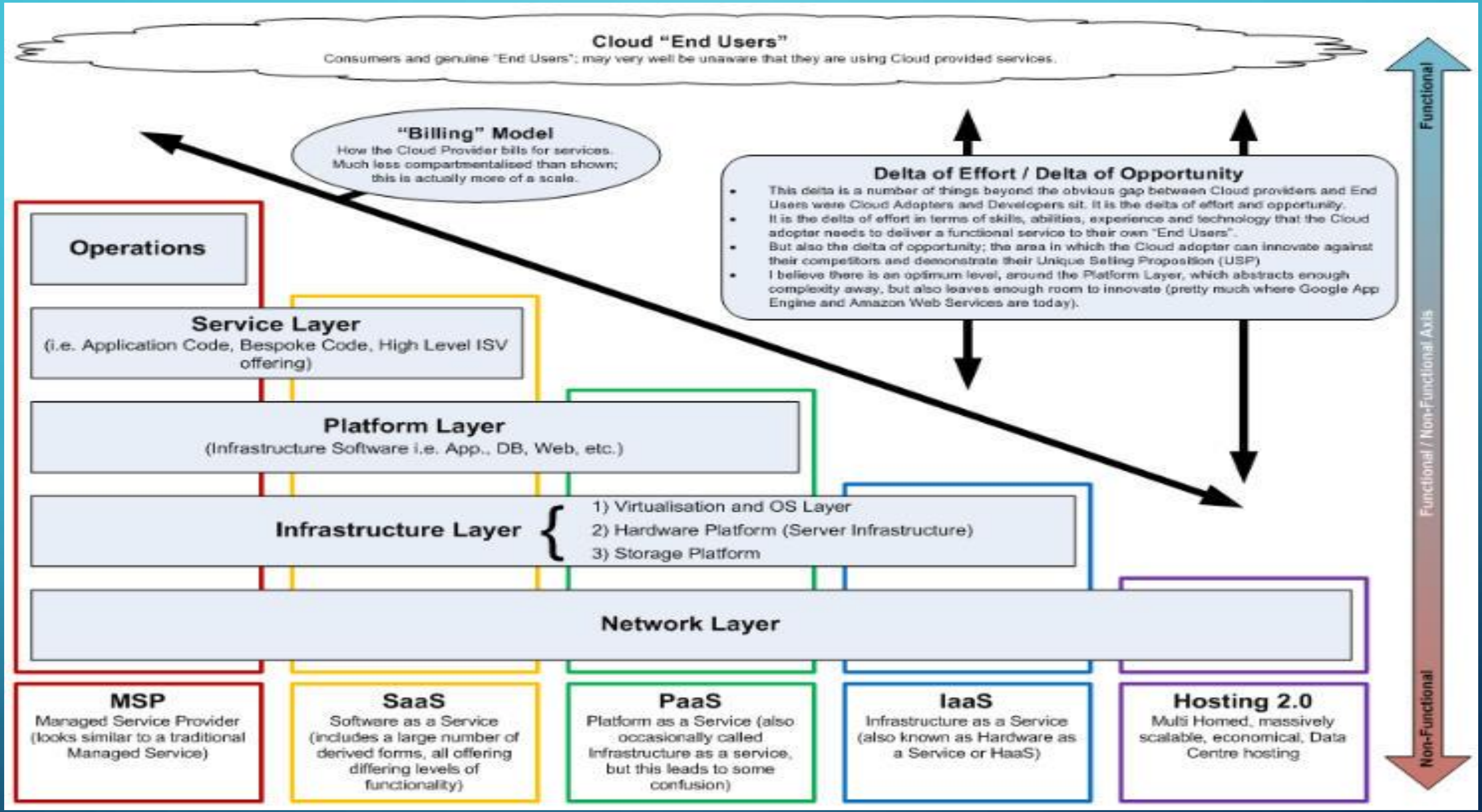
Cloud Computing for Commercial Enterprises

Dorphus Williams,
Aissatou Barry
& Moussa Samake

WHAT IS CLOUD COMPUTING?

- Cloud computing is a general term for the delivery of hosted services, compute power, database storage, applications, and other IT resources through a cloud services over the internet



Cloud "End Users"

Consumers and genuine "End Users"; may very well be unaware that they are using Cloud provided services.

"Billing" Model

How the Cloud Provider bills for services.
Much less compartmentalised than shown;
this is actually more of a scale.

Delta of Effort / Delta of Opportunity

- This delta is a number of things beyond the obvious gap between Cloud providers and End Users were Cloud Adopters and Developers sit. It is the delta of effort and opportunity.
- It is the delta of effort in terms of skills, abilities, experience and technology that the Cloud adopter needs to deliver a functional service to their own "End Users".
- But also the delta of opportunity; the area in which the Cloud adopter can innovate against their competitors and demonstrate their Unique Selling Proposition (USP)
- I believe there is an optimum level, around the Platform Layer, which abstracts enough complexity away, but also leaves enough room to innovate (pretty much where Google App Engine and Amazon Web Services are today).

Operations

Service Layer
(i.e. Application Code, Bespoke Code, High Level ISV offering)

Platform Layer
(Infrastructure Software i.e. App., DB, Web, etc.)

Infrastructure Layer {
1) Virtualisation and OS Layer
2) Hardware Platform (Server Infrastructure)
3) Storage Platform

Network Layer

MSP
Managed Service Provider (looks similar to a traditional Managed Service)

SaaS
Software as a Service (includes a large number of derived forms, all offering differing levels of functionality)

PaaS
Platform as a Service (also occasionally called Infrastructure as a service, but this leads to some confusion)

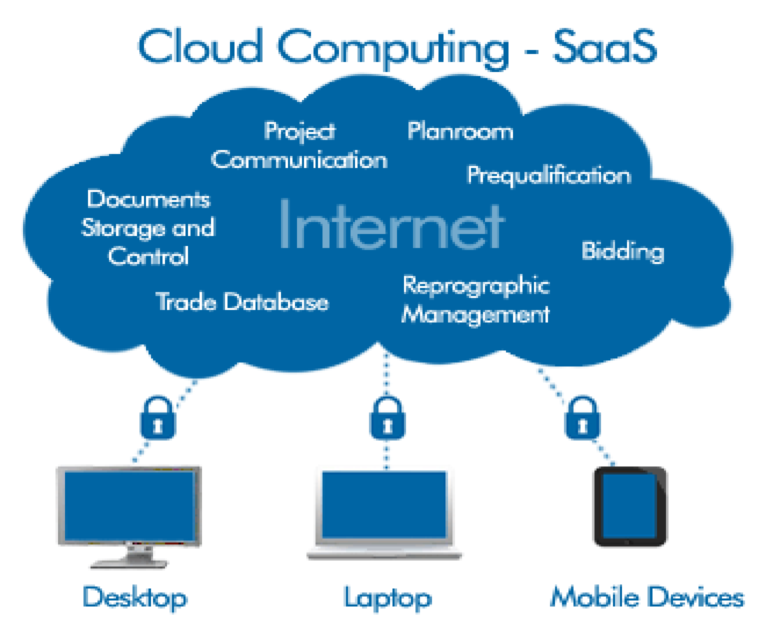
IaaS
Infrastructure as a Service (also known as Hardware as a Service or HaaS)

Hosting 2.0
Multi Homed, massively scalable, economical, Data Centre hosting

SOFTWARE AS A SERVICE {SAAS}

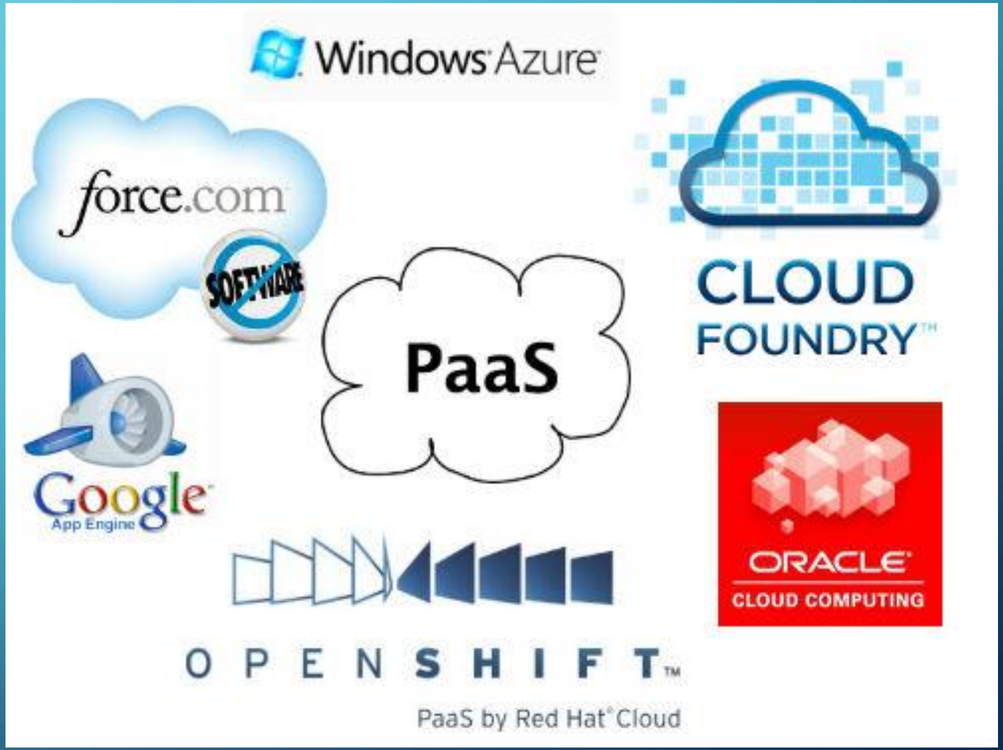
- Software as a Service (SaaS) - SaaS is a model that delivers software applications over the internet; these applications are often called web services. Users can access SaaS applications and services from any location using a computer or mobile device that has internet access.

- Example : Microsoft Office 365



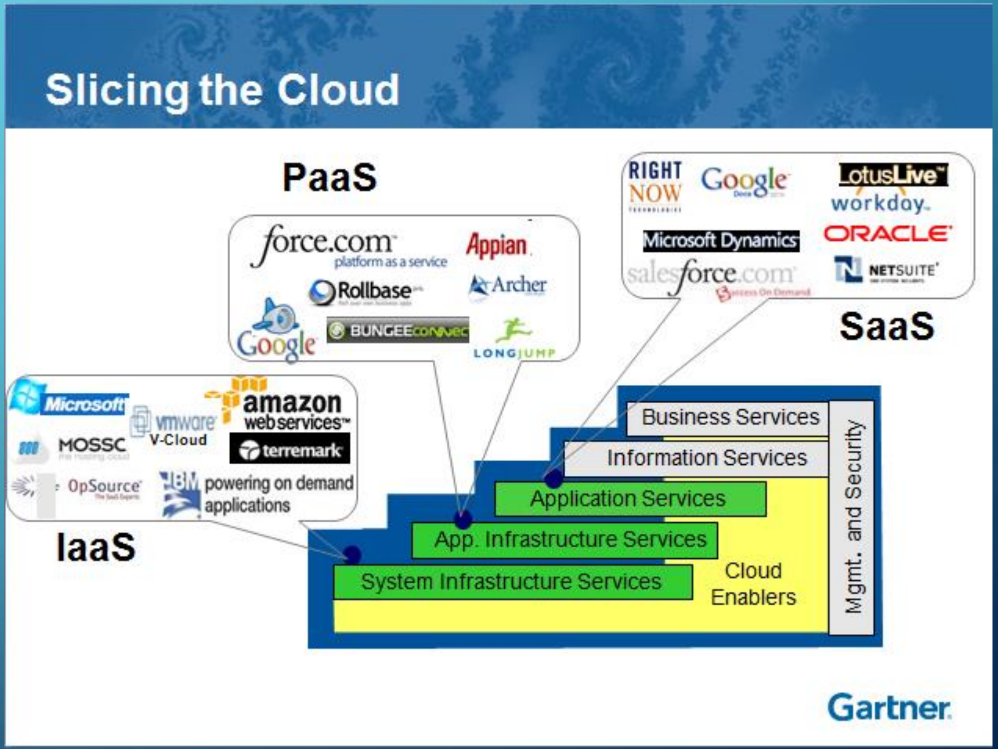
PLATFORM AS A SERVICE {PAAS}

- Platform as a Service (PaaS) - In the PaaS model, cloud provider delivers hardware and software tools -- usually those needed for application development -- to its users as a service.
- A PaaS provider hosts the hardware and software on its own infrastructure. As a result, PaaS frees users from having to install in-house hardware and software to develop or run a new application.
- Example : Elastic Beanstalk and Google App Engine.

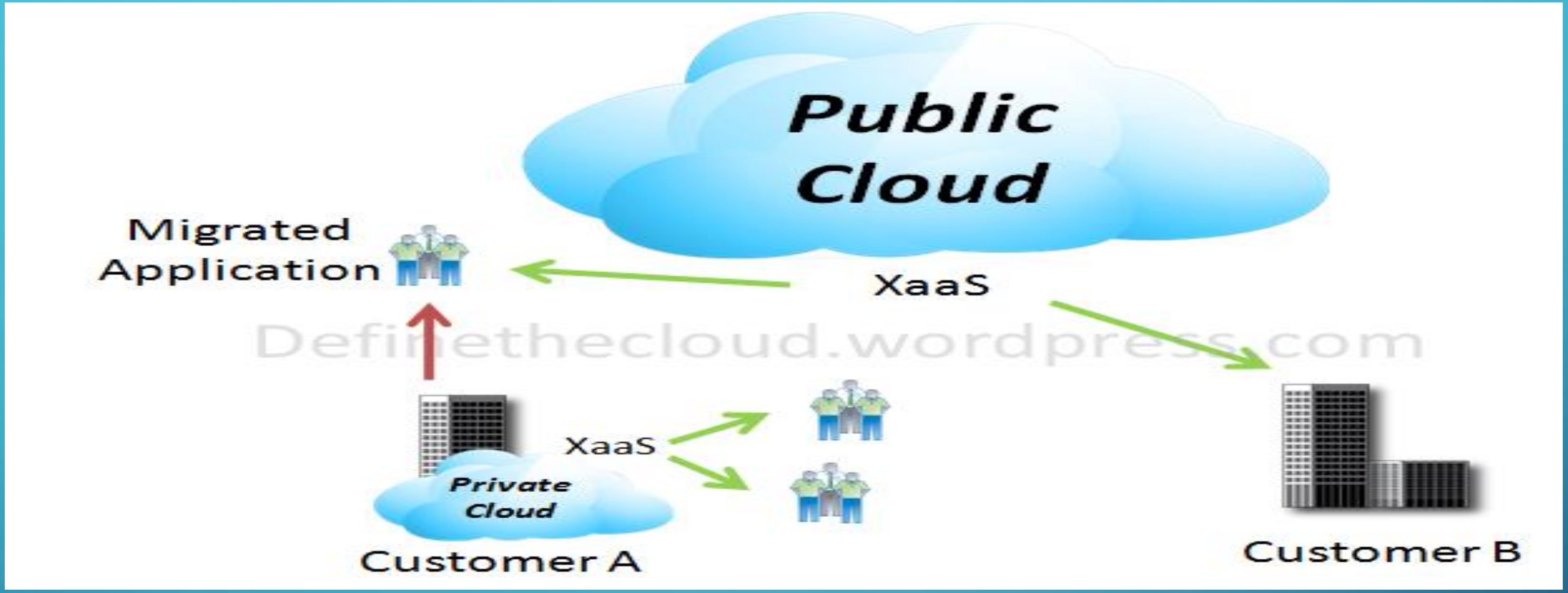


INFRASTRUCTURE AS A SERVICE {IAAS}

- Infrastructure as a Service (IaaS) - IaaS providers, such as AWS, supply a virtual server instance and storage, as well as application program interfaces (APIs) that let users migrate workloads to a virtual machine. Users have an allocated storage capacity and can start, stop, access and configure the VM and storage as desired.
- Examples – Amazon Web Services (AWS)

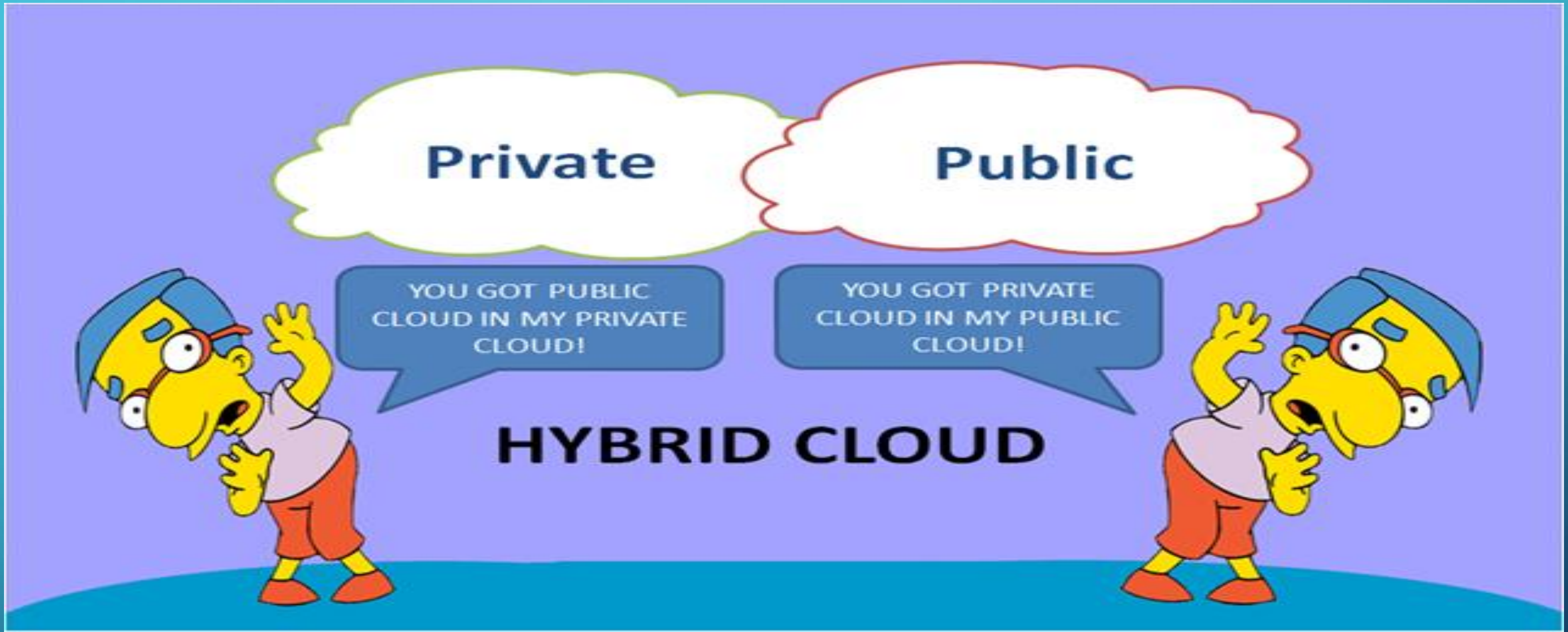


PUBLIC CLOUD



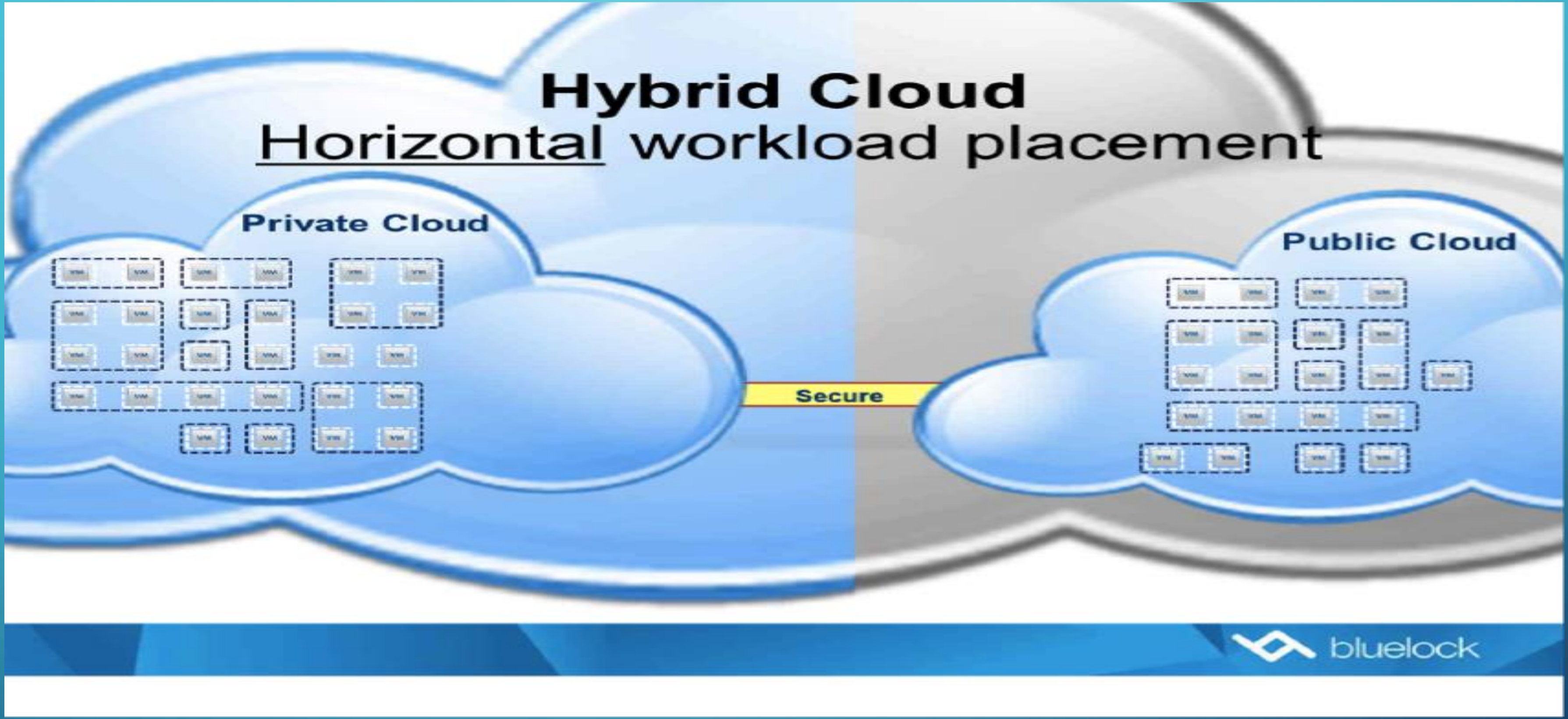
- A public cloud service is built on an external platform run by a cloud-service provider. The provider offers everything from system resources to the security and maintenance of your cloud system.
- It tends to be managed by an outside company specializing in cloud services for a large range of customers. So, users get their own cloud within a shared infrastructure.

PRIVATE CLOUD


Private
Public
YOU GOT PUBLIC CLOUD IN MY PRIVATE CLOUD!
YOU GOT PRIVATE CLOUD IN MY PUBLIC CLOUD!
HYBRID CLOUD

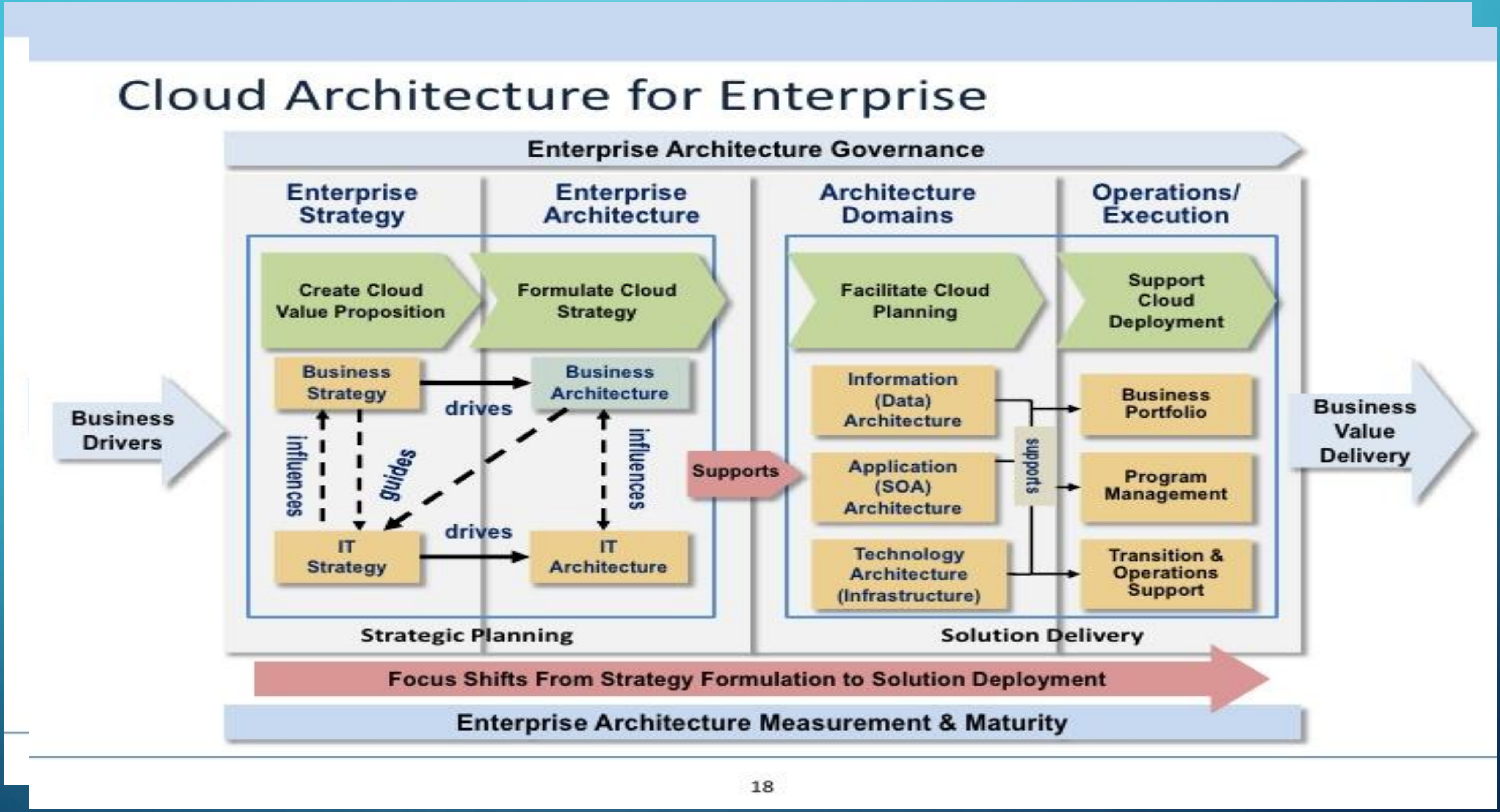
- A private cloud service is a cloud platform built within your own walls on your own hardware and software. Private cloud service, however, organizations build their own data centres.
- Since a private cloud is managed by your own internal IT team, it is ideal for businesses that deals with Highly Confidential Information, more flexibility and greater control over their cloud.

HYBRID CLOUD



- A hybrid cloud service employs both private and public clouds. An organization's own IT team manages part of the cloud in-house and the rest off-site.
- Ideally organization's own IT team manages the Most Important and sensitive information(Private Cloud) while the less-sensitive is in the Public Cloud(3rd Party)

Choosing the Right Cloud for the Enterprise



Cloud Architecture for Enterprise

Enterprise Architecture Governance

Business Drivers

Enterprise Strategy

Enterprise Architecture

Architecture Domains

Operations/ Execution

Create Cloud Value Proposition

Formulate Cloud Strategy

Facilitate Cloud Planning

Support Cloud Deployment

Business Strategy

drives

Business Architecture

influences

guides

influences

IT Strategy

drives

IT Architecture

Supports

Information (Data) Architecture

Application (SOA) Architecture

Technology Architecture (Infrastructure)

supports

Business Portfolio

Program Management

Transition & Operations Support

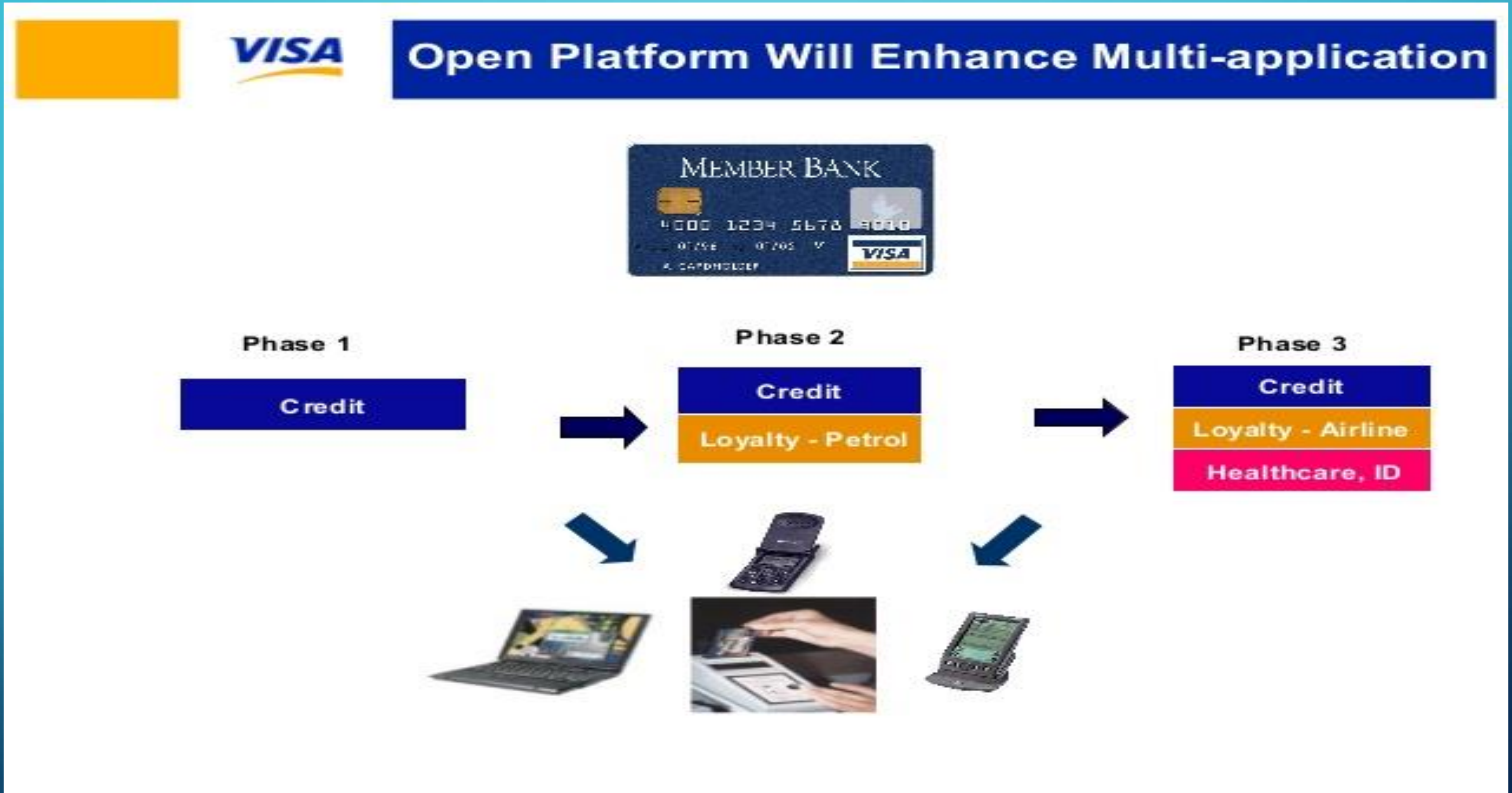
Business Value Delivery

Strategic Planning

Solution Delivery

Focus Shifts From Strategy Formulation to Solution Deployment

Enterprise Architecture Measurement & Maturity



Open Platform Will Enhance Multi-application

Phase 1

Credit

Phase 2

Credit

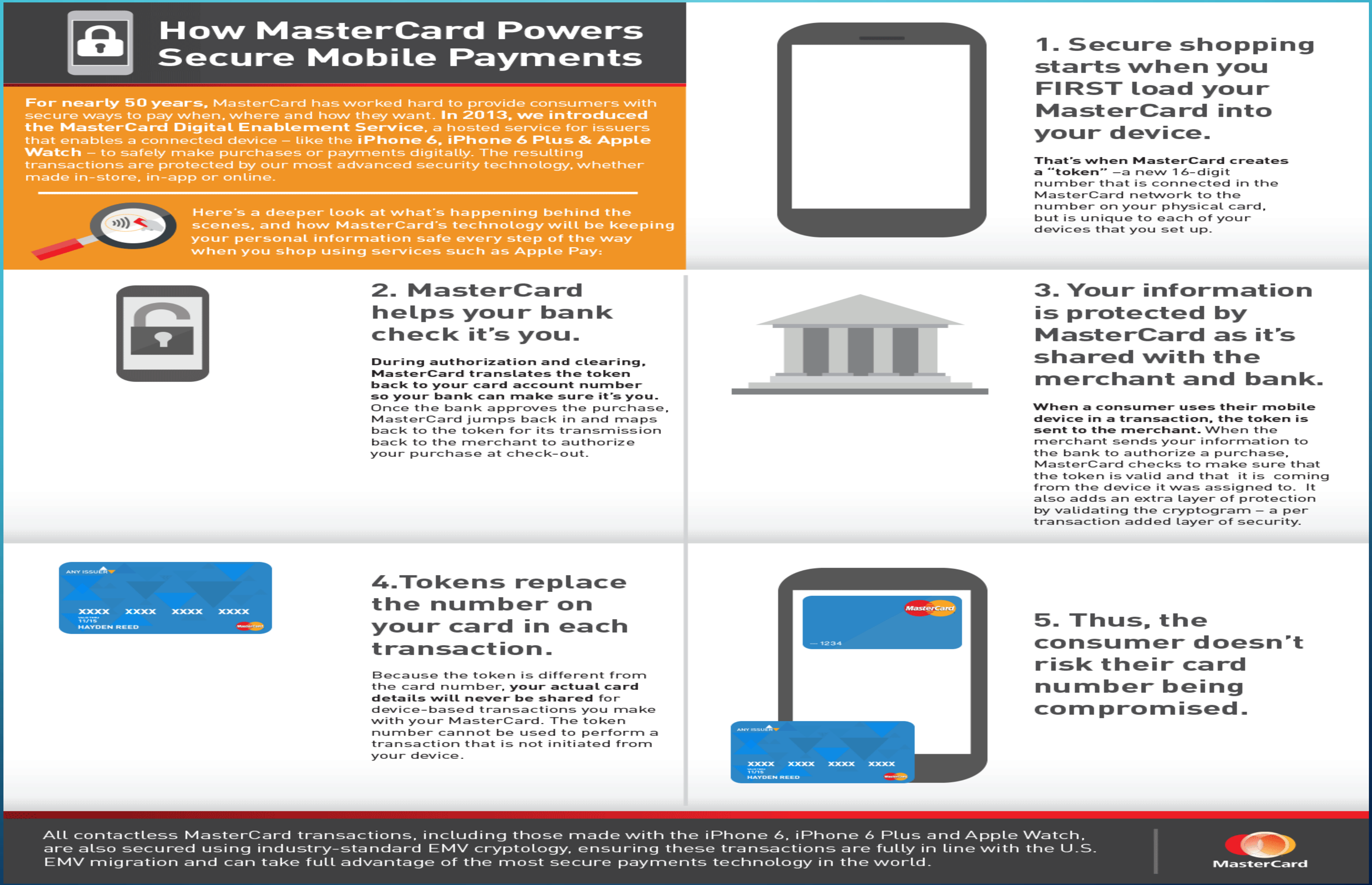
Loyalty - Petrol

Phase 3

Credit

Loyalty - Airline

Healthcare, ID



ANY ISSUER
XXXX XXXX XXXX XXXX
11/15
HAYDEN REED
MasterCard
···· 1234

How MasterCard Powers Secure Mobile Payments

For nearly 50 years, MasterCard has worked hard to provide consumers with secure ways to pay when, where and how they want. **In 2013, we introduced the MasterCard Digital Enablement Service**, a hosted service for issuers that enables a connected device – like the **iPhone 6, iPhone 6 Plus & Apple Watch** – to safely make purchases or payments digitally. The resulting transactions are protected by our most advanced security technology, whether made in-store, in-app or online.

Here's a deeper look at what's happening behind the scenes, and how MasterCard's technology will be keeping your personal information safe every step of the way when you shop using services such as Apple Pay:

1. Secure shopping starts when you FIRST load your MasterCard into your device.

That's when MasterCard creates a "token" –a new 16-digit number that is connected in the MasterCard network to the number on your physical card, but is unique to each of your devices that you set up.

2. MasterCard helps your bank check it's you.

During authorization and clearing, MasterCard translates the token back to your card account number so your bank can make sure it's you. Once the bank approves the purchase, MasterCard jumps back in and maps back to the token for its transmission back to the merchant to authorize your purchase at check-out.

3. Your information is protected by MasterCard as it's shared with the merchant and bank.

When a consumer uses their mobile device in a transaction, the token is sent to the merchant. When the merchant sends your information to the bank to authorize a purchase, MasterCard checks to make sure that the token is valid and that it is coming from the device it was assigned to. It also adds an extra layer of protection by validating the cryptogram – a per transaction added layer of security.

4.Tokens replace the number on your card in each transaction.

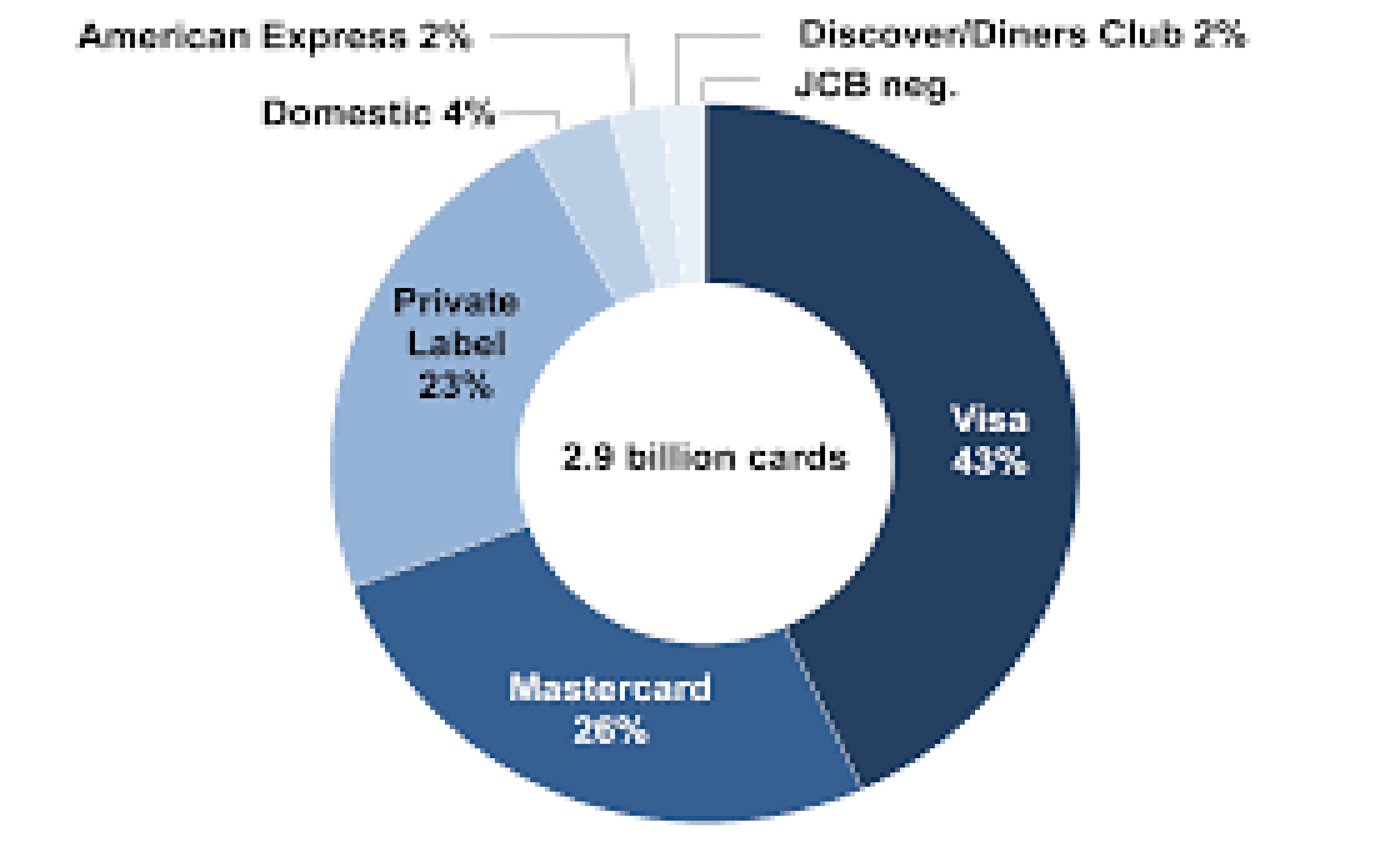
Because the token is different from the card number, **your actual card details will never be shared** for device-based transactions you make with your MasterCard. The token number cannot be used to perform a transaction that is not initiated from your device.

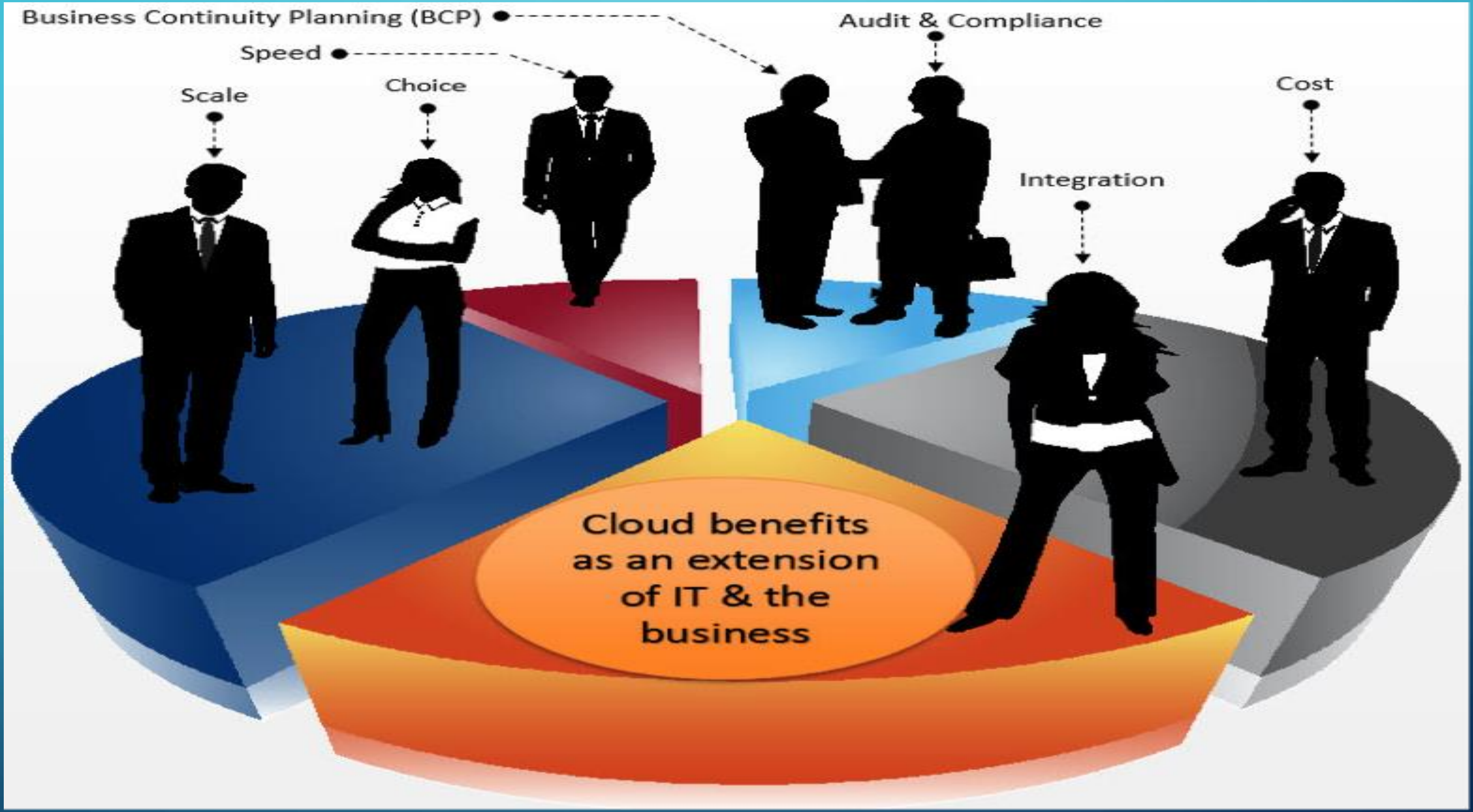
5. Thus, the consumer doesn't risk their card number being compromised.

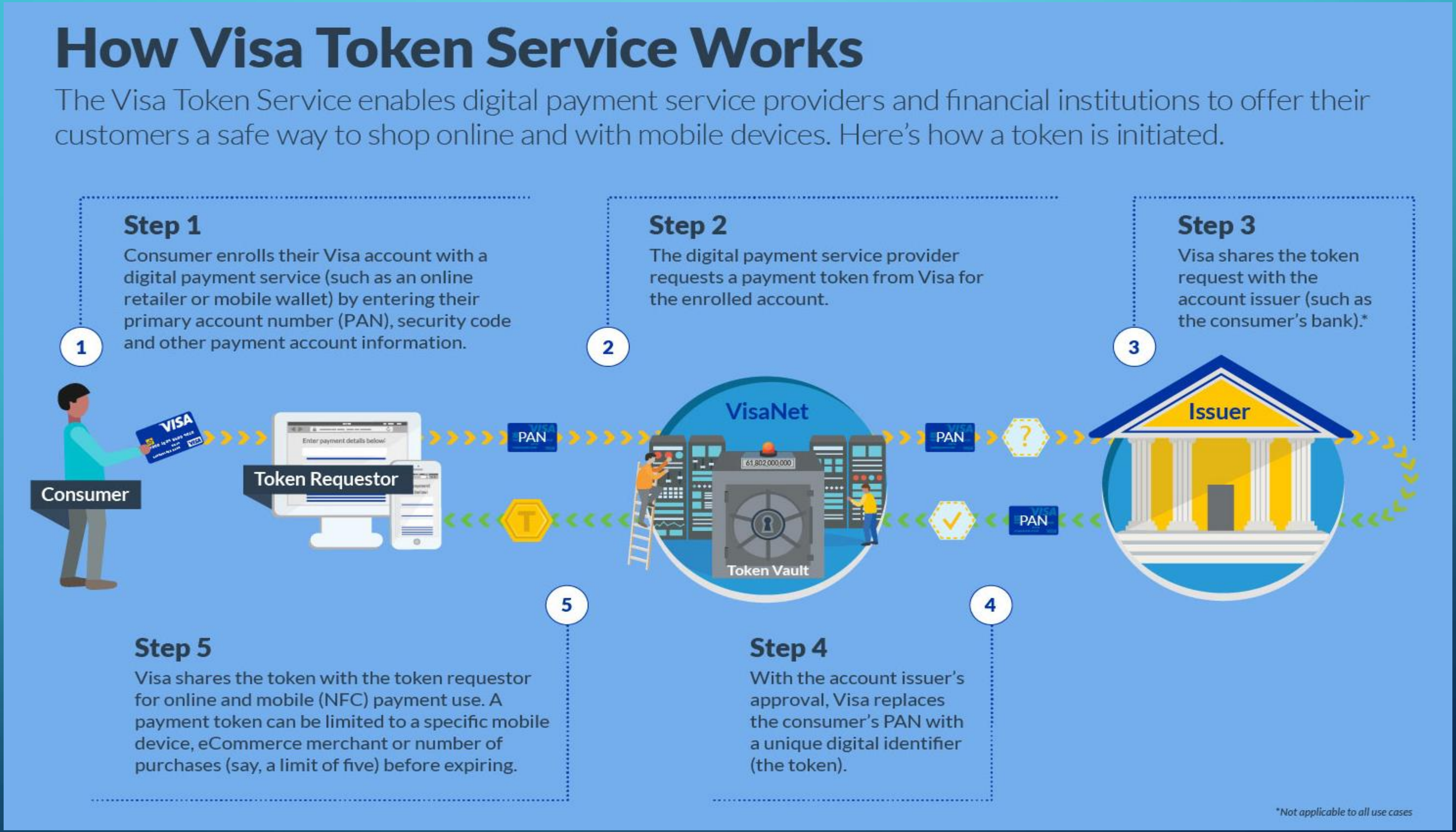
All contactless MasterCard transactions, including those made with the iPhone 6, iPhone 6 Plus and Apple Watch, are also secured using industry-standard EMV cryptology, ensuring these transactions are fully in line with the U.S. EMV migration and can take full advantage of the most secure payments technology in the world.

MasterCard

Banking Technology




Business Continuity Planning (BCP)
Speed
Scale
Choice
Audit & Compliance
Cost
Integration
Cloud benefits as an extension of IT & the business



How Visa Token Service Works

The Visa Token Service enables digital payment service providers and financial institutions to offer their customers a safe way to shop online and with mobile devices. Here's how a token is initiated.

Step 1

Consumer enrolls their Visa account with a digital payment service (such as an online retailer or mobile wallet) by entering their primary account number (PAN), security code and other payment account information.

Step 2

The digital payment service provider requests a payment token from Visa for the enrolled account.

Step 3

Visa shares the token request with the account issuer (such as the consumer's bank).*

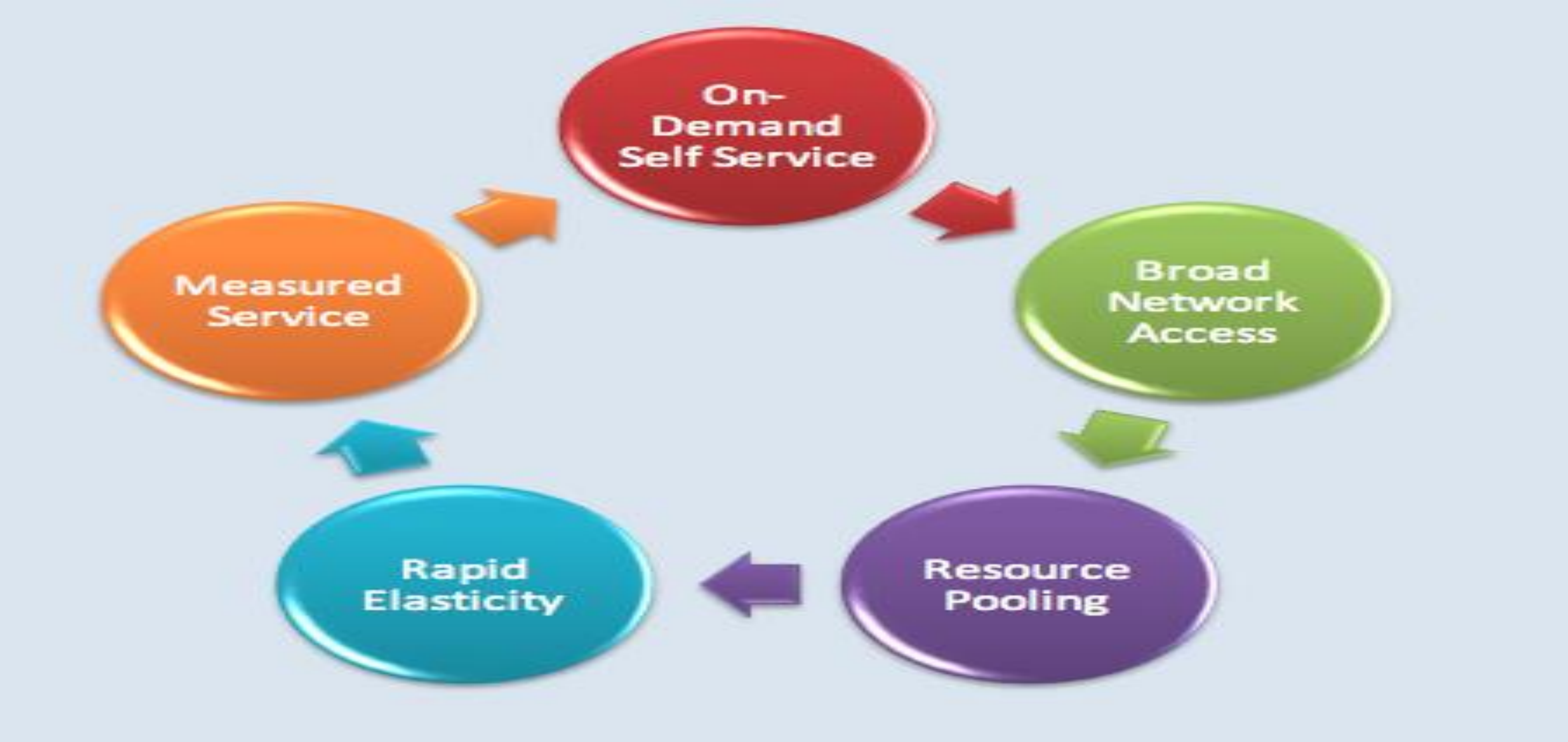
Step 5

Visa shares the token with the token requestor for online and mobile (NFC) payment use. A payment token can be limited to a specific mobile device, eCommerce merchant or number of purchases (say, a limit of five) before expiring.

Step 4

With the account issuer's approval, Visa replaces the consumer's PAN with a unique digital identifier (the token).

*Not applicable to all use cases



On-Demand Self Service

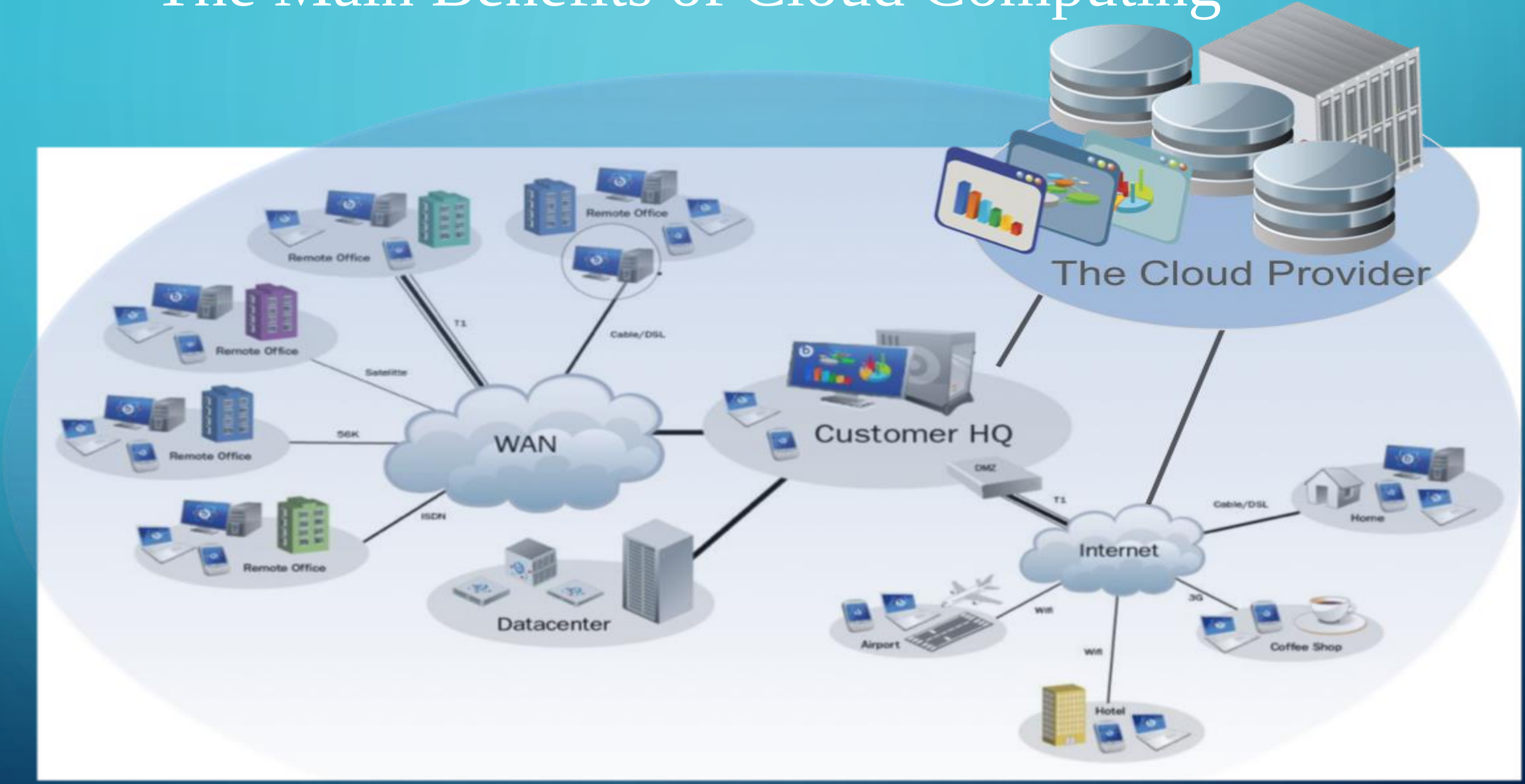
Broad Network Access

Resource Pooling

Rapid Elasticity

Measured Service

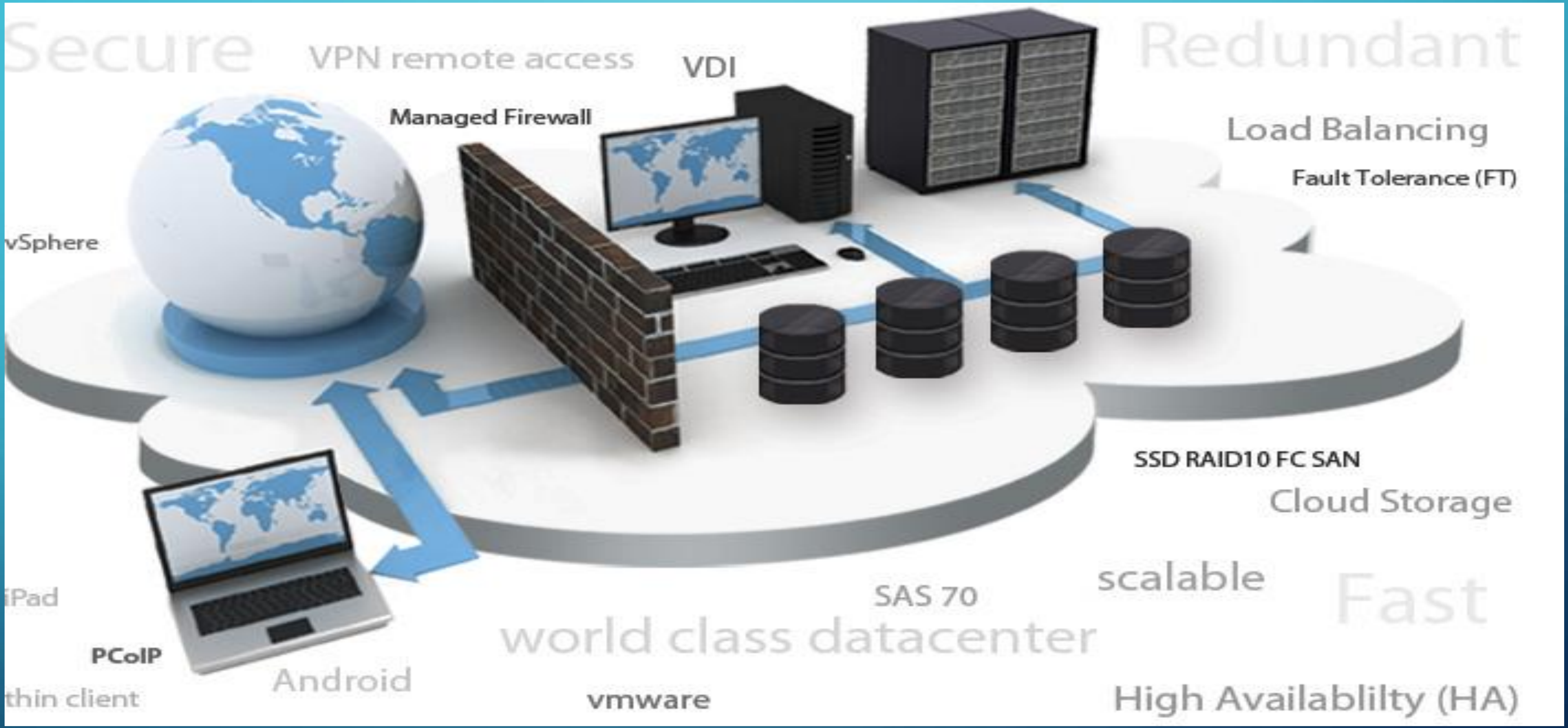
The Main Benefits of Cloud Computing



MAIN BENEFITS OF CLOUD COMPUTING

- **Flexibility:** Companies can scale up as computing needs increase and scale down again as demands decrease. This eliminates the need for massive investments in local infrastructure which may or may not remain active.
- **Pay per use:** allowing users to pay only for the resources and workloads they use. capital expenditures to operational expenditure. This lowers barriers to entry, allowing less capital required to start the business.
- **Connect form Anywhere :** It allows users to access systems using a web browser regardless of their location or what device they use . As infrastructure is off-site and accessed via the Internet, users can connect to it from anywhere

Security and Privacy Risk



SECURITY AND PRIVACY RISK

- Cloud computing poses privacy concerns because the service provider can access the data that is in the cloud at any time. It could accidentally or deliberately alter or even delete information
- Many cloud providers can share information with third parties if necessary for purposes of law and order even without a warrant. It tends to be permitted in their privacy policies, which users must agree to before they start using cloud services.
- There is the problem of legal ownership of the data (If a user stores some data in the cloud, can the cloud provider profit from it?). Many Terms of Service agreements are silent on the question of ownership.

SECURITY AND PRIVACY RISK

- Data loss is a common problem in cloud computing. If the cloud computing service provider close up his services due some financial or legal problem then here will be a loss of data for the user
- As cloud provider platform being shared by different user there may be possibility that information belonging to different customers reside on same data centre. Therefore Information leakage may arise as by mistake information for one customer is given to other
- Malicious insiders: include fraud, damage and theft or loss of confidential information caused by “trusted” insiders.
- Traffic hijacking: These threats include man-in- the-middle attacks, spam campaigns and denial-of-service attacks.