Too Many Encryption Keys

Los Angeles ISSA
July 15, 2009

Brian Tokuyoshi
Product Marketing Manager
PGP Corporation

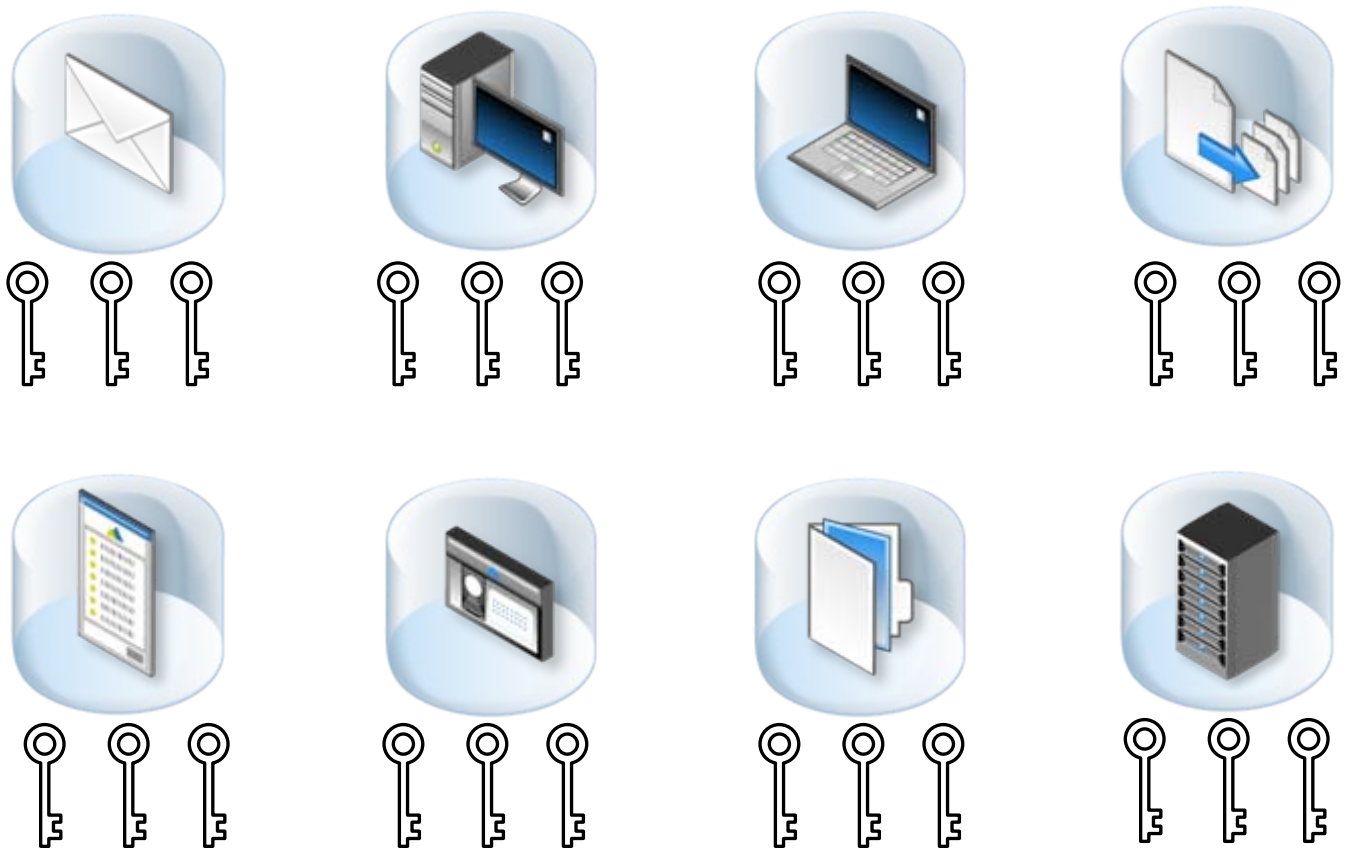
btokuyoshi@pgp.com

Agenda

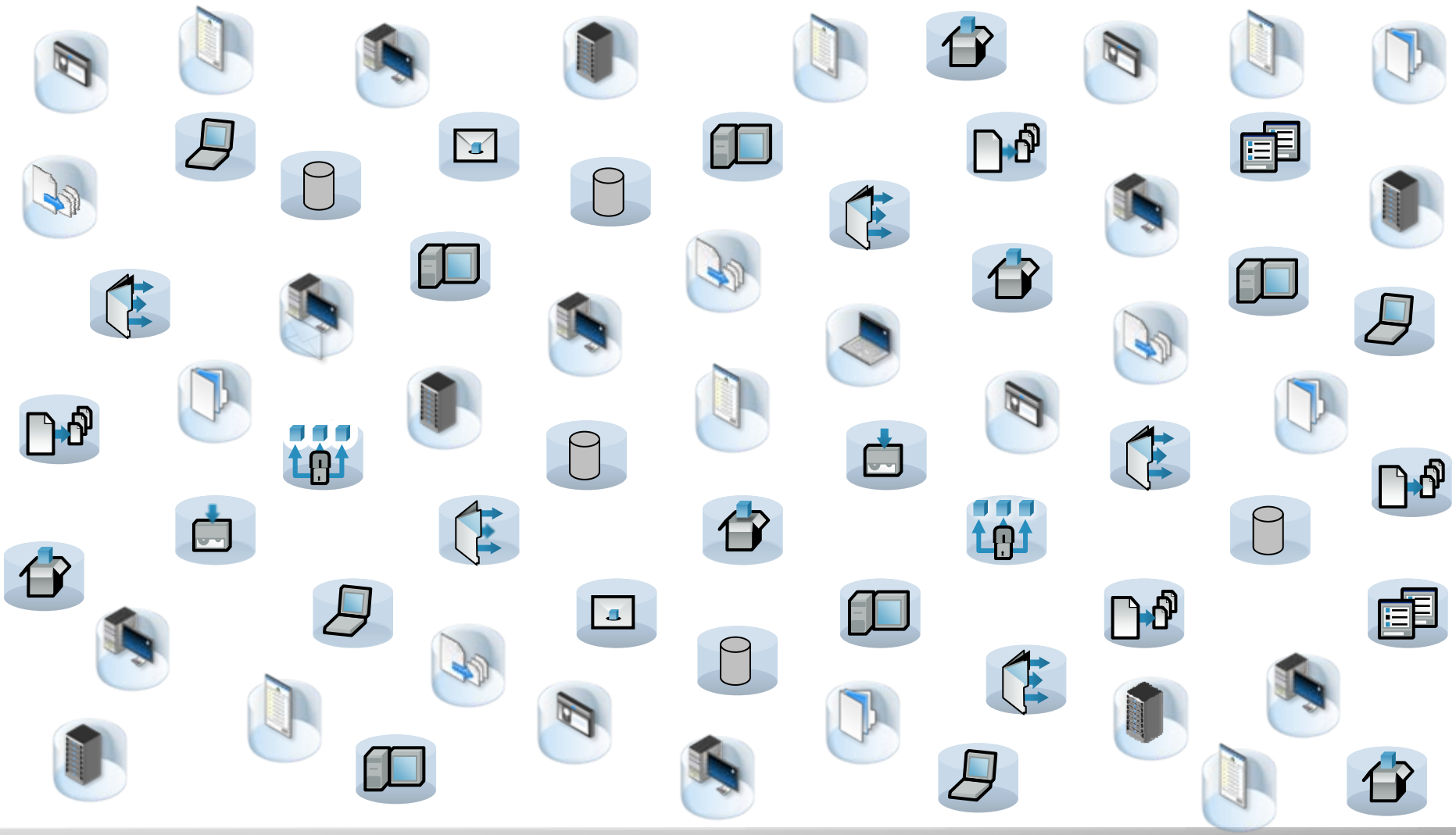
- Overview
- Market Drivers
- Analysts
- Questions to Ask your Vendor
- Quick Hits
- Conclusions

Overview

Enterprises Are Here today

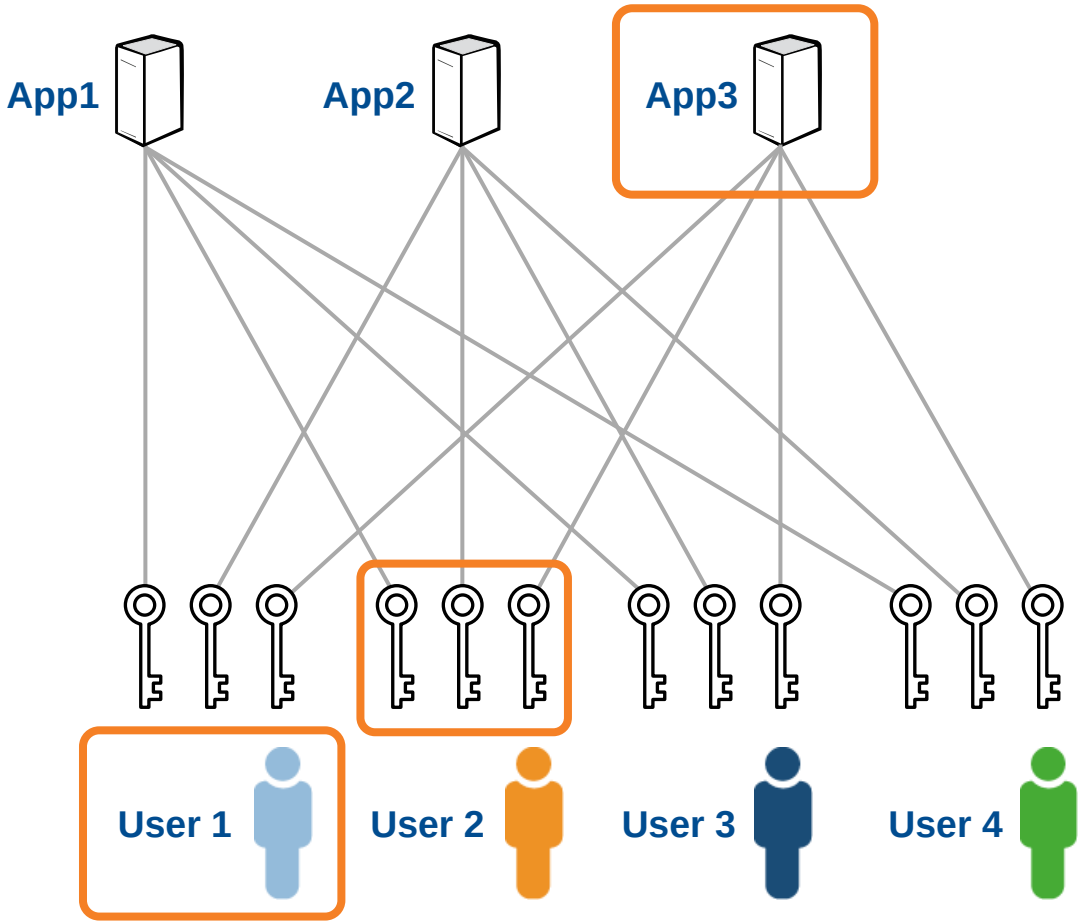


Enterprises Say They Are Going To This

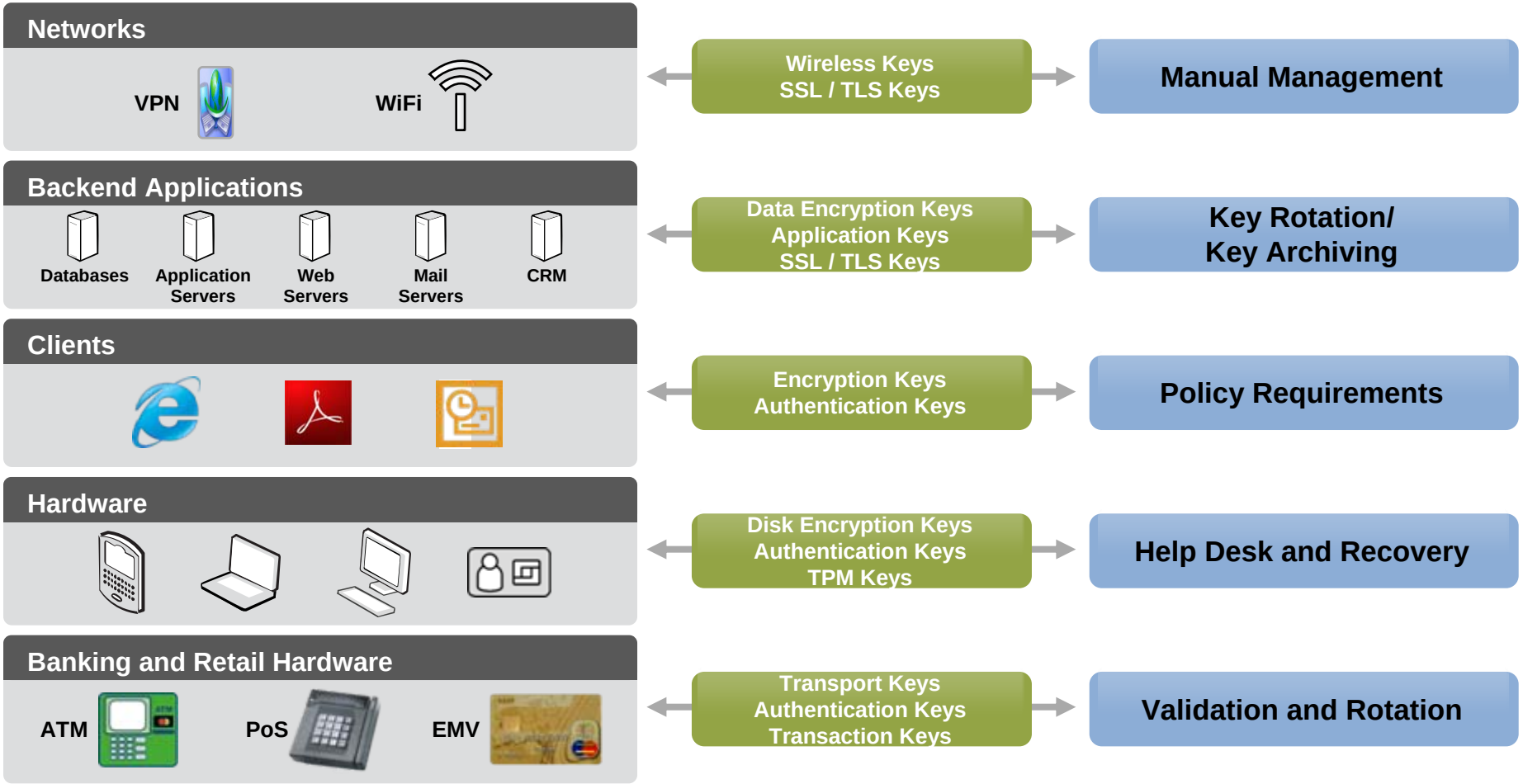


Managing Encryption Is Tough

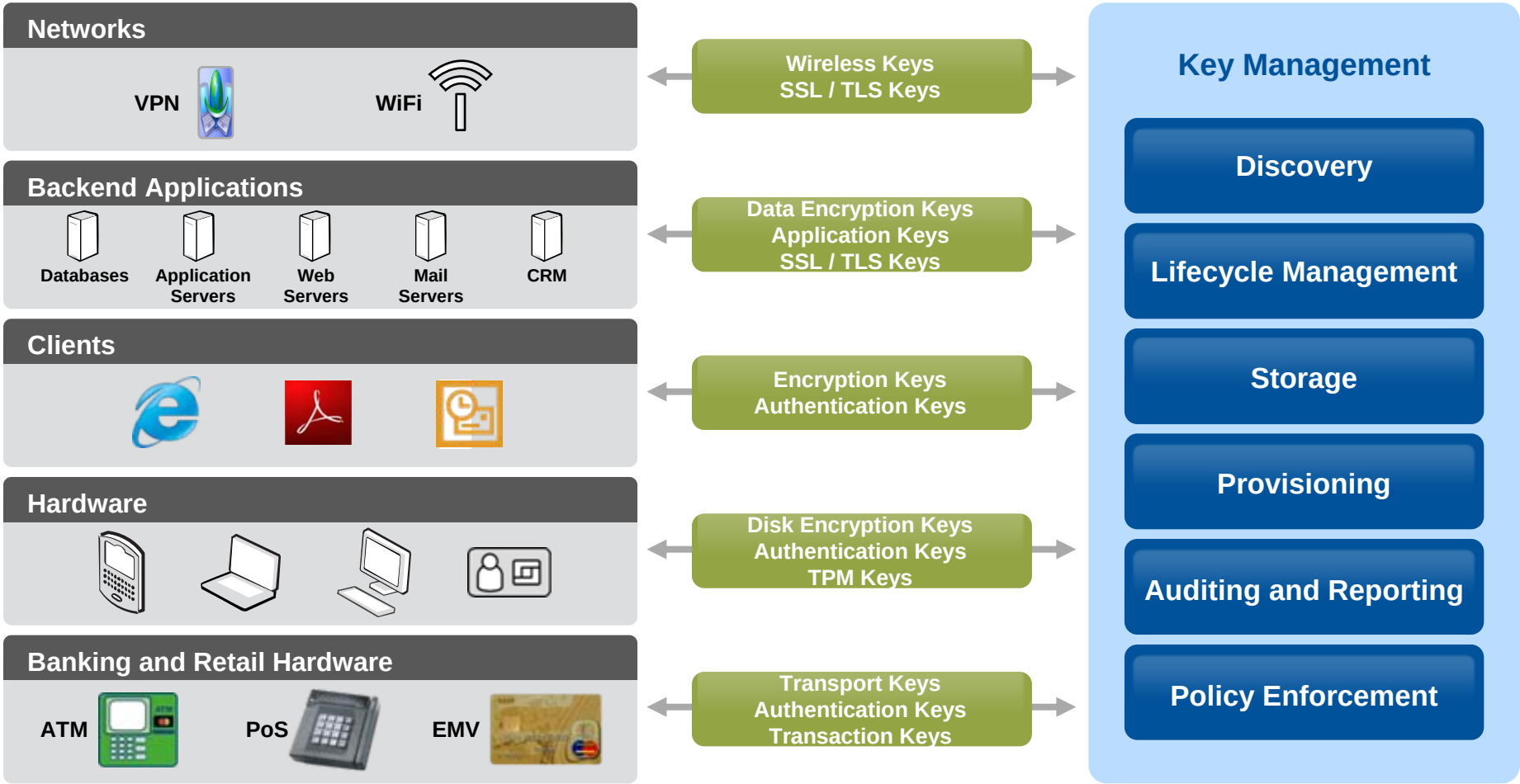
Key Management Today



Common Problems with Keys



Addressing the Problem



Market Drivers


Compliance!


Data Breaches!

Compliance and protection from data breaches are not the drivers for Enterprise Key Management

Deploying encryption without good key management is causing the problem.

The Aftermath of Compliance & Data Breaches

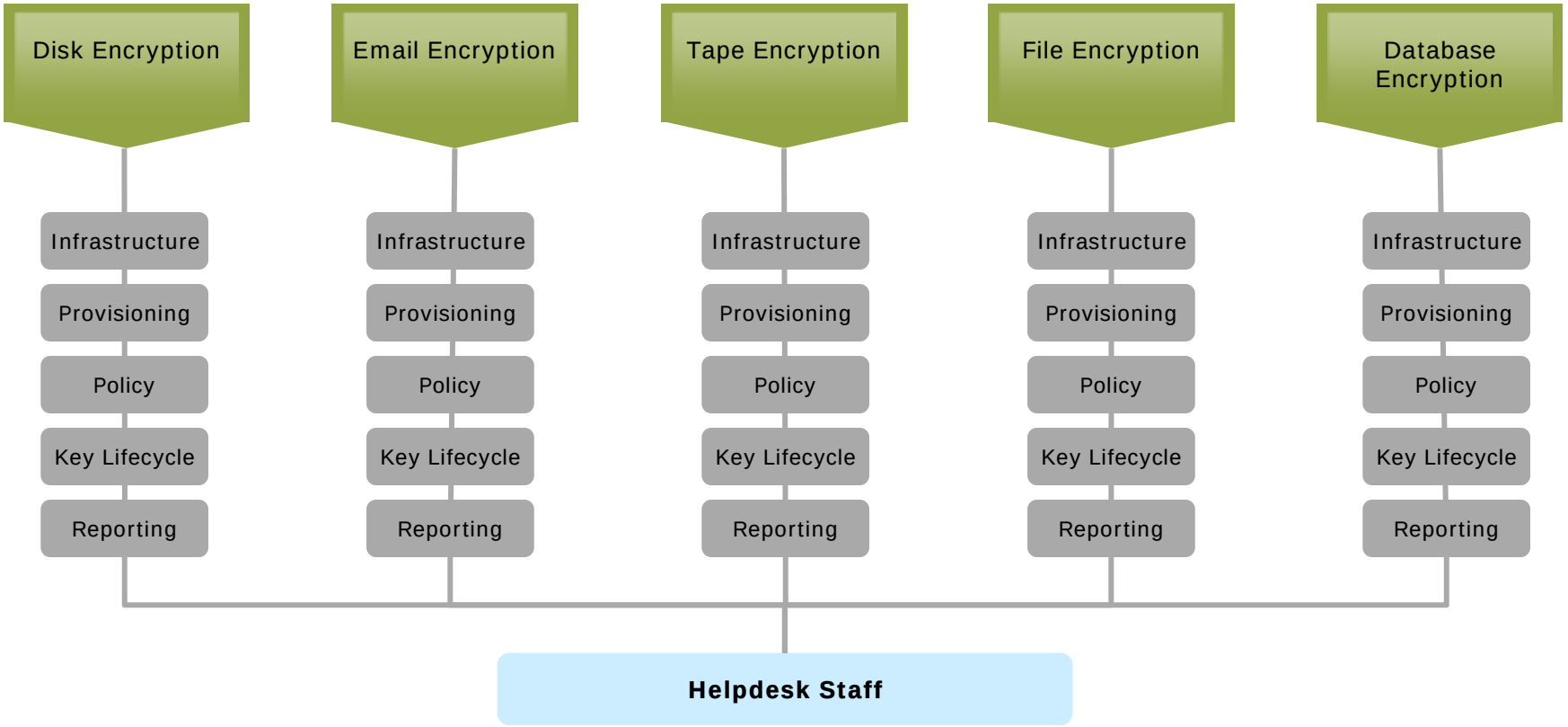
- Tight deadlines place emphasis on the goal, without considering the ramifications about the path taken
- Compliance only talks about getting the data encrypted, not how fast it should be decrypted. That's e-discovery.
- The coming hangover
  - Key Management is often done poorly
  - No overall strategy
  - GAO report on Federal efforts for DAR
  - Enterprise is next
- Deploying encryption without a plan to manage keys is the driver for enterprise key management

Best Practices

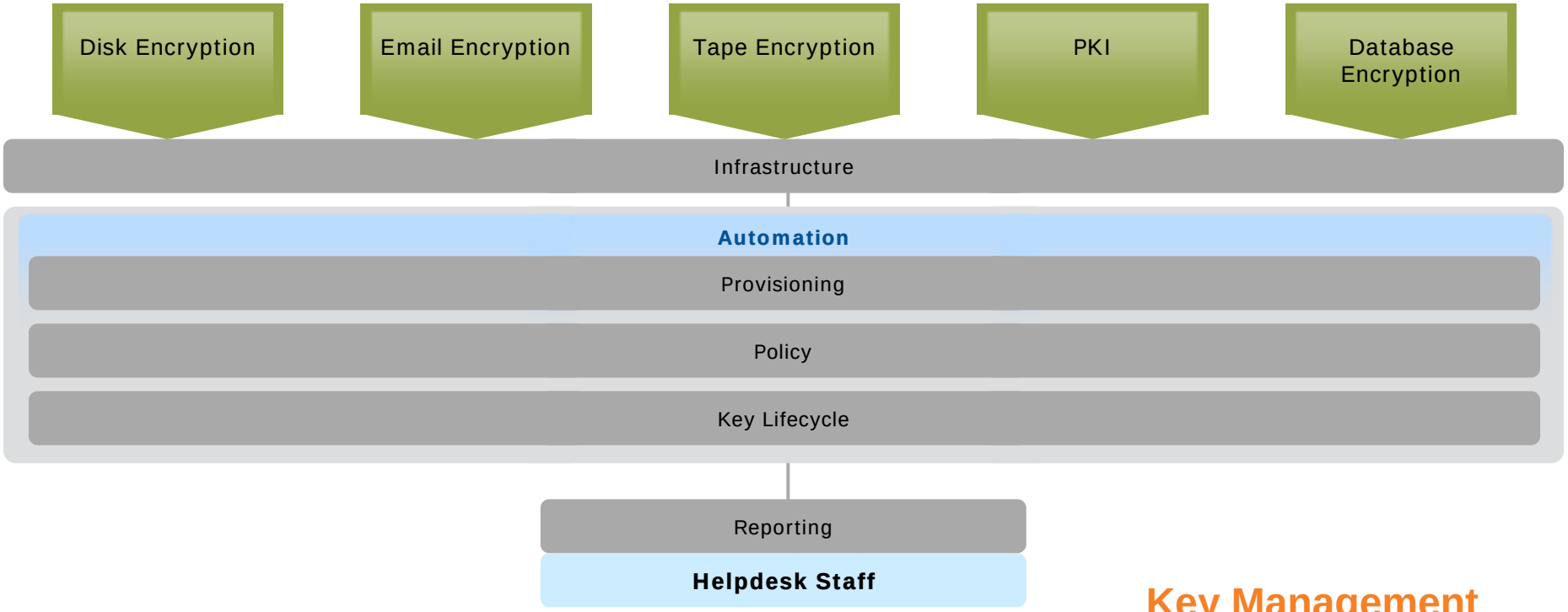
1. Survey and catalog existing data
2. Plan your long term encryption requirements
3. Develop an enterprise policy on keys
4. Deploy a framework to manage encryption
5. Deploy data protection solution
6. Tackle the next project

Key Management Silos

Point Product Proliferation

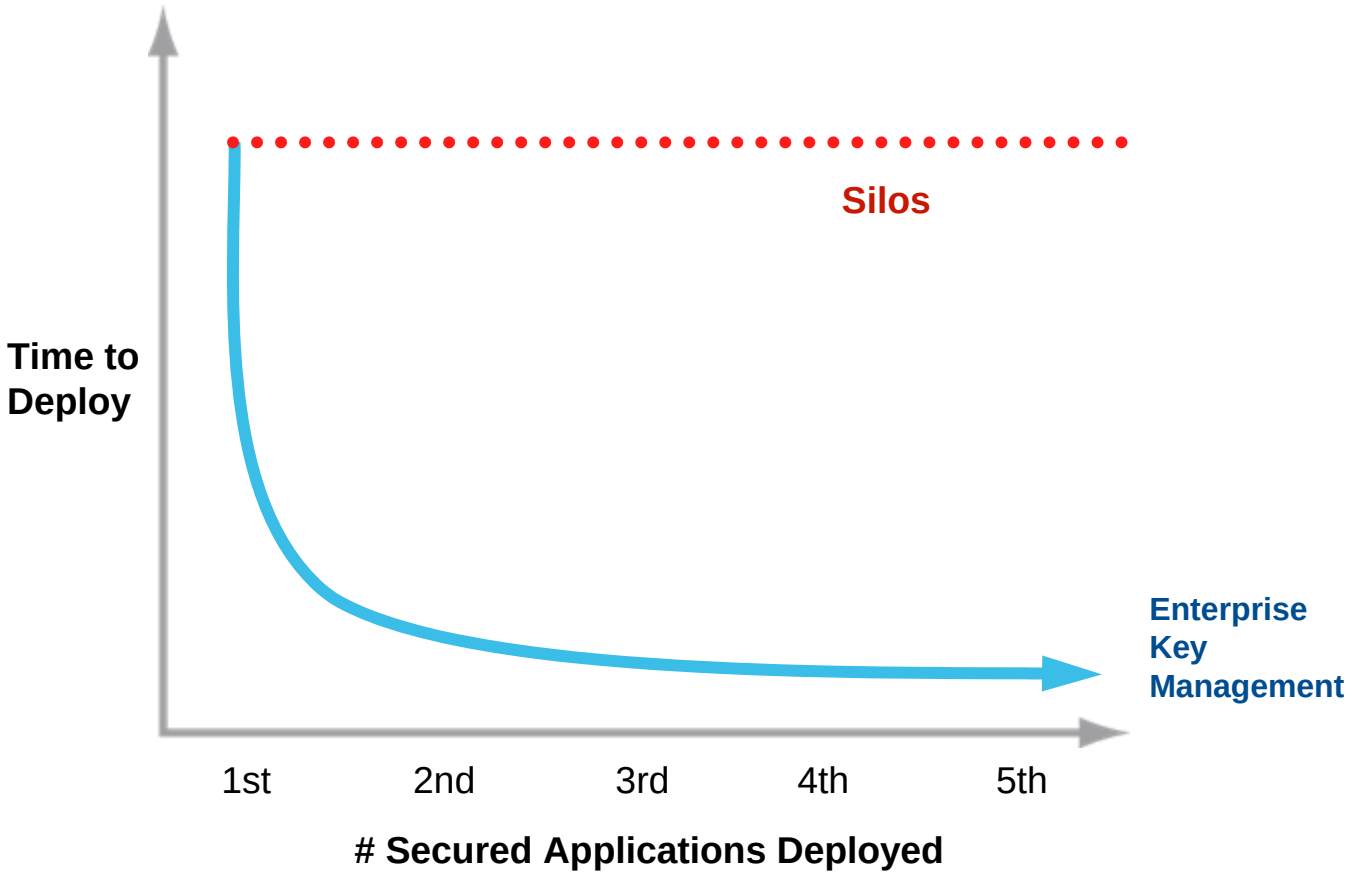


A Common Infrastructure



Key Management

Effort Comparison

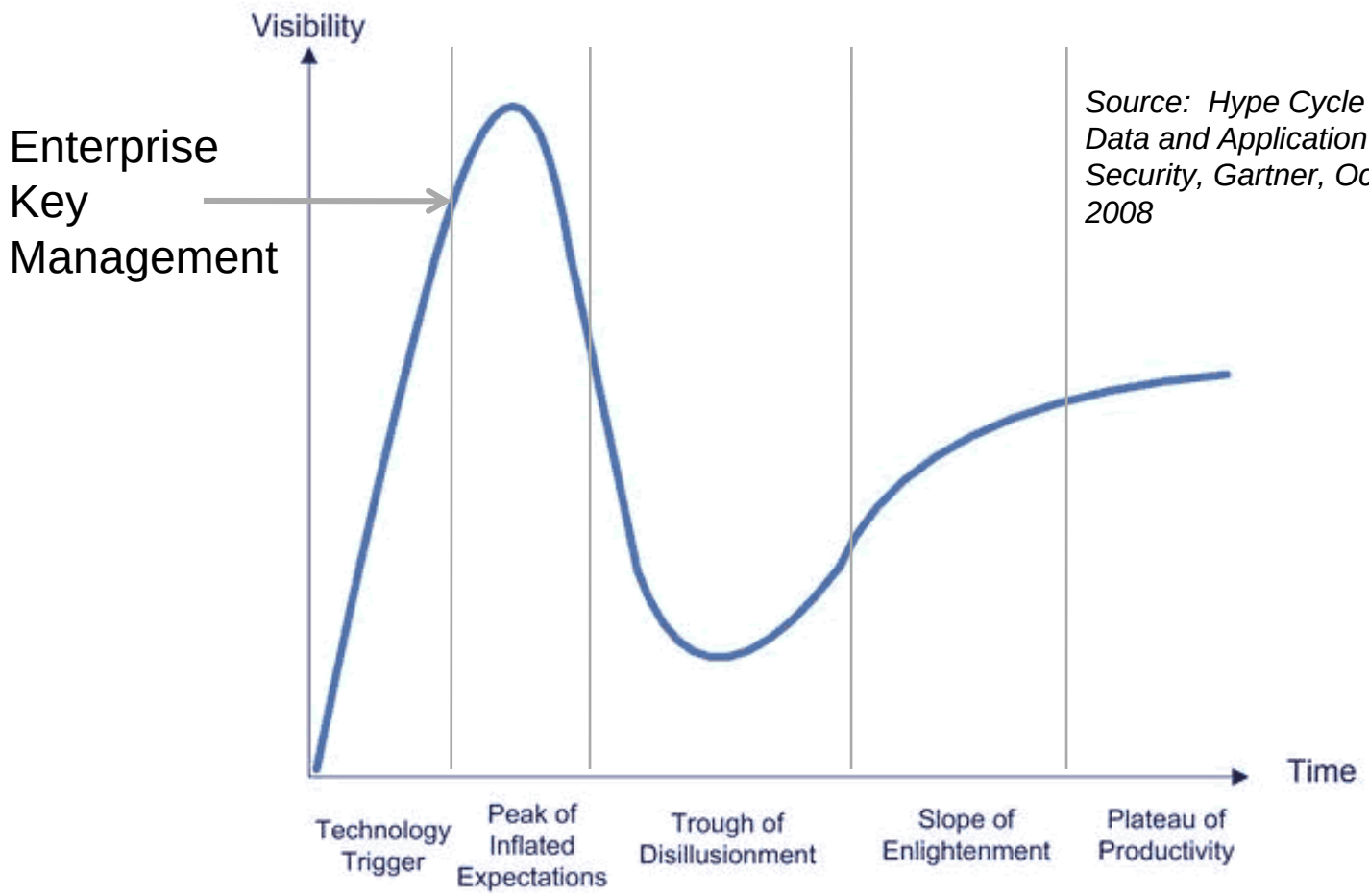


Market Drivers

- Makes encryption manageable
- Replaces custom tools
- Protects business continuity by eliminating mistakes from inadvertent key expiration
- Reduces administrative cost
- Provides the foundation for new initiatives

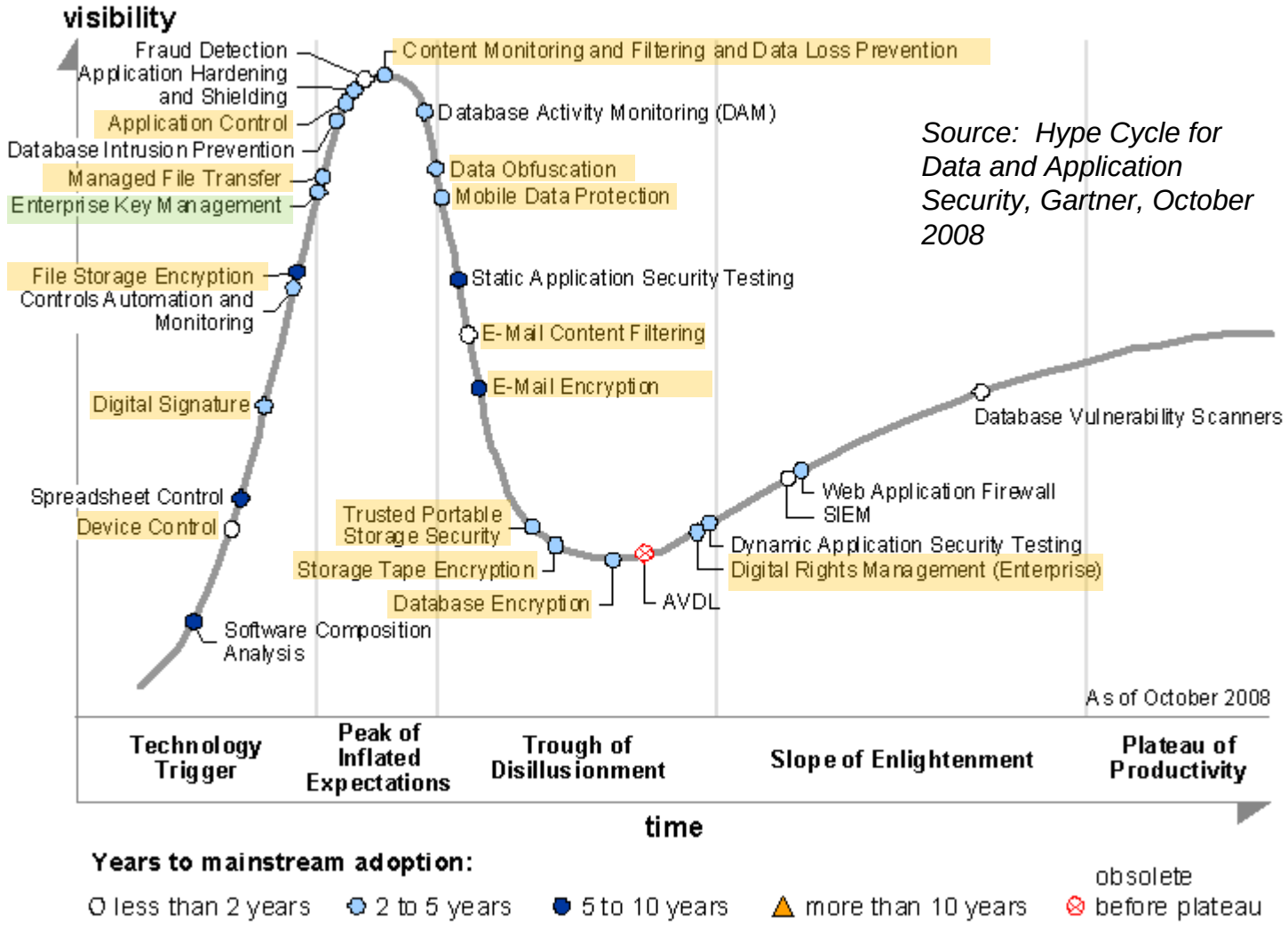
Analysts

Gartner Hype Cycle



Source: Hype Cycle for Data and Application Security, Gartner, October 2008

Gartner Hype Cycle

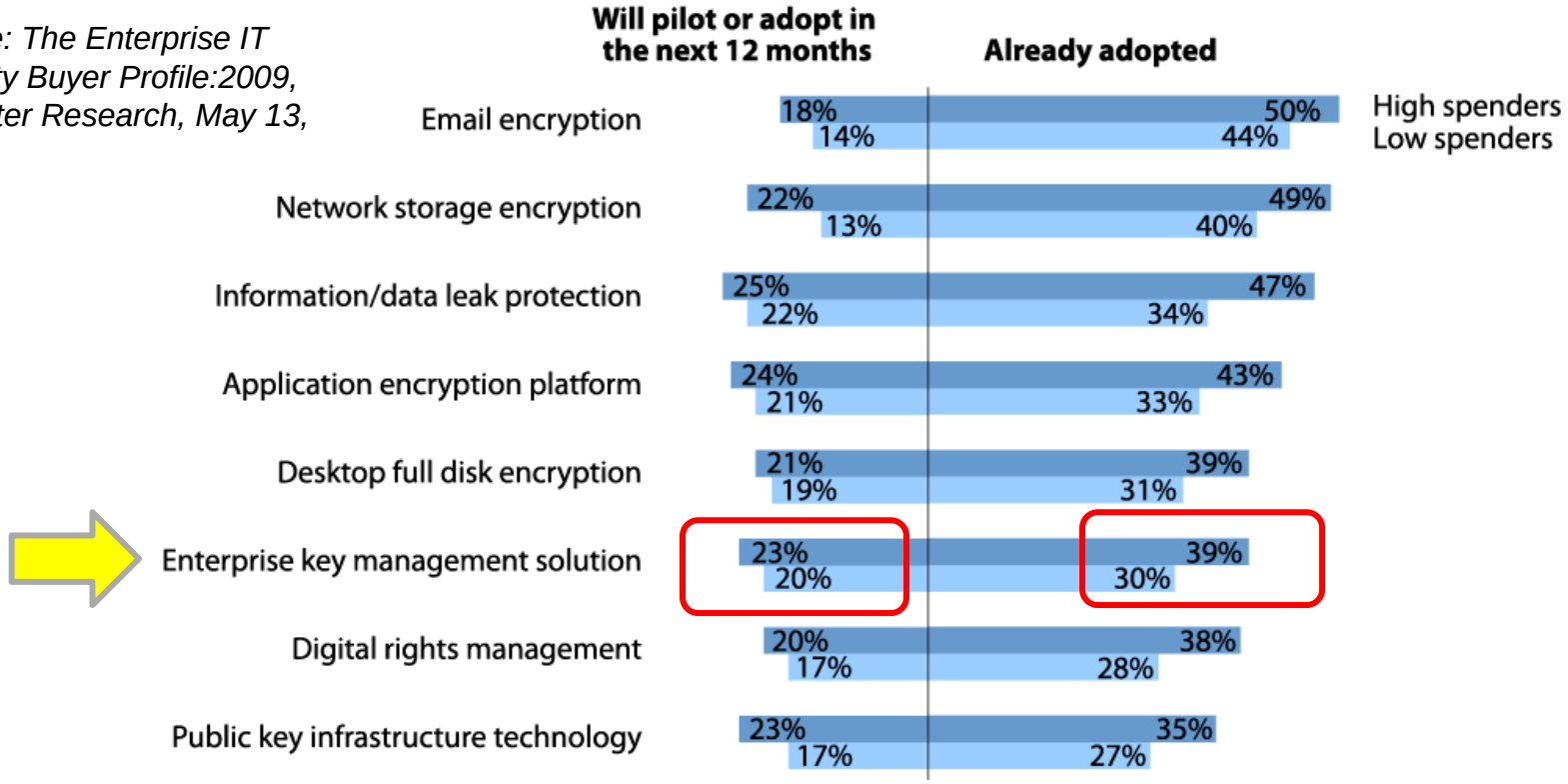


Source: Hype Cycle for Data and Application Security, Gartner, October 2008

Forrester Research

Source: The Enterprise IT Security Buyer Profile:2009, Forrester Research, May 13, 2009

"What is your organization's interest in adopting each of the following data security technologies?"



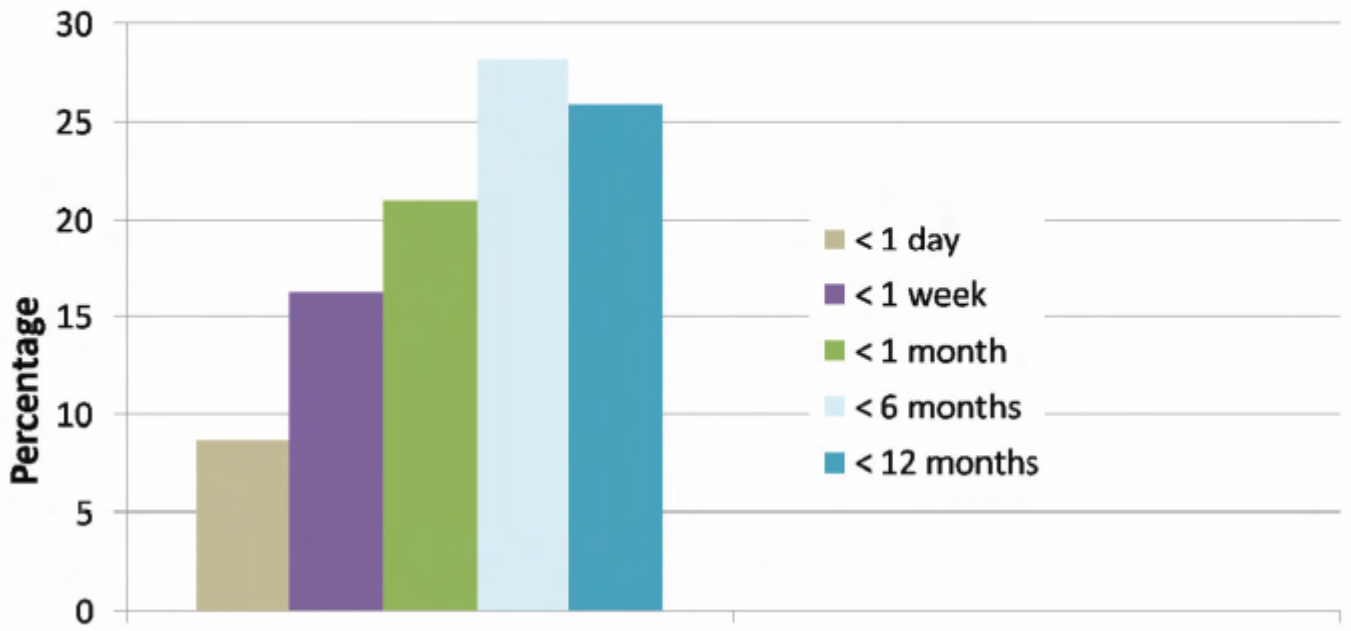
Base: 260 North American and European enterprise IT security decision-makers

Source: Enterprise And SMB Security Survey, North America And Europe, Q3 2008

High spenders defined as spending > %12.6 of budget on security

Trust Catalyst

Figure 4: How much time has your organization spent preparing for key management issues?



Source: 2008 Encryption and Key Management Industry Benchmark Report, Trust Catalyst, October 2008

Questions to Ask your Key Management Vendor

Is it key management or ENTERPRISE key management?

Enterprise Key Management

- There are many products that offer key management
  - Few are enterprise key management
  - Some are silos in disguise (key management appliances)
  - Doesn’t mean they are not valuable. But it’s not enterprise key management.

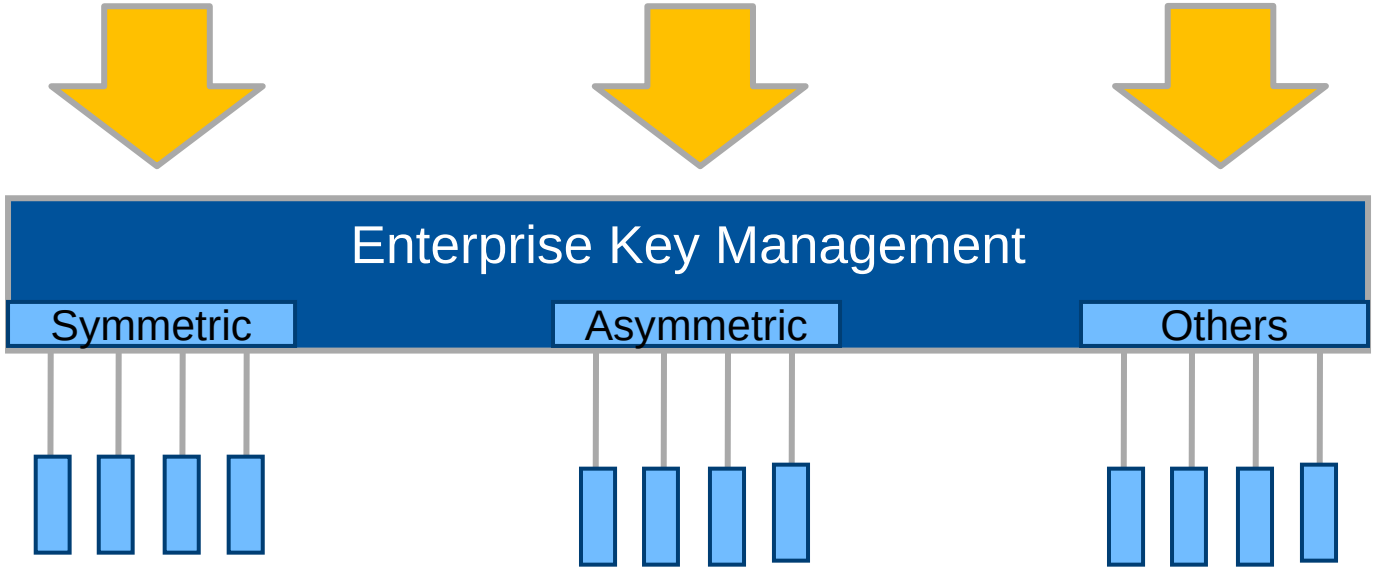
Are you talking about symmetric or asymmetric keys?

Symmetric / Asymmetric

Some vendors say this is key management

PKI vendors say this is key management

What about these?

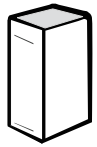


How do you handle keys in context?

Key Organization without Key Management

User

Application Server



Web Server

File Encryption
(X.509)

File Encryption
(X.509)

File Encryption
(X.509)

Disk Encryption
(Symmetric Key)

Authentication
(X.509)

SSH Key
(RSA Key)

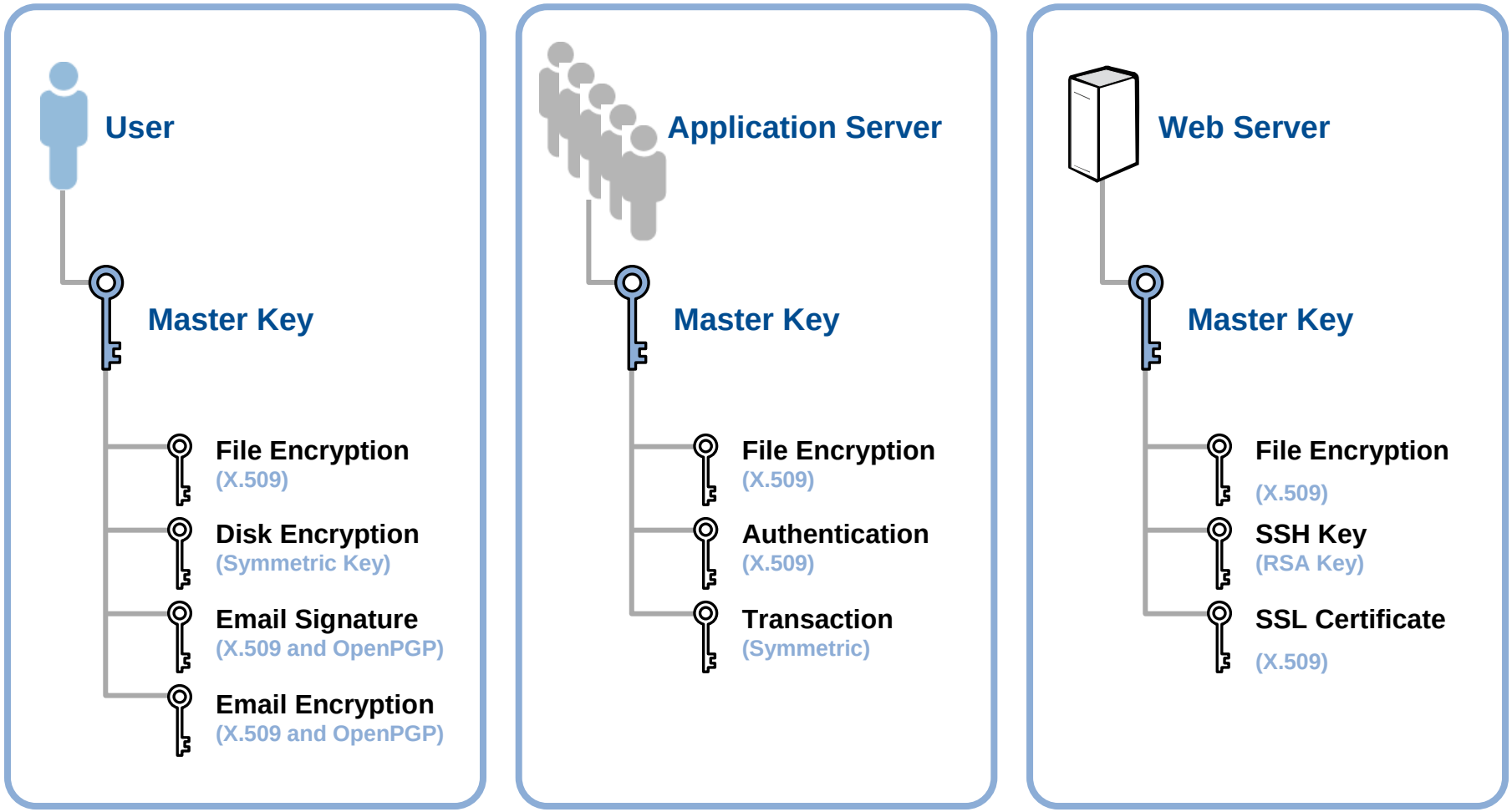
Email Signature
(X.509 and OpenPGP)

Email Encryption
(X.509 and OpenPGP)

B2B Transaction
(Symmetric)

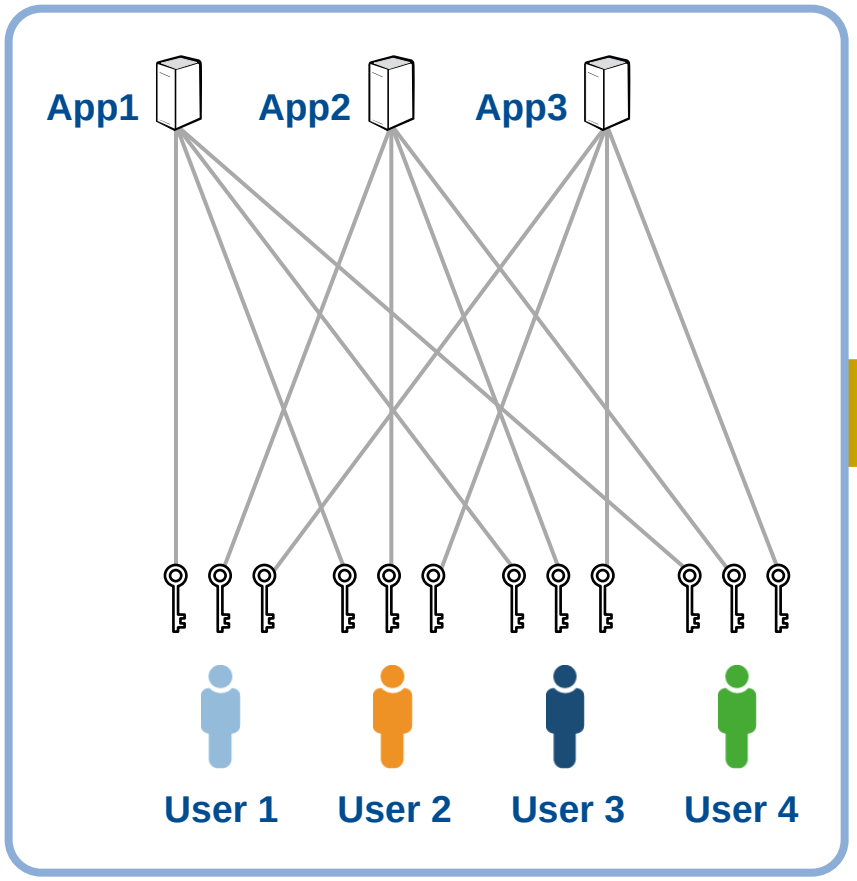
SSL Certificate
(X.509)

Group Related Keys Together

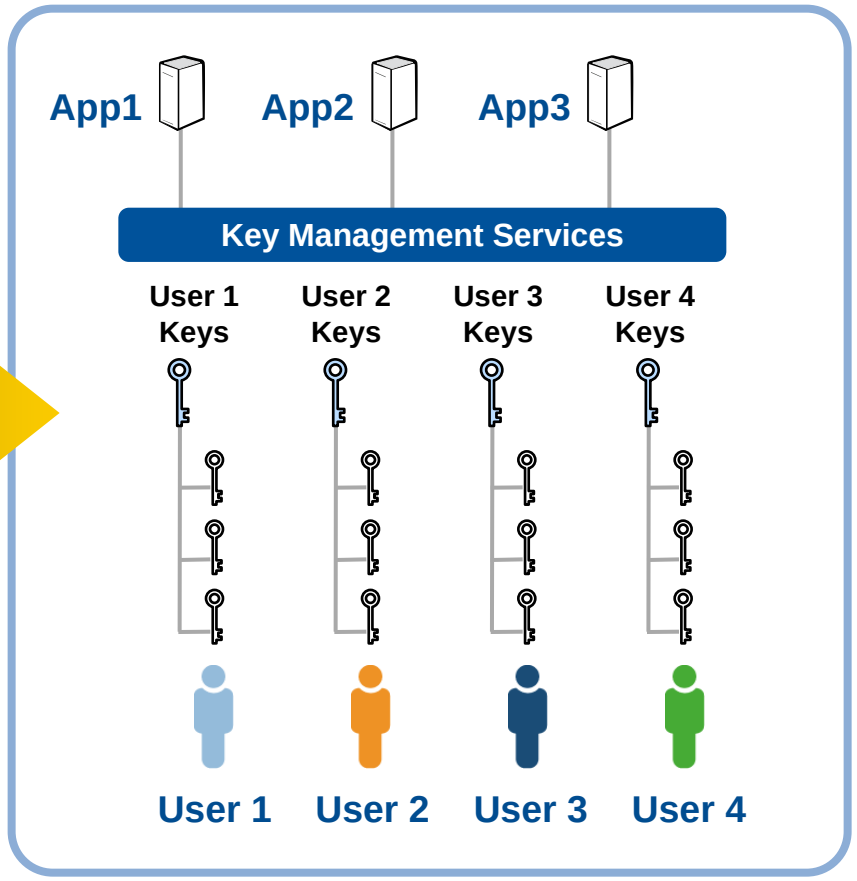


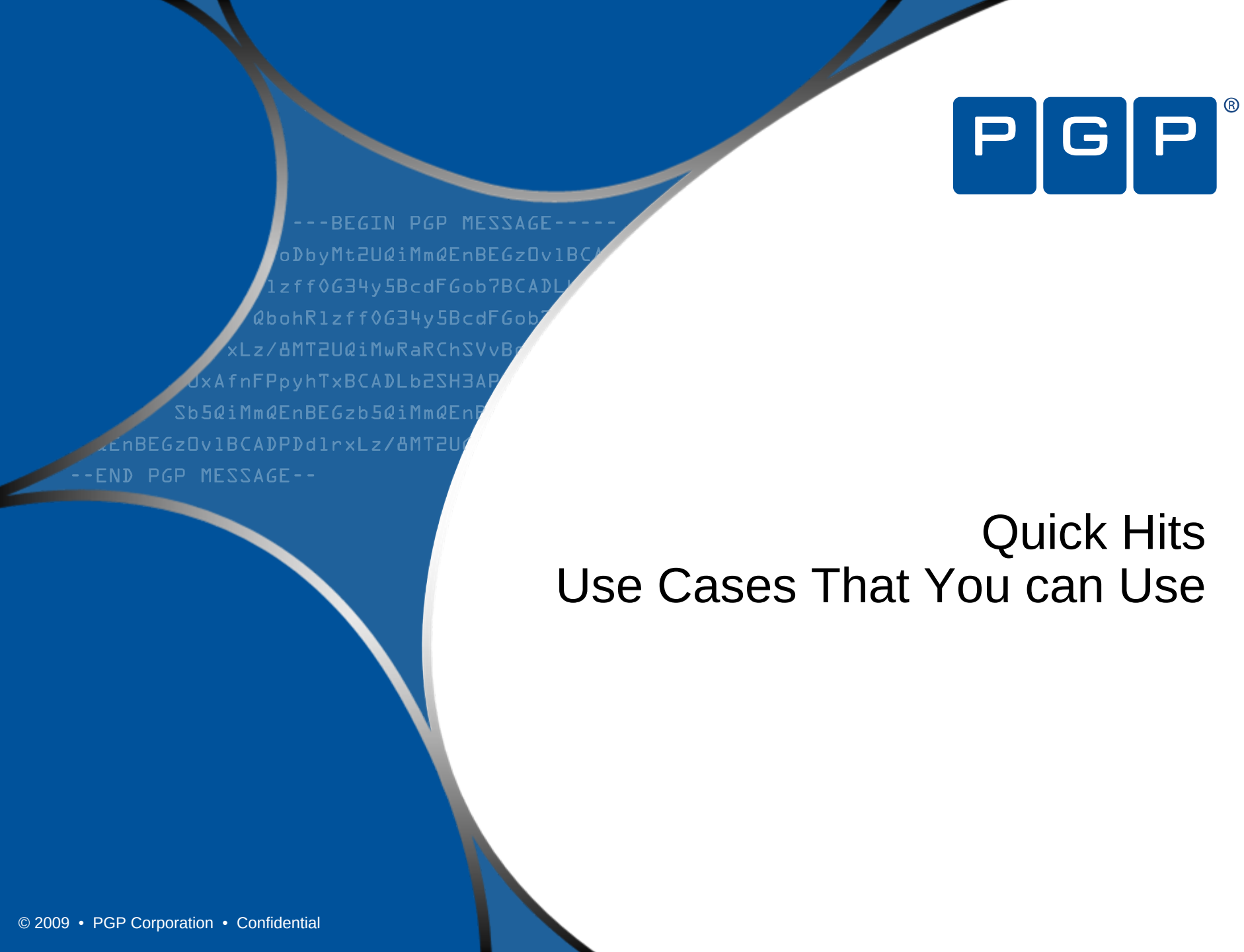
Before and After

Without Key Management



With Key Management

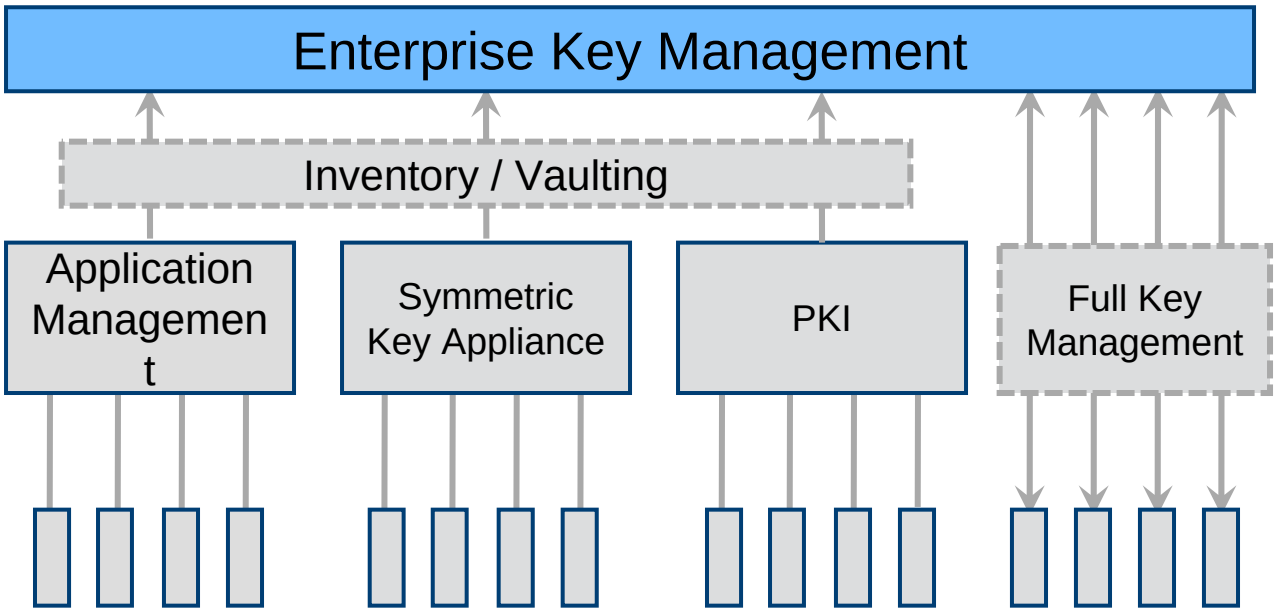




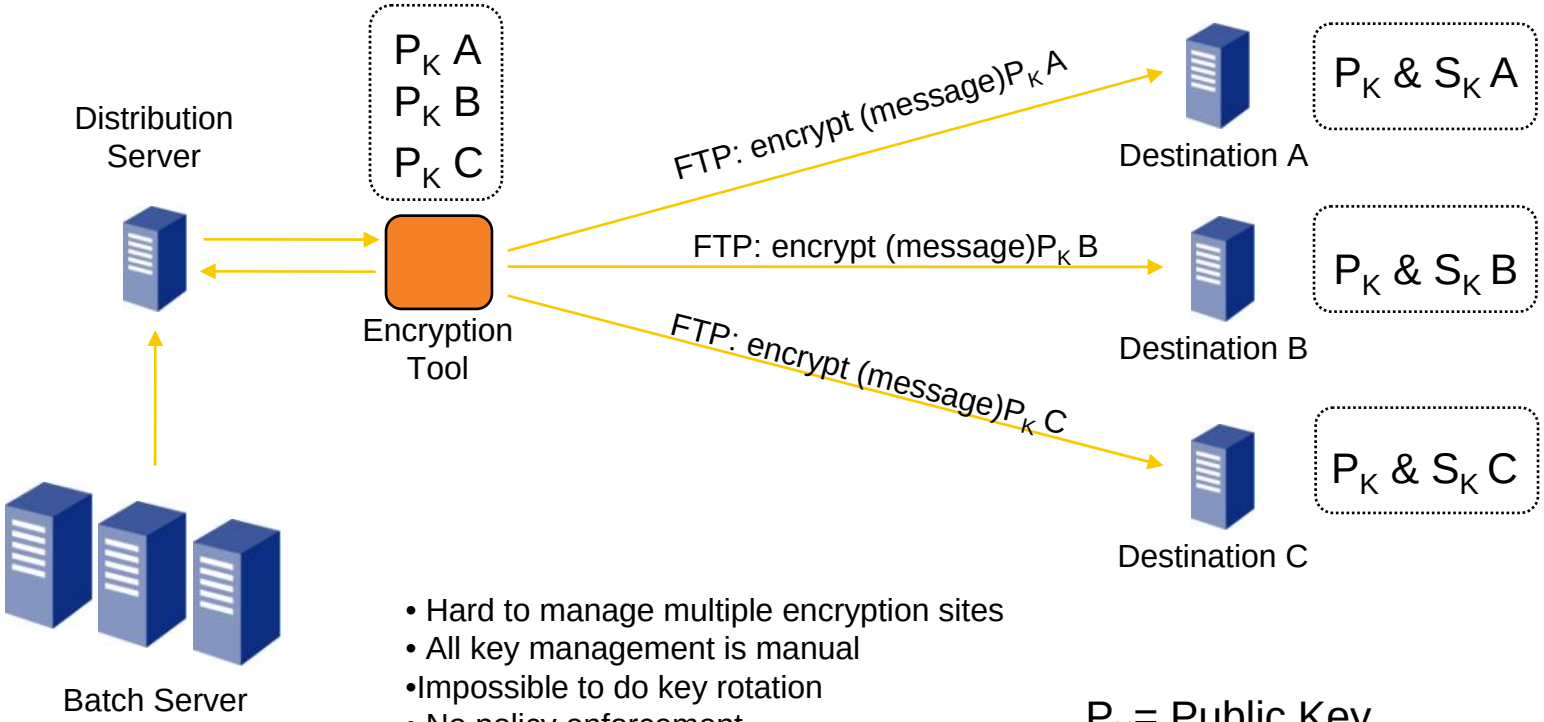
Quick Hits
Use Cases That You can Use

Key Inventory

Inventory Alone is Valuable



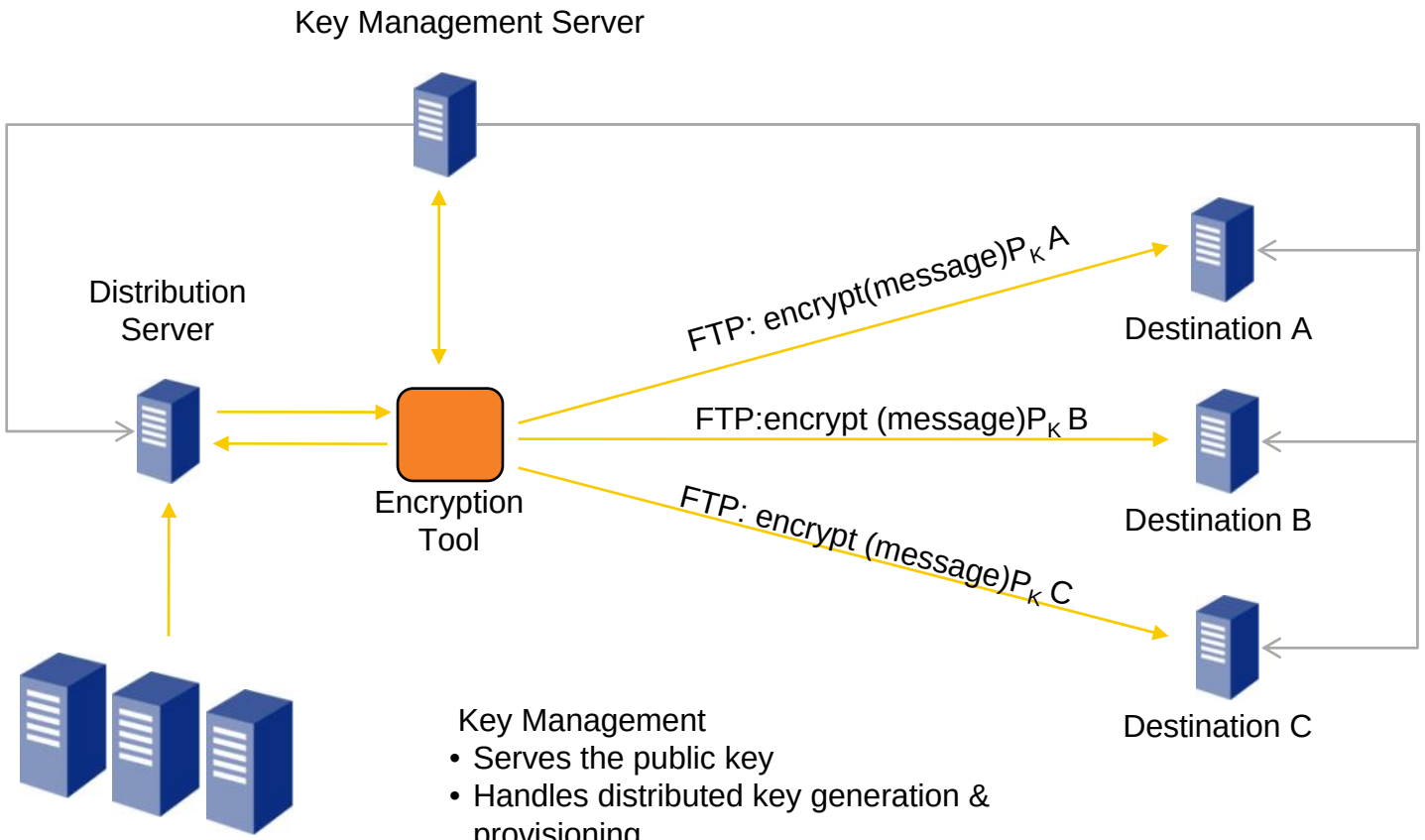
File Distribution



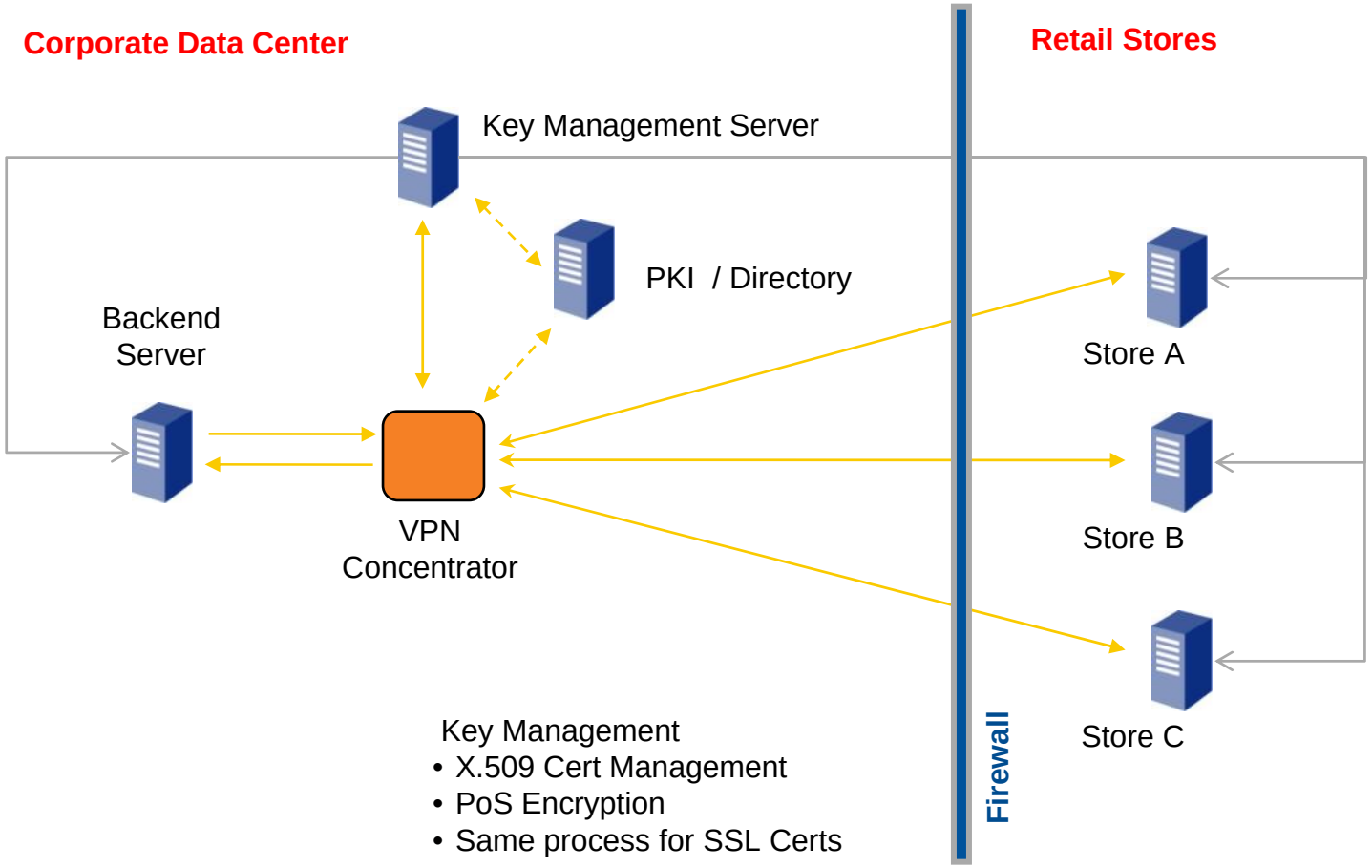
- Hard to manage multiple encryption sites
- All key management is manual
- Impossible to do key rotation
- No policy enforcement

P_K= Public Key
S_K= Private Key

Secure File Distribution (Encryption)



VPN / SSL Certificate Management (Authentication)



Conclusions

1. Add Enterprise Key Management to the environment that you have
   - Inventory / Vaulting alone solves a critical issue with key recovery
   - Positions you to get ready for future challenges

2. Build flexible key management infrastructure and build on top of it
   - Got to start somewhere
   - Starting with a good foundation helps to address future challenges

Points to Consider
From 10+ Years of Managing Keys & Applications

- Symmetric & Asymmetric are both part of a key management strategy
  - Key lifecycle management needed for both
  - No single key type
  - No single format
  - No single protocol
- Applications are not good key managers
  - Overlay needed – not just a database
- Keys in Context
- Basic Key Management Services
  - Discovery
  - Lifecycle Management
  - Provisioning
  - Storage
  - Auditing & Reporting
  - Policy
- Must adapt to wide range of use cases, with implementation flexibility
  - Corporate recovery
  - Access Control
  - Extensible integration
  - No single Key Management Protocol

Thank You