



Implementing Cloud Security Solutions

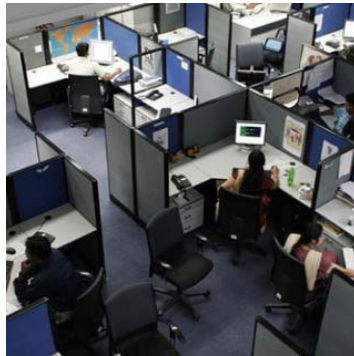
Tim Matthews
Sr. Director, Product Marketing

Ancient Times vs. Modern Times

Desktop

Data Center

1999



2009



Starbucks launches HotSpots in August 2002



Google Data Center in Lenoir, NC circa 2005

Risks at the New Corporate Perimeter

TIMES ONLINE

“ The C-word Mr Clegg will not use is coalition ” Rachel Sylvester

NEWS COMMENT BUSINESS MONEY SPORT LIFE & STYLE TRAVEL DRIVING ARTS & ENTS ARCHIVE OUR PAPERS SUBSCRIPTIONS

UK NEWS WORLD NEWS POLITICS SCIENCE ENVIRONMENT WEATHER TECH & WEB VIDEO PHOTO GALLERIES TOPICS MOBILE RSS

Where am I? Home News Tech & Web The Web

From Times Online
May 4, 2007

Hackers target wi-fi hotspots in new phishing attack

Starbucks has been targeted by hackers using 'evil twin' wi-fi networks

Jonathan Richards

RECOMMEND?

Computer users have been warned of the dangers of using wi-fi hotspots after it emerged that cyber-criminals are targeting the networks in café chains including Starbucks.

Times Online has uncovered evidence that criminals are using a technique known as an 'evil twin attack', where victims think that they are logging on to the genuine network in a café but are in fact being diverted to a 'rogue' connection.

Once logged on to the twin network, the victim's every keystroke is captured by the fraudster, who controls the connection from a nearby laptop and uses it to extract information for the purpose of committing identity fraud.

In a chatroom used to discuss the technique, also known as a 'man in the middle' attack, Times Online saw information changing

Starbucks is among the targets of the phishing scam

TECH CENTRAL

Latest posts on the blog

- Superheros show support for public transport
- So, it's goodbye to Tokyo for another year
- Follow us at the Tokyo Game Show

3D TV: HIT OR HYPE?

Does Avatar point the way to a 3D future?
TV makers add an extra

If you love animals, please help free them from cruelty.

Donate Now! WSPA

FOCUS ZONE

Business Travel:
Everything the Business Traveller needs to know to make a better trip


Breach in the Google Cloud

TechCrunch

[About](#) [Advertise](#) [Archives](#) [Company Index](#) [Contact](#) [CrunchCam](#) [Jobs](#) [Research](#)

Google Privacy Blunder Shares Your Docs Without Permission

by [Jason Kincaid](#) on March 7, 2009

250 Comments  471 [retweet](#)

In a privacy error that underscores some of the biggest problems surrounding cloud-based services, Google has sent a notice to a number of users of its Document and Spreadsheets products stating that it may have inadvertently shared some of their documents with contacts who were never granted access to them.



According to the notice, this sharing was limited to people "with whom you, or a collaborator with sharing rights, had previously shared a document" – a vague statement that sounds like it could add up to quite a few people. The notice states that only text documents and presentations are affected, not spreadsheets, and provides links to each of the user's documents that may have been shared in error.

I've contacted Google for confirmation and haven't heard back, but this seems to be legit – our tipster says that he had previously shared the document listed in his notice, but now it has been reset to show 0 collaborators (one of the precautionary measures mentioned in the note).

Update: Google has confirmed that the note is real, and says that it was an isolated incident affecting less than .05% of all documents. The damage may not be widespread, but it's still an unsettling lapse in security.

Here's the letter in full:

Dear Google Docs user,

We wanted to let you know about a recent issue with your Google Docs account. We've identified and fixed a bug which may have caused you to share some of your documents without your knowledge. This inadvertent sharing was limited to people with whom you, or



Data Protection Fundamentals



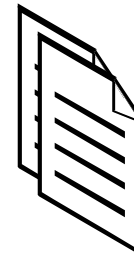
Laptop Encryption



Device Control



File Encryption



DLP



Email Encryption



Key Management

Cost of Data Breach



2009 Annual Study: Cost of a Data Breach

Understanding Financial Impact, Customer Turnover, and Preventive Solutions

Executive Summary:

This 2009 Ponemon Institute benchmark study, sponsored by PGP Corporation, examines the cost incurred by 45 organizations after experiencing a data breach. Results were not hypothetical responses; they represent cost estimates for activities resulting from actual data loss incidents. This is the fifth annual survey of this issue.

Breaches included in the survey ranged from approximately 5,000 records to more than 101,000 records from 15 different industry sectors.

Benchmark research conducted by
Ponemon Institute, LLC



January 2010



www.encryptionreports.com

Fourth annual report by The Ponemon Institute© & PGP Corporation (Feb 2010)

- Costs grew to \$204/record or \$6.7m per breach
- Lost business now accounts for 69% of breach losses
- 56% of breaches are “inside” jobs
- 42% of breaches caused by 3rd parties

Source: Ponemon, Feb 2010



Primary Cause of a Data Breach

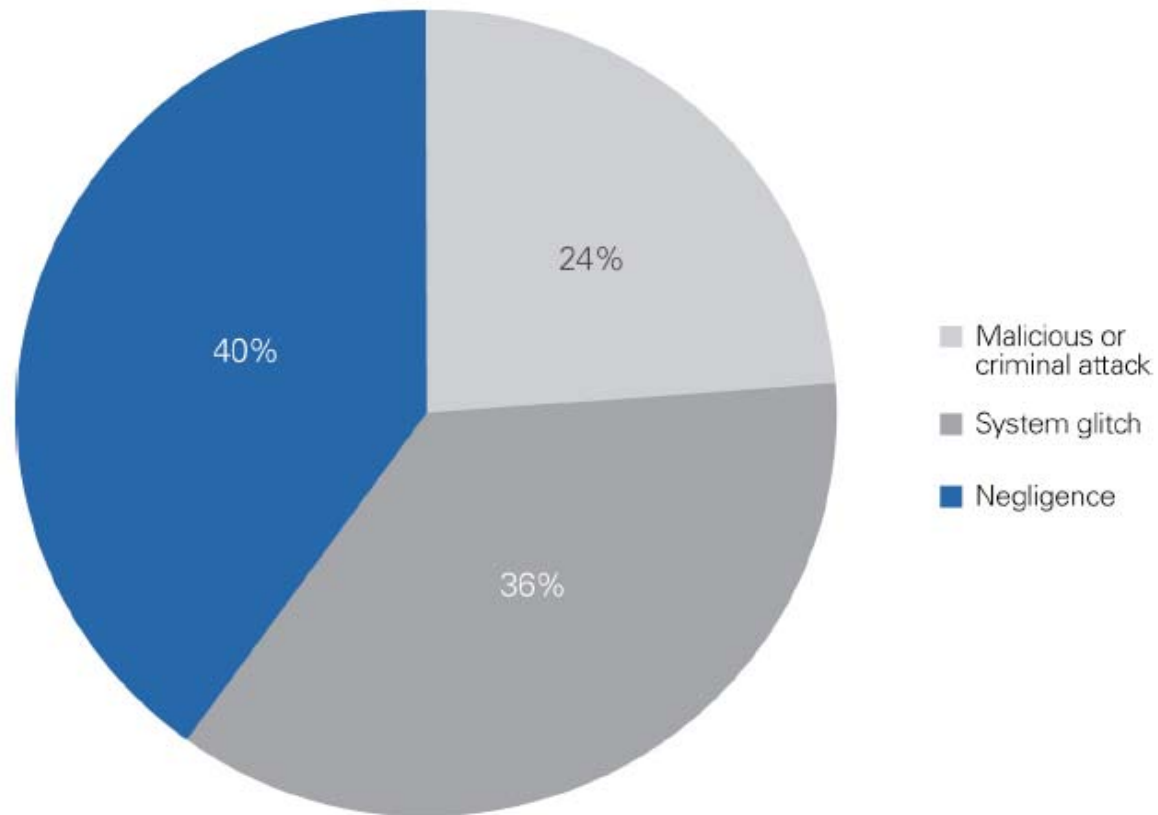


Figure 5: Malicious or criminal attacks

Where is Your Data?

Where is your data in the physical world?



USB Drives



Laptops



Smart Phones

Where is your data in the cloud?



Google Docs

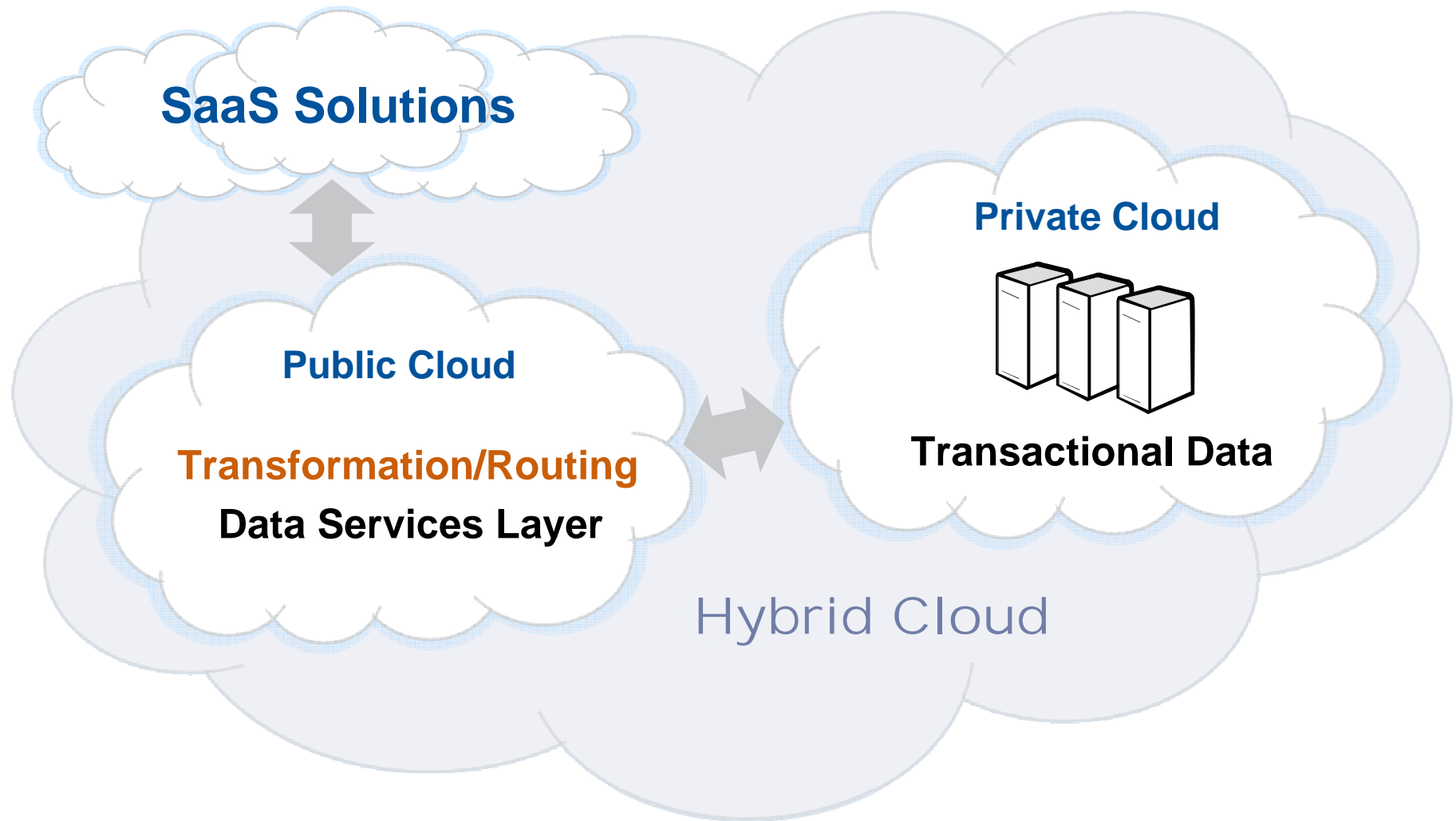


Backup

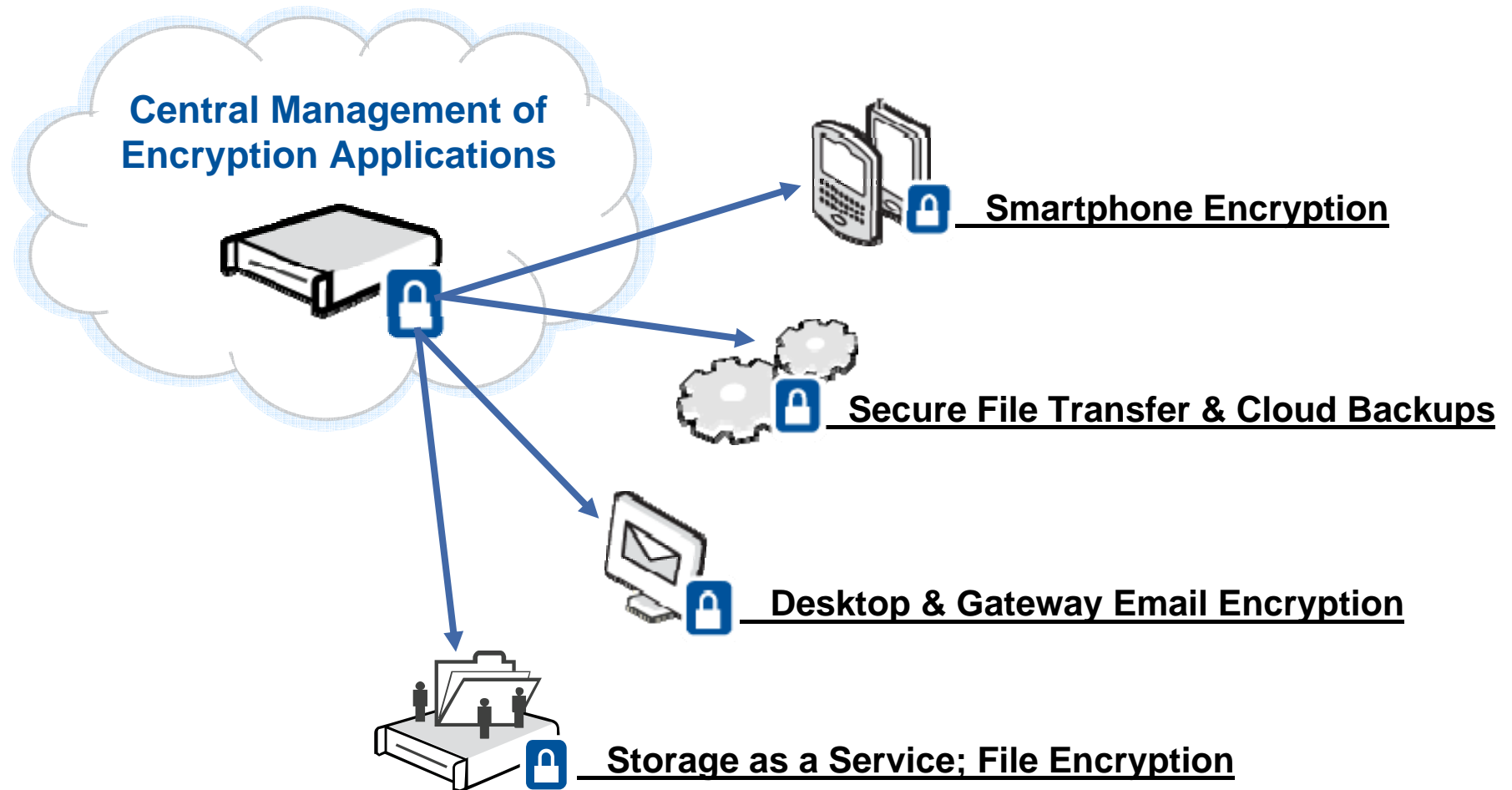


Cloud Provider Data Centers

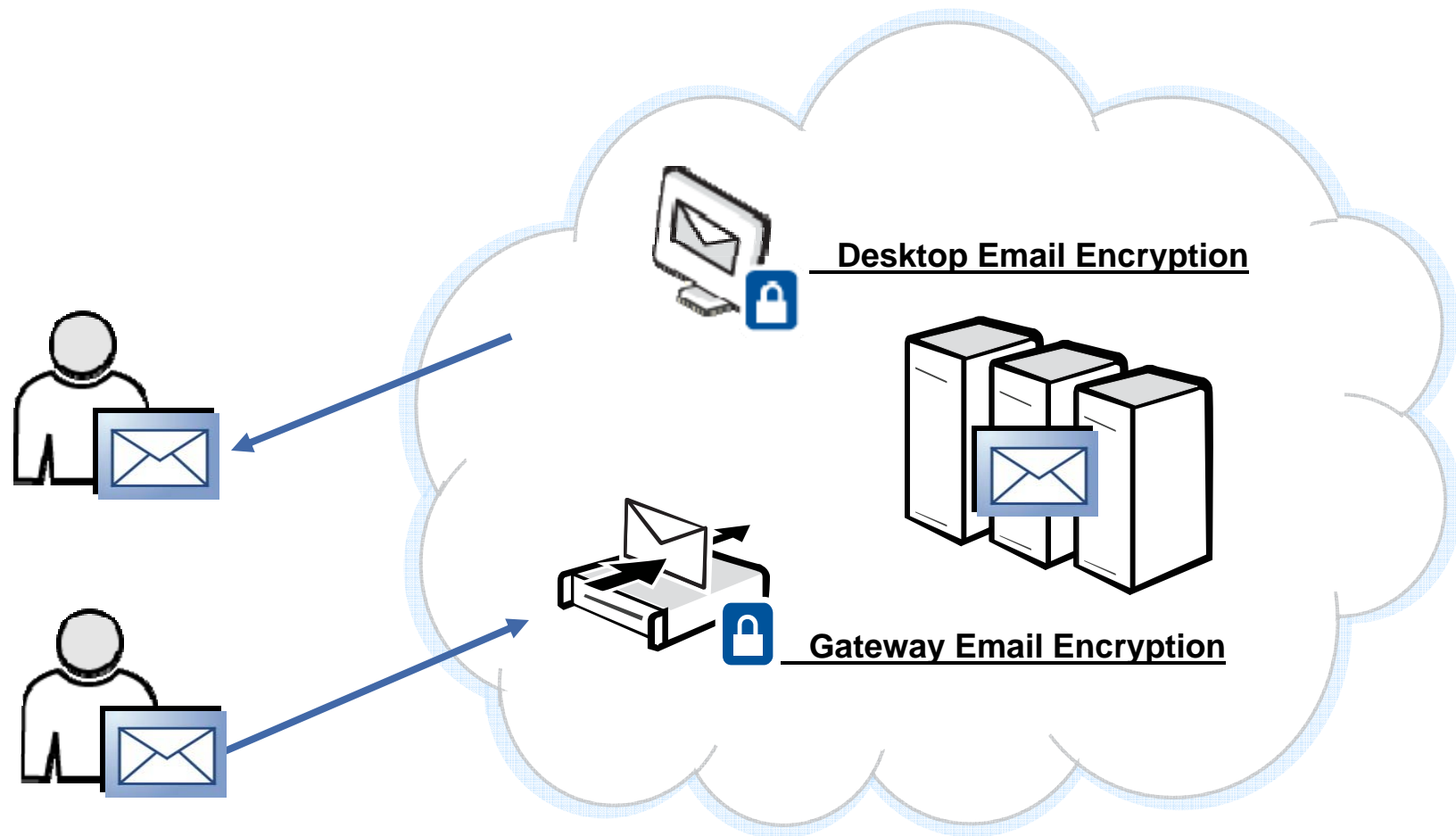
The Hybrid Cloud



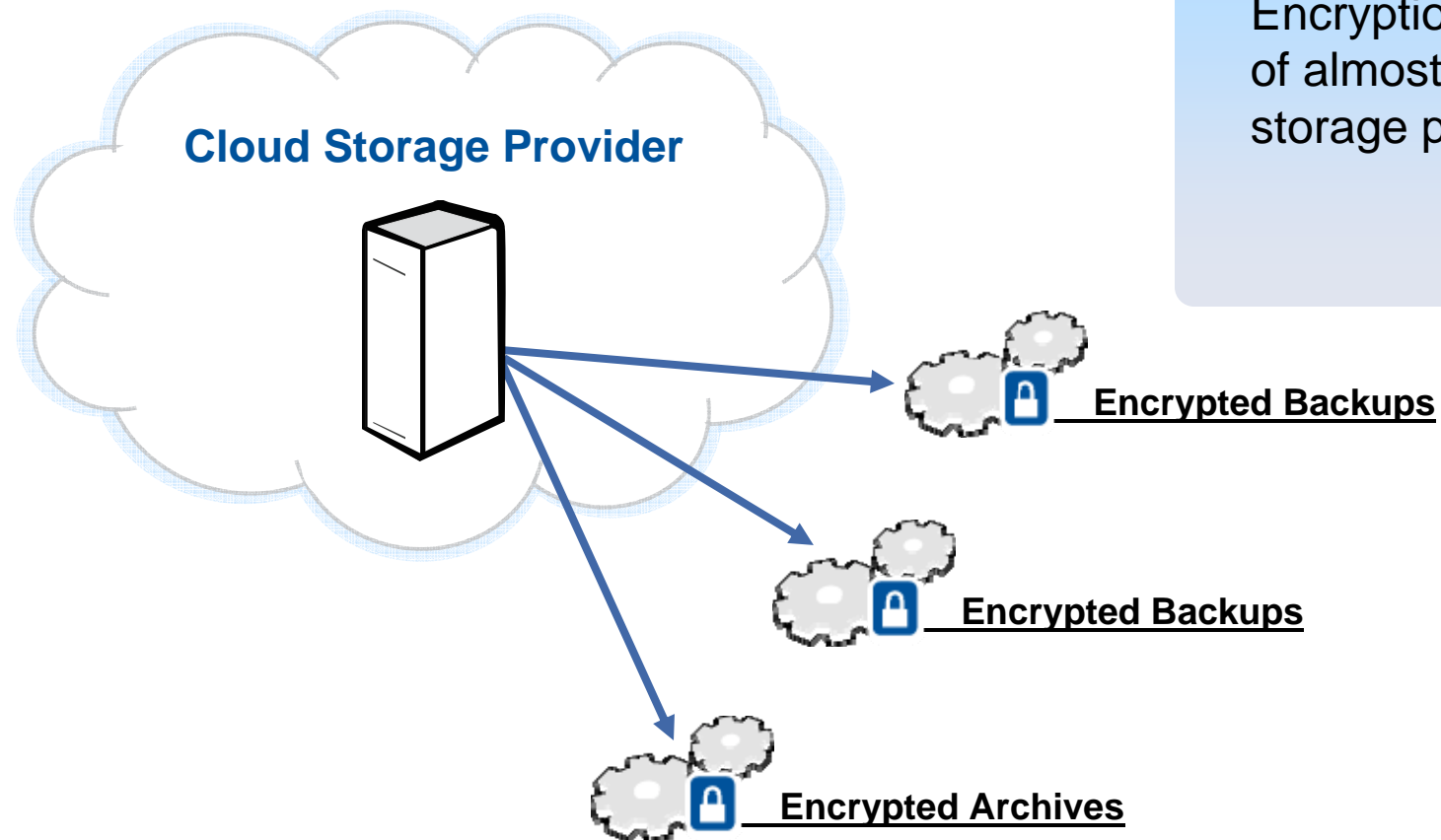
Use Case #1: Deploying Encryption Management to a Private Cloud



Use Case #2: Email Security as a Service

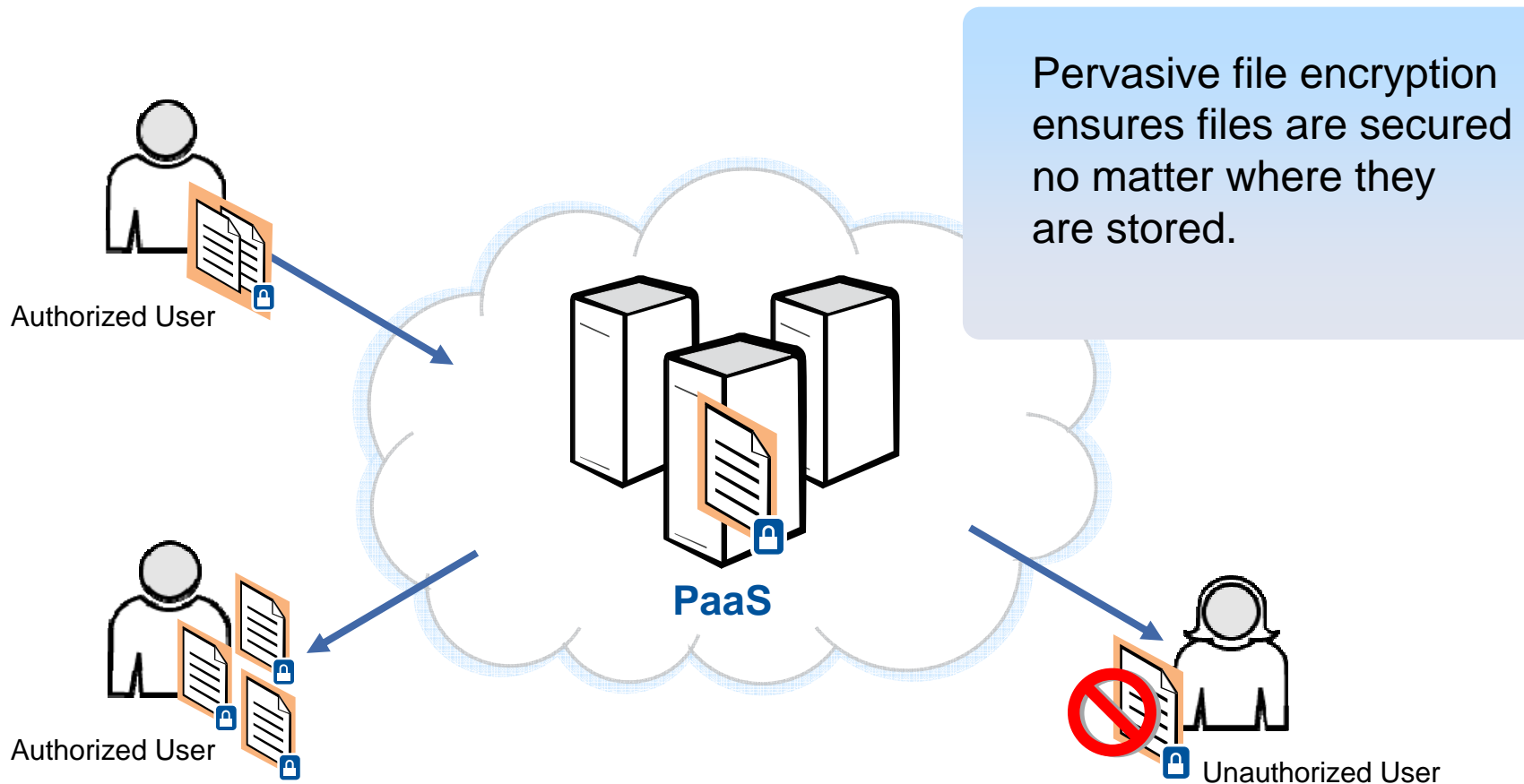


Use Case #3: Securing Backups to Cloud Storage



Encryption allows use of almost any cloud storage provider.

Use Case #4: Secure Collaboration/File Sharing



Keys and the Cloud

- Lost password, token
- Employee termination
- Employee malfeasance
- Lawsuit – eDiscovery
- Government request

Encryption, Key Recovery and the Cloud

- **Client Encryption**
 - Secure client or encrypt on client
 - Key recovery left to client, and potentially corporate key escrow
- **Server Encryption**
 - Secure server or encrypt on server
 - Key recovery managed by company, and potentially corporate key escrow
- **Cloud Encryption**
 - Data sent to cloud and encrypted by cloud provider
 - Company loses control over surrender or keys
 - Unclear what recovery options are

Security Considerations for the Cloud

