SECURITYNET Presentation Overview

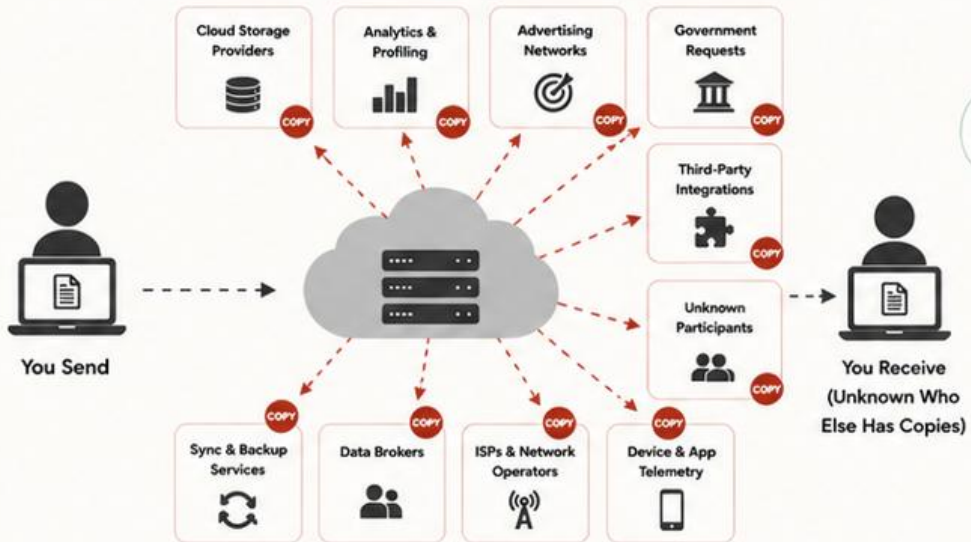
Why SecurityNet Exists

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.



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.

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

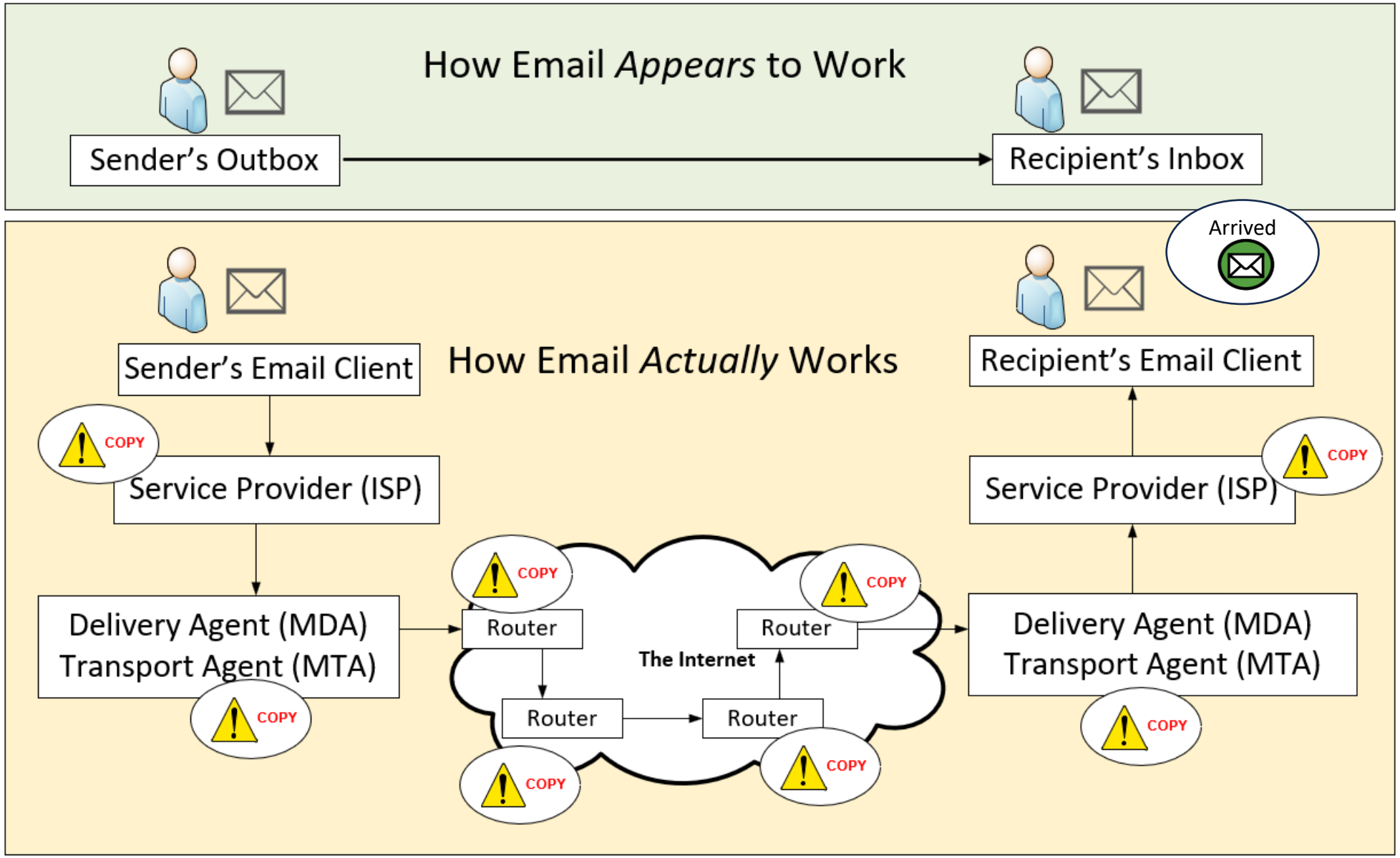
SecurityNet is not designed for anonymity.

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

Your Device (Messaging App)
↓
Your ISP (Internet Service Provider)
↓
DNS Resolver (Domain Name System)
↓
Messaging App Push Notification Service (Apple / Google / Huawei)

Metadata Exposure
- IP Address
- Domain Lookups
- Time / Date

Messaging App Client Connection (Encrypted) → Messaging App Front End Servers (Load Balancer) → Messaging App Message Servers → Messaging App Database / Storage (If Used) → Recipient Delivery Severs → Recipient ISP (Internet Service Provider) (Apple / Google / Huwaei) → Website You Visit (example.com)

Metadata Exposure
- IP Address
- Time / Date
- Device ID
- App Version
- Connection Metadata

Metadata Exposure
- IP Address
- Time / Date
- Device ID
- Approximate Location
- Connection Metadata

Metadata Exposure
- Sender ID
- Recipient ID
- Time / Date
- Message Size
- Delivery Status
- Metadata (not content*)

Metadata Exposure
- Sender ID
- Recipient ID
- Time / Date
- Backup Info (if any)
- Metadata (not content*)

Metadata Exposure
- IP Address
- Time / Date
- Device Info
- Delivery Status
- Metadata

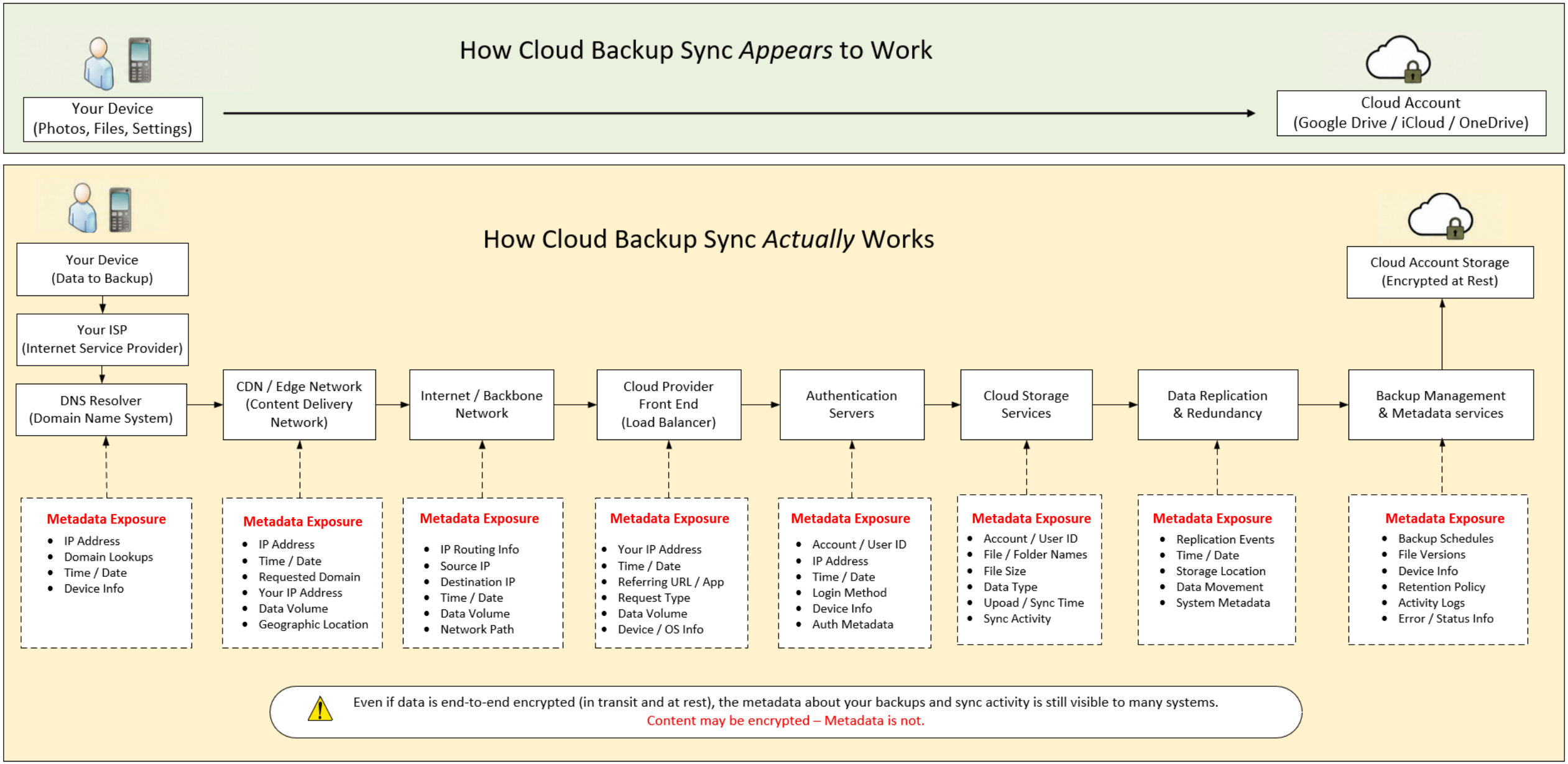
Metadata Exposure
- IP Address
- Time / Date
- Device ID
- Puch Token
- Metadata

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."

1. Traditional vs Trusted Communication

The difference is who is involved.

Traditional Systems

Many unknown intermediaries handle your data.

More copies. More metadata.
Less control. Greater exposure.

SecurityNet

Only trusted, approved participants are involved.

Fewer copies. Less metadata.
More control. Stronger privacy.

2. How SecurityNet Works

Simple. Private. Under your control.

1

Invite Trusted Contacts

You choose who can participate.

2

Approve Participants

Only approved people can communicate.

3

Send Files or Messages Directly

Data is encrypted and sent between trusted users.

4

Files Stay Under Your Control

Store on your device, removable storage, or your NAS.

5

No Central Cloud Storage

There is no central repository of your data.

You remain in control from start to finish.

3. What SecurityNet Prevents

By design, SecurityNet eliminates unnecessary exposure.

Centralized Storage

No central servers storing your files or messages.

Unnecessary Intermediaries

Data travels directly between trusted participants.

Excess Metadata Collection

Fewer copies, logs, and tracking opportunities.

Uncontrolled Data Mining

Less data available for analytics and profiling.

Automatic Cloud Sync & Backups

Your data is not automatically copied or synchronized.

Uncontrolled Mobile Exposure

Sensitive transfers stay off personal mobile devices.

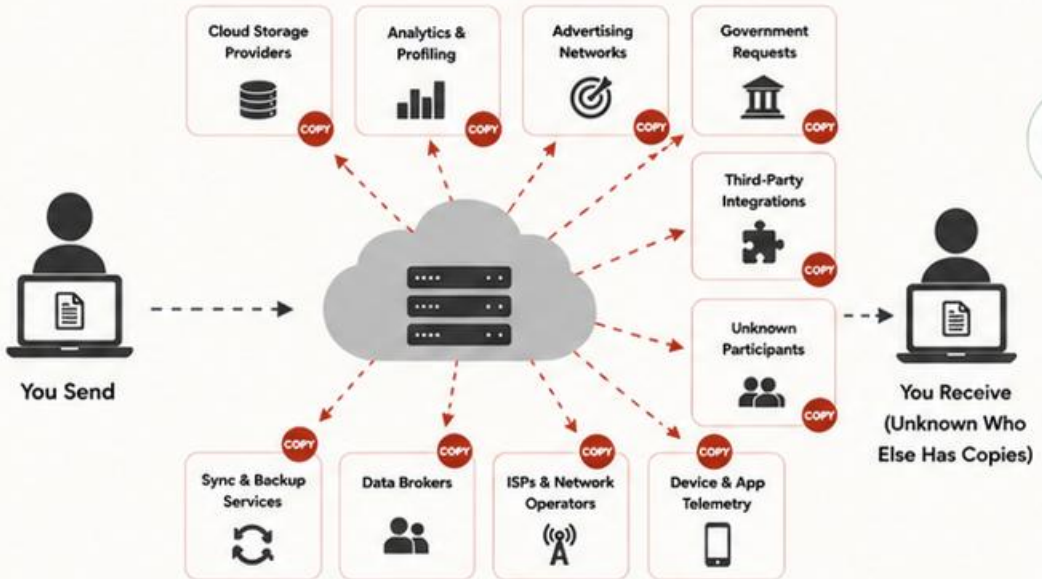
Unwanted Visibility

Only those you trust can see or access your data.

SecurityNet protects your communications and your privacy by design.

THE PROBLEM TODAY

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



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.

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.

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