

# Securing Consumer Cloud Services

Israel Cidon

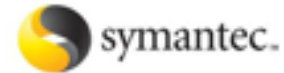
Technion



sookasa

# Evolution of Data Security

PCs



Enterprise Networks



Mobile Devices



Cloud Services

# Cloud Services are Ubiquitous



Dropbox  
300M Users



GMail  
>500M Users



Evernote  
100M Users

- “1 in 5 employees uses Dropbox for work” – GigaOm
- Advantages: increased productivity, low cost, intuitive
- Philosophy: user owns the data, KISS

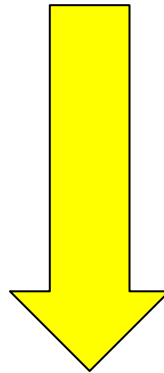
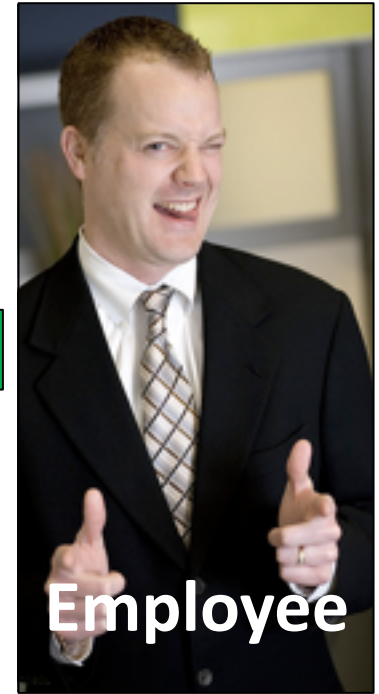
# The Conflict



Can't have  
enterprise data  
on cloud and  
private devices!



I want to use my  
devices and web  
accounts in the  
same way for  
enterprise and  
personal data



**Employees always win**

# Perceptions

Users want

Freedom  
Productivity

- Work from anywhere
- Use device of choice
- Bring your own cloud
  - Dropbox
  - Gmail
  - Evernote



CIOs want

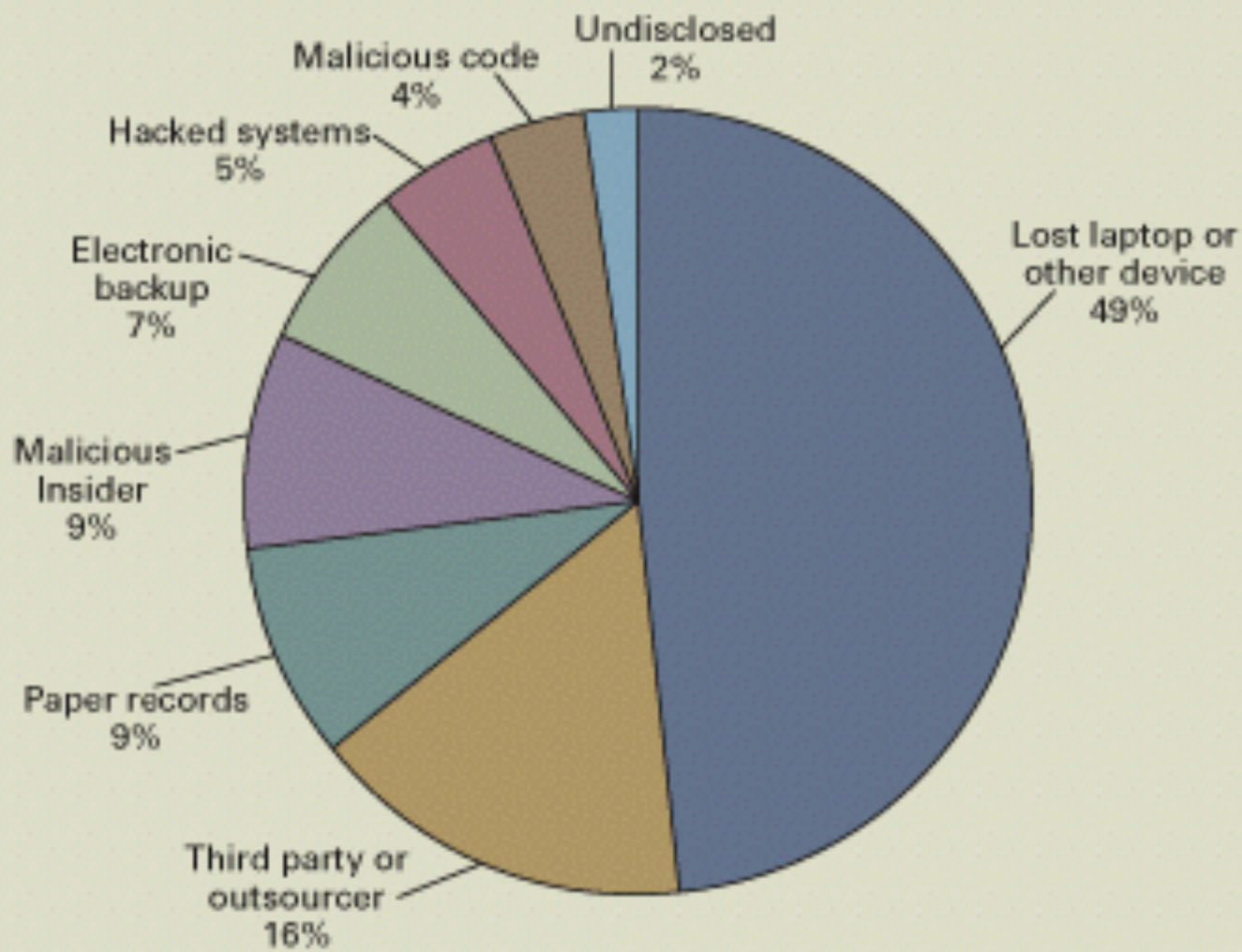
Control  
Compliance

- Security
- Access control
- Data Visibility
- Usage Audit trails
- Data Leak Prevention
- Retention
- Classification

# The Challenge

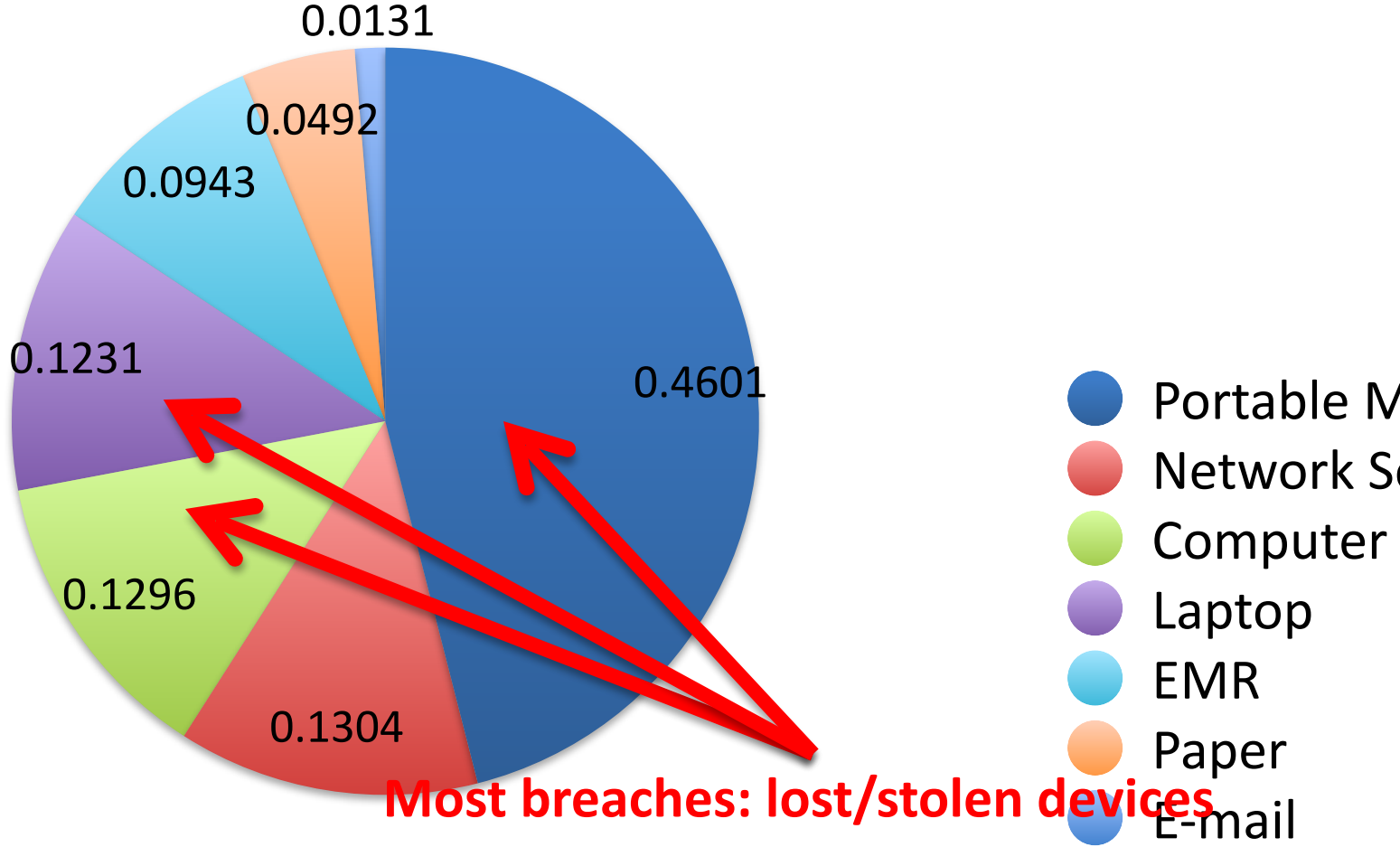
1. Most data is unstructured (80-95%)
2. “Sensitive data” is scattered across data
3. Breach can be caused by single file
4. Spread of unstructured data → increase in breaches
5. Consumers products are built on:
  - User in the center not the organization
  - Spread product and data through viral effects
    - Sync, connect, share, recursive share
  - Sharing => stickiness

# Primary Cause of a Data Breach



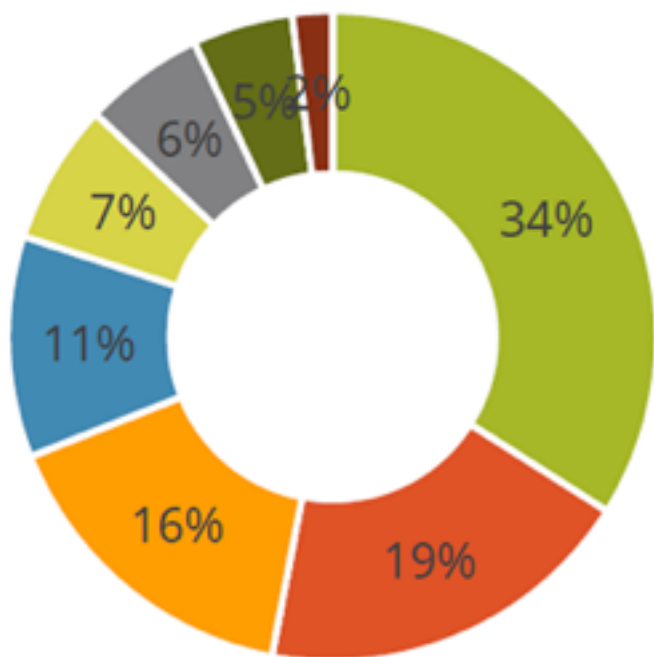
Note: Total exceeds 100 percent due to rounding.  
Source: Ponemon Institute

# HIPAA Breaches [Source: HHS]





# Causes of Data Breaches



- Negligent Insider
- Outsourcing
- Malicious Insider
- System Glitch
- Cyber Attack
- Failure to shred
- Physical loss
- Other

PERCENTAGE OF  
BREACHES CAUSED  
BY  
AUTHORIZED  
USERS

69%

# Top Cloud Data Risks

1. Device Loss with Unencrypted Files

2. Accidental Sharing of Files

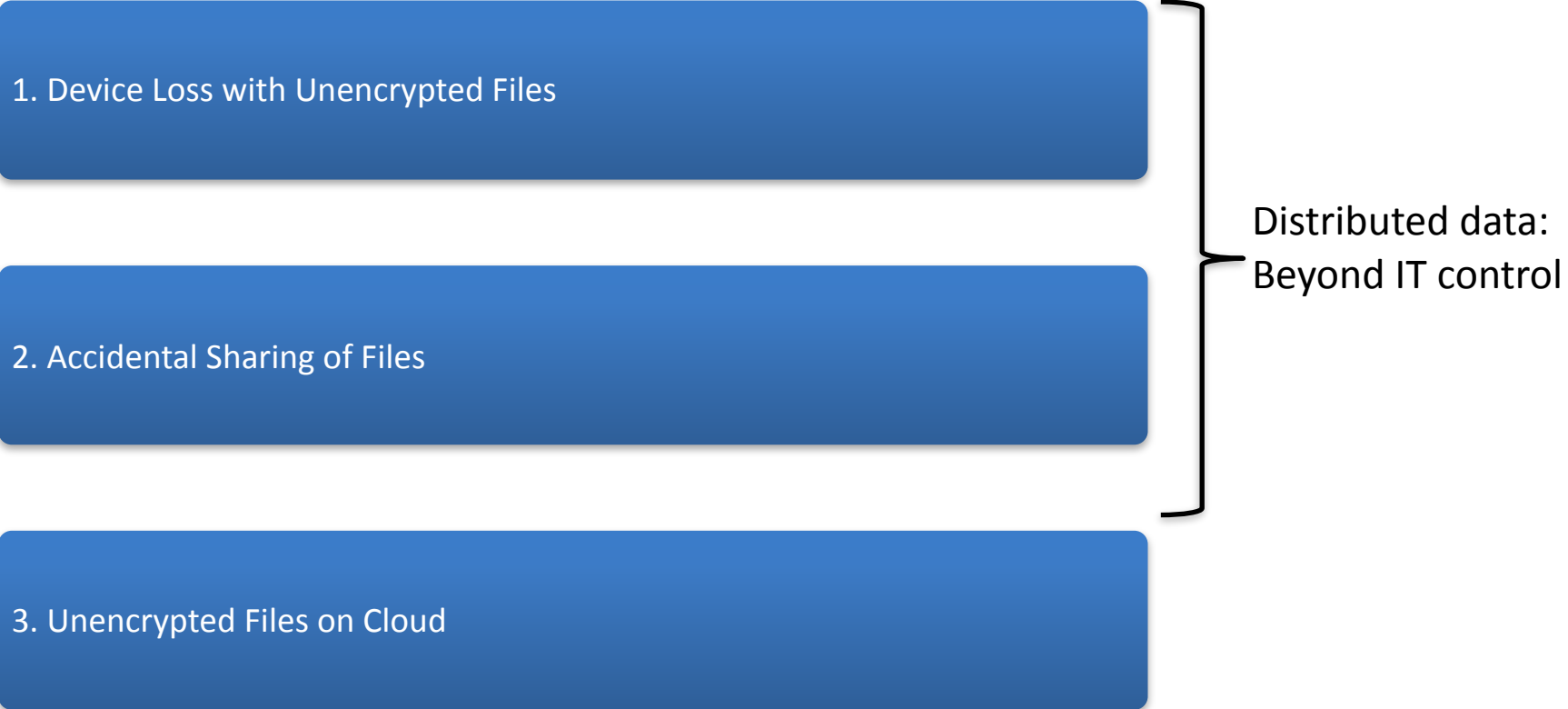
3. Unencrypted Files on Cloud

# Top Cloud Data Risks

1. Device Loss with Unencrypted Files

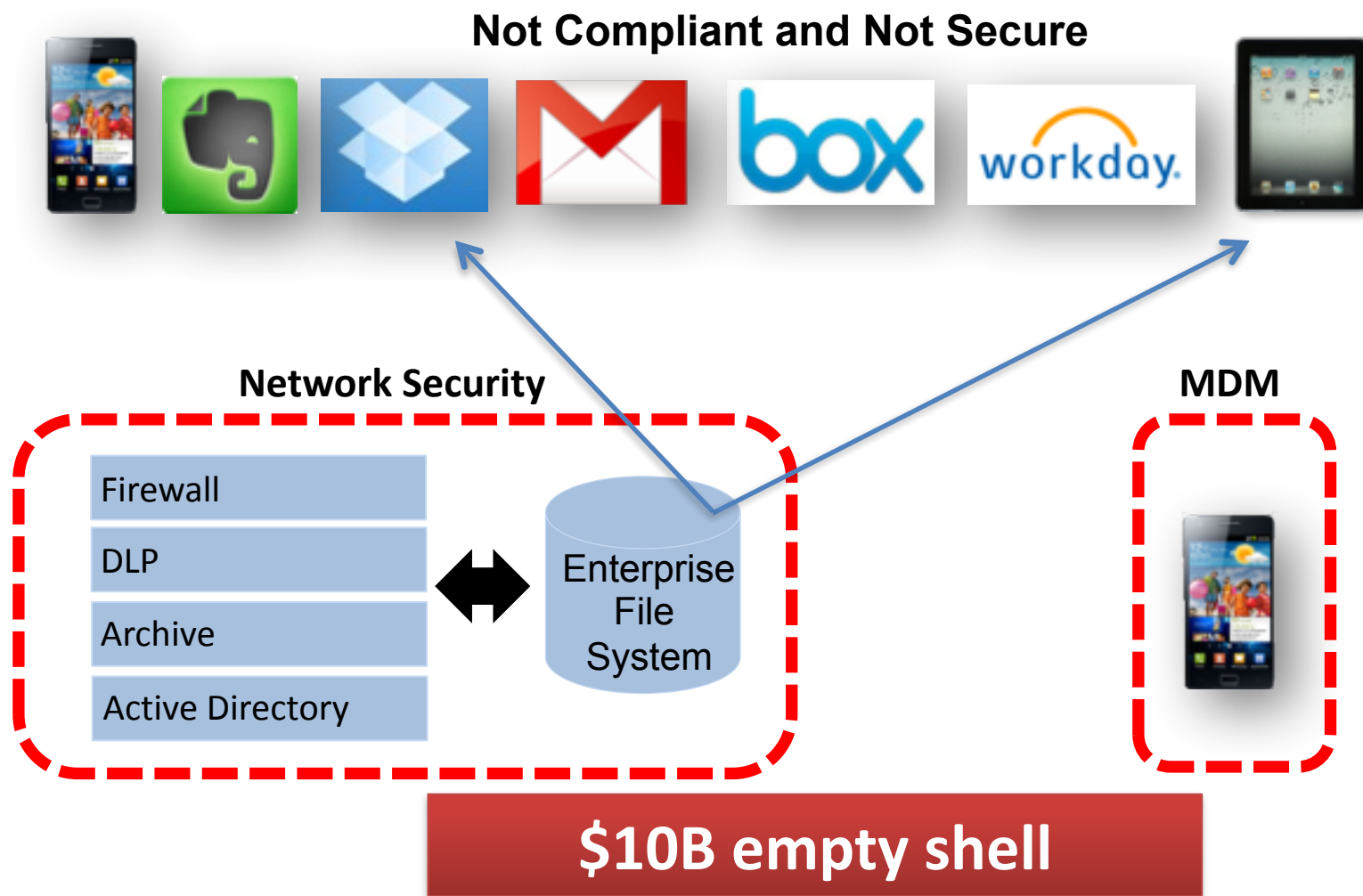
2. Accidental Sharing of Files

3. Unencrypted Files on Cloud

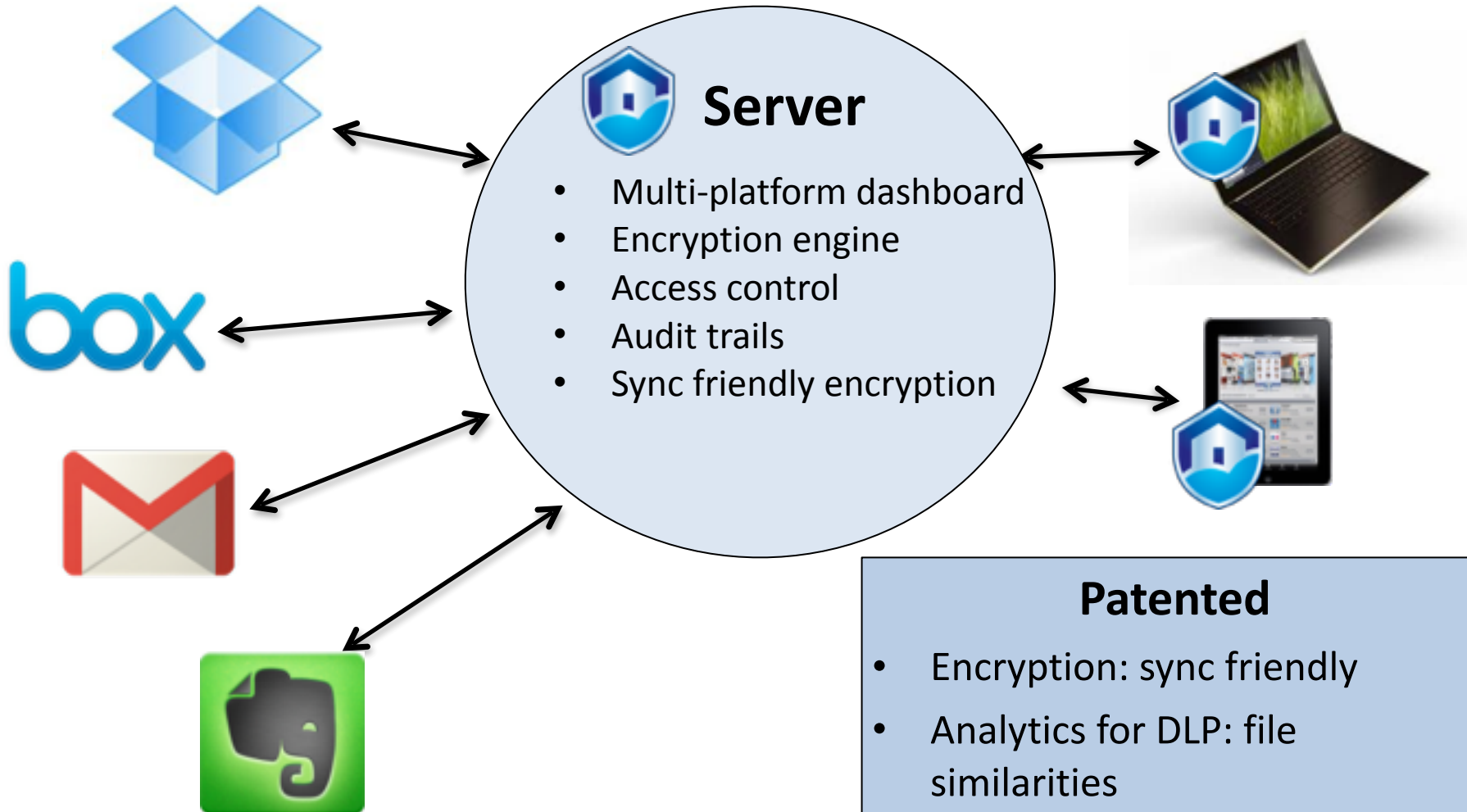


Distributed data:  
Beyond IT control

# Current Solutions Don't Work



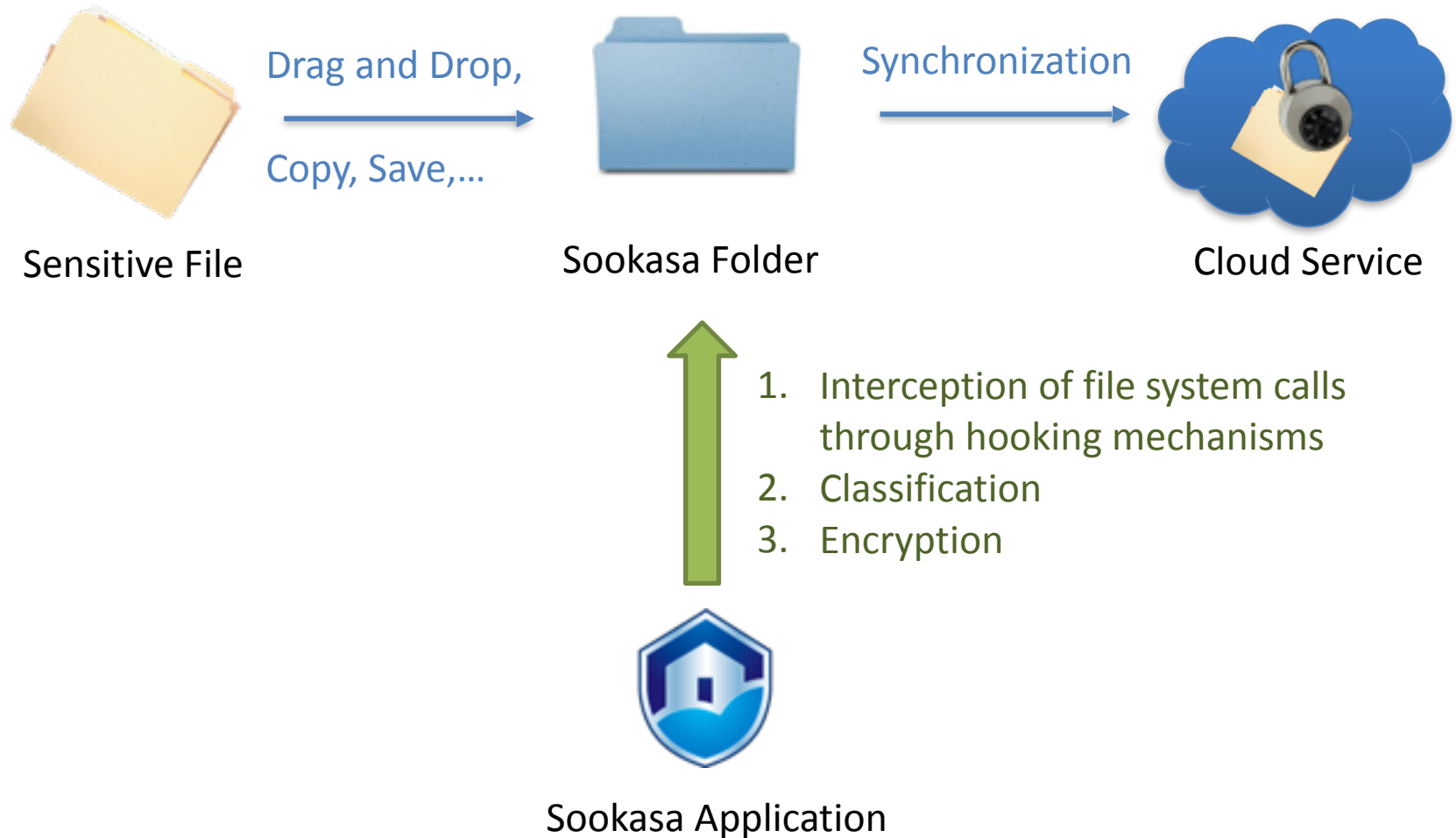
# SaaS: Security as a Service



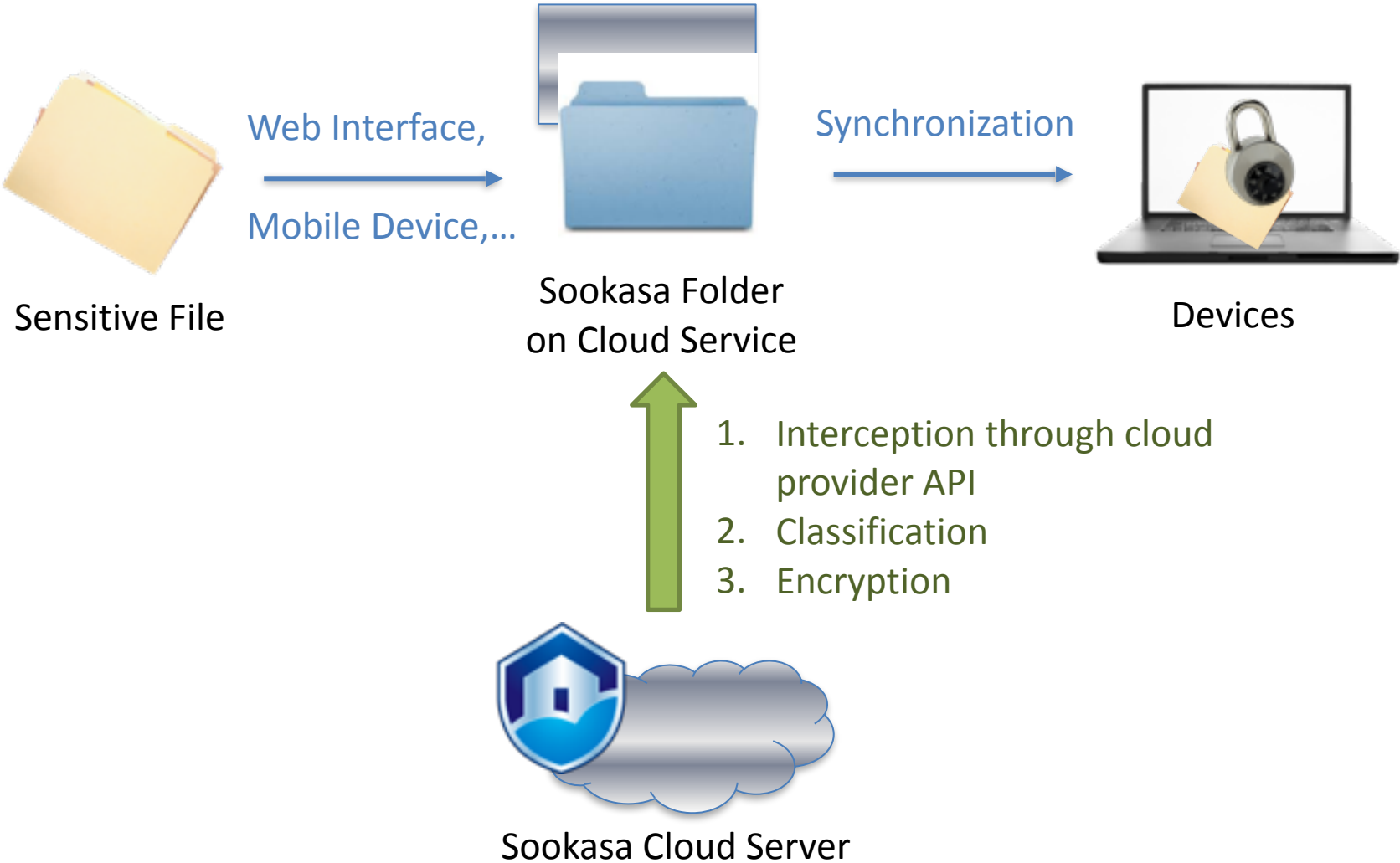
## Patented

- Encryption: sync friendly
- Analytics for DLP: file similarities
- Automated data classification
- Zero Knowledge

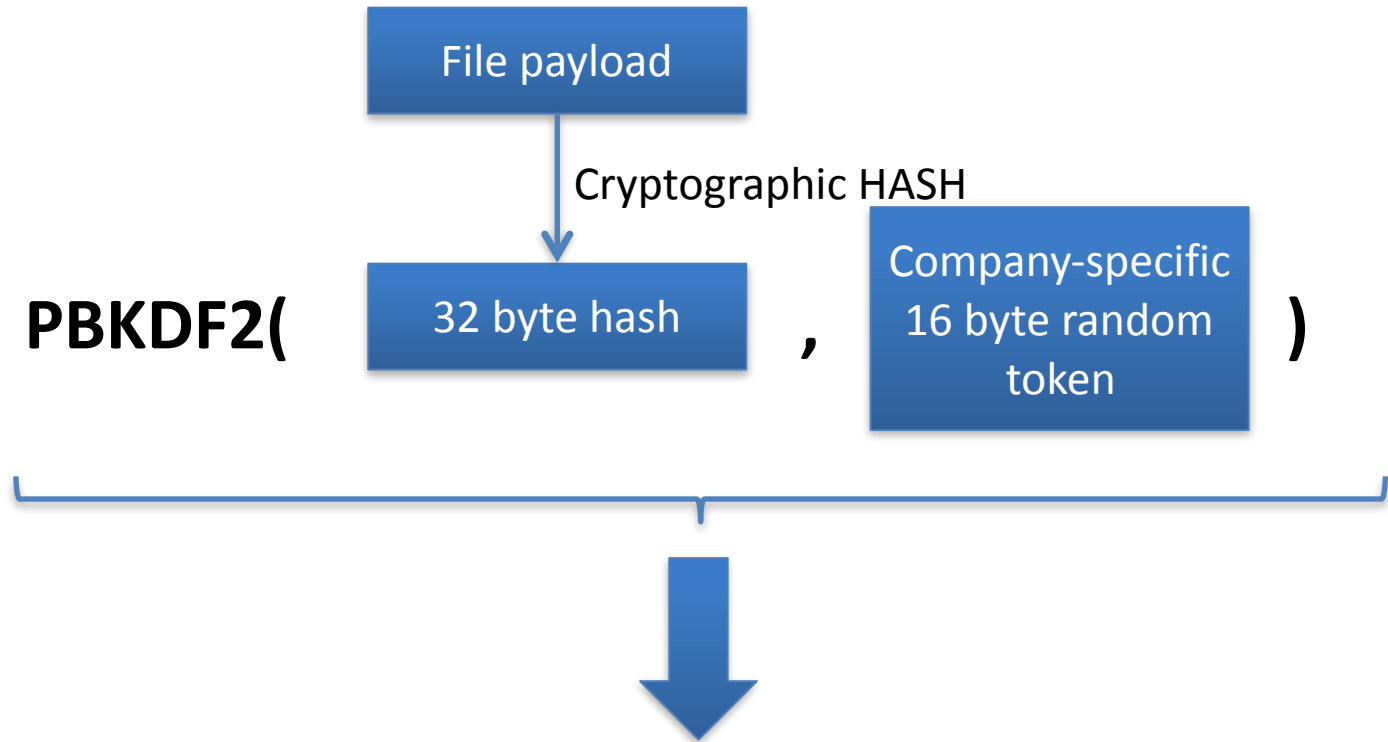
# Architecture: On-Device Encryption



# Architecture: Cloud Encryption



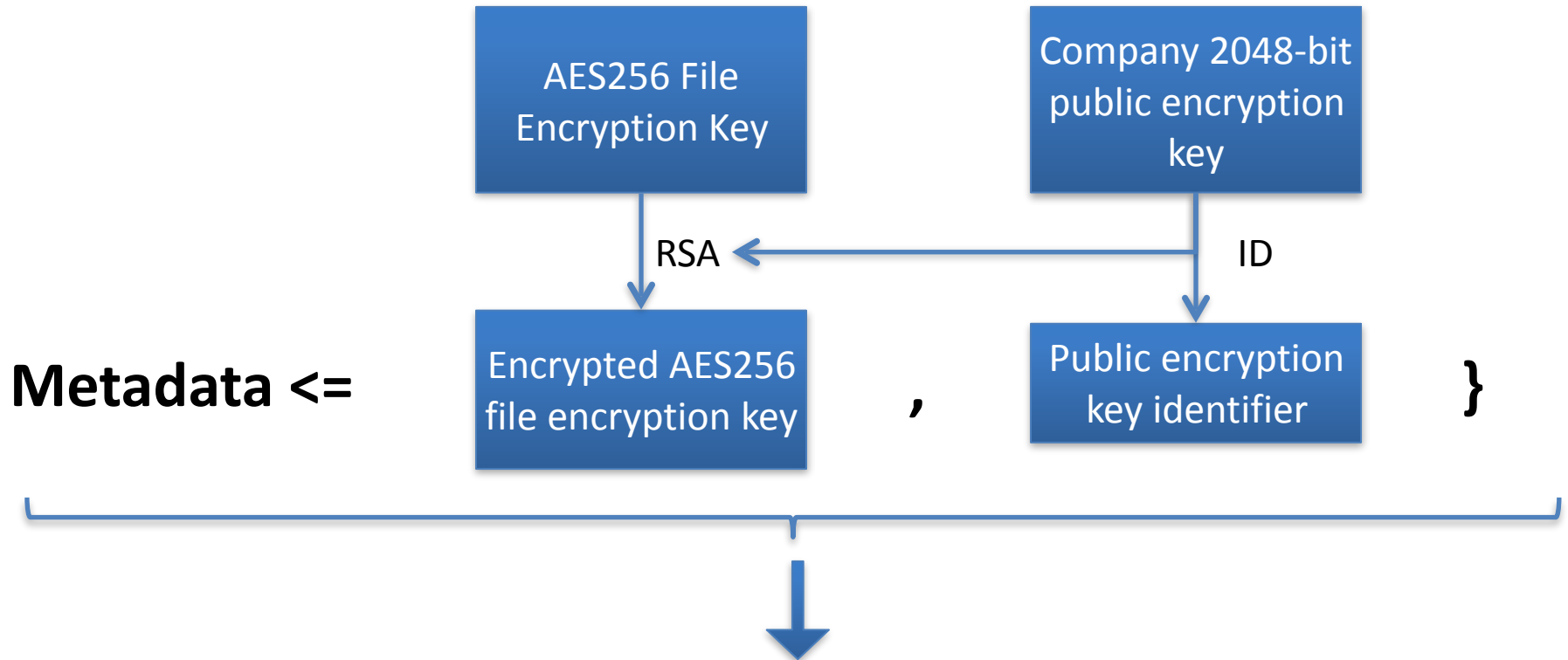
# Per-File Key Generation



- Unique AES 256-bit key that preserves full file deduplication within company
- leaks no information outside company



# Key Embedding in File Metadata

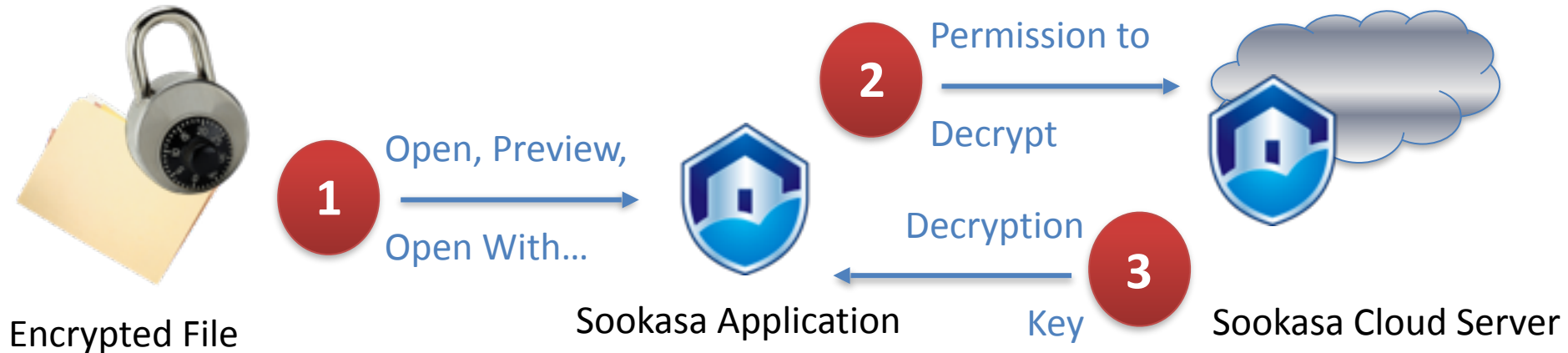


- Encrypted file can be decrypted by owner of company private key
- Metadata signed by clear data cryptographic hash, can be verified
- Metadata attached to encrypted file

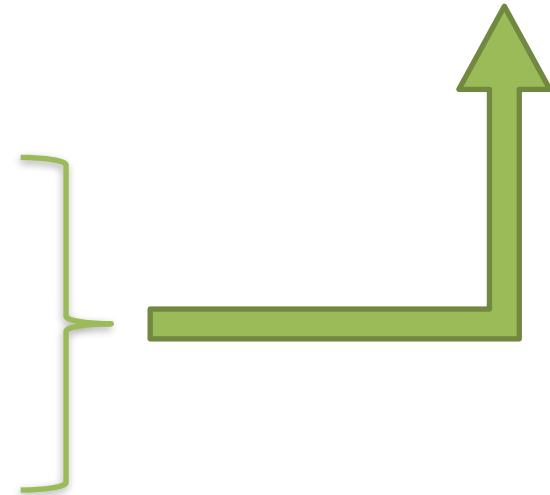
# File Metadata

- Attached to encrypted file body
- Signed against tampering
- Include access control tagging
  - Owner, origin directory
  - Sensitivity tagging by user or cypher
  - Permission policy

# Architecture: Decryption



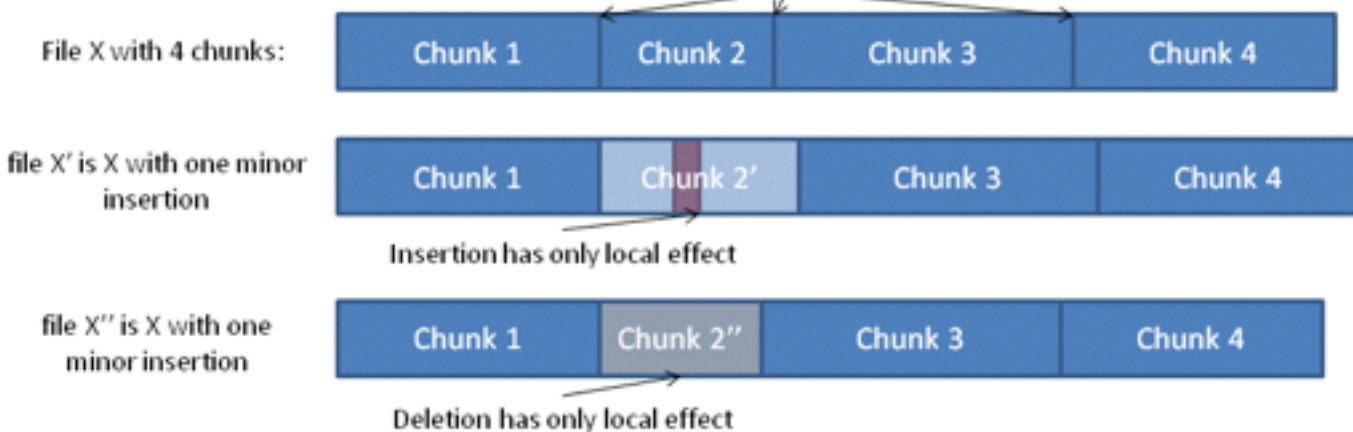
1. Signed file metadata
2. Requesting device
3. Requesting user
4. Access control lists and permission policies



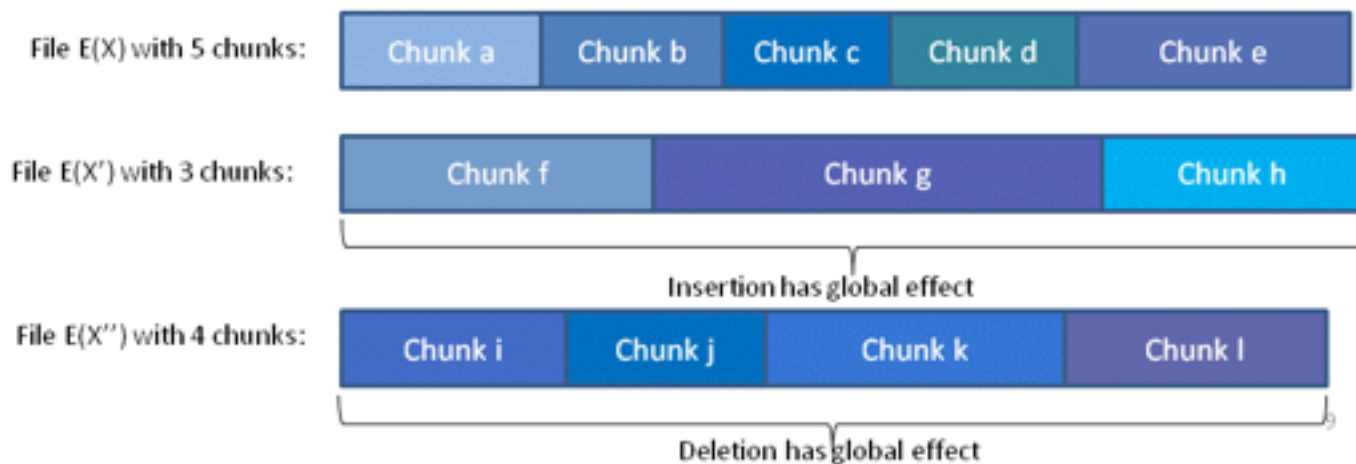
# Encryption and Deduplication

## Chunking at storage service before file encryption

*Anchors* bound chunks



## Chunking at storage service after file encryption



## Chunking file before “friendly” encryption

*Anchors* bound chunks

File X with 4 chunks:



file X' is X with one minor insertion



Insertion has only local effect

file X'' is X with one minor deletion

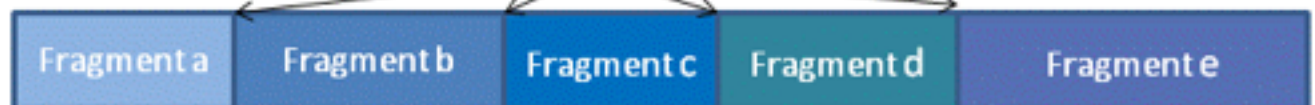


Deletion has only local effect

## Friendly Encryption –file sliced to fragments – encrypted by signature

*Anchors* bound fragments

File E(X) with 5 encrypted fragments:



File E(X') with 5 encrypted fragments:



Insertion has fragment wide effect (two fragments when anchor is affected)

File E(X') with 5 encrypted fragments:

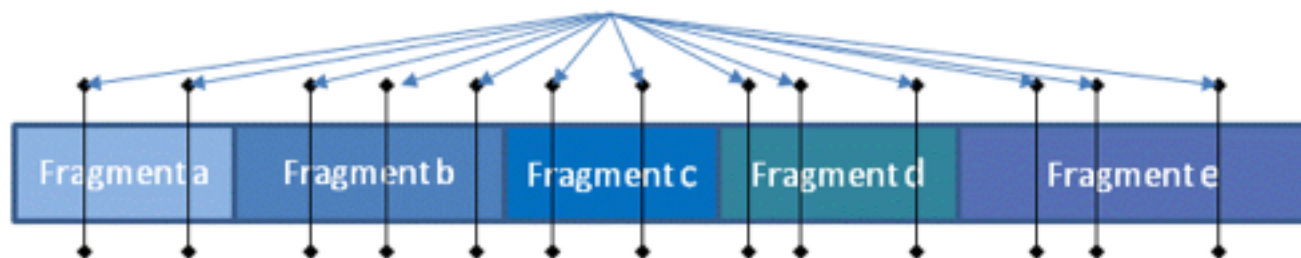


Deletion has fragment wide effect (two fragments when anchor is affected)

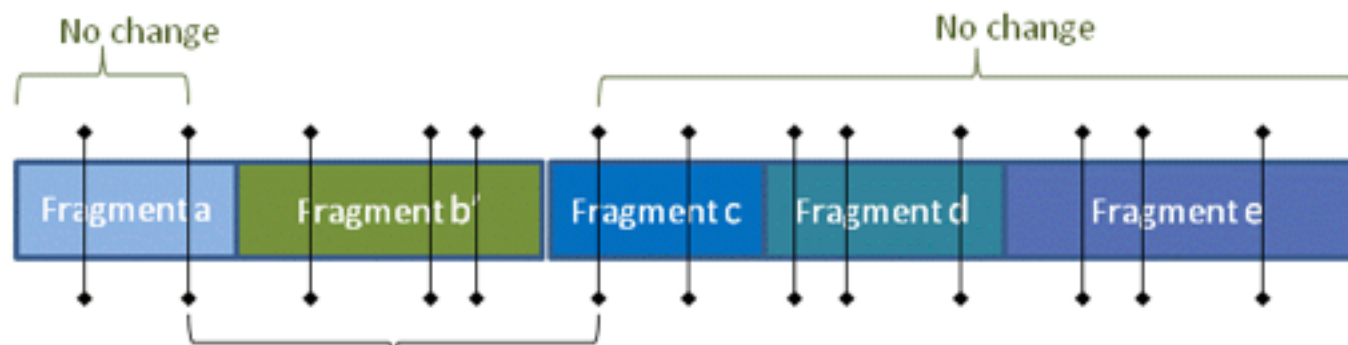
# Friendly Encryption – chunking at storage service

*Anchors* bound chunks by storage service

File E(X) with 5 encrypted fragments:

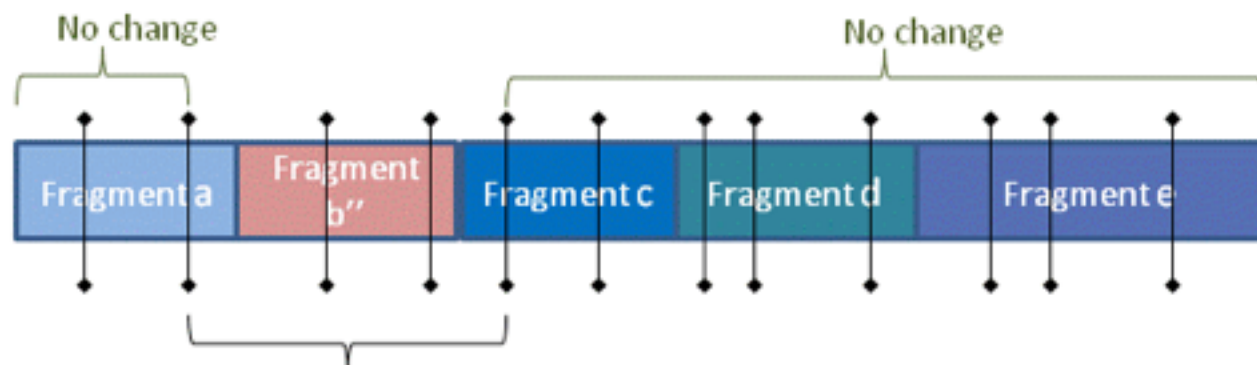


File E(X') with 5 encrypted fragments:



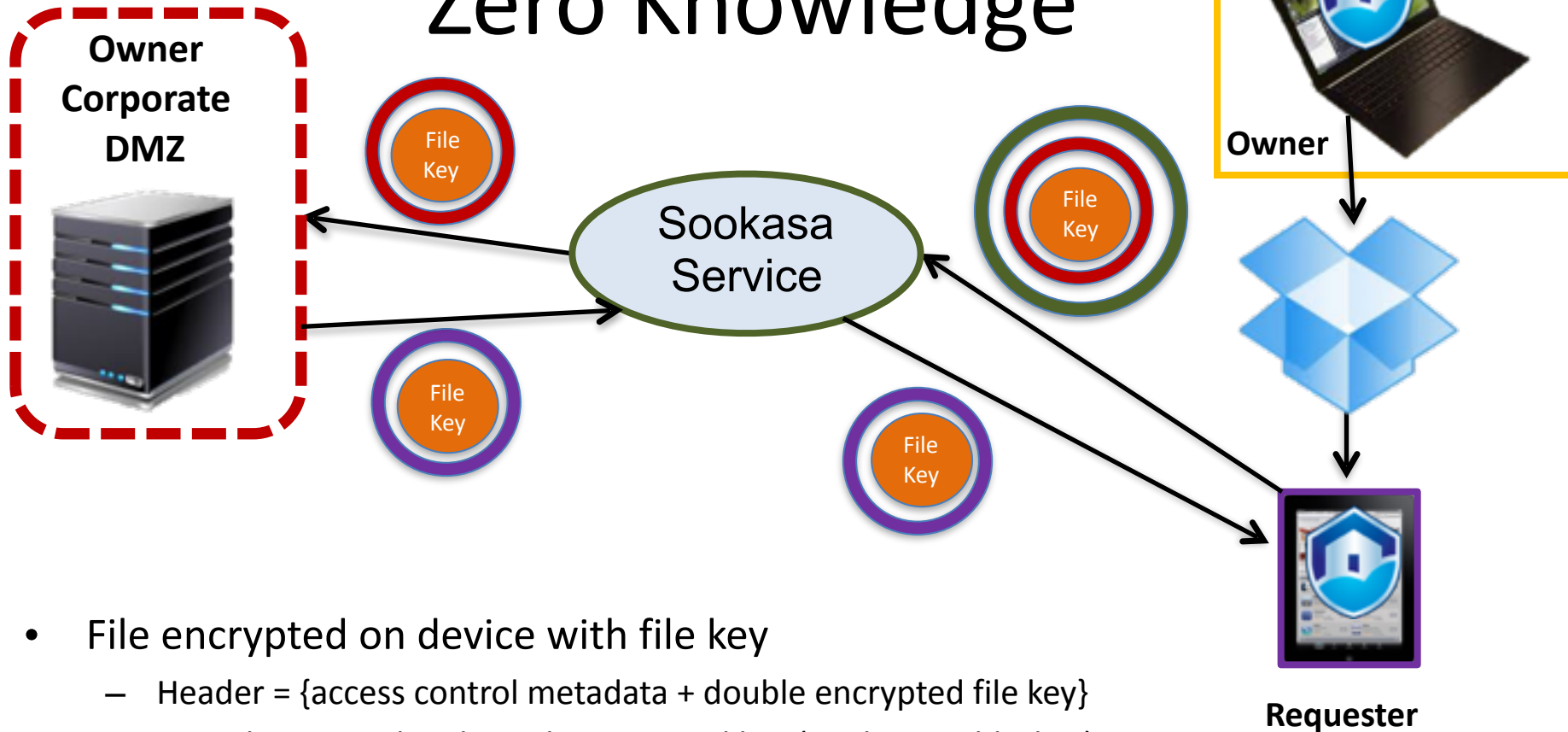
Insertion affects all chunks that touch the affected fragment(s)

File E(X') with 5 encrypted fragments:



Deletion affects all chunks that touch the affected fragment(s)

# “Zero Knowledge”



- File encrypted on device with file key
  - Header = {access control metadata + double encrypted file key}
  - Metadata signed with single encrypted key (Sookasa public key)
- Requester sends file header + device public key to Sookasa
- Sookasa authenticates metadata, requester ID and access rights
- File key extracted by corporate and encrypted by device public key

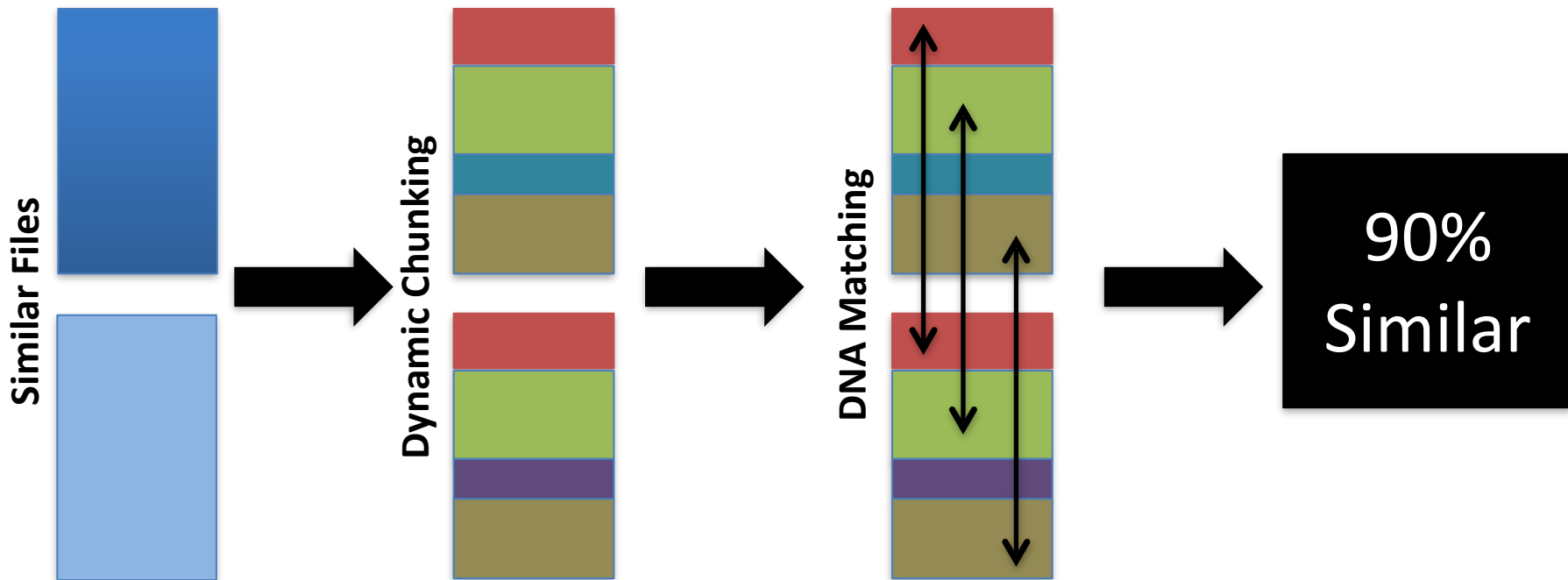
# Identify and Protect Sensitive Files

- Type and basic content (big Excel files)
- Ownership (CEO, CFO, Counsel)
- Content
  - SSN, credit card, keywords, domain terms
- Cross file property
  - Similarity (content, dedup DNA sequence)
- User behavior
  - Placement and timing
  - Crowdsourcing



# Classification with de-duplication signatures

- Detect copies and variants across users and platforms to enable visibility and security



Patented

**Thank You**

