best practice is to use a hardware security module (HSM) that offers hardware-based protection, especially if your firm uses cloud-based data storage.

**Control Interface Access**

IT staff should also control which users have access to what interfaces. Key vault access is controlled through the management plane and data plane interfaces. In most instances, a user, group, or application needs access to only one of these planes, not both, which increases the level of security.

**Store Certificates in Key Vaults**

Another best practice is to use key vaults to store high-value certificates. If certificates are compromised, the security of an application or its data can also be compromised. Employing key management to certificate storage helps control who has access to each certificate.

**Ensure Key Vault Recovery**

If a key vault is accidentally or purposefully deleted, the data stored within may be lost. IT staff should employ a management solution that lets you recover any deleted key vaults and objects.

**Practice Scalability**

Your encrypted data security solution needs to be able to scale across all your data. It should also automatically adapt to any changes in your storage methods, including especially growth in the amount of data stored.

**Integrate with Cloud Systems**

According to IDC’s Data Age 2025 report, by the year 2025, 49% of all data will be stored in the cloud. Best practices ensure that data security and encryption are applied to all cloud-based data storage. Your security and encryption should work with your cloud storage provider and any applications that use cloud-based infrastructure.
Use Secure Workstations to Access Data

All access to sensitive data and accounts should be limited to secure workstations. Using a workstation with privileged access minimizes the risk from phishing and other social engineering attacks that compromise user credentials to gain access to sensitive data.

Enable Endpoint Protection

Any device that is used to access data presents a breach risk. This includes not only workstations and desktop computers but also notebooks, smartphones, tablets, and other devices. IT security staff should create and enforce strict security policies for all devices that touch your organization's data.

Use a VPN

VPNs can help protect data in transit both within and from outside an organization. Use a site-to-site VPN to secure access from multiple on-site workstations or a point-to-site VPN for access from an individual on-site workstation. VPNs also help to secure data transfer and communications from off-site employees connected to public WiFi networks or hotspots.

Use End-to-End Encryption

End-to-end encryption ciphers messages in such a way that the messages can only be deciphered by the sender and the recipient. This is more secure than client-to-server encryption which relies on a central server to decrypt messages.
How Do I Find the Best Encrypted Collaboration App for My Enterprise?

When it comes to adopting an encrypted messaging strategy, there are several issues you need to address. Here are five key strategies your organization should employ.

1. **Look for End-to-End Data Encryption**

   Encrypting a company's messages is essential for keeping unwanted eyes off important communications. And the stronger the encryption, the more secure our data and communications.

   Encryption technology essentially scrambles a message or other data and then protects it with a super-strong password. The encrypted message is unreadable until the password is applied to decrypt or unscramble it. The stronger the password, the less likely that the encrypted data can be hacked.

   Some encryption techniques encrypt messages when they're sent to and stored at the service provider, often in the cloud. The danger with this technique is that messages can be intercepted going to or from the service provider, or even hacked when stored on the provider's servers.

   For messaging purposes, end-to-end encryption is a more secure solution. The process encrypts the message as it is sent and does not decrypt it until it has been delivered to the recipient. This ensures that any entity intercepting the message in transit cannot read it. The message remains encrypted until it is decrypted by the recipient.

   End-to-end encryptions ensure that cybercriminals, hackers, and other malicious third parties cannot access, steal, or share your company’s private conversations.

   Your company needs to adopt a strategy of strict end-to-end encryption and choose a messaging app that employs this method.
2. Look for a Multi-Platform Solution

The people in your organization communicate with each other in many different ways, using many different types of devices. It is especially true when it comes to messaging; some people use their phones, others tablets, still others use their laptop or desktop computers. Your company’s messaging solution must be able to work across all platforms and operating systems – Windows, MacOS, Android, iOS, even Linux.

According to StatCounter, Android has the largest market share of the operating system market, at 39.6%, followed by Windows (35.8%), iOS (13.8%), and OS X (6.1%). This means that a messaging app designed exclusively for use on mobile phones is useless for most organizations. The app must work across all phone and computing platforms. It must apply the same end-to-end encryption on all platforms and devices and must do so seamlessly. You need a messaging solution that does not exclude any device or platform used by your employees, vendors, or customers. It must be a multi-platform solution.

3. Look for a Solution That Deletes Old Messages

Your encrypted messaging solution is stronger if old messages are not stored forever, either on a central server or on individual devices. Stored messages, especially those that are not encrypted, are ripe for cybercriminals. Why bother intercepting a message in transit when you can steal it at its source, or in the cloud?

Consider where messages can be stored. Messages can be stored on their original sending devices – employees’ computers or mobile phones. Messages can also be stored on recipients’ devices. And messages can be stored at the service provider.

Messages stored at any of these points are likely to be unencrypted – especially employees’ personal devices. A malicious third-party gaining access to a single unprotected phone could gain access to all of the messages sent and received by that person.

For example, in November 2018, 26 million text messages were exposed in a data breach at a California-based communications firm. The messages were stored in a database in the company’s servers – and weren’t even password protected. If those messages had been deleted instead of being stored, they couldn’t have been stolen.

For that reason, your encrypted message strategy should include automatic deletion of secure messages, on all devices, such as Wickr’s “burn on read” functionality. There should also be no messages stored centrally on the provider’s servers. History, as it were, should be deleted before it can fall into the wrong hands.
4. Look for a Solution That Does Not Collect Metadata

In addition to deleting message content, your messaging solution should delete or simply not store metadata relating to those messages. Metadata is information apart from the message itself that includes data about the message activity – the identity of the sender and recipient, when the message was sent, IP address, device types, and more.

Accessing metadata can tell a third party quite a bit about a company's communications. In the hands of a skilled cybercriminal, it can even suggest the content of the attached messages. It is unfortunate that many popular consumer messaging apps collect a bevy of metadata about every message sent on their services.

For these reasons, your encrypted message strategy should include solutions that either do not collect metadata or that automatically delete it upon message receipt.

5. Adopt a Solution that Integrates with Your IT Platforms

Ensuring your encrypted messaging app integrates with services and platforms your company already uses makes the set up process easy. Apps that support SSO, MDM and Active Directory help simplify deployment and ensure you control your data.
How Can You Tell If a Platform is Truly Secure?

We have seen a great number of new commercial and government inquiries into Wickr since the world was forced to work from home less than two months ago. They are confused about what they need to protect themselves against breaches like we have seen from other communication platforms. It’s important to focus on the outcome they are looking for rather than the buzzword that the vendor is applying. Typical results of a secure communications platform include:

- Prevents anyone not invited to a message or meeting to see or hear the content.
- Protects any specific personal information.
- Maintains the history for only as long as required by law and makes sure only the users can have access to it; doesn’t even allow the provider to have access.
- Works in any country, regardless of government censored communications.
- Supports big rooms full of people with the same security as individual conversations.
- Functions like normal collaboration tools, but is as secure as Fort Knox.

Focusing on the results and asking the vendors you are considering how they help achieve those results will help you determine whether a solution is right for your company.

Wickr – For End-to-End Data Encryption

Wickr is the most robust and secure encrypted messaging solution available today and should be part of your organization's data encryption best practices. Wickr is fully encrypted, enterprise-ready, and easy to set up and manage. Wickr’s end-to-end encrypted platform enables you to secure text messaging, voice and video calls, and file transfers.