

DISRUPTION

ENTERPRISE CYBER SECURITY

DEPLOYMENT

OVERVIEW

- understand the different deployment architectures for an enterprise.
- security concerns surrounding different deployment options.
- potential legal, ethical and social issues surrounding such deployments.

DEPLOYMENT



Capital



Operational



Mixture

DEPLOYMENT CONTEXT

- capital expenditure refers to significant investment in actual systems, software and infrastructure.
- operational expenditure refers to expense of paying for the use of systems, software and infrastructure.
- enterprises can opt for a mix model, in cloud computing, that affords some of both.

DEPLOYMENT CONTEXT

- many deployment options are perceived as an opportunity to focus on core competencies and outsource necessities.
- managed service providers can provide bespoke, operation solutions that can support emerging subsystems.
- complex compliance and other security concerns can be outsourced to experts.

CAPITAL VS OPERATIONAL

- capital expenditure represents significant investment but an organisation has greater control.
- operational expenditure affords an organisation greater ability without significant expense, but limited control.
- capital expenditure can be a significant hurdle to many organisations and may stifle emerging subsystems.
- operational expenditure can prove expensive in the longer term and is not without some capital costs.

CAPITAL



CAPITAL MOTIVATION

- typical on-site deployment where an organisation **invests in hardware and software** systems.
- **within the perimeter** of the organisation and confidentiality should be easier to maintain.
- highly bespoke solution affords systems that are **tailored to the needs of the organisation**.
- efficient and effective use of information technology could make for a **highly competitive and secure subsystem**.

CONCERNS

- organisations need to recruit and sustain their own **specialist staff trained in security** to support bespoke systems.
- challenging to ensure **compliance, standards as well as defending against emerging threats**.
- **considerable investment** in terms of maintenance to ensure systems operate effectively.
- additional expense in terms of adding new systems or operations.

CONCERNS

- expense in terms of **maintaining backups** and recovery points for data.
- bespoke systems could simply represent an investment in products from **other companies**.
- **limited portability** in terms of switching away from one product to another product.
- **exposure to security problems** of the product themselves and reliant on the vendor.

OPERATIONAL



APPLICATION SERVICE PROVIDER (ASP)

- application service provider can support an organisation with access to specific applications.
- affords organisations access to latest versions of software.
- applications are typically limited, but can offer access without significant costs.
- investment may still be required in terms of hardware, software and other infrastructure.

APPLICATION SERVICE PROVIDER (ASP)

- data being processed and stored by the application could be **vulnerable in transit and rest**.
- critical data that is pertaining to clients as well as crucial to business is **beyond the perimeter**.
- **potential espionage** as any single provider could be managing data for any number of organisations.
- **poor visibility** of how data is processed and stored, potential impact on switching away.

MANAGED SERVICE PROVIDER (MSP)

- managed service providers can manage whole units for an enterprise or organisation.
- providers can manage entire infrastructure or aspects of it, including network and security, e.g. MSSP.
- can afford an organisation high-levels of support and access to highly trained staff.
- **Service Level Agreements (SLAs)** can be used to ensure priorities

MANAGED SERVICE PROVIDER (MSP)

- act as a **clearing house** for security and compliance for a specific domain.
- generic **compliance concerns** can be rapidly addressed as this can be addressed through the application.
- provider can **maintain security** for infrastructure, both physical security and operational security.
- provider can **maintain and monitors logs** as well as **duplicate** data for compliance and recovery purposes.

SERVICE LEVEL AGREEMENT (SLA)

- contract or **agreement between enterprise and provider** for minimum levels of service.
- clear **repercussions** for the provider if they do not meet the minimum levels of service.
- requirements that are considered, typically include **reliability** and **availability**.
- clear visibility of how such **requirements are monitored** and analysed by provider.

CONCERNS

CONCERNS

- concern over tie-in to a specific vendor delivering a crucial element of the business.
- potential culture clash between organisation and external provider could produce problems.
- sensitive data being shared outside of perimeter and potentially alongside other organisations.
- concerns over the quality of the provider in terms of staff, training and education.

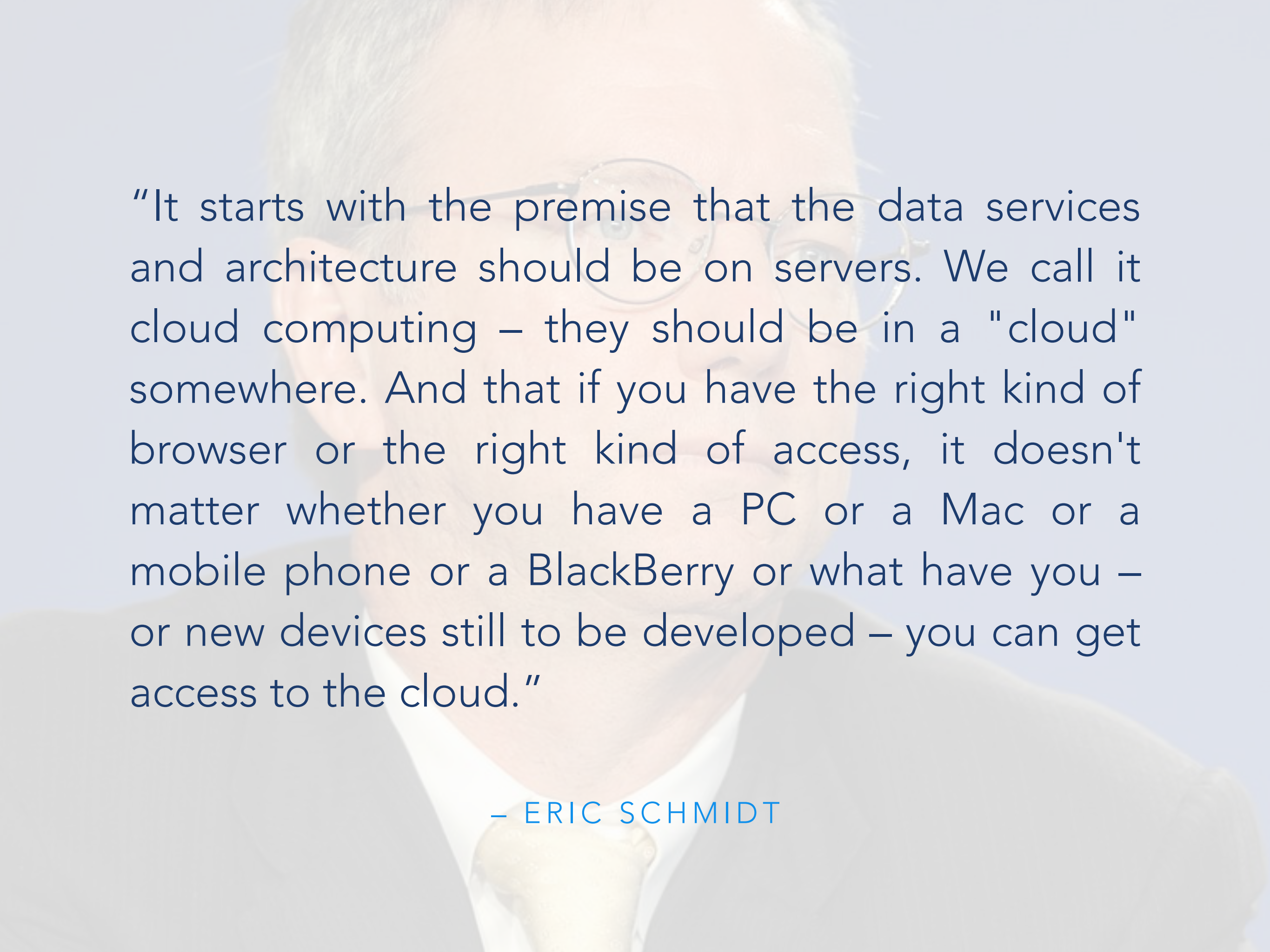


CLOUD COMPUTING

EDISON ELECTRIC LIGHT STATION

- not the world's first but certainly the most ambitious.
- businesses used to rely on their own infrastructure for energy.
- challenges faced in delivery, but rewards worth the effort.



A faded, light blue-tinted background image of Eric Schmidt, wearing glasses and a suit, looking directly at the camera.

"It starts with the premise that the data services and architecture should be on servers. We call it cloud computing – they should be in a "cloud" somewhere. And that if you have the right kind of browser or the right kind of access, it doesn't matter whether you have a PC or a Mac or a mobile phone or a BlackBerry or what have you – or new devices still to be developed – you can get access to the cloud."

– ERIC SCHMIDT

OPPORTUNITY

- business intelligence was becoming increasingly important to enterprises to remain competitive.
- required integrating systems both internally and externally to gain a deeper understanding of organisation.
- opportunity to disrupt aspects of organisation by pushing it towards the customer, e.g. commerce.
- Internet was perceived as an opportunity to achieve all these different goals.

CHARACTERISTICS

- servers and storage can be provisioned **on-demand** without human interaction.
- **standardised access** for heterogeneous thin and thick clients to resources and capabilities.
- **resource pooling** through multi-tenant access to infrastructure.
- **rapid elasticity** of capabilities towards demands of client, affording almost unlimited resources for short bursts.
- **measured service** that can be monitored and used to determine resource usage.

CLOUD DEPLOYMENT



Private



Community



Public



Hybrid

CLOUD DEPLOYMENT

- there are essentially four cloud deployment models, defined in terms of control of infrastructure.
- **provider and location** of the actual physical servers and other resources.
- controller of the **virtualisation software** that generate and manage virtual machines.
- **configuration, support and maintenance** of the infrastructure, effectively who is responsible when something goes wrong.

PRIVATE

- infrastructure is for the exclusive use of an enterprise and its business units.
- infrastructure itself may be managed internally or an third-party organisation may manage the infrastructure.
- management could be a mixture between the enterprise and third-party.
- infrastructure, whether its managed by third-party or enterprise, could be located on or off premises.

COMMUNITY

- infrastructure is for the exclusive use of a community of organisations with a shared concern.
- shared concern could be specific security requirements, compliance considerations or policy.
- infrastructure is managed by one or more members of the community or external party.
- infrastructure, whether its managed by third-party or enterprise, could be located on or off premises.

PUBLIC

- infrastructure is managed by a provider and open for use to the public.
- provider may be an enterprise, government, research organisation or mixture of them.
- infrastructure exists on the premises of the organisation managing it.
- configuration and support is handled by the provider of the infrastructure.

HYBRID

- composition of two or more of private, community or public infrastructures.
- sown together using standards or proprietary technology.
- infrastructure remain independent entities but are pulled together to enable application portability and data integration.
- cloud bursting is one example, where a private cloud can make use of public cloud when demand increases.

CLOUD DEPLOYMENT



Private



Community

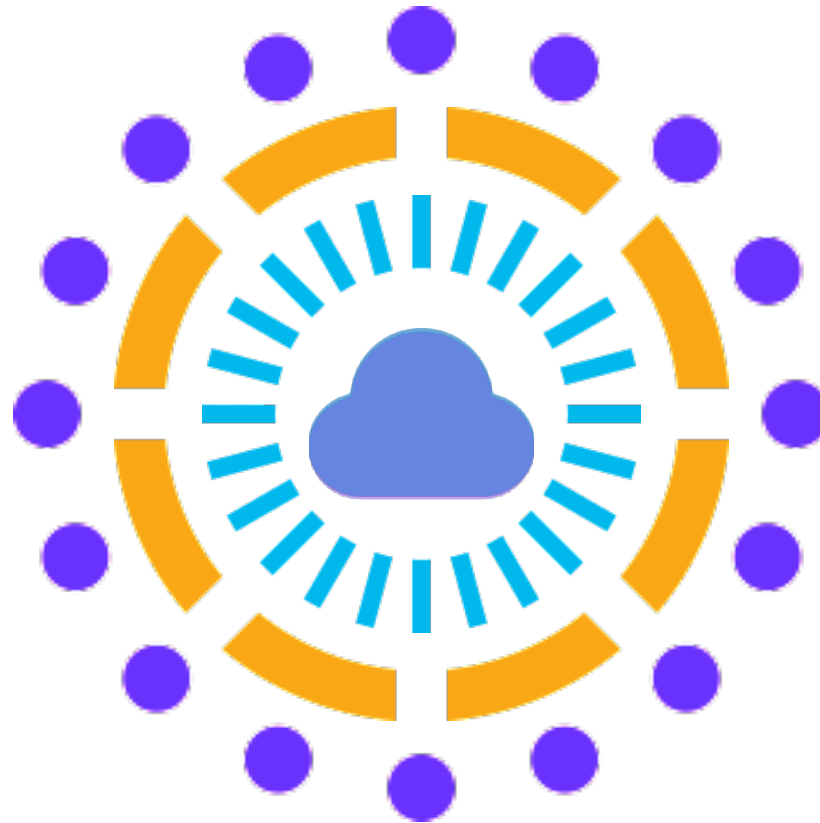


Public



Hybrid

CLOUD SERVICE



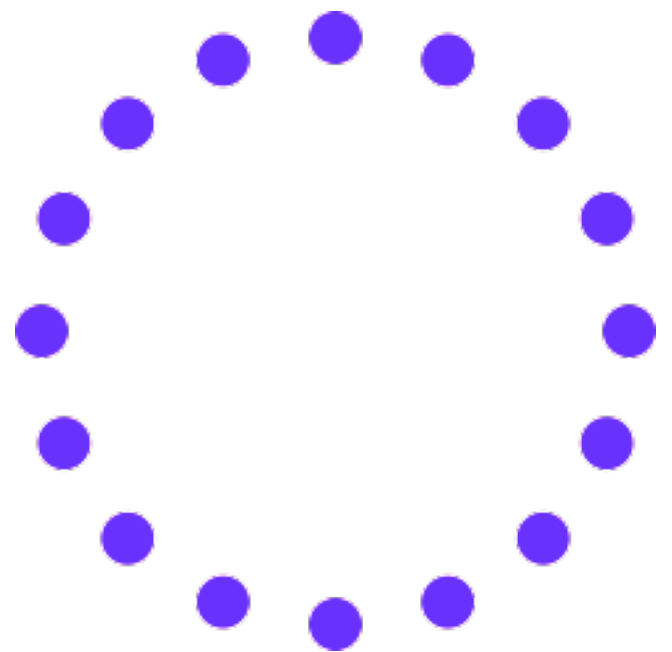
CLOUD SERVICE



IaaS



PaaS



SaaS

INFRASTRUCTURE AS A SERVICE

- the most basic or **fundamental service model** for delivering infrastructure.
- enterprises are **provided basic computing elements** such as processing, storage, network infrastructure etc.
- conceived as **virtual machines** that the enterprise can manage, but has no real control of the underlying physical infrastructure.
- enterprise are close to the metal while they have more control than other models they also have **support and responsibility costs.**

PLATFORM AS A SERVICE

- enterprises can deploy **applications on a platform** built atop the infrastructure.
- applications can be developed using **languages, libraries, services, tools** and frameworks supported by the platform provider.
- enterprises have no real insight into the underlying infrastructure underneath the platform.
- enterprises may have control over applications they have deployed, including specific settings and configuration.

Security of Customer Content:

Moving IT infrastructure to AWS means that both the customer and AWS have important roles for the operation and management of security in their areas of responsibility. AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the AWS services operate. The customer is responsible for management of the guest operating system (including updates and security patches to the guest operating system) and associated application software, as well as the configuration of the AWS provided security group firewall and other security-related features. The customer will generally connect to the AWS environment through services provided by third parties (for example internet service providers). AWS does not provide these connections and the customer should consider the security of such connections and the security responsibilities of such third parties in relation to their systems. This is really no different from working with a network service provider who brings connectivity to on-premises data centers.

This model is shown below in Figure 1:



Security of Customer Content:

Moving IT infrastructure to AWS means that both the customer and AWS have important roles for the operation and management of security in their areas of responsibility. AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the AWS services operate. The customer is responsible for management of the guest operating system (including updates and security patches to the guest operating system) and associated application software, as well as the configuration of the AWS provided security group firewall and other security-related features. The customer will generally connect to the AWS environment through services provided by third parties (for example internet service providers). AWS does not provide these connections and the customer should consider the security of such connections and the security responsibilities of such third parties in relation to their systems. This is really no different from working with a network service provider who brings connectivity to on-premises data centers.

This model is shown below in Figure 1:



Security of Customer Content:

Moving IT infrastructure to AWS means that both the customer and AWS have important roles for the operation and management of security in their areas of responsibility. AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the AWS services operate. The customer is responsible for management of the guest operating system (including updates and security patches to the guest operating system) and associated application software, as well as the configuration of the AWS provided security group firewall and other security-related features. The customer will generally connect to the AWS environment through services provided by third parties (for example internet service providers). AWS does not provide these connections and the customer should consider the security of such connections and the security responsibilities of such third parties in relation to their systems. This is really no different from working with a network service provider who brings connectivity to on-premises data centers.

This model is shown below in Figure 1:



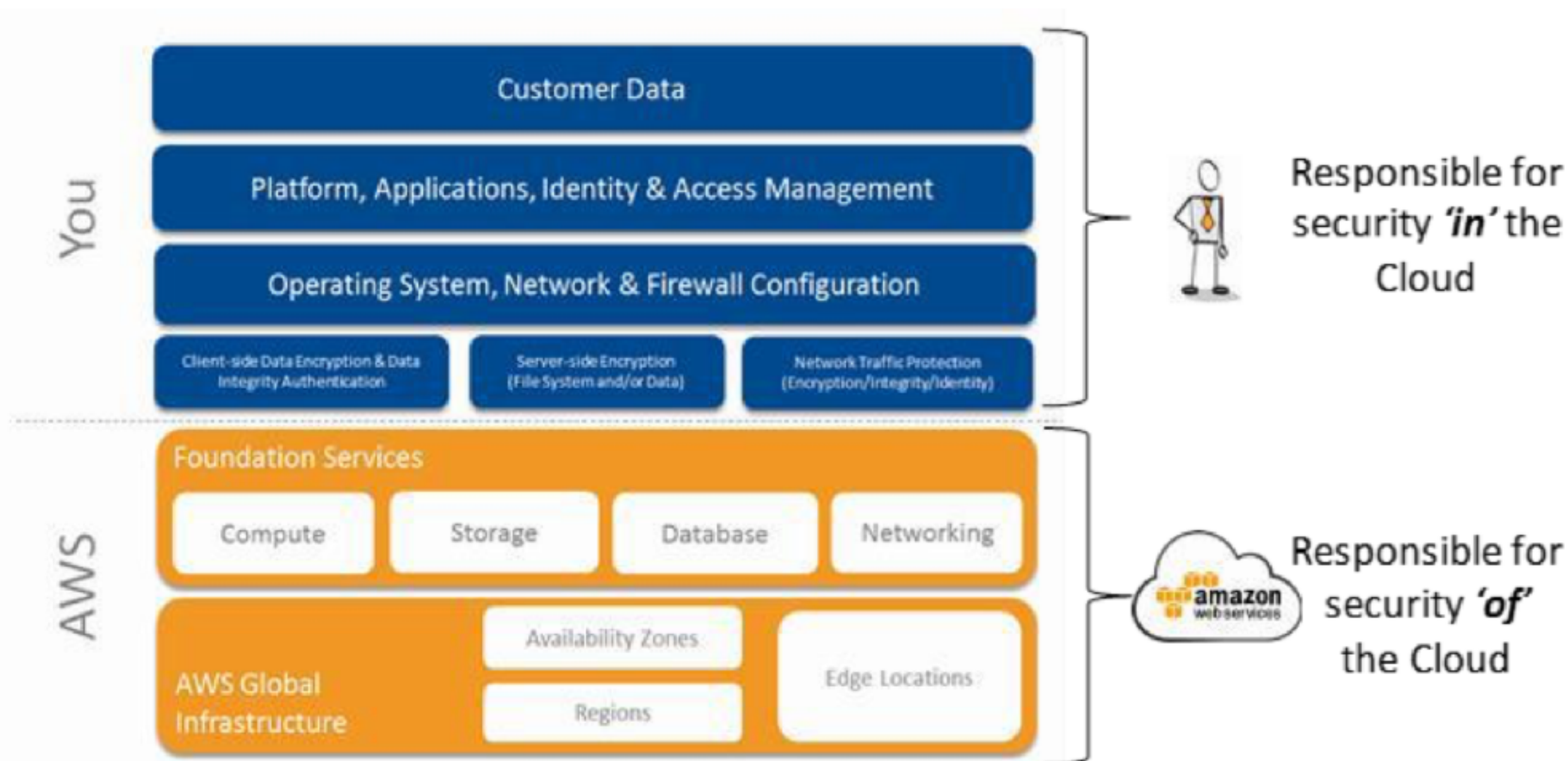


Figure 1 – Security Model

SOFTWARE AS A SERVICE

- enterprises are granted **access to applications and services** from provider.
- applications are **accessible from thin-clients** as well as more complex clients (program interface).
- enterprises have no sense of the underlying infrastructure or significant control over platform or application.

CONCERNS

- complexity at the level is significant with many different elements to be considered.
- difficult to get complete assurance from software providers about their solutions.
- aim for the enterprise is to preserve, at a minimum, the level of security they have with legacy applications.
- SAAS provider may not be relying on their own infrastructure, creating further complexity.

CONCERNS

- business process are increasingly being perceived as crucial to core competency, so want to retain control
- data could be stored alongside data from other organisations on the same infrastructure.
- data could also be replicated across different providers and countries to support availability and integrity.
- it may reside on some 'sub-infrastructure' with other unrelated application data

CONCERNS

- enterprises are used to data residing within their perimeter under their control
- they can develop policies to manage and process data.
- concerns about data breaches, application vulnerabilities that could lead to legal and compliance concerns.
- difficult when considering the challenge of securing the transit and rest of data across various infrastructures.

RESTING DATA

- deployment and service models used in cloud computing could result in data having poor visibility.
- enterprise may be relying on vendor to encrypt data and provide authentication.
- management of cloud infrastructure can impact on the strength of this encryption.
- access and progression through the system is typically thoroughly logged for live and subsequent analysis.

DATA IN TRANSIT

- employees input data into application that is processed and put to rest by the provider.
- data transit needs to be secured between the various points to ensure data does not spill.
- concerns may surround the transit of data to application but also during processing and when put to rest.
- network penetration and packet analysis as well as explore configurations and session concerns.

RESTING DATA LOCALITY

- determine the location of actual data can be challenge for SAAS.
- data may not even reside on the infrastructure of the organisation providing the application.
- laws and compliance issues differ between countries, EU laws, USA laws and UK laws.
- enterprises need to have confidence of the locality of resting data to ensure they meet compliance issues.