Tökéletes védelem a felhőben – lehetetlen?

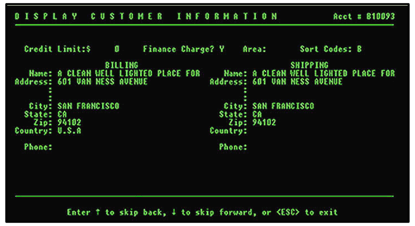
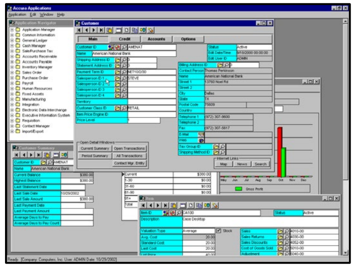
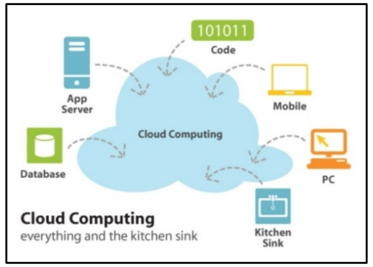
Mihály Zala
Advisory Associate Partner, Ernst & Young

Building a better
working world

What is cloud computing?

Cloud computing is using the internet to access someone else's software running on someone else's hardware in someone else's data center.

Evolving toward the cloud

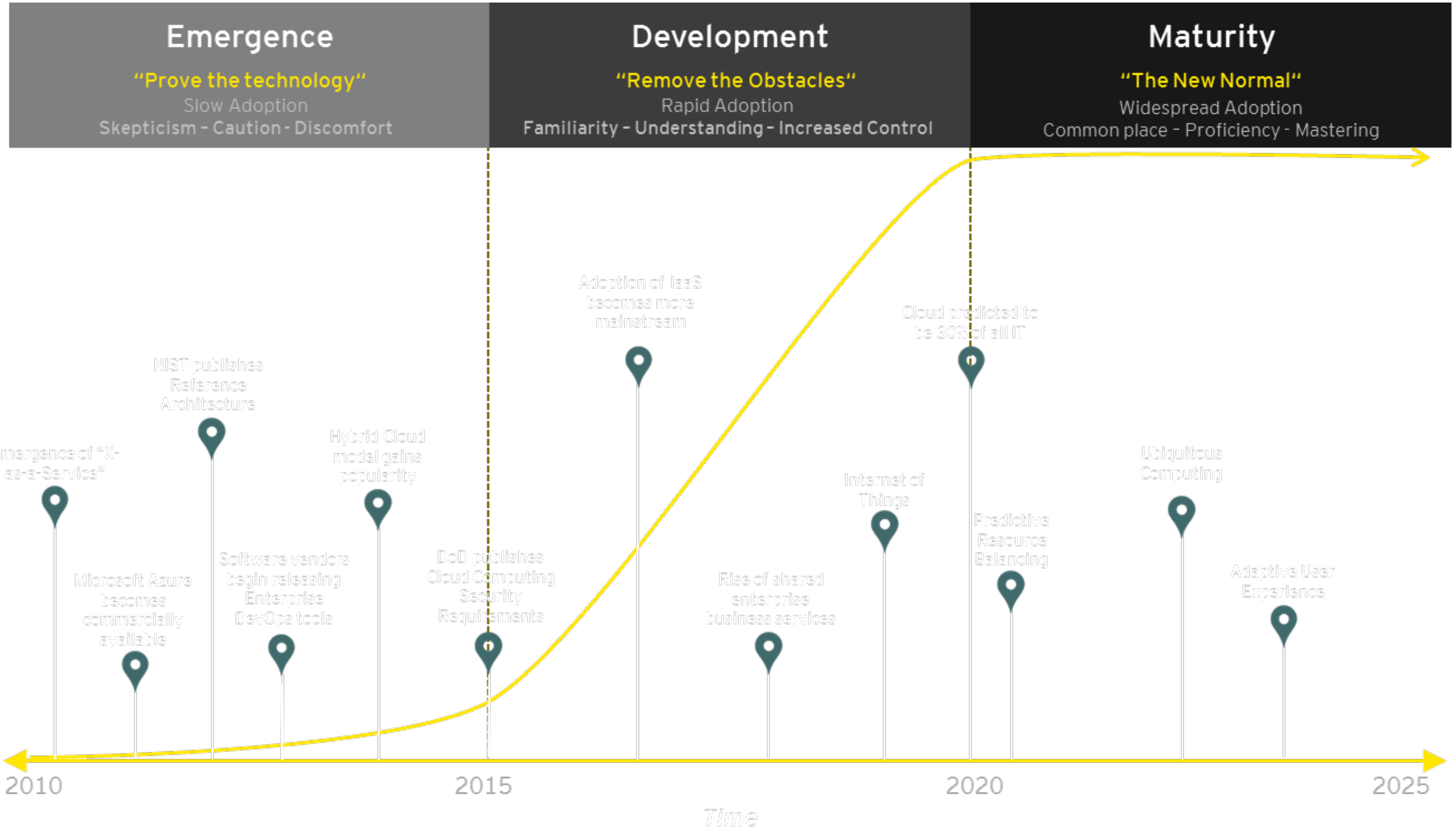
	1960s Centralized computing	1980s Client-server computing	1990s Internet applications	2000s Cloud computing
				
Client	▸ Minimal processing power, display only	▸ Strong client processing ▸ Some data stored/processed on client	▸ Strong client, but not used for processing ▸ Unstructured data (photos, documents) stored on client	▸ Minimal processing power needed (smartphones, etc)
Server	▸ Strong central processing ▸ Data stored centrally	▸ Some data stored / processed on client	▸ Processing done centrally	▸ Processing and data storage takes place centrally

```
D I S P L A Y   C U S T O M E R   I N F O R M A T I O N          Acct # B10093

  Credit Limit:$     0    Finance Charge? Y    Area:       Sort Codes: B

                  BILLING                                  SHIPPING
   Name: A CLEAN WELL LIGHTED PLACE FOR       Name: A CLEAN WELL LIGHTED PLACE FOR
Address: 601 VAN NESS AVENUE               Address: 601 VAN NESS AVENUE
       :                                          :
       :                                          :
   City: SAN FRANCISCO                        City: SAN FRANCISCO
  State: CA                                  State: CA
    Zip: 94102                                 Zip: 94102
Country: U.S.A                             Country:

  Phone:                                     Phone:

          Enter ↑ to skip back, ↓ to skip forward, or <ESC> to exit
```

Cloud computing trends

By 2020, cloud adoption will dominate IT and become the new normal

- In the last five to six years, cloud services have emerged and gained a rapid foothold.
- Key challenges over the initial period focused on:
  - The uncertainty of where data was going and who had access to this data
  - How to secure infrastructure owned by cloud service providers
  - How to regulate cloud computing
- With the publication of cloud security standards and reference architectures by NIST, ISO and the DoD (among others), companies have begun to adopt cloud strategies at an increasing rate.



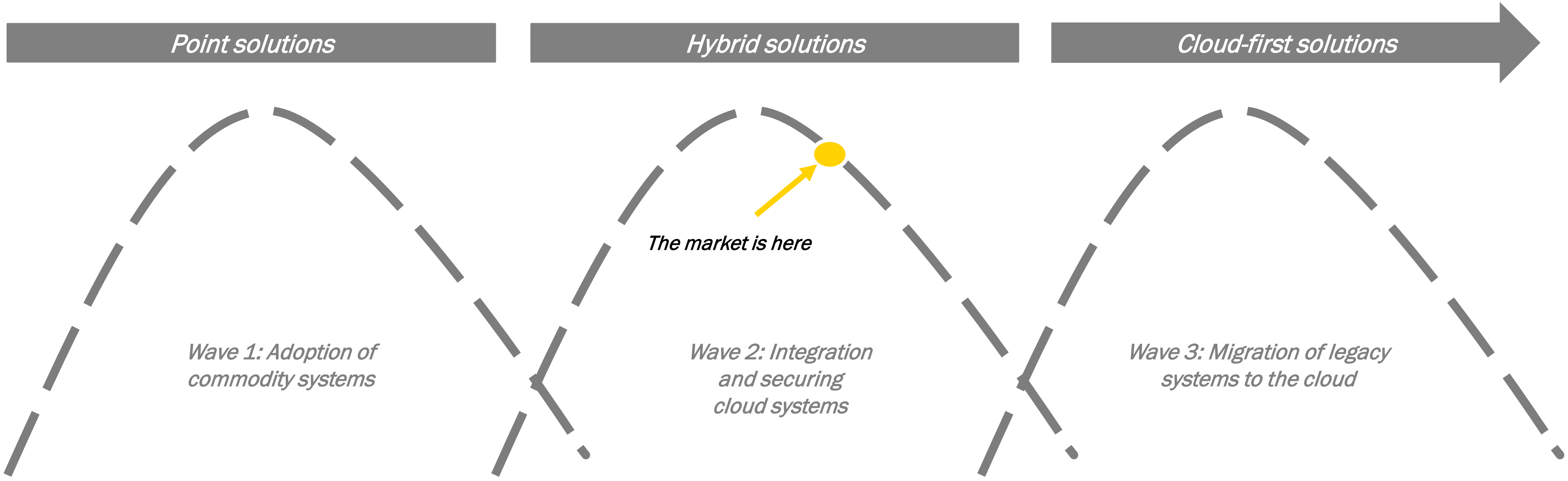
Emergence
"Prove the technology"
Slow Adoption
Skepticism - Caution - Discomfort

Development
"Remove the Obstacles"
Rapid Adoption
Familiarity - Understanding - Increased Control

Maturity
"The New Normal"
Widespread Adoption
Common place - Proficiency - Mastering

Emergence of "X-as-a-Service"
Microsoft Azure becomes commercially available
NIST publishes Reference Architecture
Software vendors begin releasing Enterprise DevOps tools
Hybrid Cloud model gains popularity
DoD publishes Cloud Computing Security Requirements
Adoption of IaaS becomes more mainstream
Rise of shared enterprise business services
Internet of Things
Cloud predicted to be 30% of all IT
Predictive Resource Balancing
Ubiquitous Computing
Adaptive User Experience
2010
2015
2020
2025
Time

With every wave of adoption, there are unique set of challenges


Point solutions
Hybrid solutions
Cloud-first solutions
The market is here
Wave 1: Adoption of commodity systems
Wave 2: Integration and securing cloud systems
Wave 3: Migration of legacy systems to the cloud

Wave 1 challenges faced:

- Cloud strategy development
- Software as a service (SaaS) implementation
- Infrastructure as a service (IaaS) implementation

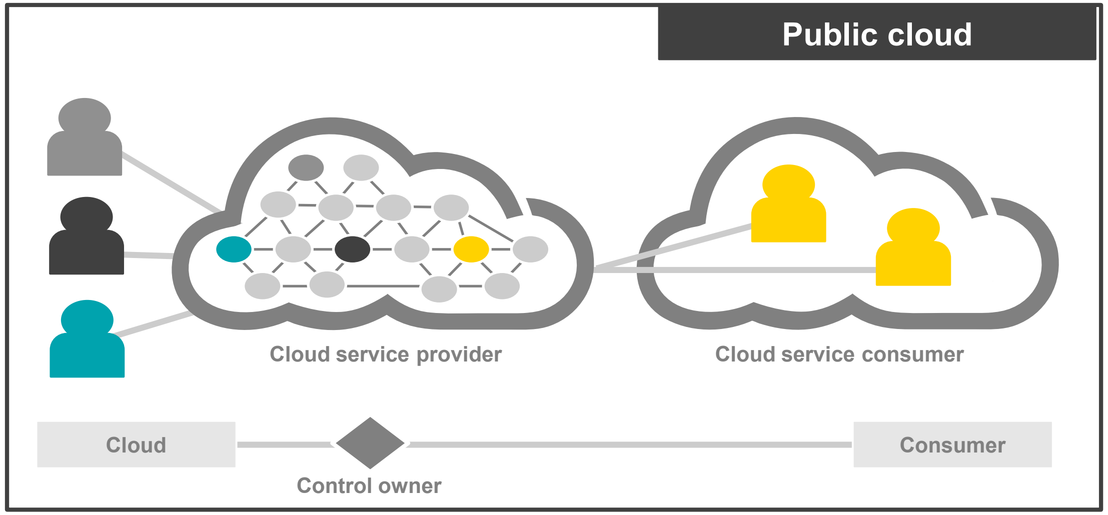
Wave 2 challenges faced:

- Cloud governance
- IT operating model evolution
- Hybrid architectures
- SaaS integration
- Cloud security
- Data center evolution

Wave 3 challenges faced:

- Vertical platform as a service (PaaS) solutions
- Identity and access management
- Business continuity management
- Service management integration
- IT as a Service (ITaaS)

Typical cloud computing implementation models



Public cloud

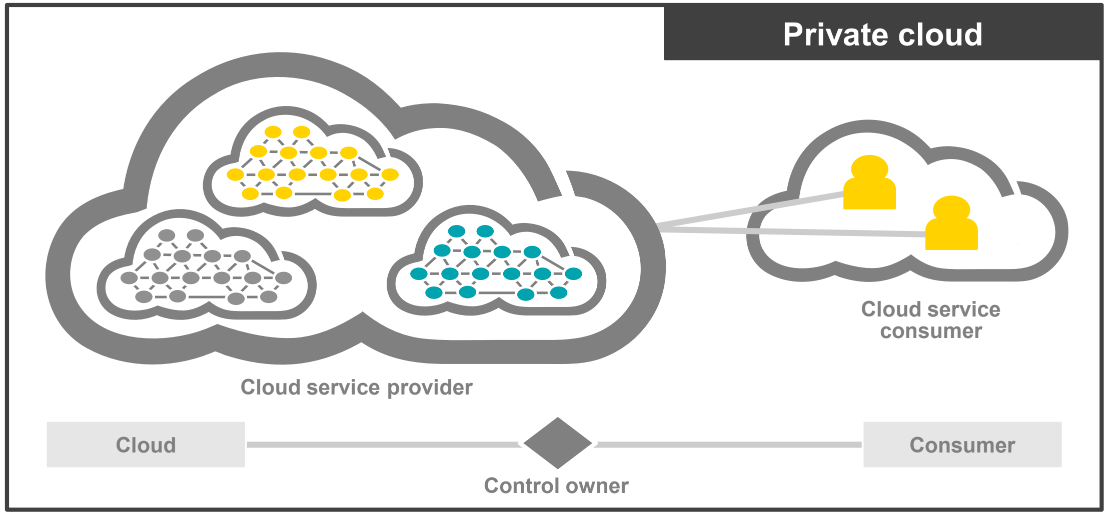
Cloud service provider

Cloud service consumer

Cloud

Consumer

Control owner



Private cloud

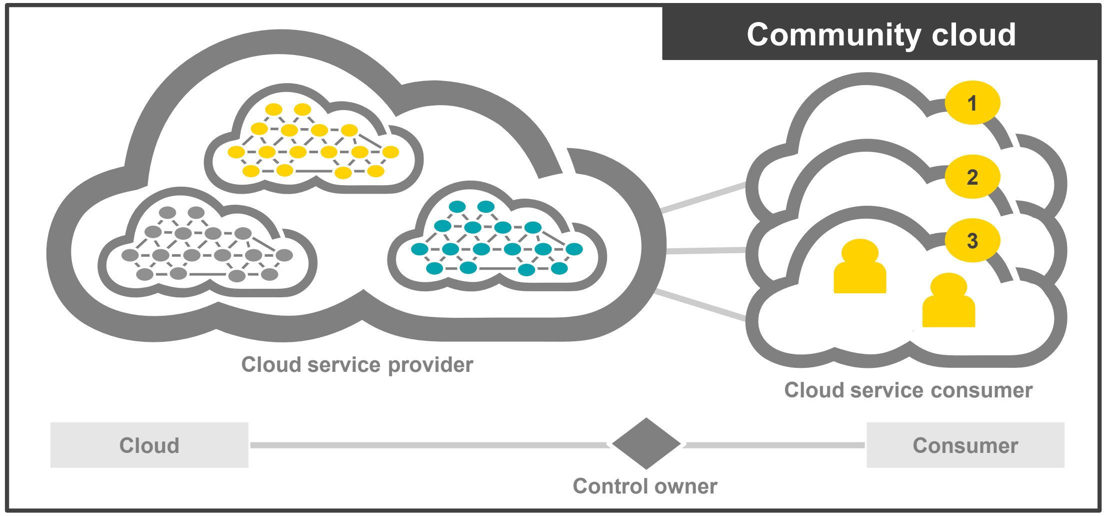
Cloud service provider

Cloud service consumer

Cloud

Consumer

Control owner



Community cloud

1

2

3

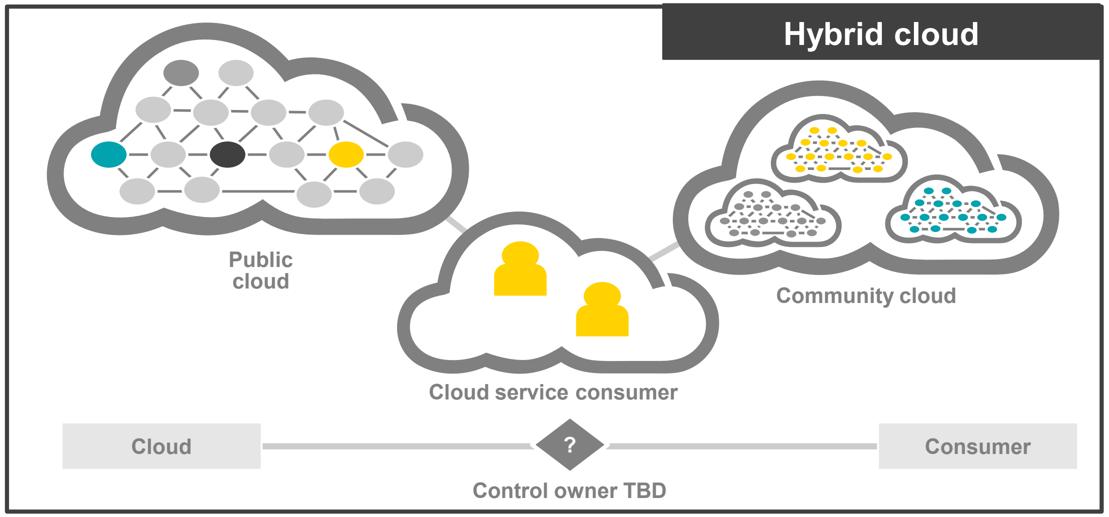
Cloud service provider

Cloud service consumer

Cloud

Consumer

Control owner



Hybrid cloud

Public cloud

Community cloud

Cloud service consumer

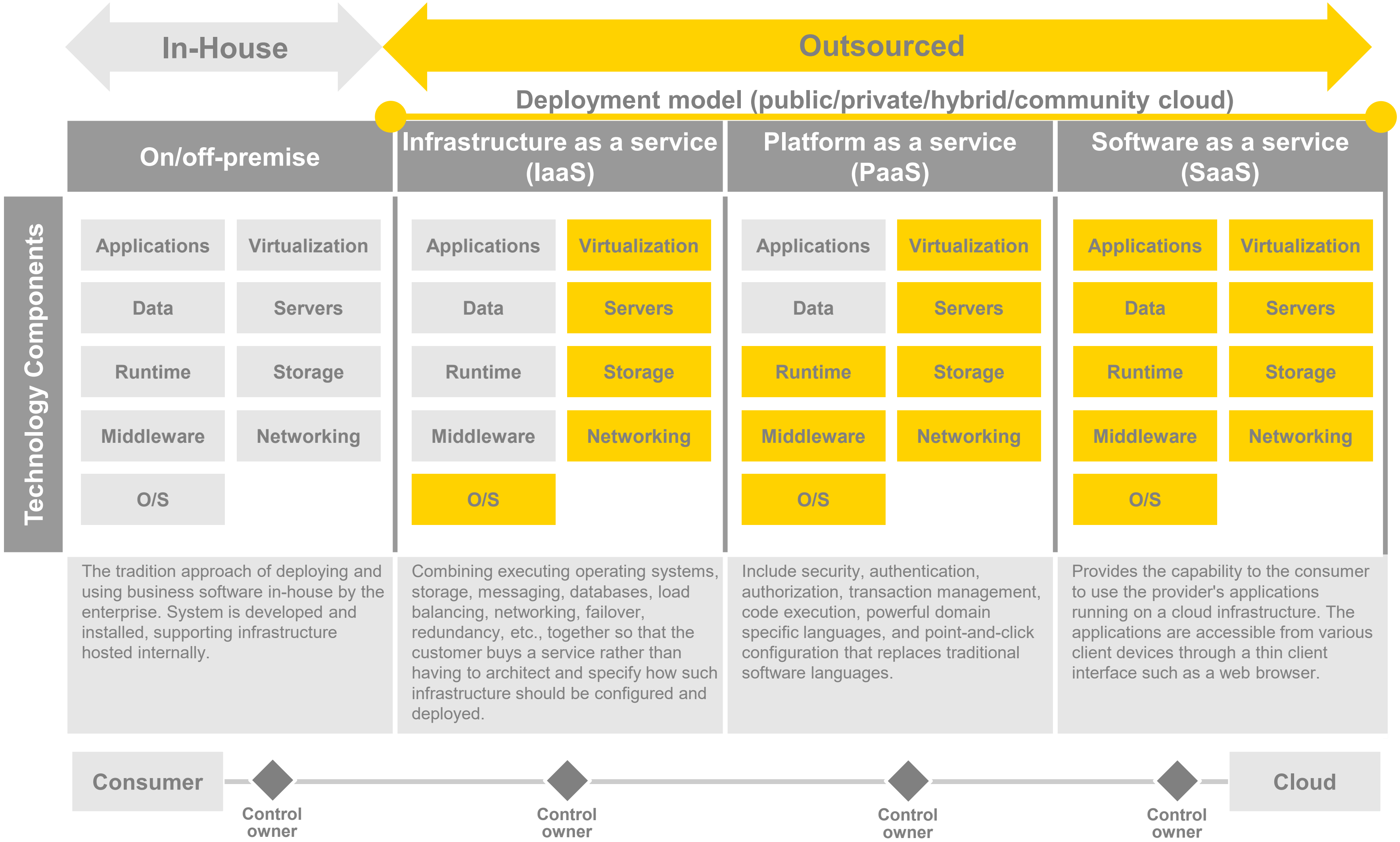
Cloud

?

Consumer

Control owner TBD

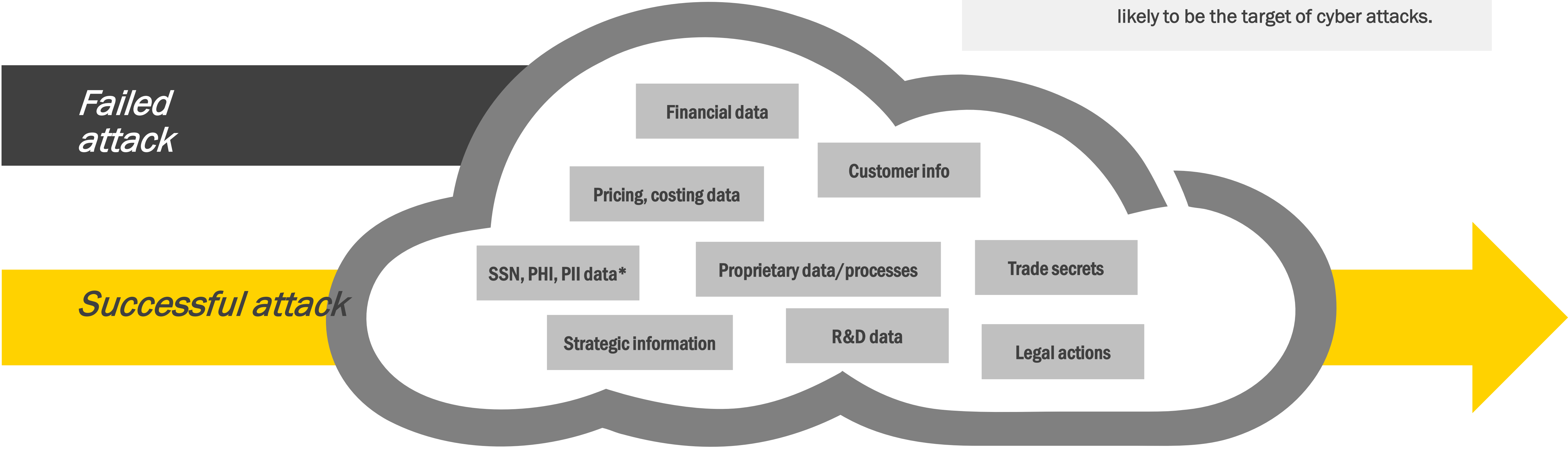
The type of services you implement changes the controls you need



	On/off-premise	Infrastructure as a service (IaaS)	Platform as a service (PaaS)	Software as a service (SaaS)
Technology Components	Applications Virtualization Data Servers Runtime Storage Middleware Networking O/S	Applications Virtualization Data Servers Runtime Storage Middleware Networking O/S	Applications Virtualization Data Servers Runtime Storage Middleware Networking O/S	Applications Virtualization Data Servers Runtime Storage Middleware Networking O/S
	The tradition approach of deploying and using business software in-house by the enterprise. System is developed and installed, supporting infrastructure hosted internally.	Combining executing operating systems, storage, messaging, databases, load balancing, networking, failover, redundancy, etc., together so that the customer buys a service rather than having to architect and specify how such infrastructure should be configured and deployed.	Include security, authentication, authorization, transaction management, code execution, powerful domain specific languages, and point-and-click configuration that replaces traditional software languages.	Provides the capability to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser.

Does cloud create a better, stronger fortress or easier access to the crown jewels?

Our research indicates that cloud solutions are more likely to be the target of cyber attacks.



Failed attack

Successful attack

Financial data

Customer info

Pricing, costing data

SSN, PHI, PII data*

Proprietary data/processes

Trade secrets

Strategic information

R&D data

Legal actions

Cloud providers consistently invest in enhancing the security controls of their solutions.

* Social security number, personal health information, personally identifiable information

Cloud computing security considerations

Typical areas under consideration	
Privileged user access	Who will have access to customer data? What controls are in place to restrict this access?
Regulatory compliance	How will using the cloud affect the ability to comply with regulatory requirements? Is there a independent third party audit or certification conducted?
Data location and ownership	Where will the data be stored? Will it be replicated out of the country? Can the customer restrict where the data is stored? Who owns the data once it is in the cloud?
Data segregation	How can the provider demonstrate that its other customers cannot "see" the user's data? What kind of encryption is in place? How are the keys managed?
Recovery	What happens to the user data in the event of a disaster? Is it backed up or replicated somewhere else? How are backups accessed? How long does it take to restore the user data?
Investigative support	If there is any kind of legal investigation, can the provider give me the investigation agencies the data support needed?
Notification of third-party data requests	If law enforcement asks the provider for user data, does the provider have an obligation to notify the user? What if it is instructed not to?

Cloud service provider control scale

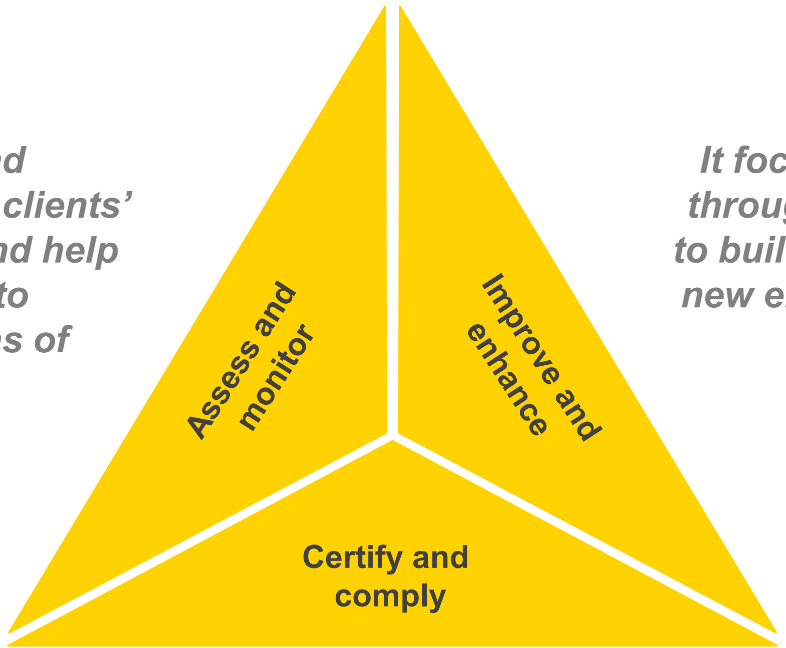
Minimum
Balanced
Rigorous

- Not all cloud service providers offer the same level of controls and subsequent trust levels.
- There is no wrong answer as to what is best for the needs of a cloud consumer; it depends on the requirements of what is being moved to the cloud.
- More rigorous control environments are required for mission-critical applications, infrastructure and platforms.
- **New encryption techniques (e.g: Hidden Vector Encryption, Predicatum Encryption)**

EY’s Cloud Trust Services Framework enables a secure, trusted and audit-ready environment

EY Cloud Trust Services Framework

It aims to evaluate and periodically examine clients’ current risk profile and help them develop a plan to address any key areas of exposure.



It focus on guiding clients through a maturity journey to build trust by developing new enhanced capabilities.

Its objective is to promote a compliant and audit-ready environment for clients via certification, proactive audits and agreed-upon procedures.

Thank You

EY

Building a better
working world