SECURITYNET Presentation Overview

Why SecurityNet Exists

We live in a connected world. Every day, our messages, files and activity create digital footprints.

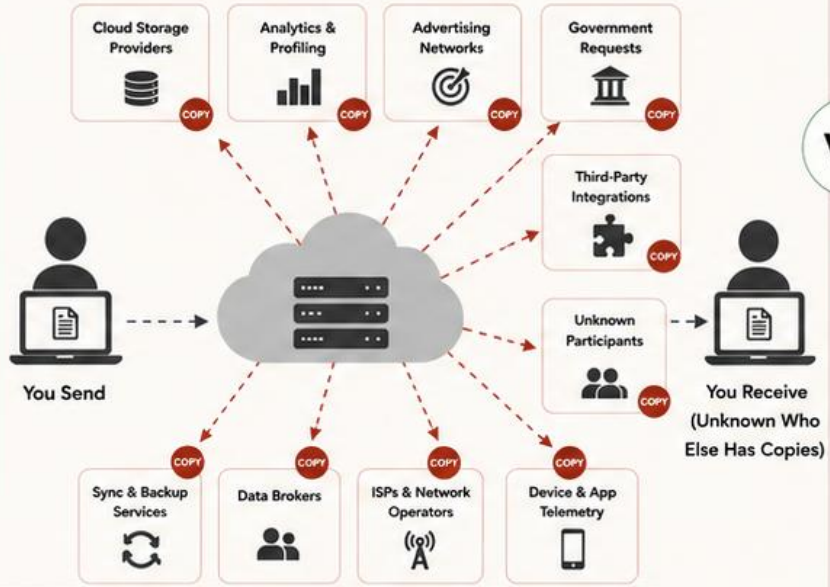
This presentation shows the problem – and how SecurityNet changes the model.

THE PROBLEM TODAY

Every chat, file and message sent from phones and desktops creates copies, reveals activity and exposes sensitive information.

What This Creates

- Multiple copies of your data
- Persistent activity and identifiers
- Tracking and correlation
- Profiling and analytics
- Data retained indefinitely
- Exposure to unknown parties



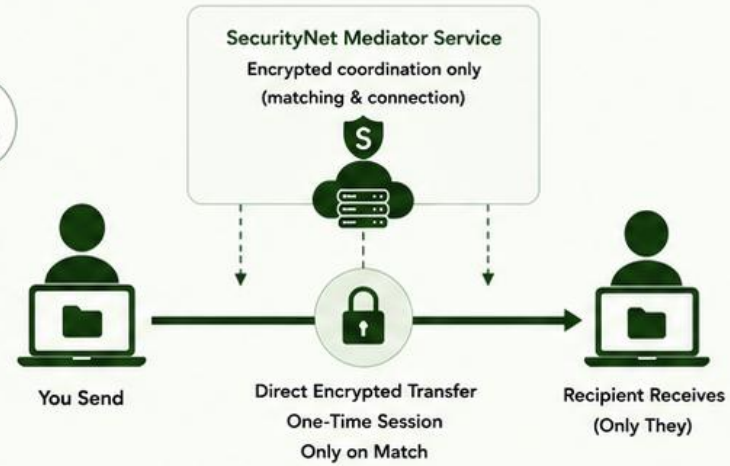
Your data travels through many systems and is duplicated, logged, analyzed and stored without your control.

VS.

THE SECURITYNET DIFFERENCE

Traditional messaging spreads information across phones, apps and clouds

SecurityNet keeps communication contained and controlled.



What This Prevents

- No central storage
- No passive synchronization
- No waiting cloud queue
- No persistent metadata or identifiers
- No copies made
- No analytics or profiling
- No unknown participants
- No data retained on our servers

Files and chats remain on the sender's machine until the recipient is online. Transfer happens only between trusted, authorized participants.

In This Presentation You Will Learn

How modern communication creates copies and exposes sensitive information → How SecurityNet limits participation to trusted people only → How secure transfer occurs only when both sides are online → Why this model dramatically reduces exposure and protects your privacy

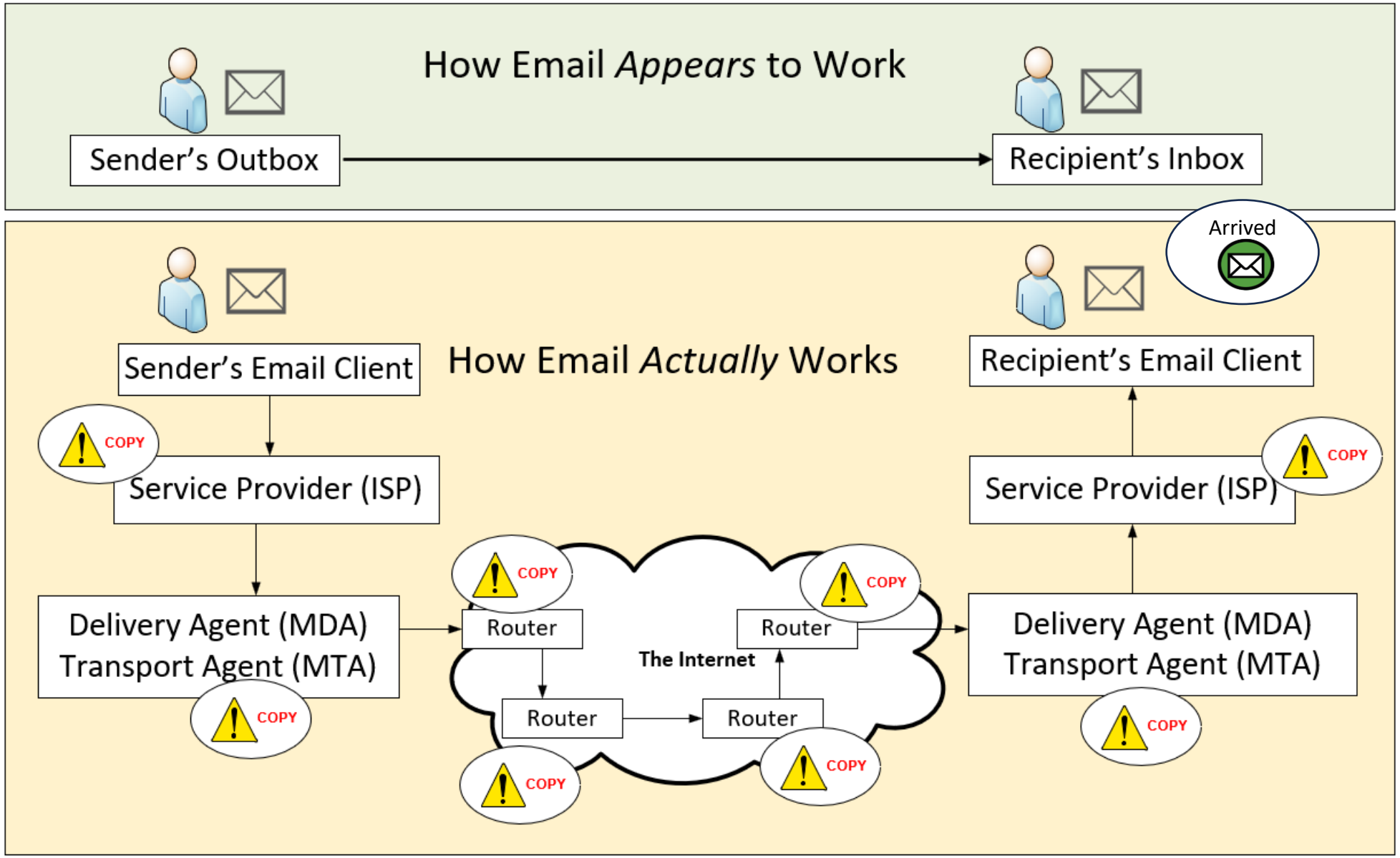
SecurityNet is not designed for anonymity.

It is designed for secure transfers with little or no metadata storage.

License owners are known to the website for account, payment and support purposes.

Invited users are known only by their SecurityNet ID. No personal details are collected or stored.

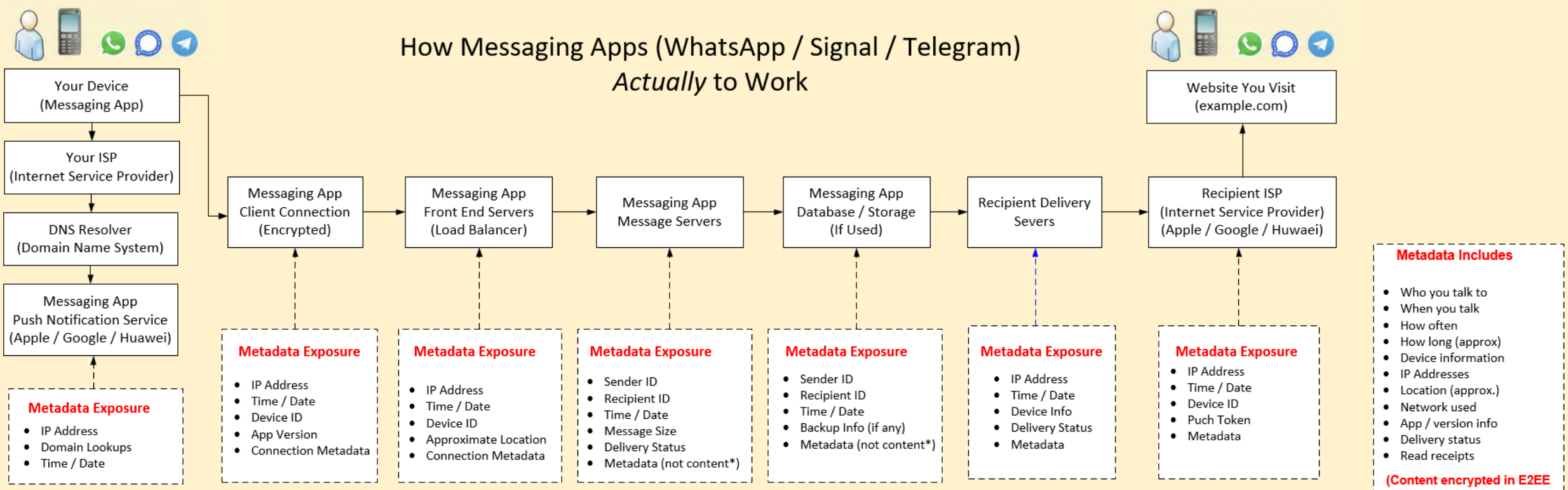
Trusted people.
Secure transfers.
Less exposure. More control.


How Email *Appears* to Work
Sender's Outbox
Recipient's Inbox
How Email *Actually* Works
Sender's Email Client
Service Provider (ISP)
Delivery Agent (MDA)
Transport Agent (MTA)
Router
Router
Router
Router
The Internet
Service Provider (ISP)
Recipient's Email Client
Arrived
COPY
COPY
COPY
COPY
COPY
COPY
COPY
COPY

How Messaging Apps (WhatsApp / Signal / Telegram) *Appear* to Work

You Send a Message → They Receive the Message

How Messaging Apps (WhatsApp / Signal / Telegram) *Actually* to Work



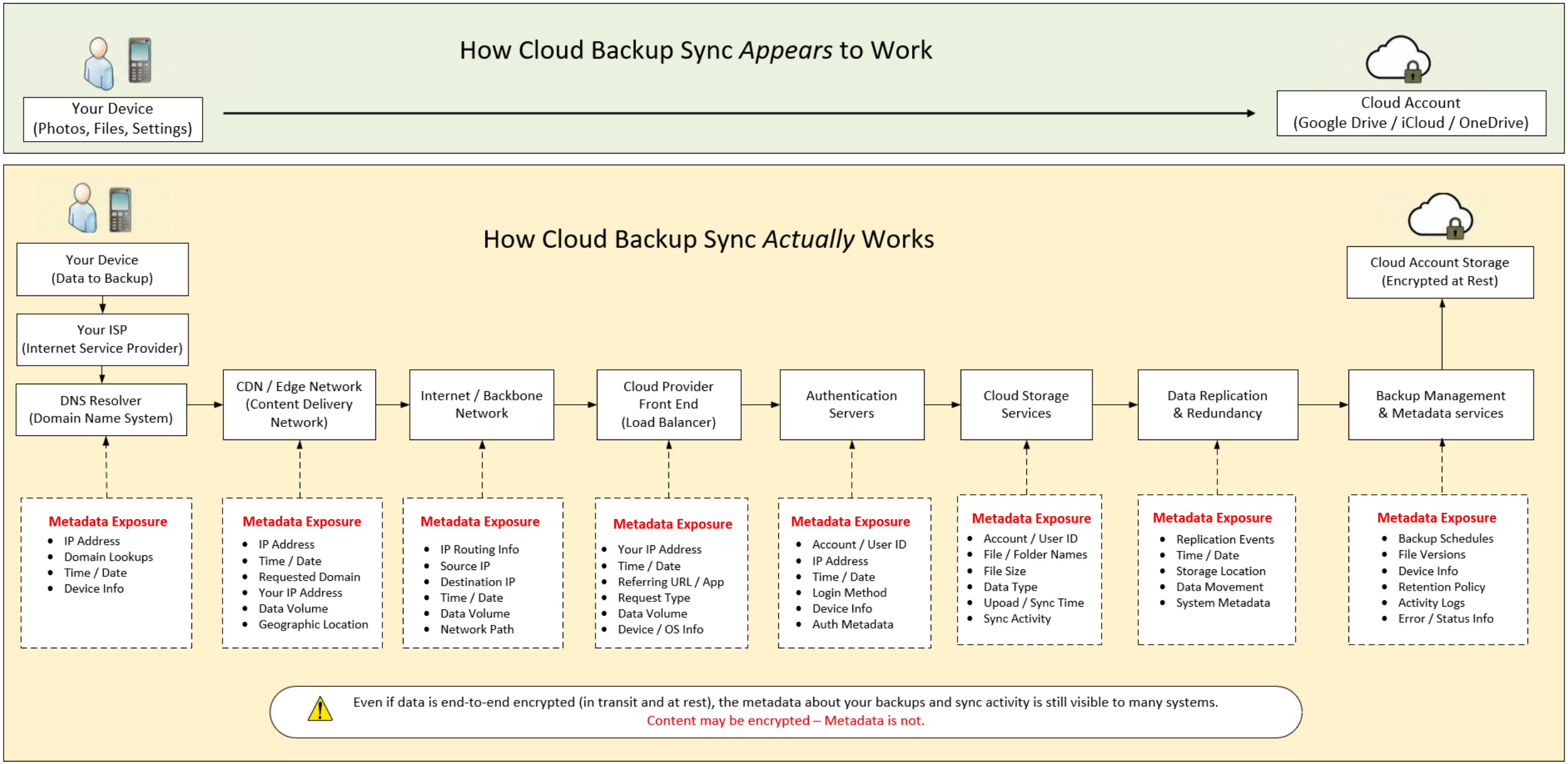
Metadata Includes

- Who you talk to
- When you talk
- How often
- How long (approx)
- Device information
- IP Addresses
- Location (approx.)
- Network used
- App / version info
- Delivery status
- Read receipts

(Content encrypted in E2EE apps, but metadata is not)

⚠ Even if messages are end-to-end encrypted (like Signal or WhatsApp), the metadata is still visible to many systems.
Who communicates, when, how often, device information, IP addresses and patterns can all be collected and analysed.

*** Some apps may store limited metadata for backups, multi-device sync, fraus prevention, or legal compliance**


How Cloud Backup Sync *Appears* to Work
Your Device
(Photos, Files, Settings)
Cloud Account
(Google Drive / iCloud / OneDrive)
How Cloud Backup Sync *Actually* Works
Your Device
(Data to Backup)
Your ISP
(Internet Service Provider)
DNS Resolver
(Domain Name System)
CDN / Edge Network
(Content Delivery Network)
Internet / Backbone Network
Cloud Provider
Front End
(Load Balancer)
Authentication Servers
Cloud Storage Services
Data Replication & Redundancy
Backup Management & Metadata services
Cloud Account Storage
(Encrypted at Rest)
Metadata Exposure
IP Address
Domain Lookups
Time / Date
Device Info
Metadata Exposure
IP Address
Time / Date
Requested Domain
Your IP Address
Data Volume
Geographic Location
Metadata Exposure
IP Routing Info
Source IP
Destination IP
Time / Date
Data Volume
Network Path
Metadata Exposure
Your IP Address
Time / Date
Referring URL / App
Request Type
Data Volume
Device / OS Info
Metadata Exposure
Account / User ID
IP Address
Time / Date
Login Method
Device Info
Auth Metadata
Metadata Exposure
Account / User ID
File / Folder Names
File Size
Data Type
Upoad / Sync Time
Sync Activity
Metadata Exposure
Replication Events
Time / Date
Storage Location
Data Movement
System Metadata
Metadata Exposure
Backup Schedules
File Versions
Device Info
Retention Policy
Activity Logs
Error / Status Info
Even if data is end-to-end encrypted (in transit and at rest), the metadata about your backups and sync activity is still visible to many systems.
Content may be encrypted – Metadata is not.

Introducing SecurityNet

- Traditional communication creates unnecessary copies and exposure
- Phones, apps and cloud systems spread sensitive information
- SecurityNet is designed to reduce exposure and restore user control
- SecurityNet limits communication to trusted participants
- Files transfer directly between participants
- No central cloud storage or passive synchronization
- Users retain greater control and privacy

SENDER

Your Device

How SecurityNet *Actually* Works

Direct, encrypted transfer between trusted participants.
No files or chats are stored in the cloud. No passive synchronization.

RECEIVER

Recipient's Device

1 Sender

User A selects recipients and files or starts a chat.
The data remains on the sender's device.

2 MySQL Informed

The sender app informs the SecurityNet MySQL database that it intends to send data to specific recipient(s).

Metadata Revealed

- Sender ID (encrypted)
- Recipient ID(s) (encrypted)
- Time / Date
- (No file or chat content)

IDs are encrypted. Not stored, collected or shared.

3 VPS Mediator Handshake

The sender app connects to the SecurityNet VPS mediator to initiate the transfer process.

Metadata Revealed

- VPS URL (domain)
- Destination IP Address
- Time / Date

(Not saved, collected or shared)

Sender IP address is not revealed.

4 Mediator Authorizes

The mediator verifies both sender and recipient are online and authorized to communicate.
No file or chat information is seen.

Metadata Revealed

- Authorization confirmation
- Time / Date

(No content)

5 SecurityNet Sender App

Once authorized, the sender app prepares the encrypted data and establishes a direct secure tunnel.

Metadata Revealed

- Encrypted tunnel initiation
- Time / Date

(No content)

6 Encrypted Tunnel

A one-time, end-to-end encrypted tunnel is created directly between sender and recipient.

Metadata Revealed

- Tunnel exists
- Time / Date

(No content)

7 Send / Receive Data Transfer

Files or chat messages are sent directly through the encrypted tunnel. The mediator does not see the data.

Metadata Revealed

- Transfer in progress
- Time / Date
- Data volume

(No content)

8 *Receiver App Receives Data*

The recipient app receives and decrypts the data directly. Nothing is stored in any central system.

Metadata Revealed

- Delivery confirmation
- Time / Date

(No content)

About Metadata in SecurityNet

Only minimal metadata is revealed during:

- VPS handshake
- Destination IP address (during connection)

This is not stored, collected or shared.

No file content, no chat content, no metadata about content is ever seen by the mediator or anyone else.

All other metadata is encrypted, transient and discarded immediately after use.

SecurityNet never stores, collects or shares your files, chats or metadata.
Transfers occur only when both sender and recipient are online at the same time.

Metadata Disclosure Key

Minimal Metadata Revealed	VPS handshake and destination IP only (not stored, collected or shared)
No Metadata Revealed	No content, no file/chat data, no message content

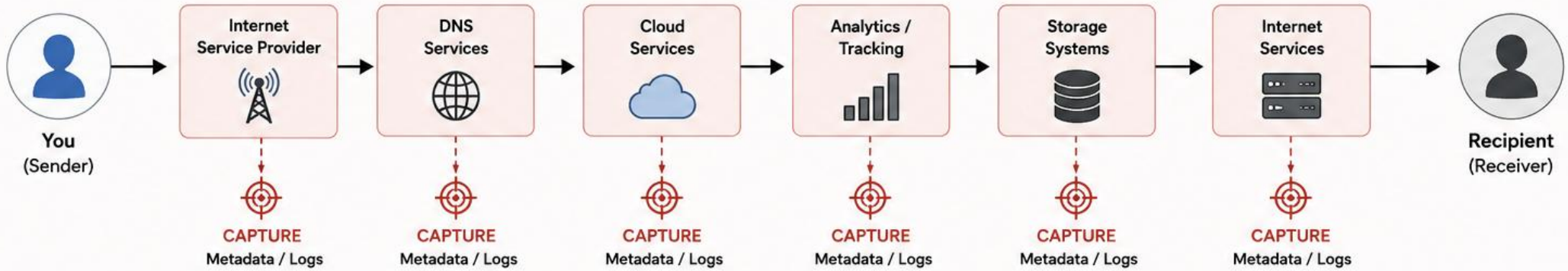
SecurityNet is designed for direct, real-time, private communication between trusted participants.
No central storage. No passive sync. No unnecessary exposure."

Traditional Communication vs Trusted Communication

Who participates in your communication makes all the difference.

Traditional Internet Communication

Many unknown systems participate. Metadata is captured along the way.



Many unknown systems participate in communication.

SecurityNet Trusted Communication

Only trusted, approved participants communicate over an encrypted connection.

Only trusted authorized participants communicate.
Fewer intermediaries. Less metadata. Greater privacy.

KEY TAKEAWAY

Traditional Internet

Many intermediaries.
Many capture points.
More metadata.
More exposure.

ApprotyNet

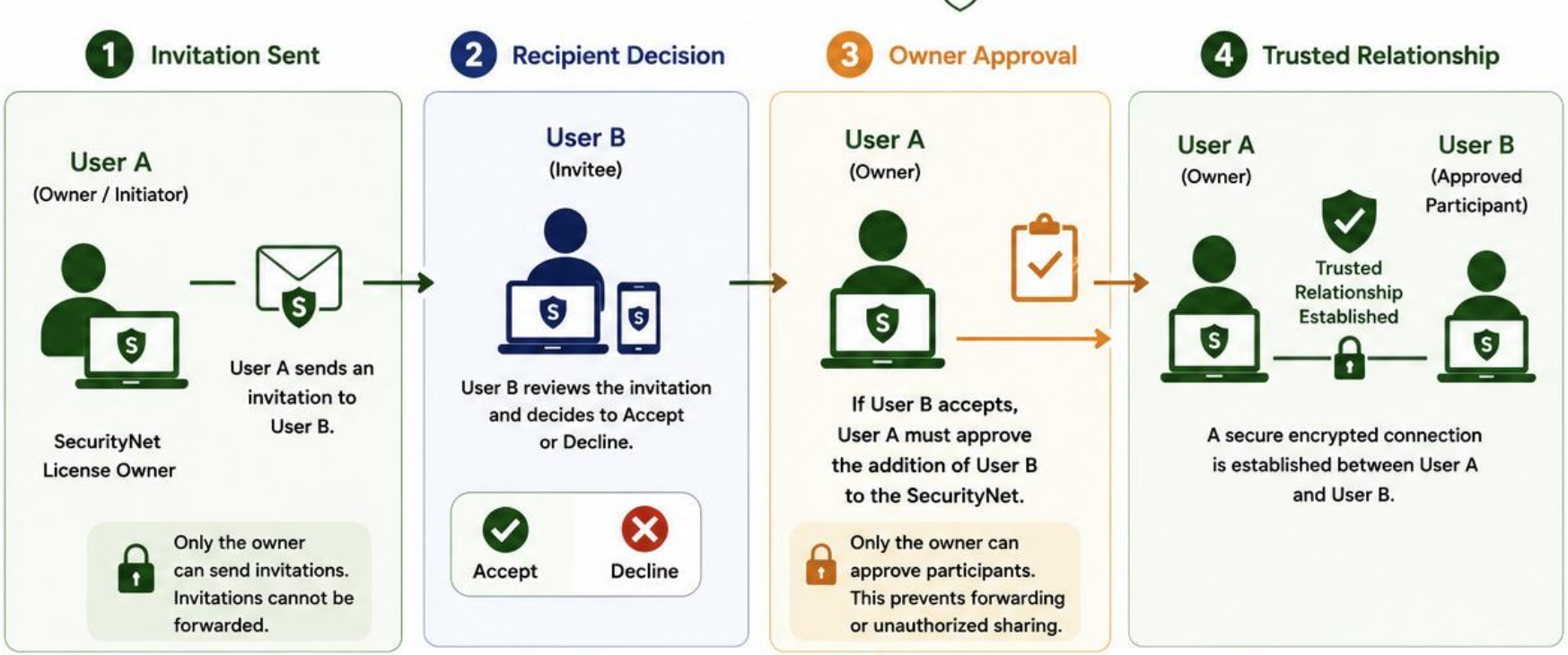
Trusted participants only.
Encrypted connection.
Less metadata.
Stronger privacy.

SECURITYNET

2 Invite & Approval

Controlled Trust Authorization

Only the SecurityNet owner can invite and approve participants.
Trust cannot be forwarded or delegated.



Pending Acceptance
No trusted connection yet.

After Owner Approval
Encrypted trusted connection is now active.

Controlled Trust Model

Owner Initiated
Only the SecurityNet owner can send invitations.

Recipient Accepts
The invited user must explicitly accept.

Owner Approves
The owner must approve before the user is added to the network.

No Forwarding
Invitations cannot be forwarded or used to add others.

Authorized Participation
Only approved participants can establish trusted communication.

KEY TAKEAWAY

Only the SecurityNet owner can authorize trusted participants.
Invitations must be accepted by the recipient and approved by the owner before a trusted relationship is established.

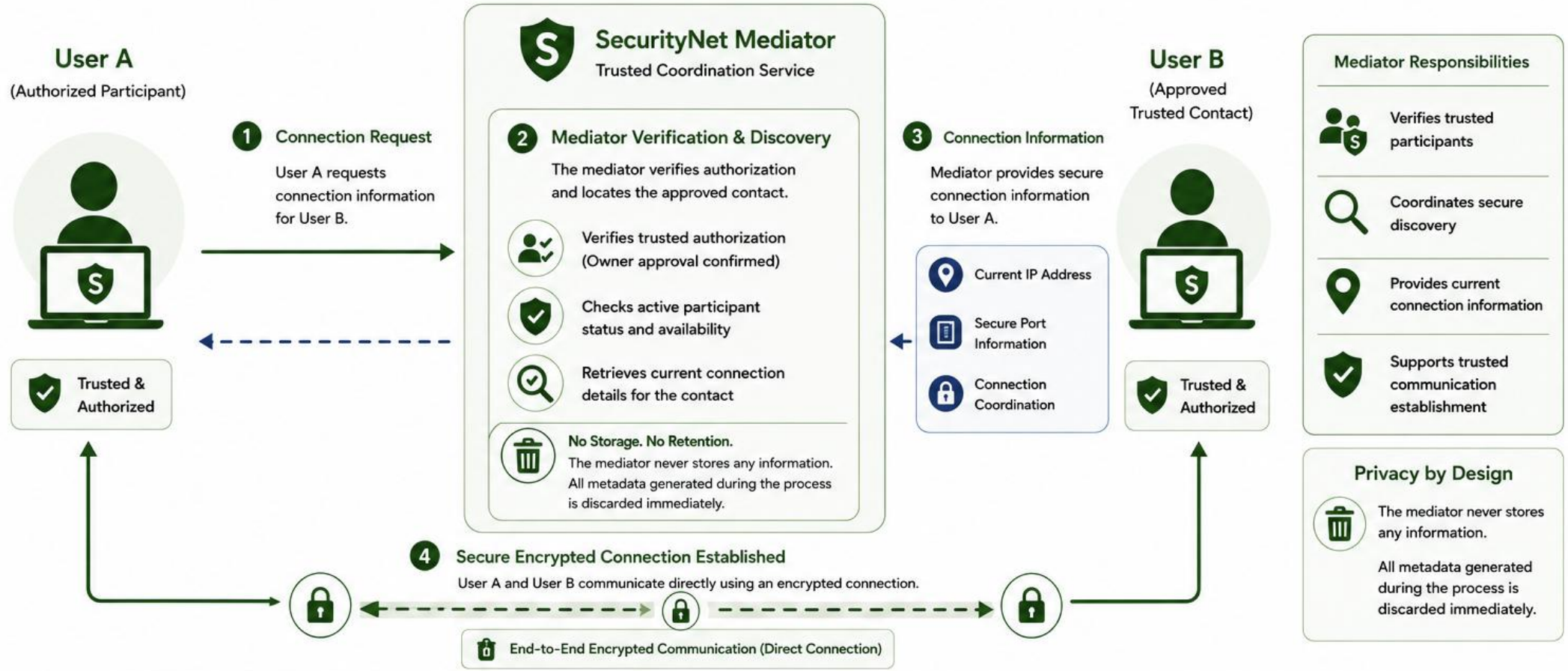
This controlled process ensures trust cannot be delegated, forwarded, or abused.

SECURITYNET

3 Mediator Coordination & Discovery

Mediator Coordination & Secure Discovery

The SecurityNet Mediator securely locates trusted participants
and provides connection information for encrypted communication.



KEY TAKEAWAY

Only authorized trusted participants can discover and establish secure communication paths.

No Open Participation | No Storage. No Metadata Retention. | Trust. Control. Privacy. | Secure Communication Between Trusted People.

SECURITYNET 4 Secure Transfer

Secure Transfer of Files

SecurityNet creates an encrypted tunnel using a one-time password and encrypts all files in transit using a one-time session code.

1 ENCRYPTED TUNNEL ESTABLISHMENT

One-Time Password
User A generates a one-time password and initiates the connection.

Authenticate
User B enters the one-time password to authenticate the connection.

Secure Tunnel Created
A secure encrypted tunnel is established between User A and User B.

Key Point
The tunnel exists only for this session.
It cannot be reused.
Once the session ends, it is gone.

User A
Sender

Before Transfer
Files are in original (unencrypted) form on User A's system.

2 File Encryption
Files are encrypted with a one-time session code.

ENCRYPTED TUNNEL
Secure, End-to-End Encrypted Channel

PDF

All data (files + metadata within the transfer) is encrypted in transit and protected from unauthorized access.

3 File Decryption
User B uses the one-time session code + password to decrypt the files.

User B
Recipient

After Transfer
Files are decrypted using th's one-time session code + password and are available to User B.

4 Session Ends – Everything Discarded

When the transfer is complete, the tunnel closes, the session code expires, and all related metadata is discarded. Nothing is retained.

Security by Design

One-Time Password
Used to establish the encrypted tunnel.

One-Time Session Code + Password
Used to encrypt all files and decrypt on the receiving end.

End-to-End Protection
Files are encrypted on User A's system and only decrypted on User B's system.

No Residual Data
No files, passwords, session codes or metadata are stored by SecurityNet or the Mediator.

All metadata generated during the process is discarded immediately.

KEY TAKEAWAY

SecureNet ensures that both the communication channel and the files are protected with one-time credentials and end-to-end encryption.

One-Time Password + Encrypted Tunnel + One-Time Session Code + Password = Secure Transfer

No Open Participation
Only trusted participants.

No Storage. No Retention.
All metadata is discarded.

Trust. Control. Privacy.
You stay in control.

Secure Communication
Between Trusted People.

Strong Encryption
Every step of the way.

SECURITYNET 5 Authorized Match-Based Transfer

Deferred Secure Transfer Activation

Files and chats are never stored in the cloud.
They remain on the sender's machine until each intended recipient is online.
Transfers occur only when both sender and recipient are online at the same time.

1 Select Recipients and Content

User A selects recipients:

- One or more individual users

OR

- One trusted group

Files or chats remain on User A's machine until recipients are online.

2 Pending Send Recorded (Encrypted)

A pending send record is created in the SecurityNet MySQL coordination database.

No file content is stored.

All coordination data in MySQL is encrypted. No user relationships are revealed.

3 Scanner Monitors for Online Matches

The SecurityNet Scanner monitors for authorized recipients (or group members) coming online.

No match, no transfer.

The system does not sync or scan content. It only looks for authorized online matches.

4 Authorized Match Detected

When an intended recipient (or group member) is online, an authorized match is detected using encrypted coordination data.

The mediator process is initiated.

5 Mediator Engaged

The Scanner engages the SecurityNet Mediator to coordinate the secure connection between both parties.

No data about the files or users is revealed.

The mediator never stores any files, metadata or session information.

6 One-Time Session Created (On Match)

Only after the match is confirmed does the system create:

- One-time encrypted tunnel
- One-time password
- One-time session code

Credentials are generated dynamically for this session only and never persist.

7 Encrypted Transfer Occurs

The file(s) or chat message are encrypted and sent directly from User A to the online recipient.

Recipient decrypts using the one-time session code + password.

End-to-end encrypted direct transfer. No central storage. Metadata is discarded after use.

If a recipient (or group member) is offline, nothing happens.
The pending send (encrypted coordination record) and the files/chats remain on the sender's machine.
Transfer will occur automatically when the recipient comes online.

Key Characteristics

On-Demand Activation
Nothing happens until there is something to send.

Both Must Be Online
Sender and recipient must be online at the same time for the transfer to occur.

Encrypted Coordination
Only encrypted coordination records are stored in MySQL. No files. No metadata.

No Central Storage
Files and chats are never stored on any server. They remain on the sender's machine.

Ephemeral Sessions
Tunnels, passwords and session codes are one-time use and discarded.

No Retention
All session information and metadata are discarded immediately after use.

Groups – Distributed Local Copies

- When content is sent to a group, it is delivered to ALL members of that group.
- Each group member maintains their own local copy.
- Transfers occur individually as each authorized member comes online.
- If a member (e.g., User X) is offline, the files/chats destined for them remain on the sender's machine until they return online.

Communication Types

Individual Send
Send files or chats to one or more individual users.

Group Send
Send files or chats to one trusted group.

Key Principle

SecurityNet does not push. It delivers only when both parties are present and authorized.

No storage. No waiting in the cloud.
Just real-time, secure, direct transfer.

Encrypted MySQL Coordination

The MySQL database contains only encrypted coordination records to track pending sends and online status.

- No file content
- No user metadata
- No relationships revealed
- No messages or chats stored

It only enables secure matching and activation.

KEY TAKEAWAY

SecurityNet transfers files and chats only when both sender and recipient are online.
Files and chats stay on the sender's machine until direct encrypted delivery occurs.
Encrypted coordination. One-time sessions. Total privacy by design.

Sender + Recipient + One-Time Session = Secure Transfer

No Open Participation. Only trusted participants.

No Storage. No Retention. All metadata is discarded.

Trust. Control. Privacy. You stay in control.

Secure Communication Between Trusted People.

Strong Encryption Every step of the way.

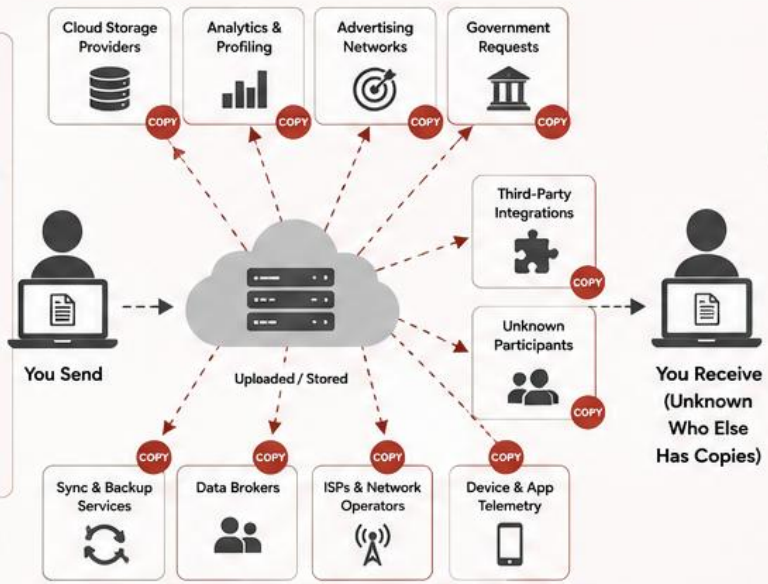
SECURITYNET 6 What SecurityNet Prevents

SecurityNet Drastically Reduces Exposure

Fewer systems. Fewer copies. Fewer risks. Only trusted participants.

Traditional Internet & Cloud Systems

Many unknown systems participate.
Your data is copied, analyzed, and retained.



What This Creates

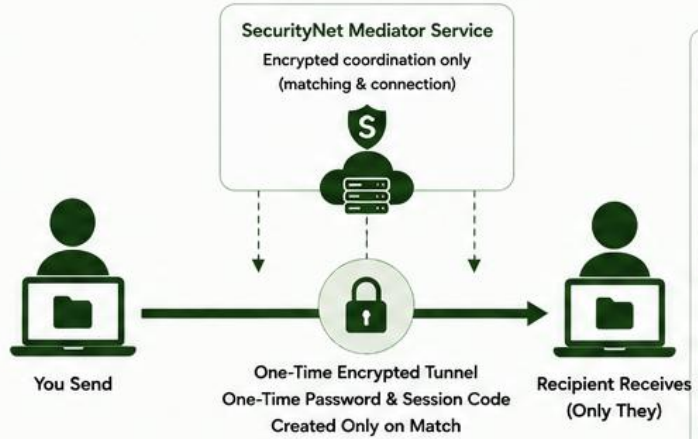
- Multiple copies of your data
- Persistent metadata and identifiers
- Tracking and correlation
- Profile building and analytics
- Data retained indefinitely
- Exposure to unknown parties

Your data travels through many systems and is duplicated, logged, analyzed, and stored without your control.

VS.

SecurityNet

Only trusted, authorized participants take part.
Direct encrypted transfer. No copies. Minimal metadata.



What SecurityNet Prevents

- No central storage
- No passive synchronization
- No waiting cloud queue
- No persistent metadata or identifiers
- No copies made
- No analytics or profiling
- No unknown participants
- No data retained on our servers

Files and chats remain on the sender's machine until the recipient is online. Transfer happens only between trusted, authorized participants.

KEY TAKEAWAY

SecurityNet reduces exposure by limiting communication to trusted authorized participants using direct encrypted transfer.

Sender + Recipient + One-Time Session = Secure Transfer

You Stay in Control
Files and chats stay on your machine until direct delivery.

Minimal Exposure
Only the intended recipient receives your data.

Trusted by Design
Only authorized participants can exchange information.

Strong Encryption
One-time tunnels, passwords and session codes.

No Retention
No storage. No logs of content. No metadata kept.

SecurityNet is not designed for anonymity.
The license owner is known to the website for account, payment and support purposes.
Invited users are known only by their SecurityNet ID. No personal details are collected or stored.

SecurityNet's mission:
Secure transfers. Little or no metadata storage.

SecurityNet In Summary

- Traditional systems create unnecessary copies and exposure
- Phones, apps and cloud systems spread sensitive information
- SecurityNet limits communication to trusted participants
- Files transfer directly between approved users
- No central cloud storage or passive synchronization
- Users retain greater control and privacy