Practical Advice for Cloud Data Protection

Ulf Mattsson
CTO, Protegrity

Ulf.Mattsson@protegrity.com

protegrity

protecting your data.
protecting your business.

Ulf Mattsson, Protegrity CTO

- Cloud Security Alliance (CSA)
- PCI Security Standards Council
  - Cloud & Virtualization SIGs
  - Encryption Task Force
  - Tokenization Task Force
- ANSI X9
  - American National Standard for Financial Services
- IFIP WG 11.3 Data and Application Security
  - International Federation for Information Processing
- ISACA (Information Systems Audit and Control Association)
- ISSA (Information Systems Security Association)

Security - We Are Losing Ground

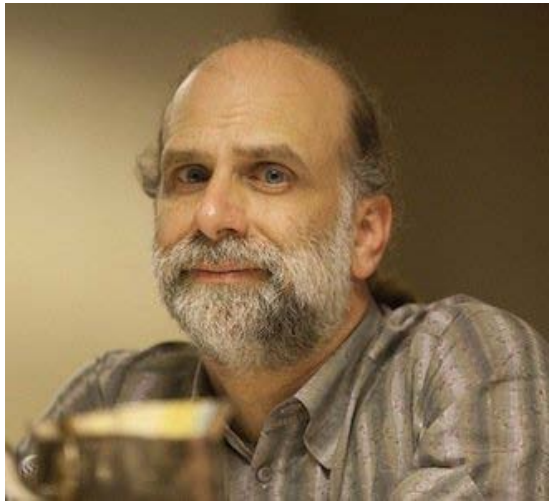
"It's clear **the bad guys are winning at a faster rate than the good guys** are winning, and we've got to solve that."

- 2014 Verizon Data Breach Investigations Report

Source: searchsecurity.techtarget.com/news/2240215422/In-2014-DBIR-preview-Verizon-says-data-breach-response-gap-widening

Security - We Are Losing Ground – Cloud is Next

"…Even though security is improving, things are getting worse faster, so **we're losing ground even as we improve**."



- Security expert Bruce Schneier

Source: http://www.businessinsider.com/bruce-schneier-apple-google-smartphone-security-2012-11

Key Topics

- What are the Concerns with Cloud?
- What is the Guidance for Cloud Data Security?
- What New Data Security Technologies are Available for Cloud?
- How can Cloud Data Security work in Context to the Enterprise?
- What are the Common Use Cases?
- How can Search and Indexing be Performed?

What are the Concerns with Cloud?

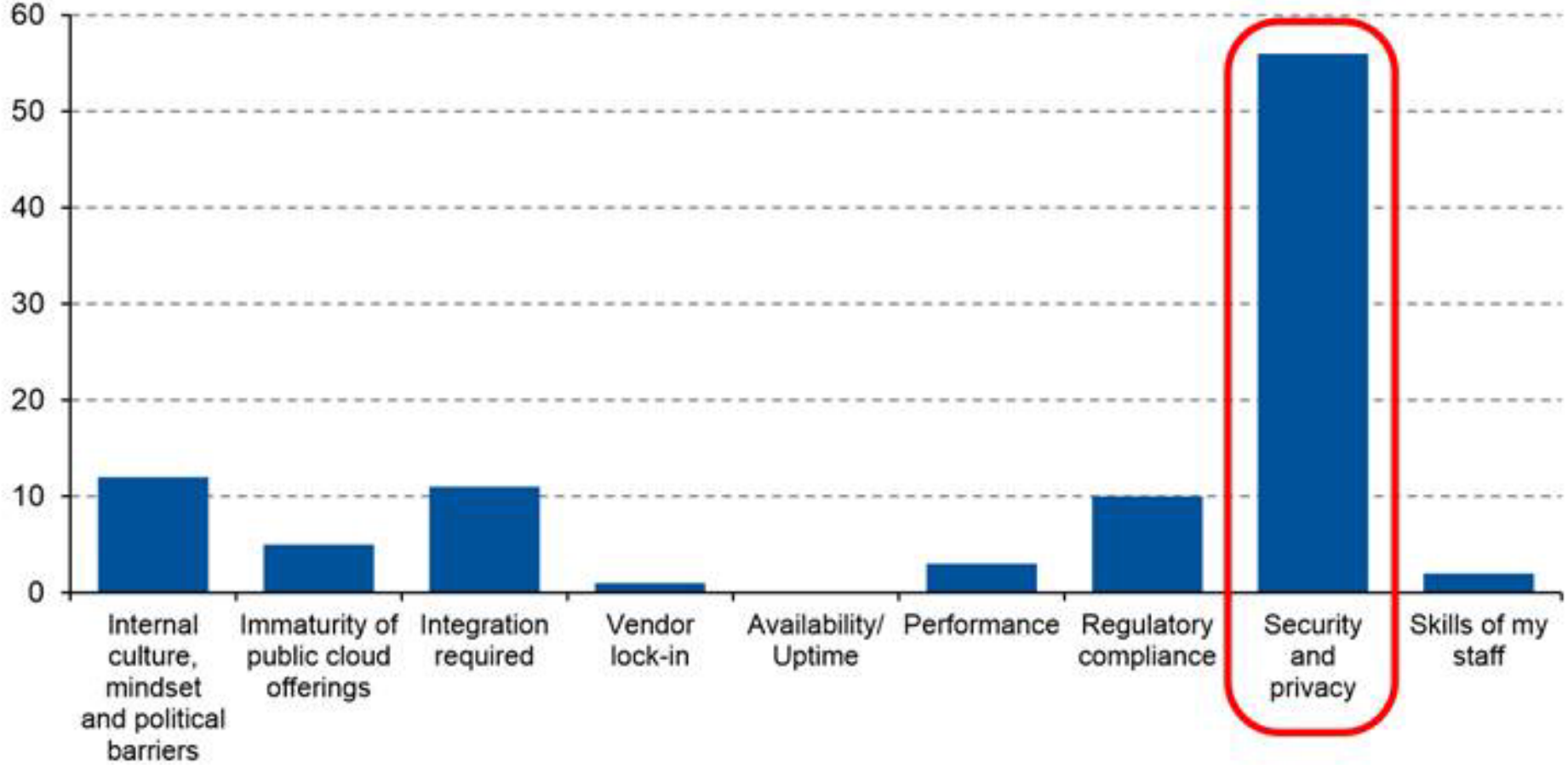
Gartner

Ponemon INSTITUTE

CSA cloud security alliance®

protegrity

What Is Your No. 1 Issue Slowing Adoption of Public Cloud Computing?



Sensitive Data in the Cloud

82%

Of organizations currently (or plan to) transfer sensitive/confidential data to the cloud in the next 24 mo.

Lack of Cloud Confidence

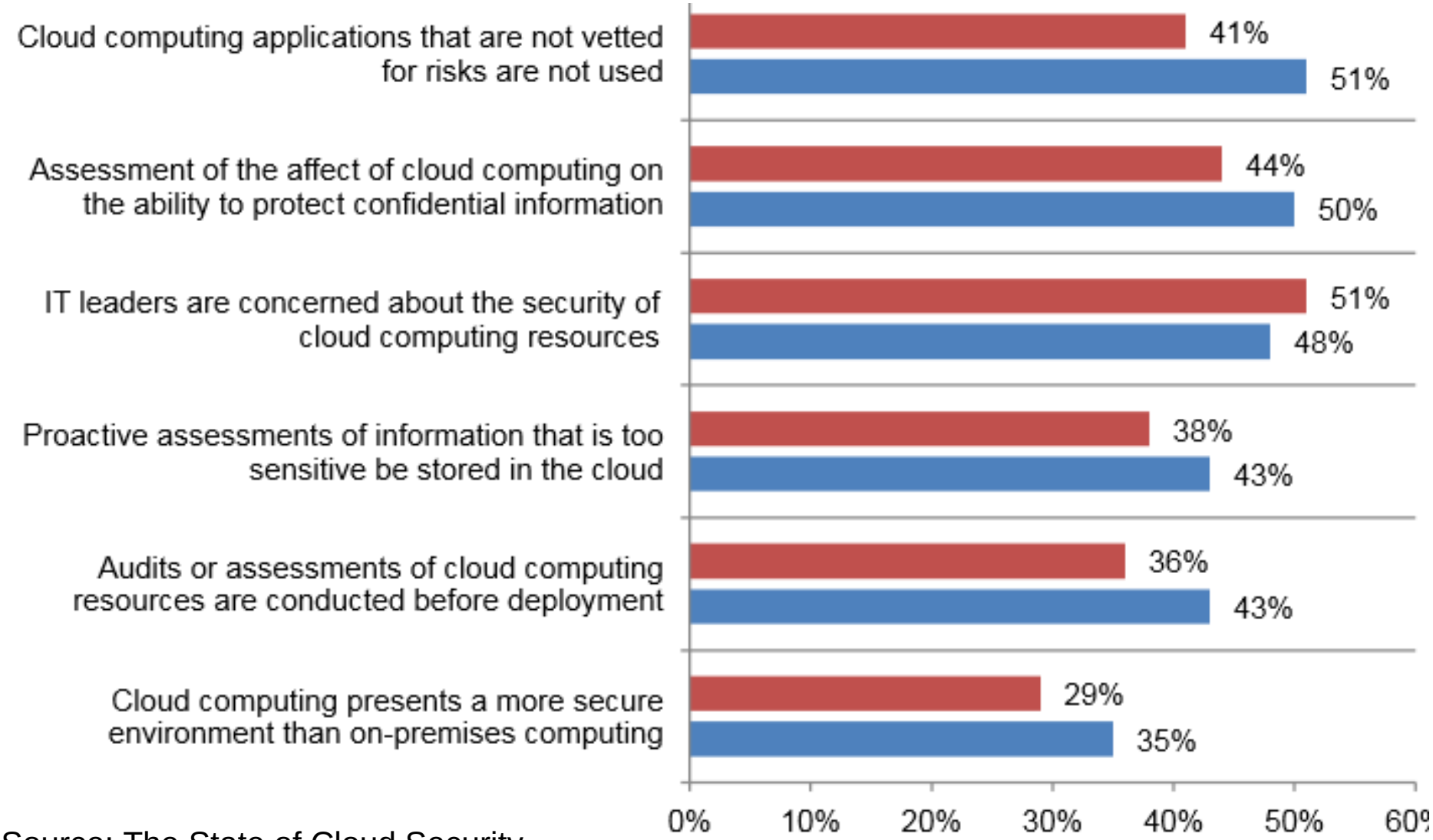
Ponemon INSTITUTE

2/3

Number of survey respondents that either agree or are unsure that the cloud services used by their organization are NOT thoroughly vetted for security.

protegrity

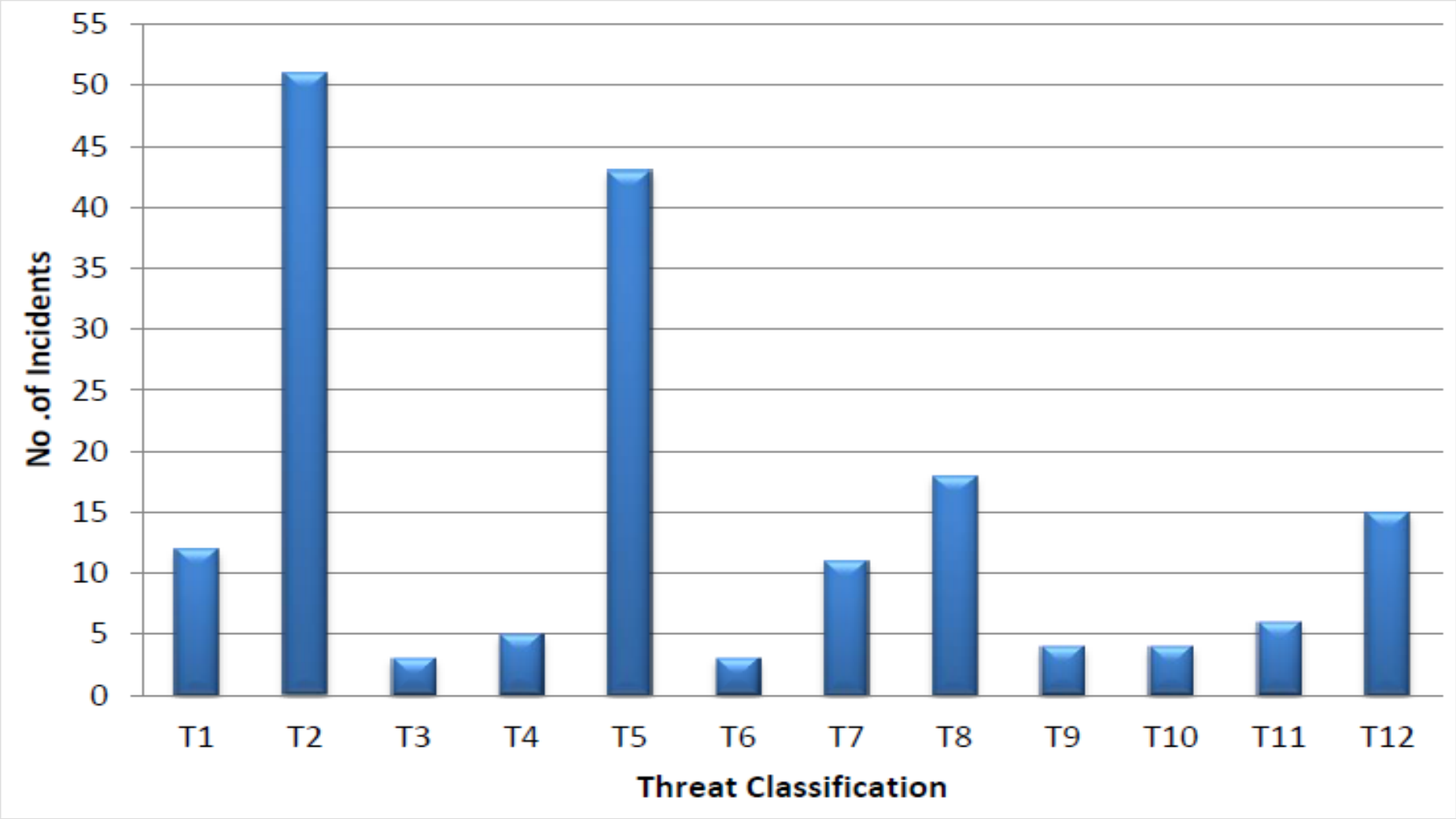
Stopped or Slowed Adoption



Source: The State of Cloud Security

Blue: Most recent data

Data Loss & Insecure Interfaces



Number of Cloud Vulnerability Incidents by Threat Category

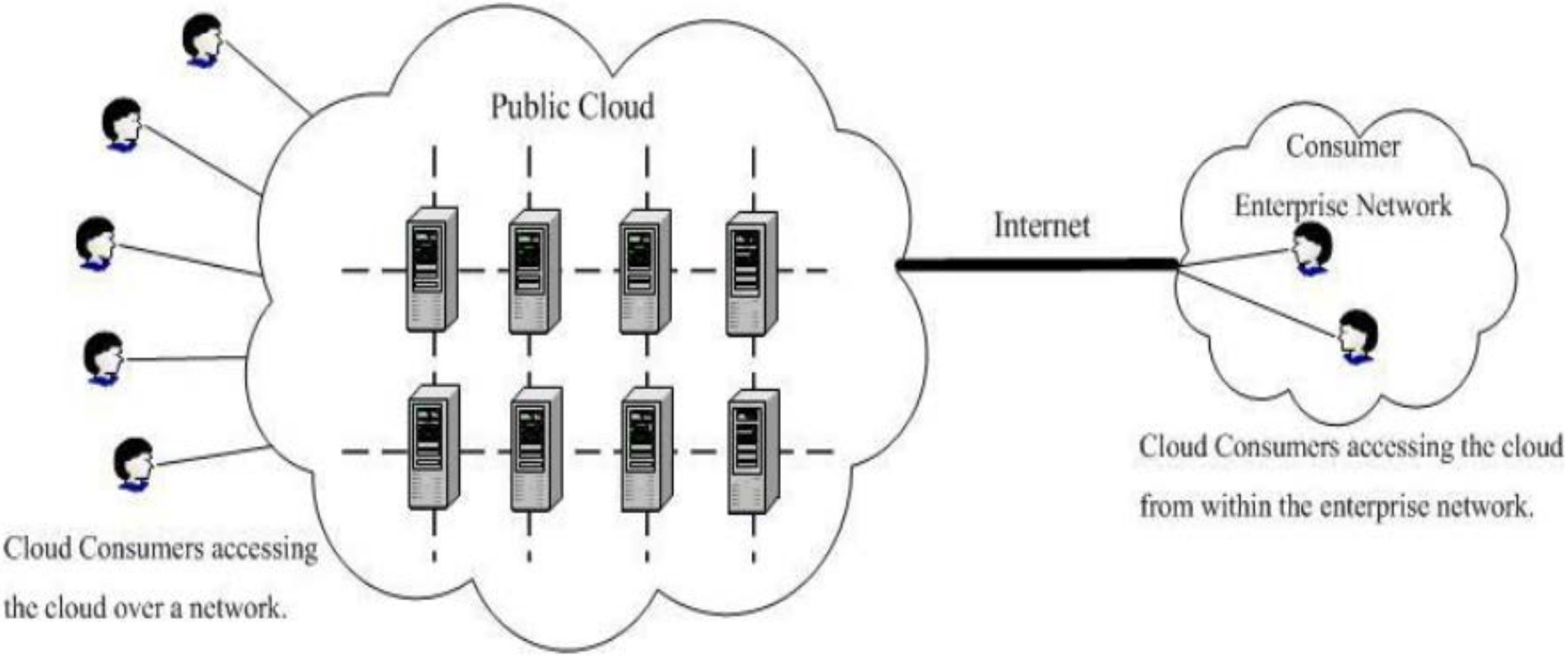
What is Cloud Computing?

- Computing as a Service:
  - Software as a Service (SaaS)
  - Platform as a Service (PaaS)
  - Infrastructure as a Service (IaaS)

- Delivered Internally or Externally to the Enterprise:
  - Public
  - Private
  - Community
  - Hybrid

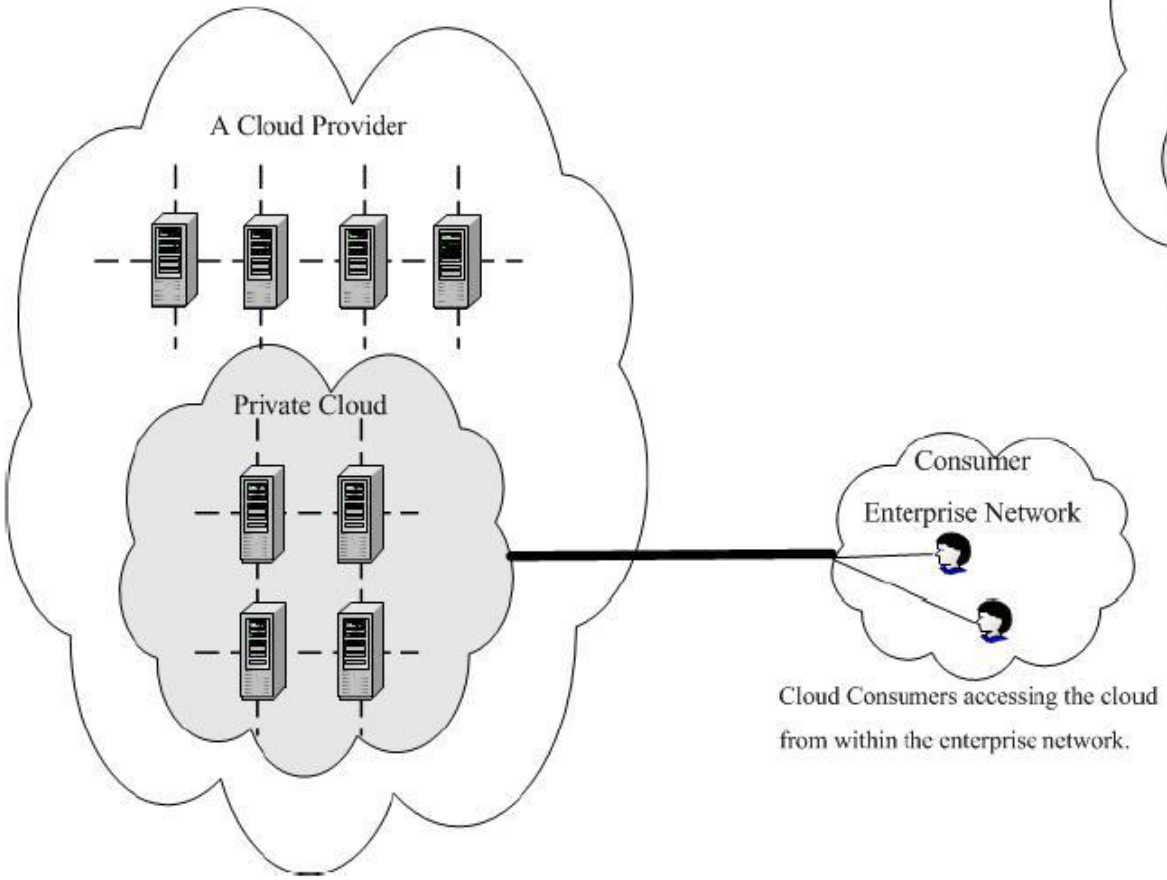
Public Cloud

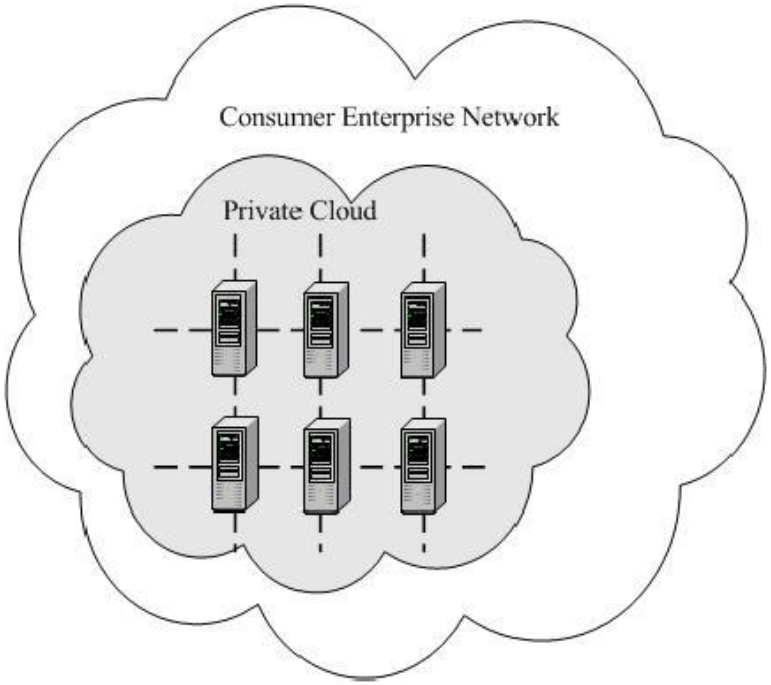
Public Cloud



Private Cloud

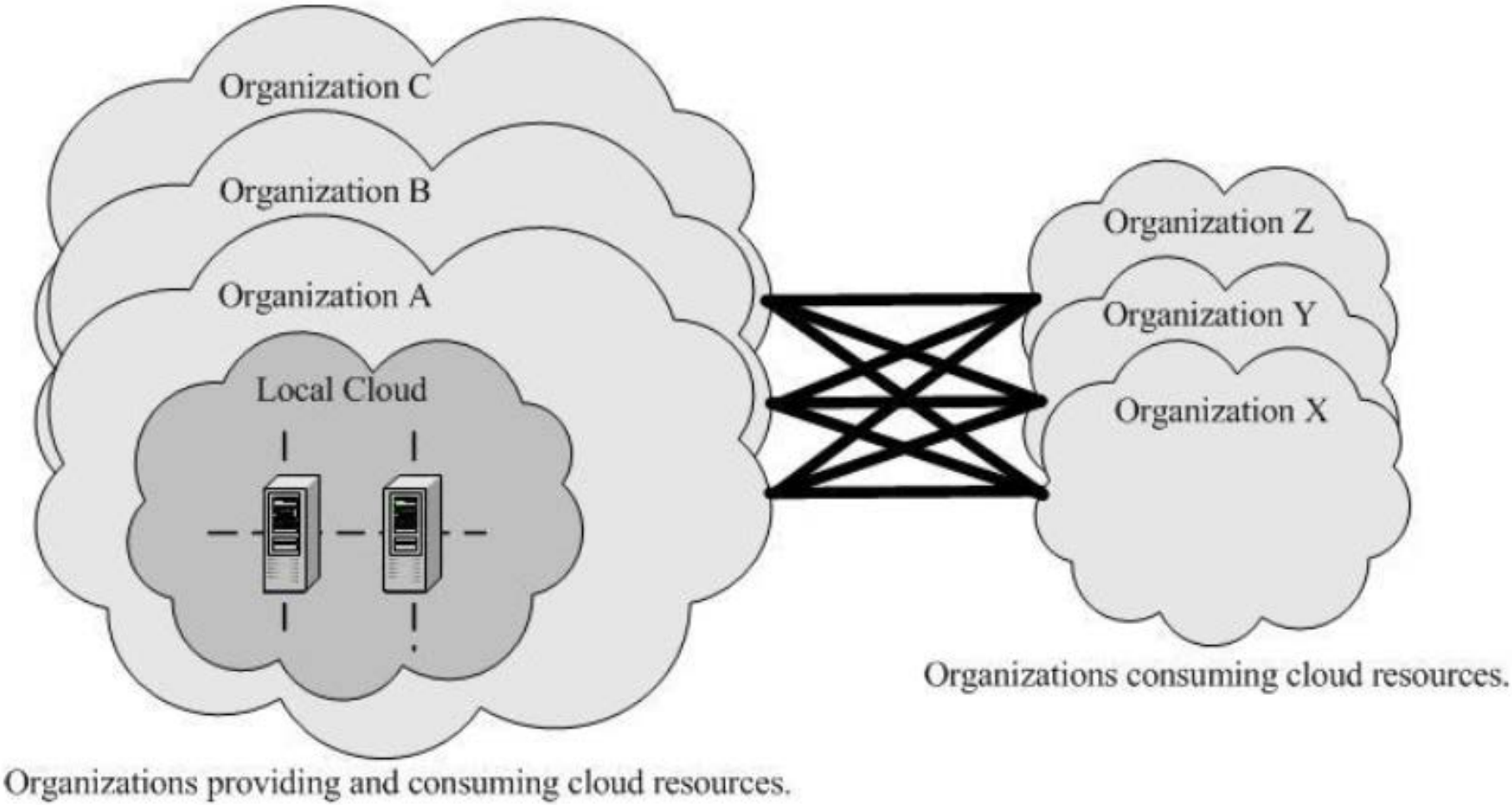
Outsourced
Private Cloud



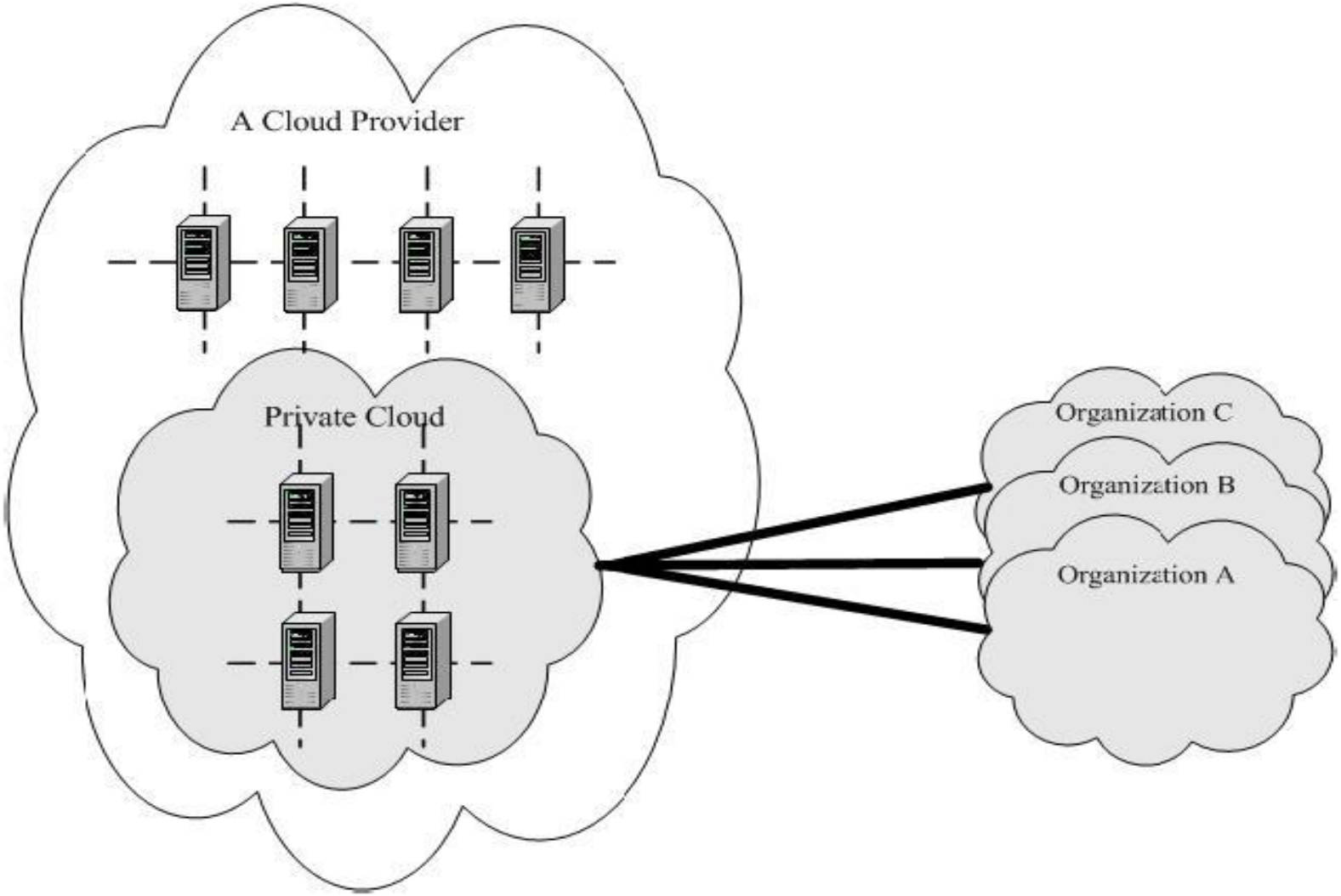


On-site
Private Cloud

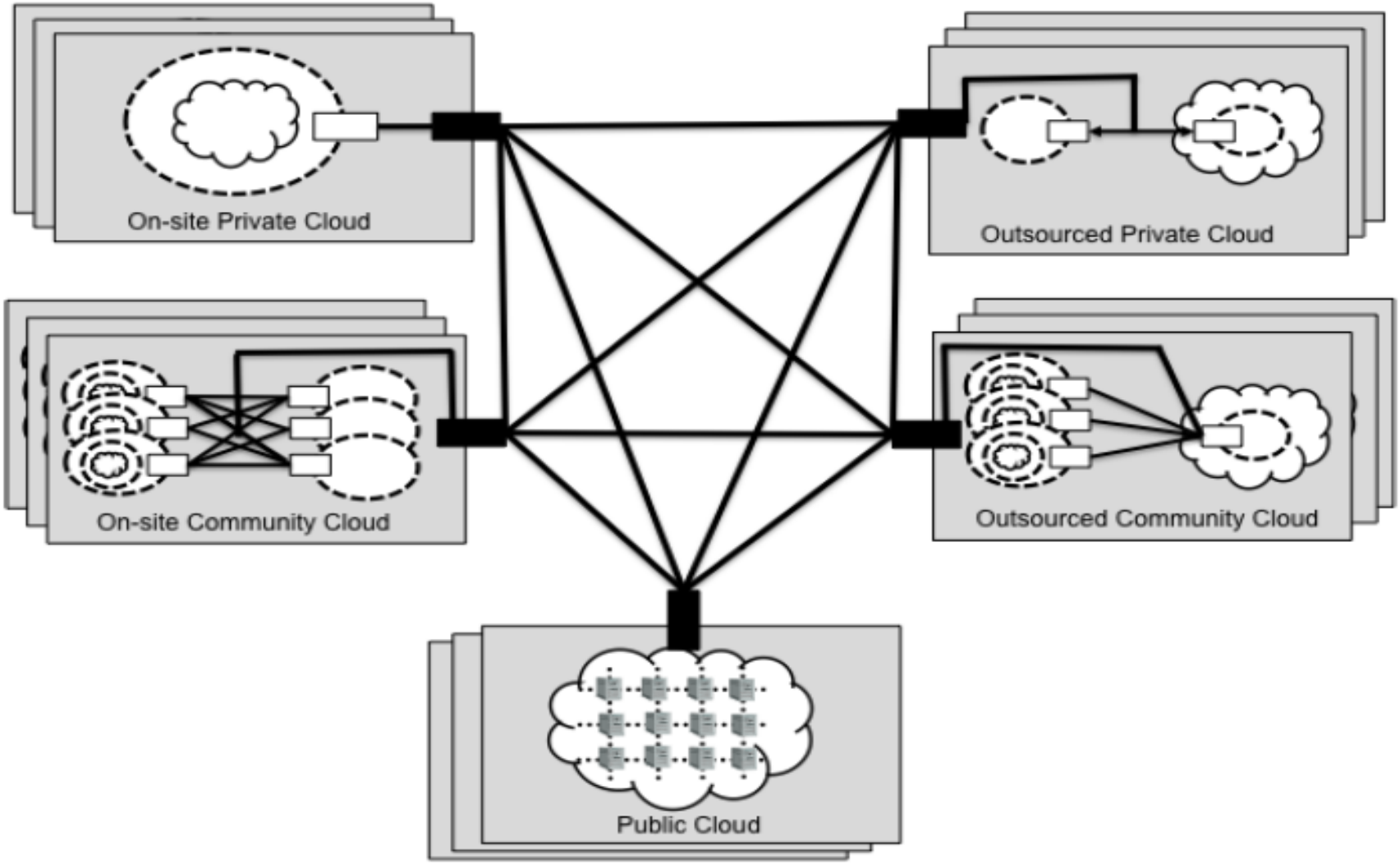
On-site Community Cloud



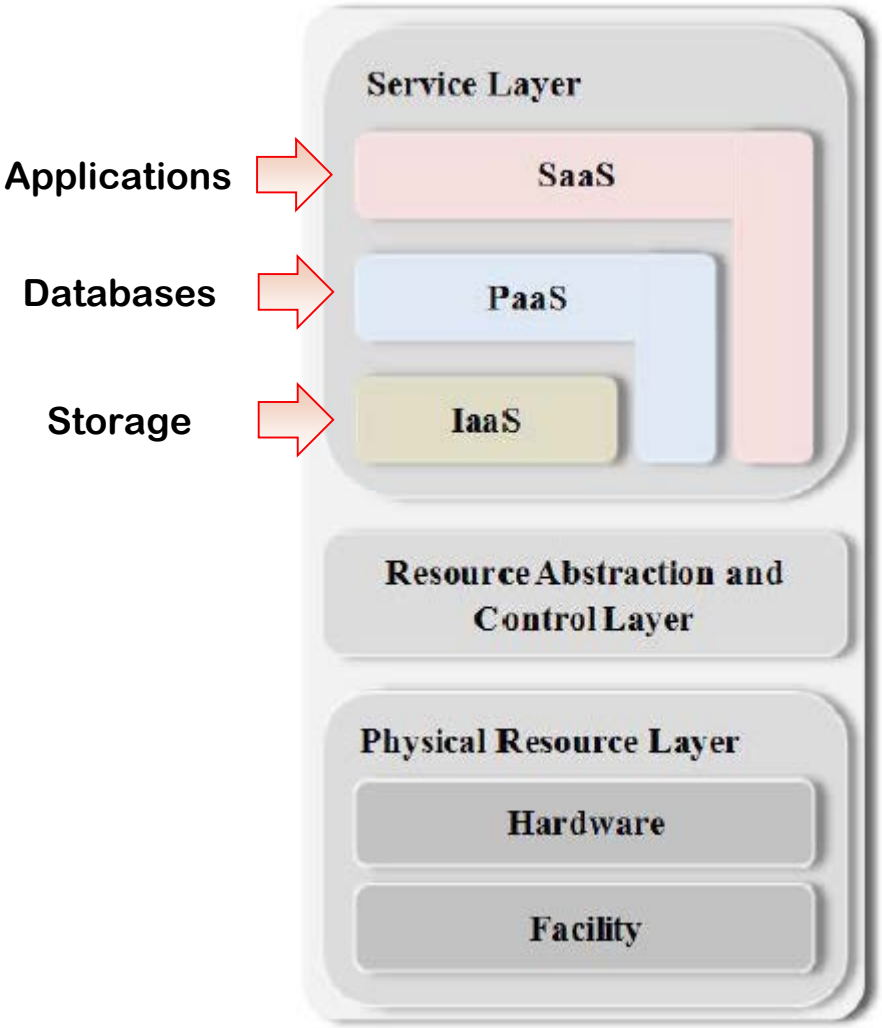
Outsourced Community Cloud



Hybrid Cloud



Service Orchestration



- Software as a Service (SaaS)

  Typically web accessed internet-based applications (“on-demand software”)

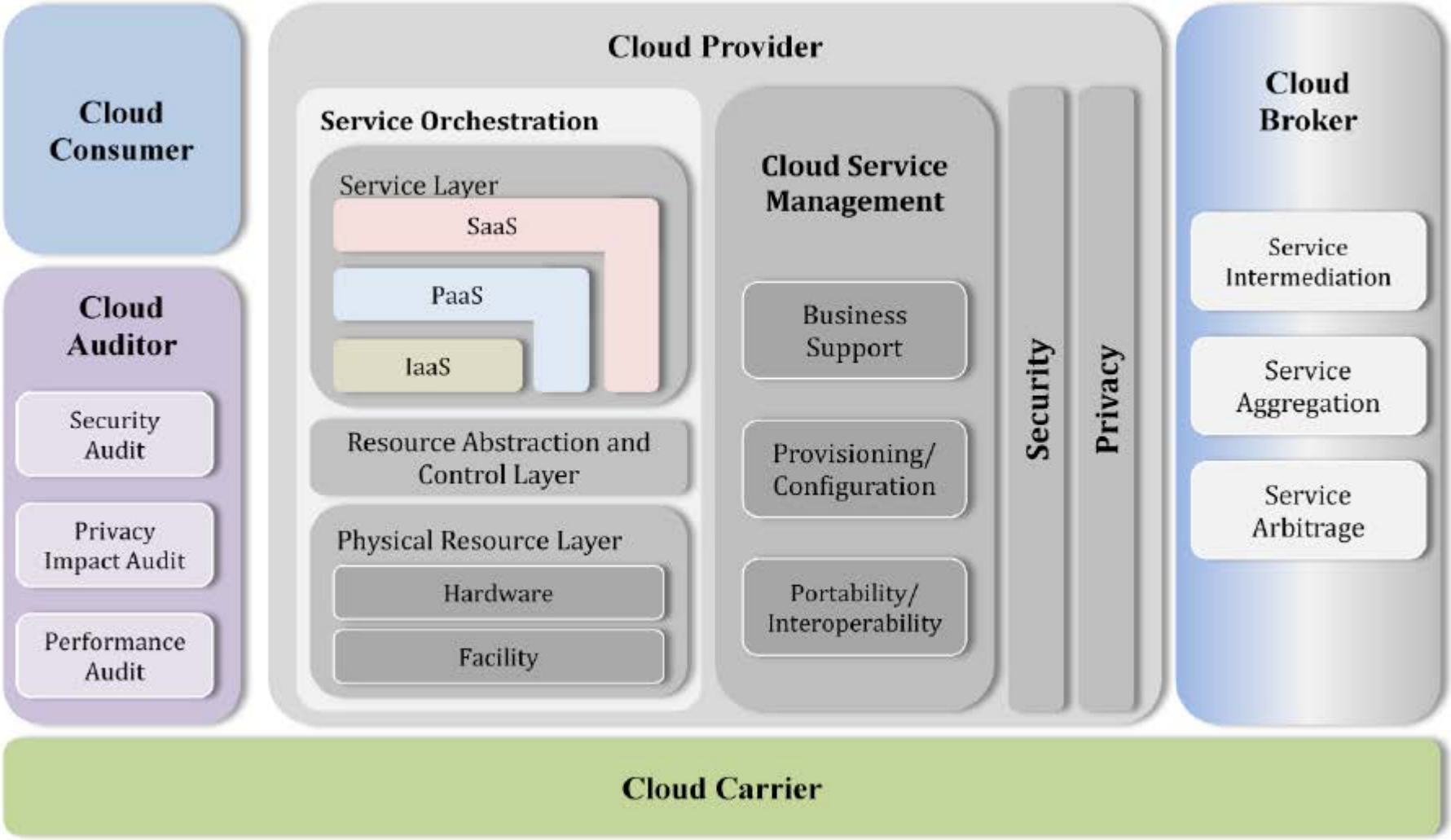
- Platform as a Service (PaaS)

  An internet-based computing platform and solution stack. Facilitates deployment of applications at much lower cost and complexity

- Infrastructure as a Service (IaaS)

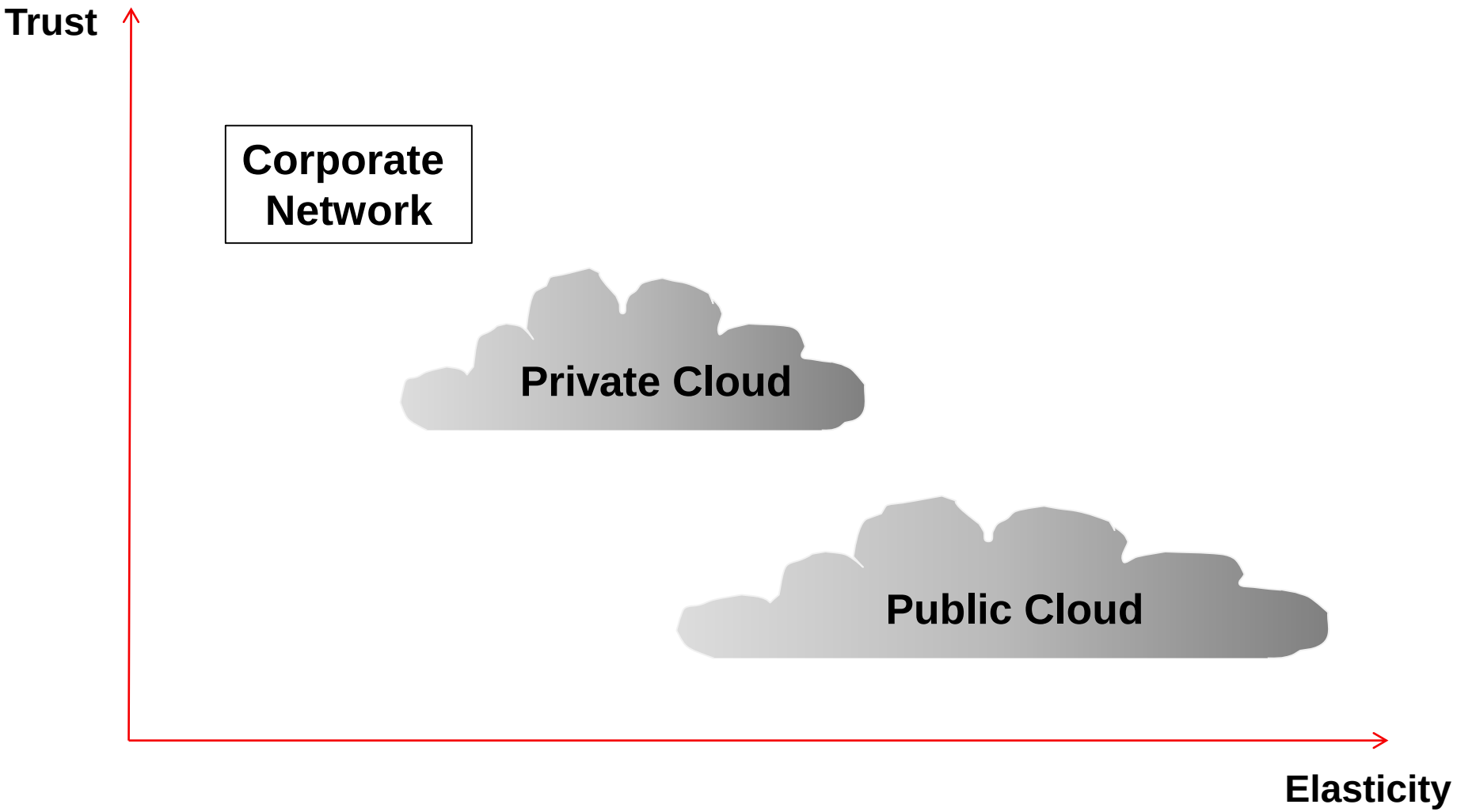
  Delivers computer infrastructure (typically a virtualized environment) along with raw storage and networking built-in

The Conceptual Reference Model

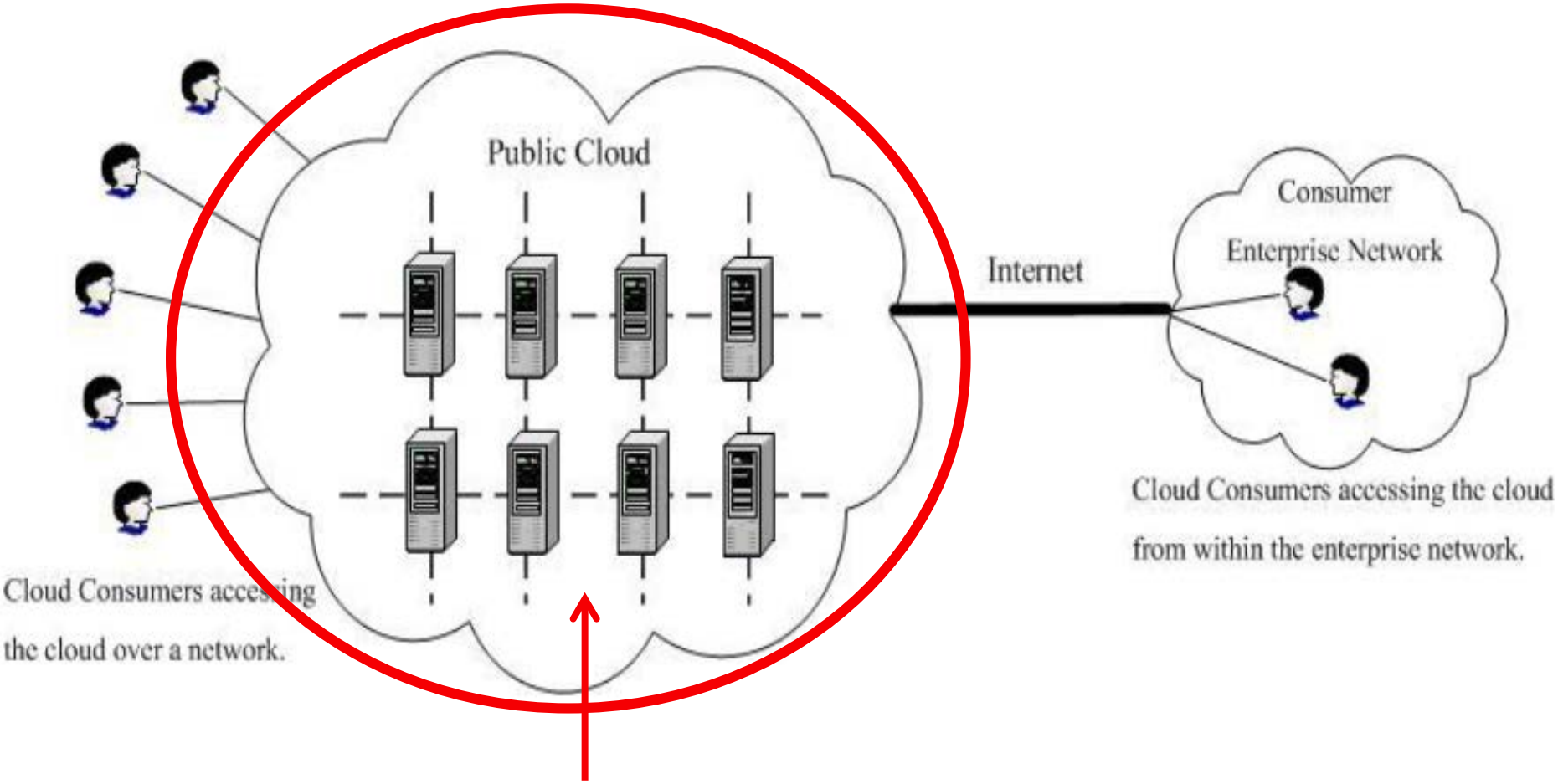


Governance, Risk Management and Compliance

Trust vs. Elasticity



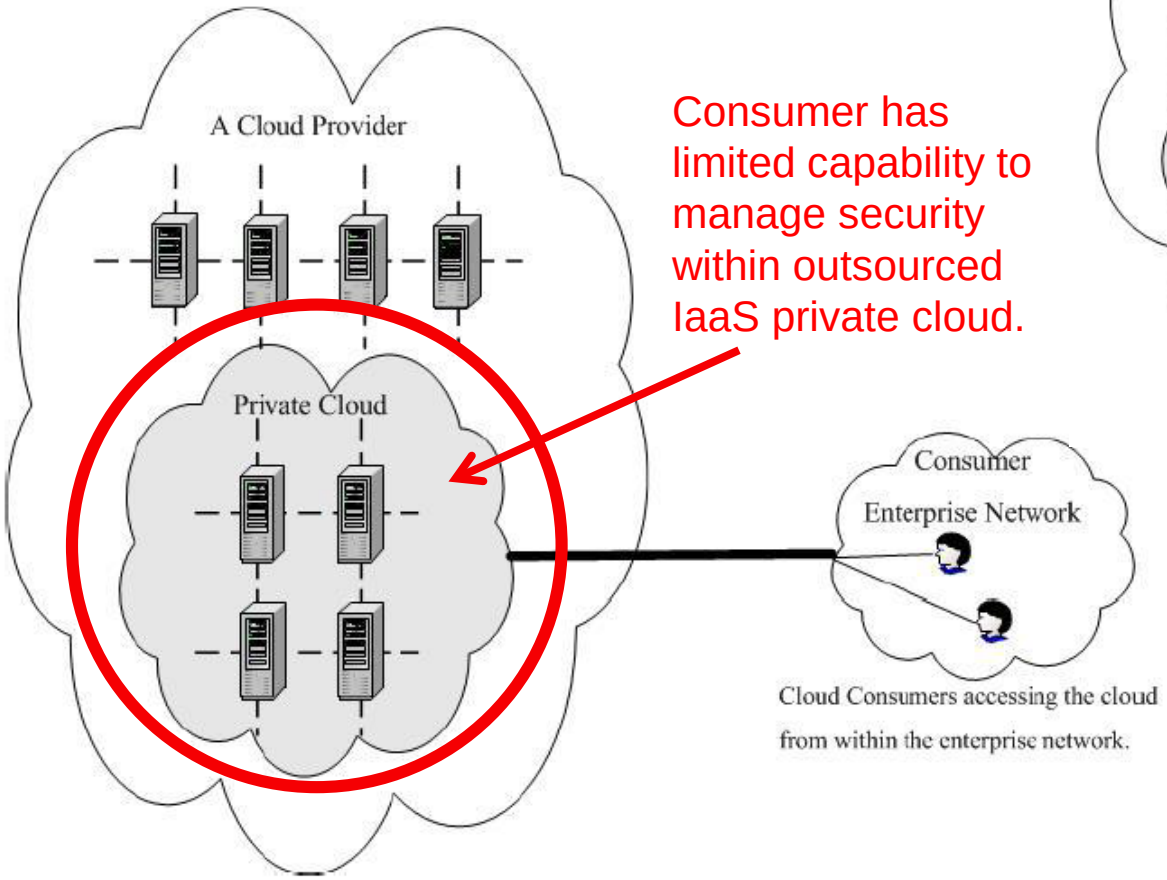
Public Cloud – No Control



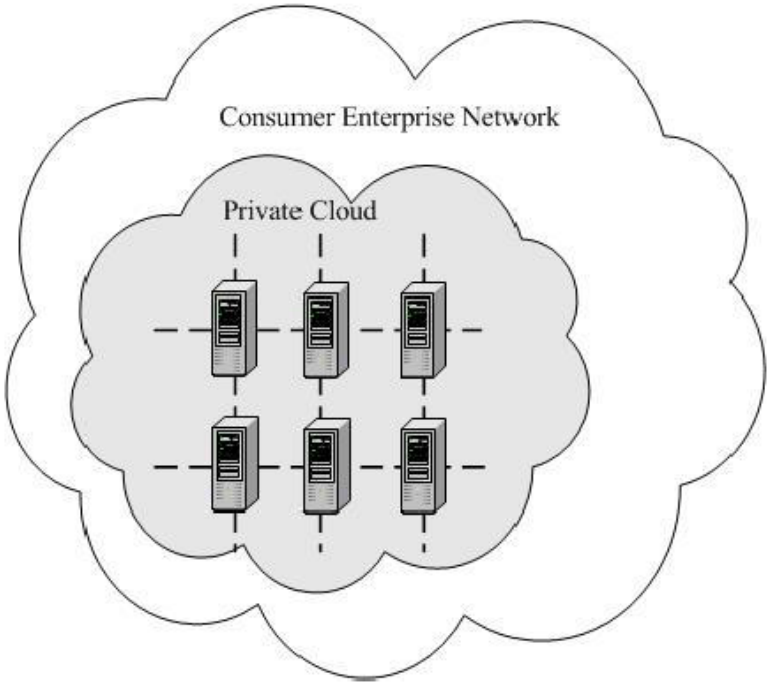
Consumers have no control over security once data is inside the public cloud. Completely reliant on provider for application and storage security.

Private Cloud – Limited Control

Outsourced
Private Cloud

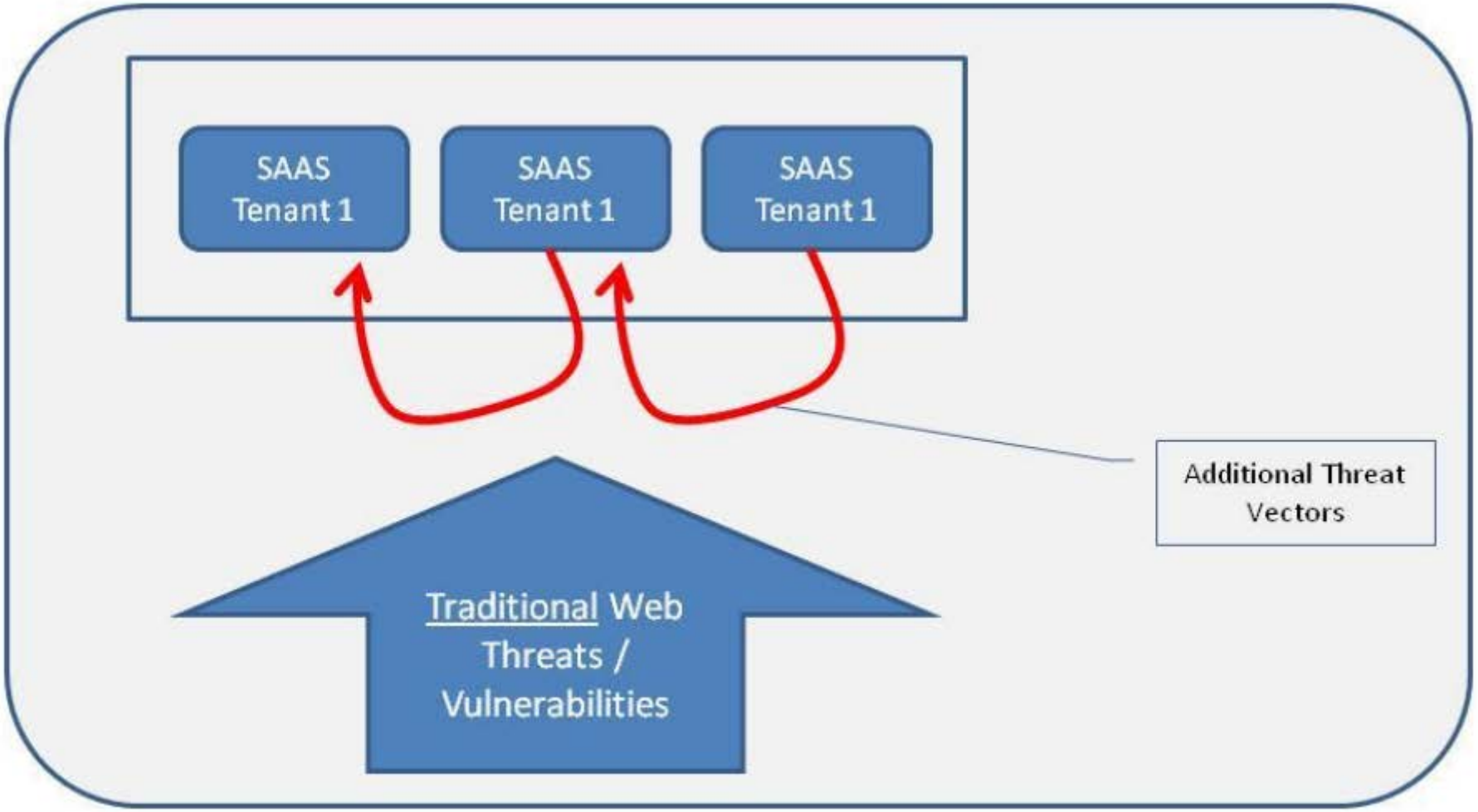


Consumer has limited capability to manage security within outsourced IaaS private cloud.



On-site
Private Cloud

Threat Vector Inheritance

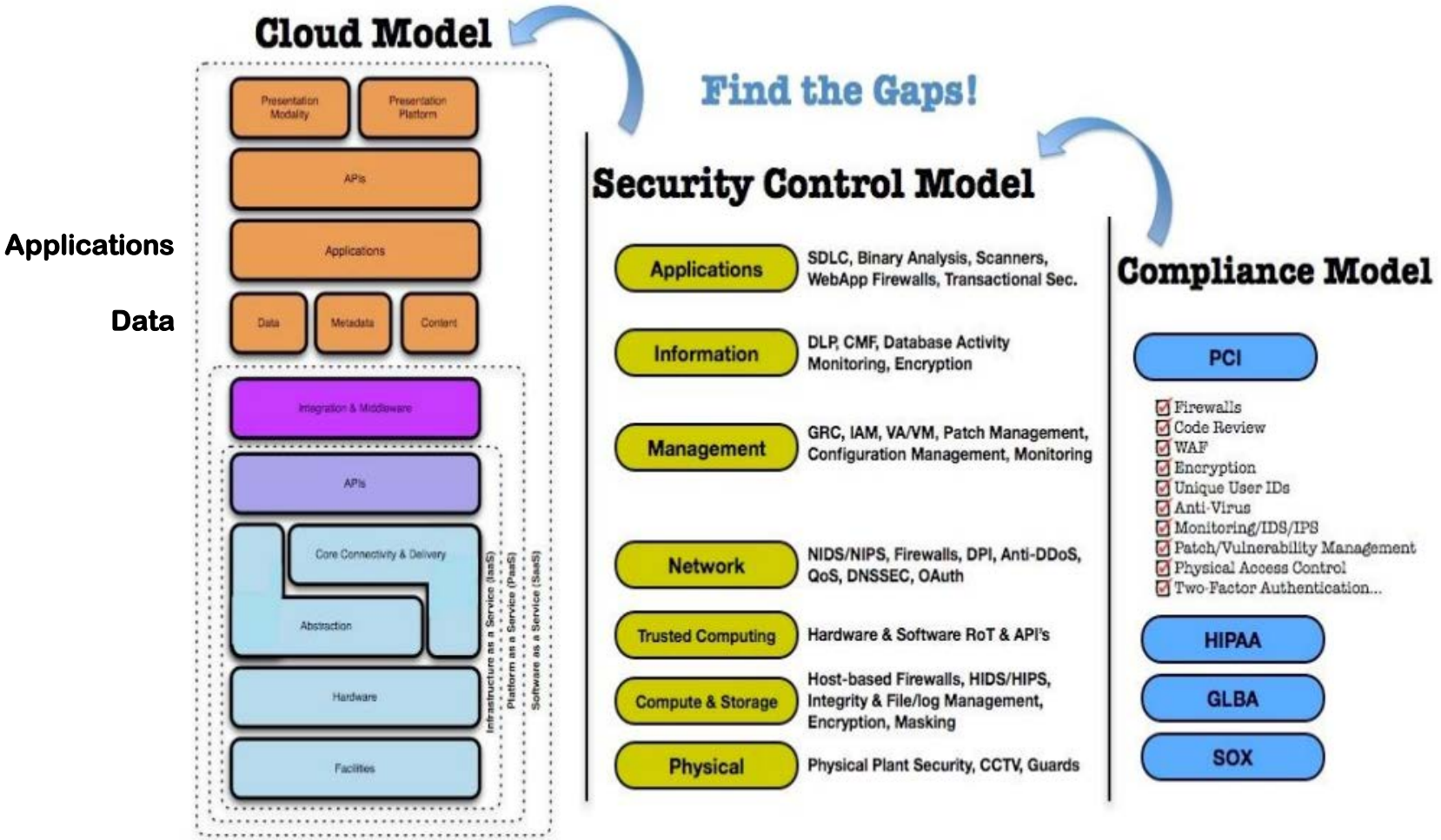


Virtualization Concerns in Cloud

- Virtual machine guest hardening
- Hypervisor security
- Inter-VM attacks and blind spots
- Performance concerns
- Operational complexity from VM sprawl
- Instant-on gaps
- Virtual machine encryption
- Data comingling
- Virtual machine data destruction
- Virtual machine image tampering
- In-motion virtual machines

PCI DSS Requirement	Example responsibility assignment for management of controls		
	IaaS	PaaS	SaaS
1: Install and maintain a firewall configuration to protect cardholder data	Both	Both	CSP
2: Do not use vendor-supplied defaults for system passwords and other security parameters	Both	Both	CSP
3: Protect stored cardholder data	Both	Both	CSP
4: Encrypt transmission of cardholder data across open, public networks	Client	Both	CSP
5: Use and regularly update anti-virus software or programs	Client	Both	CSP
6: Develop and maintain secure systems and applications	Both	Both	Both
7: Restrict access to cardholder data by business need to know	Both	Both	Both
8: Assign a unique ID to each person with computer access	Both	Both	Both
9: Restrict physical access to cardholder data	CSP	CSP	CSP
10: Track and monitor all access to network resources and cardholder data	Both	Both	CSP
11: Regularly test security systems and processes	Both	Both	CSP
12: Maintain a policy that addresses information security for all personnel	Both	Both	Both
PCI DSS Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers	CSP	CSP	CSP

Mapping the Cloud Model to Security Control & Compliance



Governance, Risk Management and Compliance

GRC™
GRC Stack

An Integrated Suite of Four CSA Initiatives

Cloud Audit
The A6 Working Group

CCM™
Cloud Controls Matrix

CAI™
Consensus Assessments Initiative

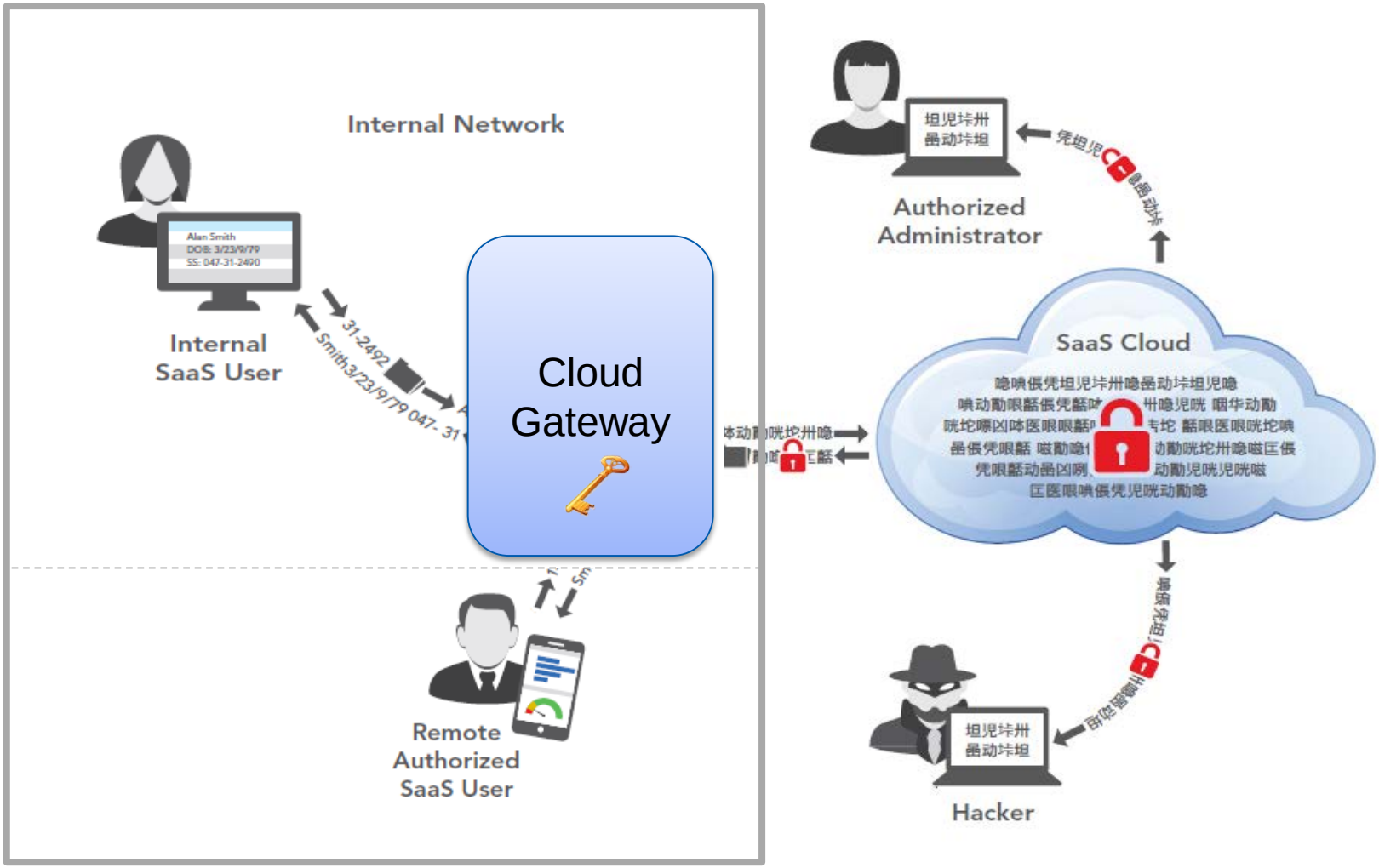
CTP
Cloud Trust Protocol

Data Protection Solutions

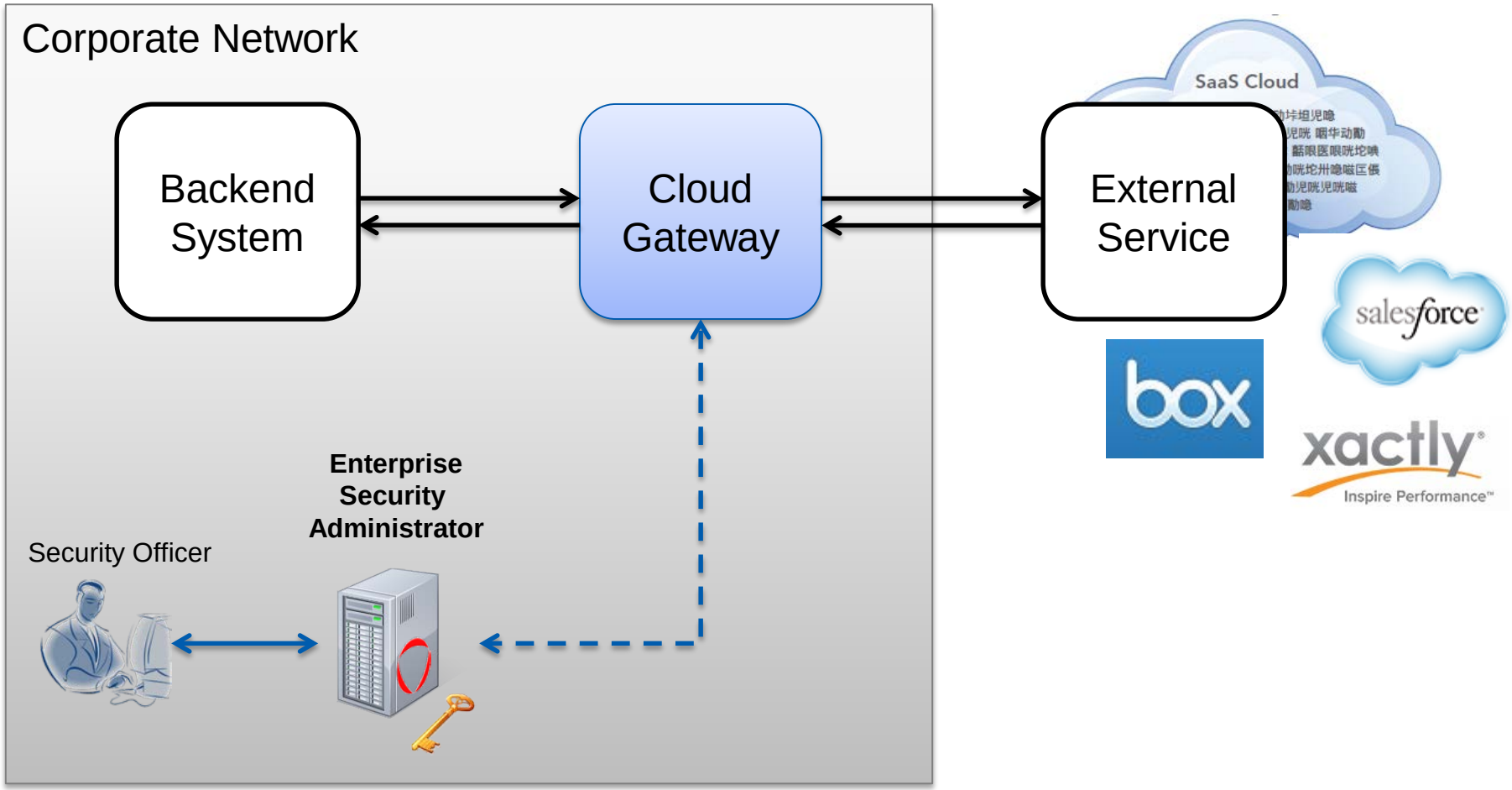
Cloud Gateways Provide Enterprise Control

- Cloud Encryption Gateways
  - SaaS encryption
- Cloud Security Gateways
  - Policy enforcement
- Cloud Access Security Brokers (CASBs)
- Cloud Services Brokerage (CSB)
- Secure Email Gateways
- Secure Web gateway

Public Cloud Gateway – SaaS Example



Security Gateway Deployment – Application Example

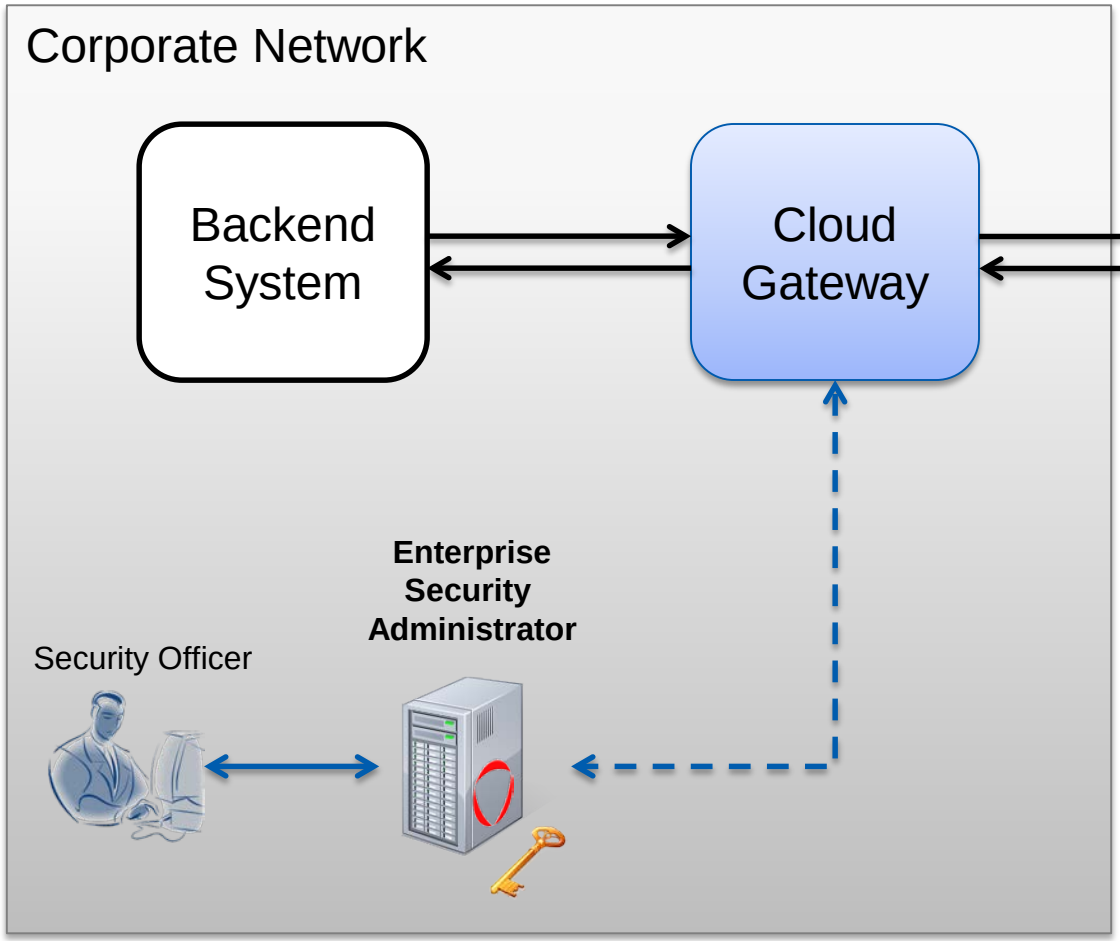


Example of Cloud Security Gateway Features

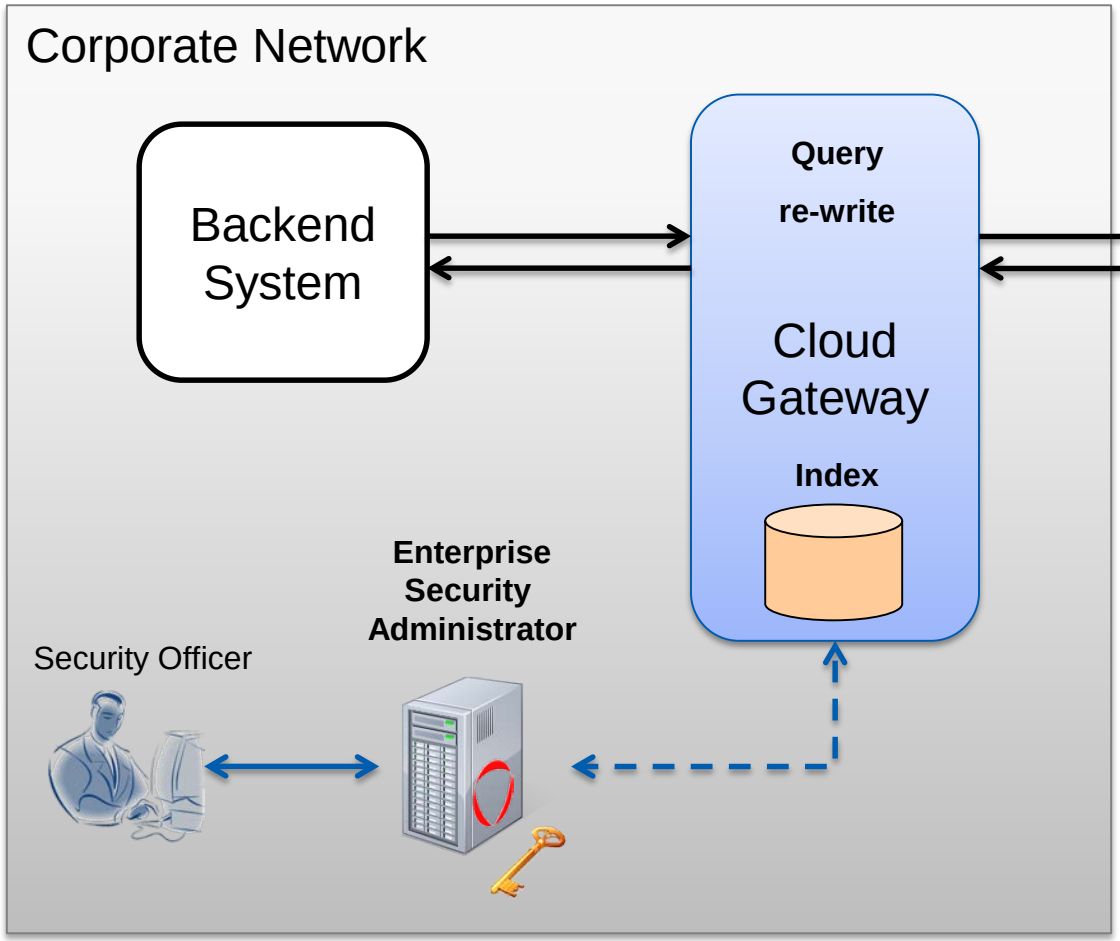
- High-Performance Gateway Architecture
- Enterprise-extensible platform
- Tokenization and encryption
- Enterprise-grade key management
- Flexible policy controls
  - File or Field Security
  - Advanced function & usability preservation
- Comprehensive activity monitoring & reporting
- Support for internal, remote & mobile users
- Multiple deployment options

protegrity

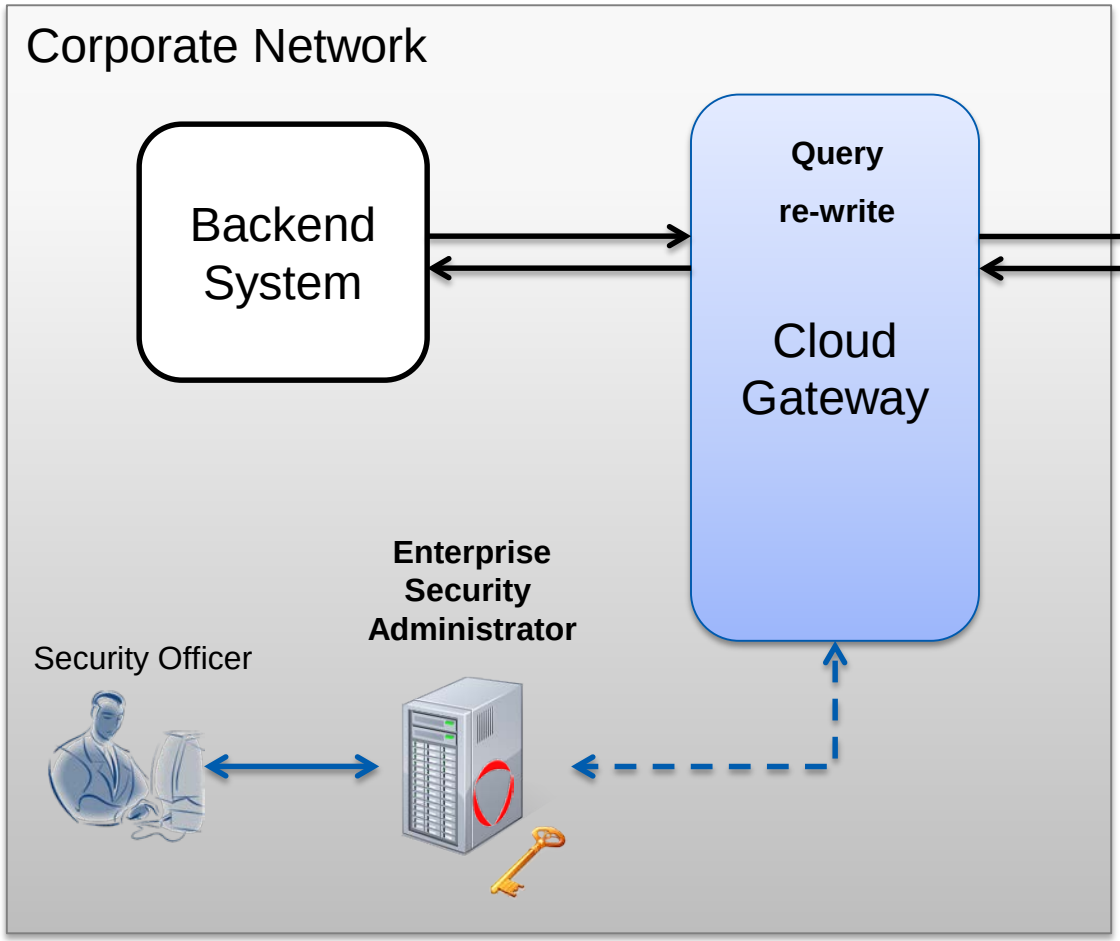
Security Gateway Deployment – Database Example



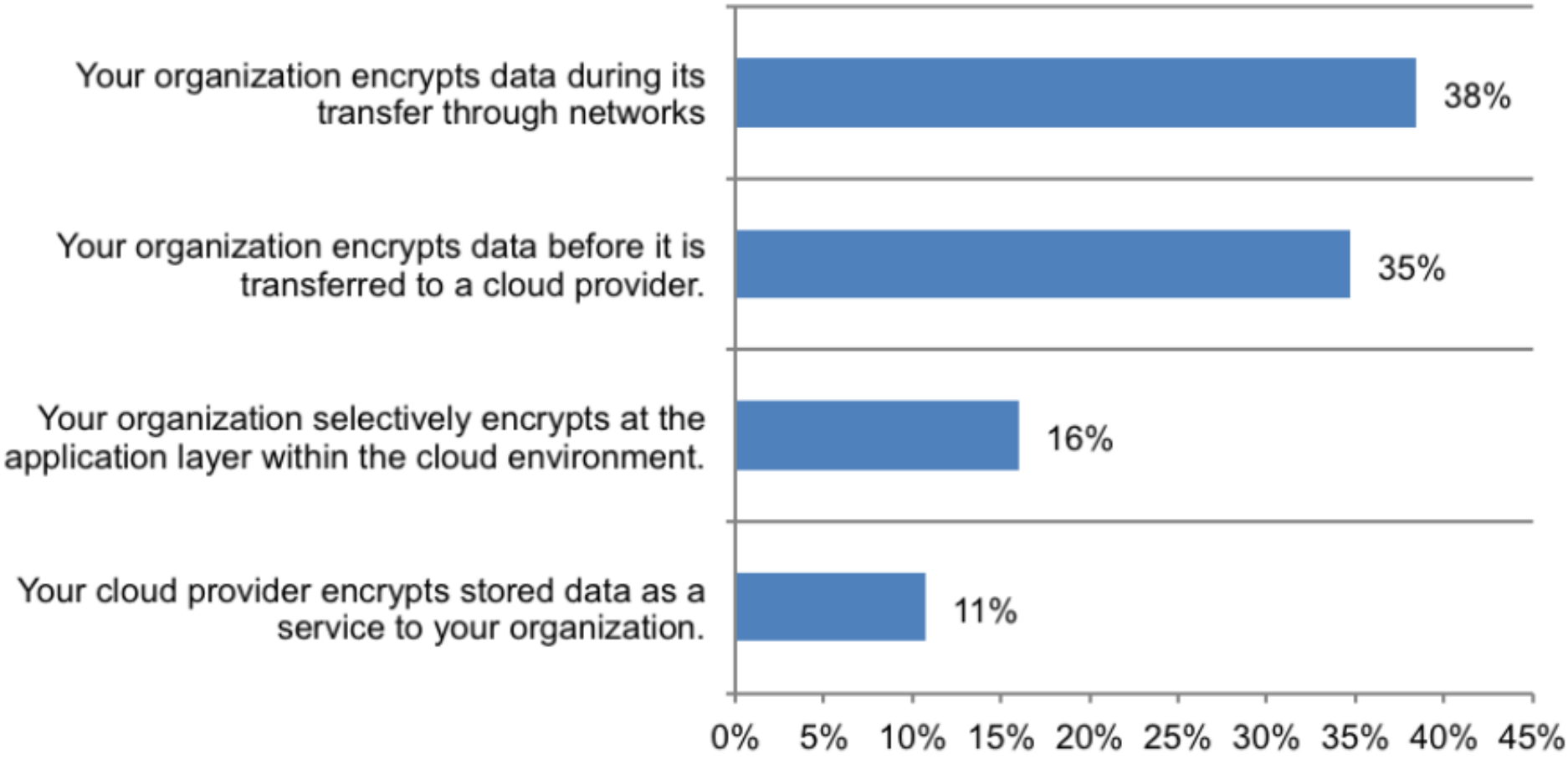
Security Gateway Deployment – Indexing



Security Gateway Deployment – Search



Where is Encryption Applied to Protect Data in Cloud?



How Data-Centric Protection Increases Security in Cloud Computing and Virtualization

- Rather than making the protection platform based, the security is applied directly to the data, protecting it wherever it goes, in any environment

- Cloud environments by nature have more access points and cannot be disconnected – data-centric protection reduces the reliance on controlling the high number of access points

Encryption Guidance from CSA

- Encrypting the transfer of data to the cloud does not ensure the data is protected in the cloud
- Once data arrives in the cloud, it should remain protected both at rest and in use
- Do not forget to protect files that are often overlooked, but which frequently include sensitive information
  - Log files and metadata can be avenues for data leakage
- Encrypt using sufficiently durable encryption strengths (such as AES-256)
- Use open, validated formats and avoid proprietary encryption formats wherever possible

CSA: Look at Alternatives to Encryption

- Data Anonymization and De-identification
  - This is where (for example) Personally Identifiable Information (PII) and Sensitive are stripped before processing.
- Utilizing access controls built into the database

De-identification / Anonymization

Field	Real Data	Tokenized / Pseudonymized
Name	Joe Smith	csu wusoj
Address	100 Main Street, Pleasantville, CA	476 srta coetse, cysieondusbak, CA
Date of Birth	12/25/1966	01/02/1966
Telephone	760-278-3389	760-389-2289
E-Mail Address	joe.smith@surferdude.org	eoe.nwuer@beusorpdqo.org
SSN	076-39-2778	076-28-3390
CC Number	3678 2289 3907 3378	3846 2290 3371 3378
Business URL	www.surferdude.com	www.sheyinctao.com
Fingerprint		Encrypted
Photo		Encrypted
X-Ray		Encrypted
Healthcare / Financial Services	Dr. visits, prescriptions, hospital stays and discharges, clinical, billing, etc. Financial Services Consumer Products and activities	Protection methods can be equally applied to the actual data, but not needed with de-identification

Data Tokenization

- De-identification / Pseudonomization / Anonymization
- Replaces real data with fake data – “Tokens”
- Data is protected before it goes to the cloud
- Benefits:
  - Eliminates data residency issues
  - Data remains usable in applications without modification
  - Vaultless tokenization
    - No data replication/collision issues,
    - High scalability

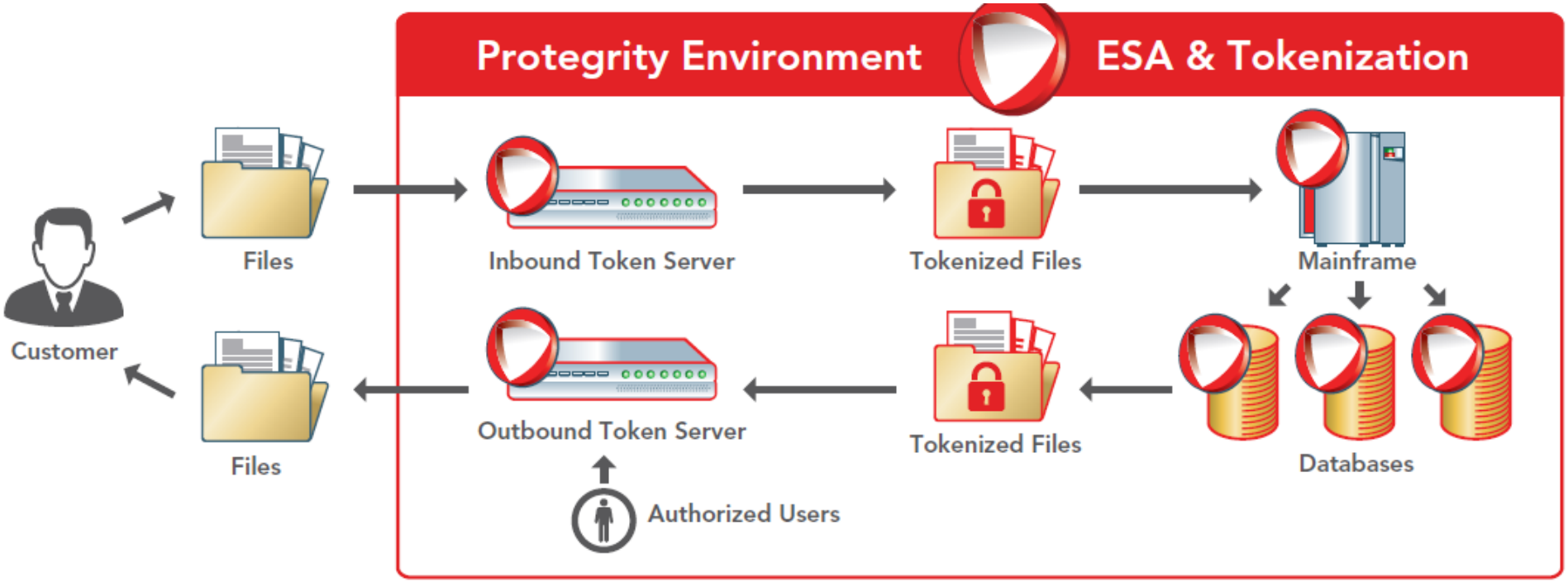
protegrity

Significantly Different Tokenization Approaches

Property	Vault-based: Dynamic	Vault-based: Pre-generated	Vaultless
Footprint	Large, Expanding	Large, Static	Small, Static
Replication	Complex replication required	No replication required	No replication required
Collisions	Prone to collisions	No collisions	No collisions
Latency / Performance	Will impact performance and scalability	Will impact performance and scalability Faster than the traditional dynamic approach	Little or no latency Fastest tokenization in the industry
Tokenizing many data categories	Potentially impossible	Potentially impossible	Can tokenize many data categories with minimal or no impact on footprint or performance

protegrity

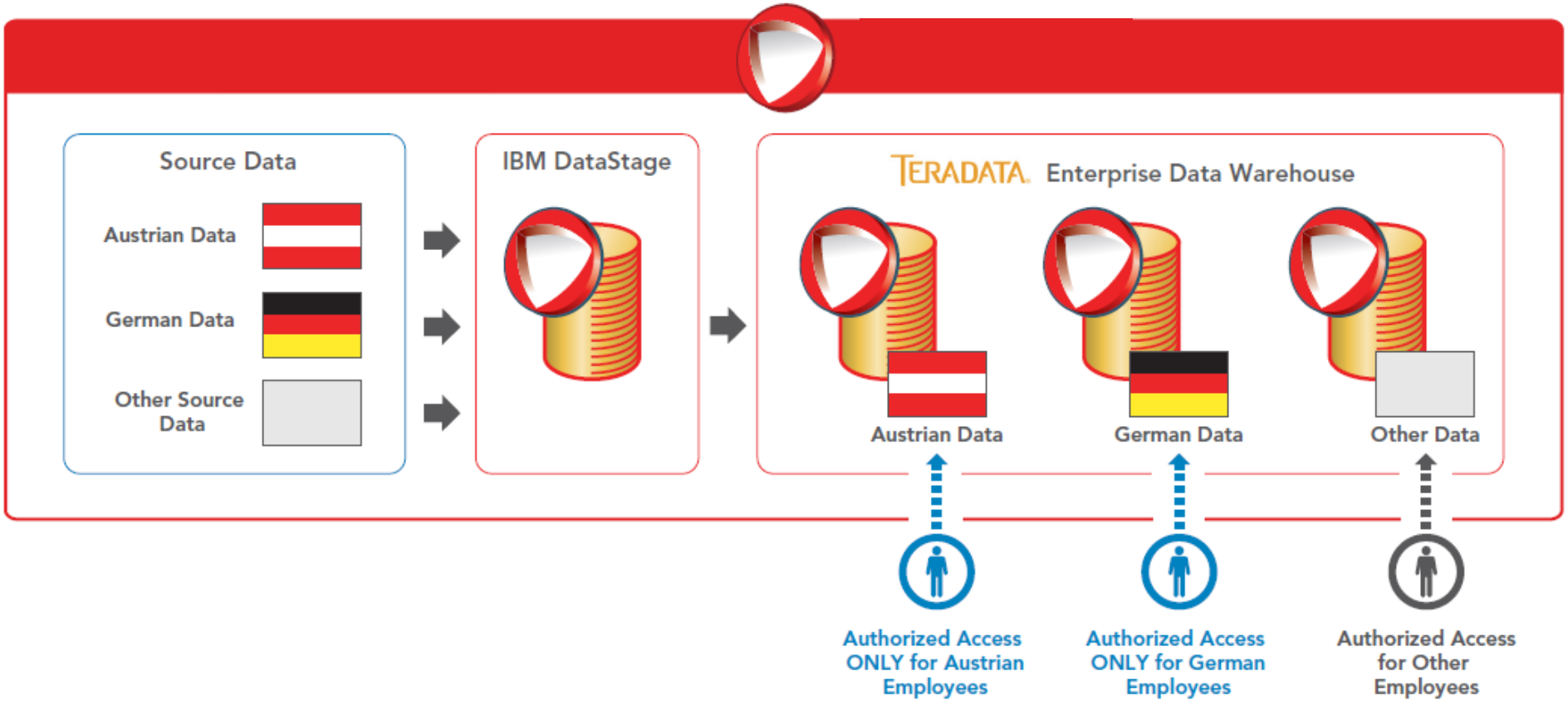
Use Case - Commercial Information and Business Insight Company



The company received trade files from customers daily, containing sensitive Card Holder Data (CHD), making them subject to Payment Card Industry Data Security Standard (PCI DSS) regulations.

Use Case - Increasing Pressure from International Data Protection Regulations

Implementation Diagram



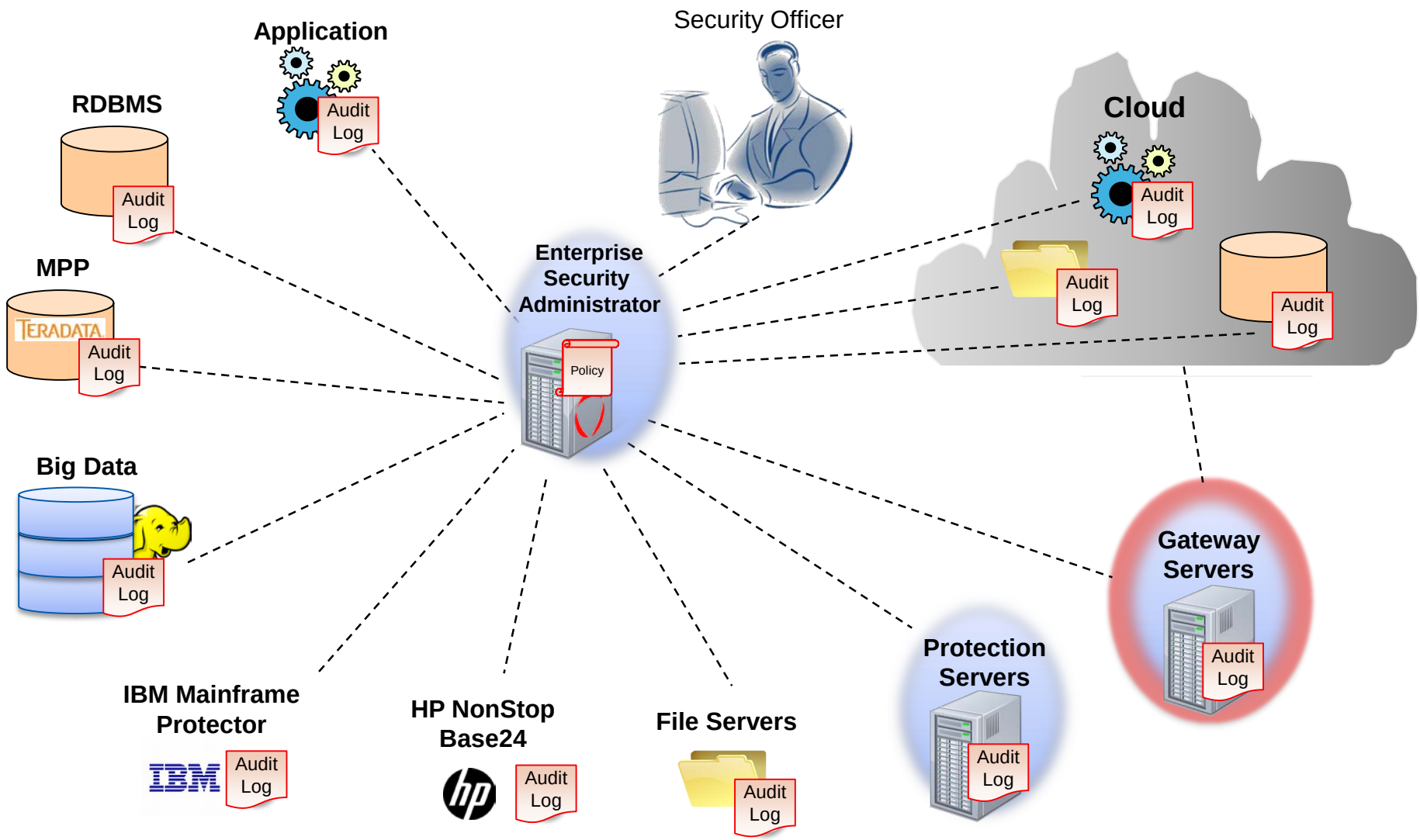
protegrity

Enterprise Data Security Policy

What	What is the sensitive data that needs to be protected.
How	How you want to protect and present sensitive data. There are several methods for protecting sensitive data. Encryption, tokenization, monitoring, etc.
Who	Who should have access to sensitive data and who should not. Security access control. **Roles & Users**
When	When should sensitive data access be granted to those who have access. Day of week, time of day.
Where	Where is the sensitive data stored? This will be where the policy is enforced.
Audit	Audit authorized or un-authorized access to sensitive data.

protegrity

Centralized Policy Management - Example



Summary

- What are the Concerns with Cloud?
- How is Cloud Computing Defined?
- What is the Guidance for Cloud Data Security?
- What New Data Security Technologies are Available for Cloud?
- How can Cloud Data Security work in Context to the Enterprise?

Thank you!

Questions?

Please contact us for more information

www.protegrity.com

Ulf.Mattsson@protegrity.com

protegrity

protecting your data.
protecting your business.