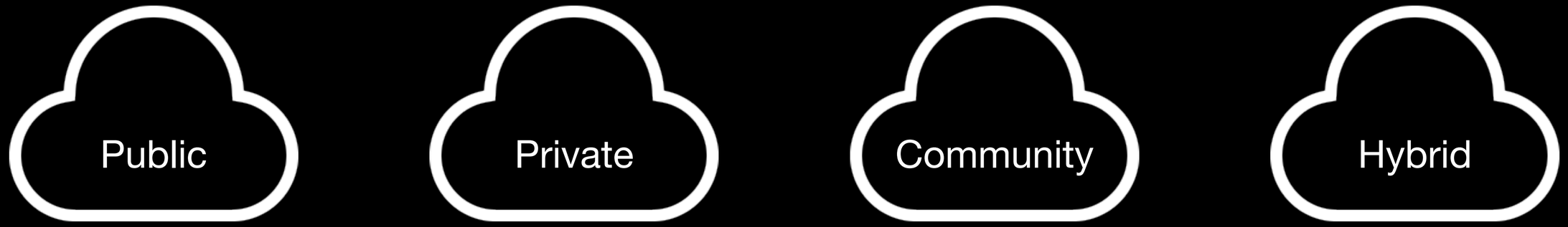
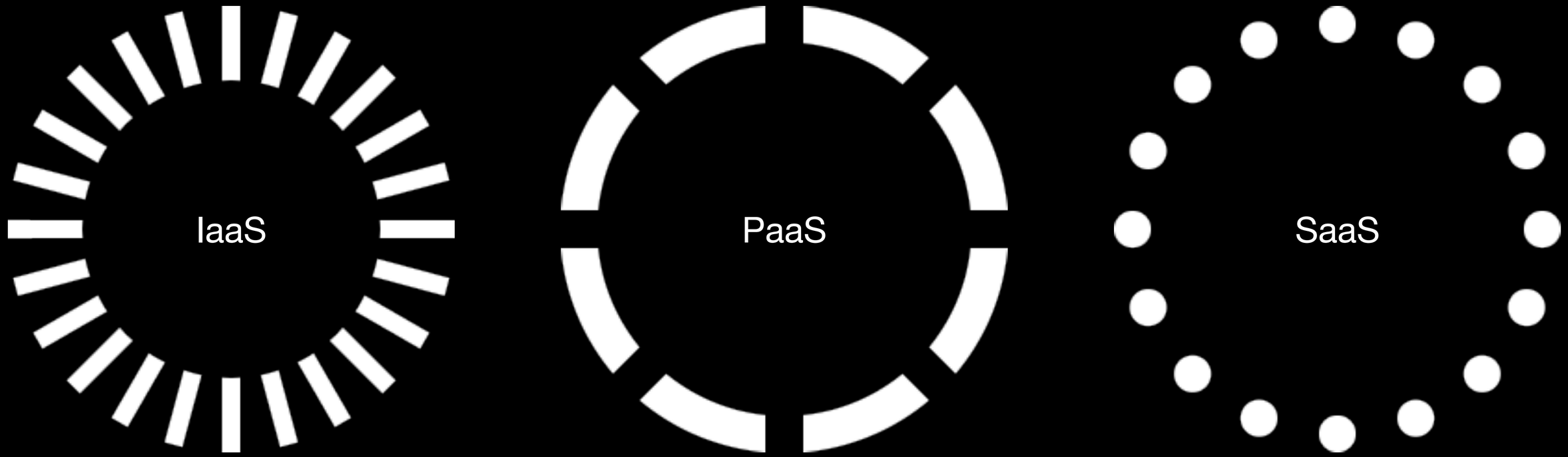
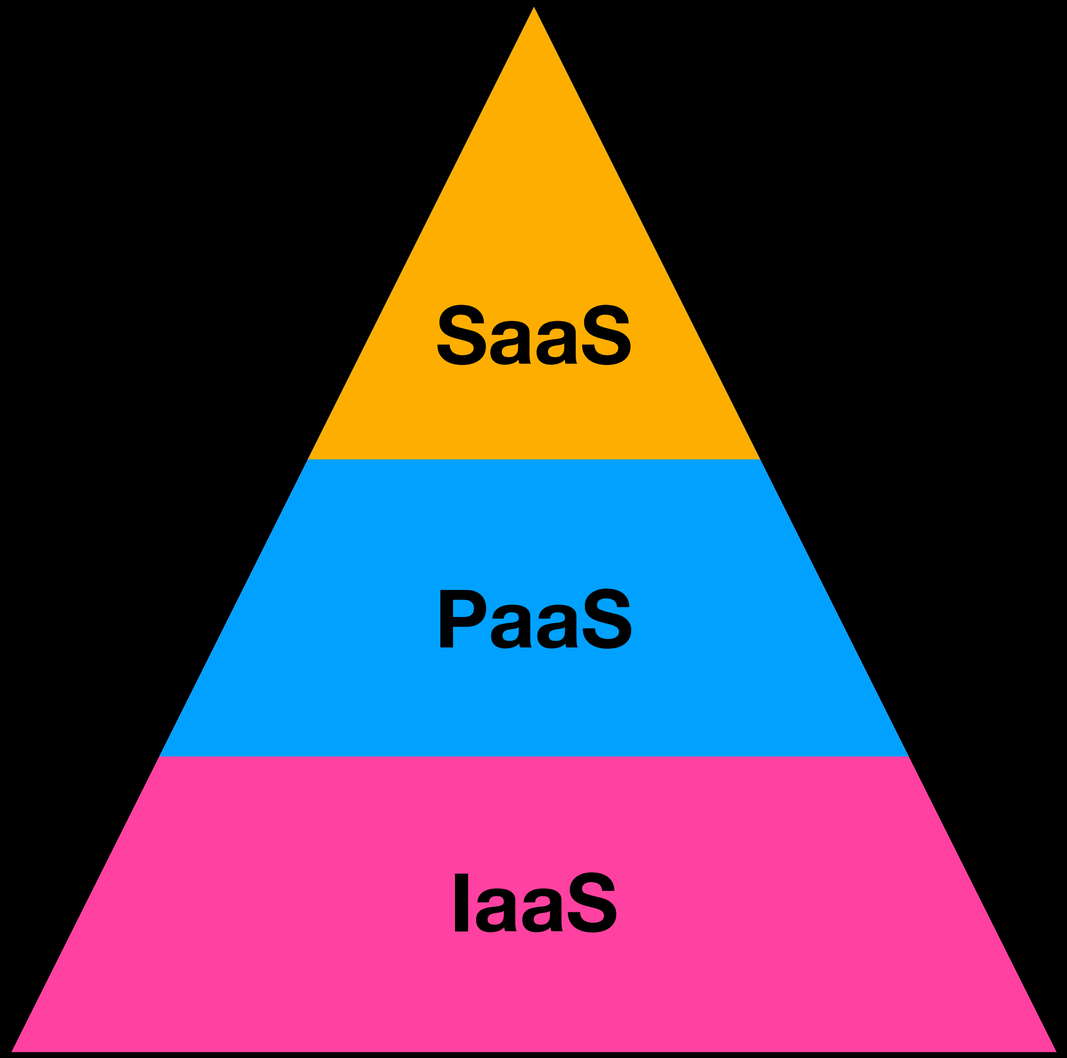
Service models

Architecture

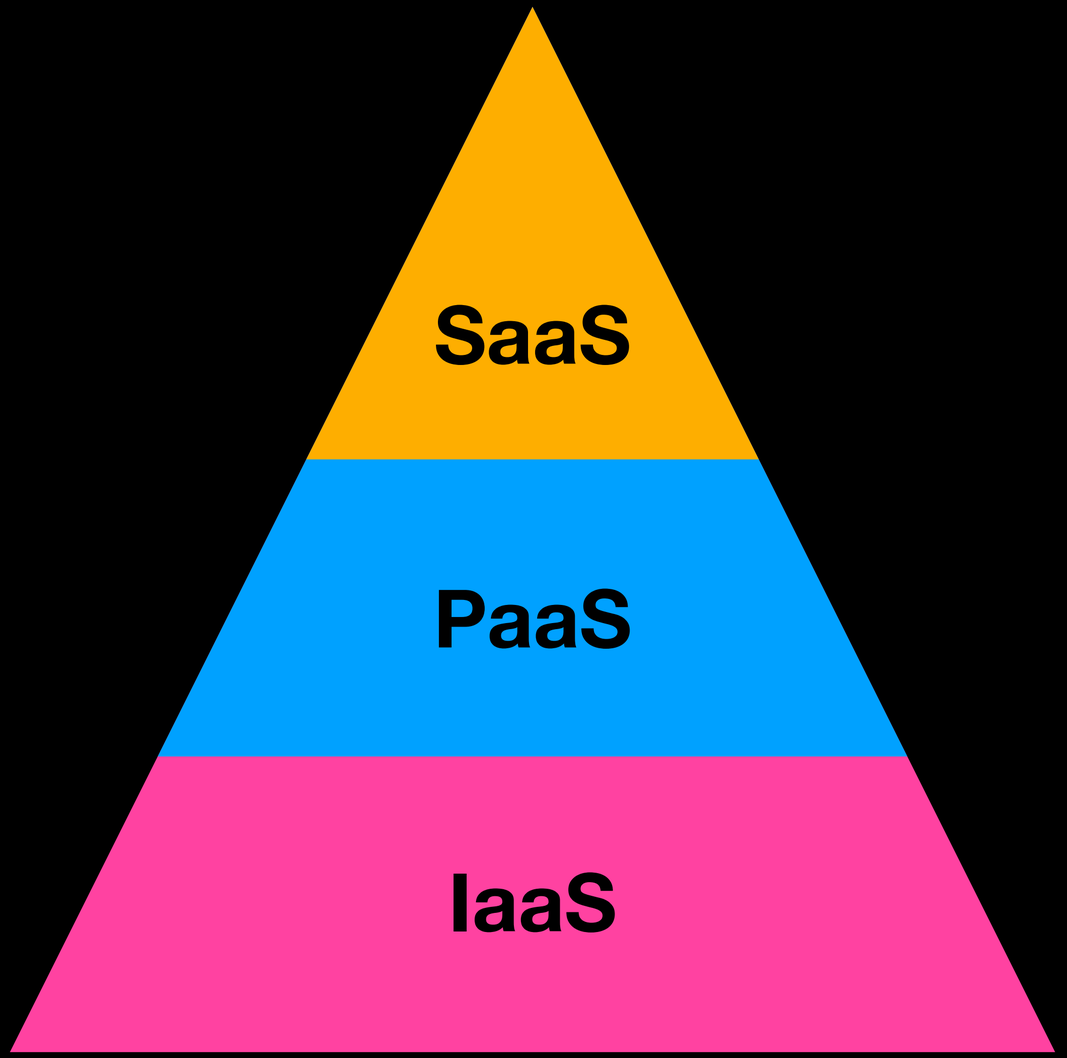

Public
Private
Community
Hybrid


IaaS
PaaS
SaaS

Cloud Provider



Cloud Provider

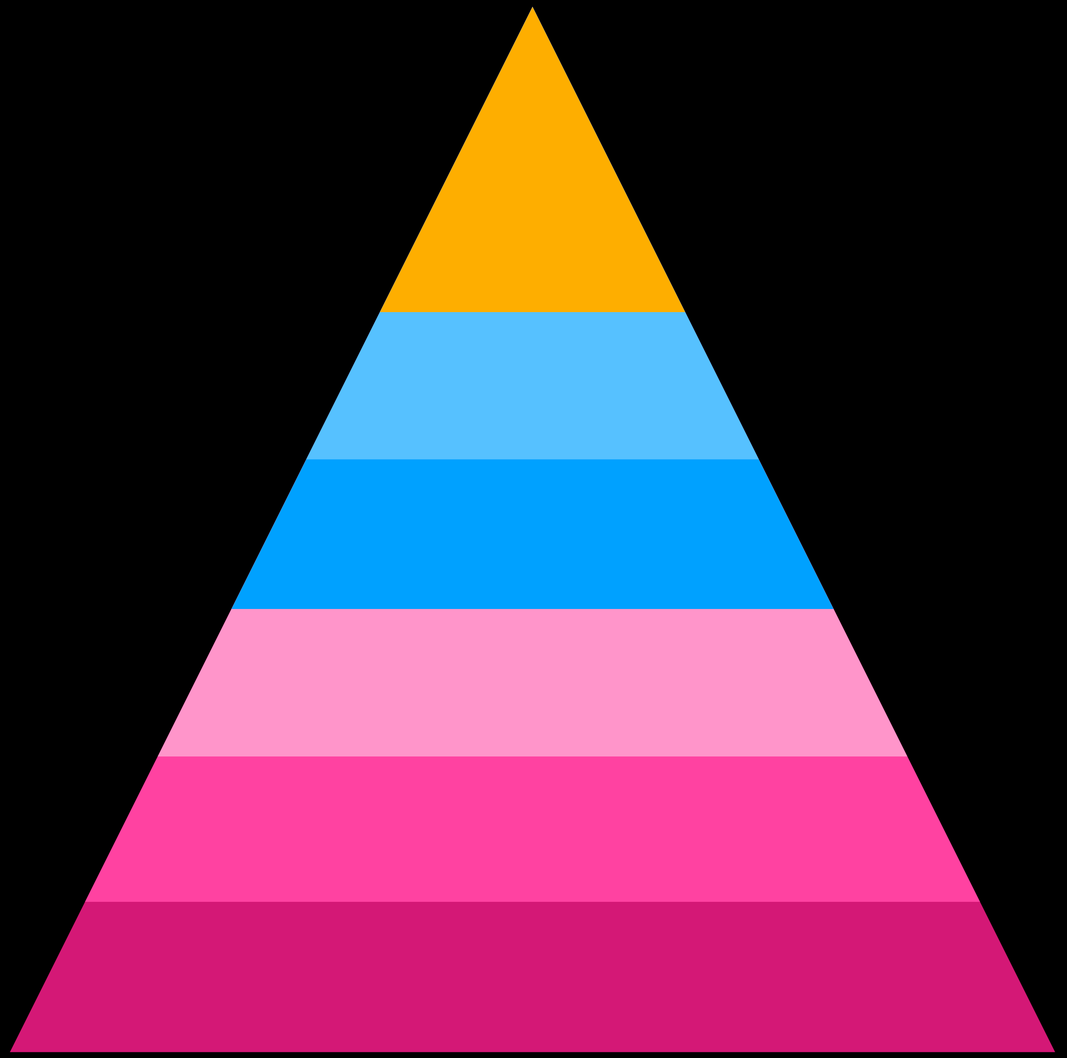


User

Engineer or Developer

System manager

Cloud Provider



Applications

Network controls

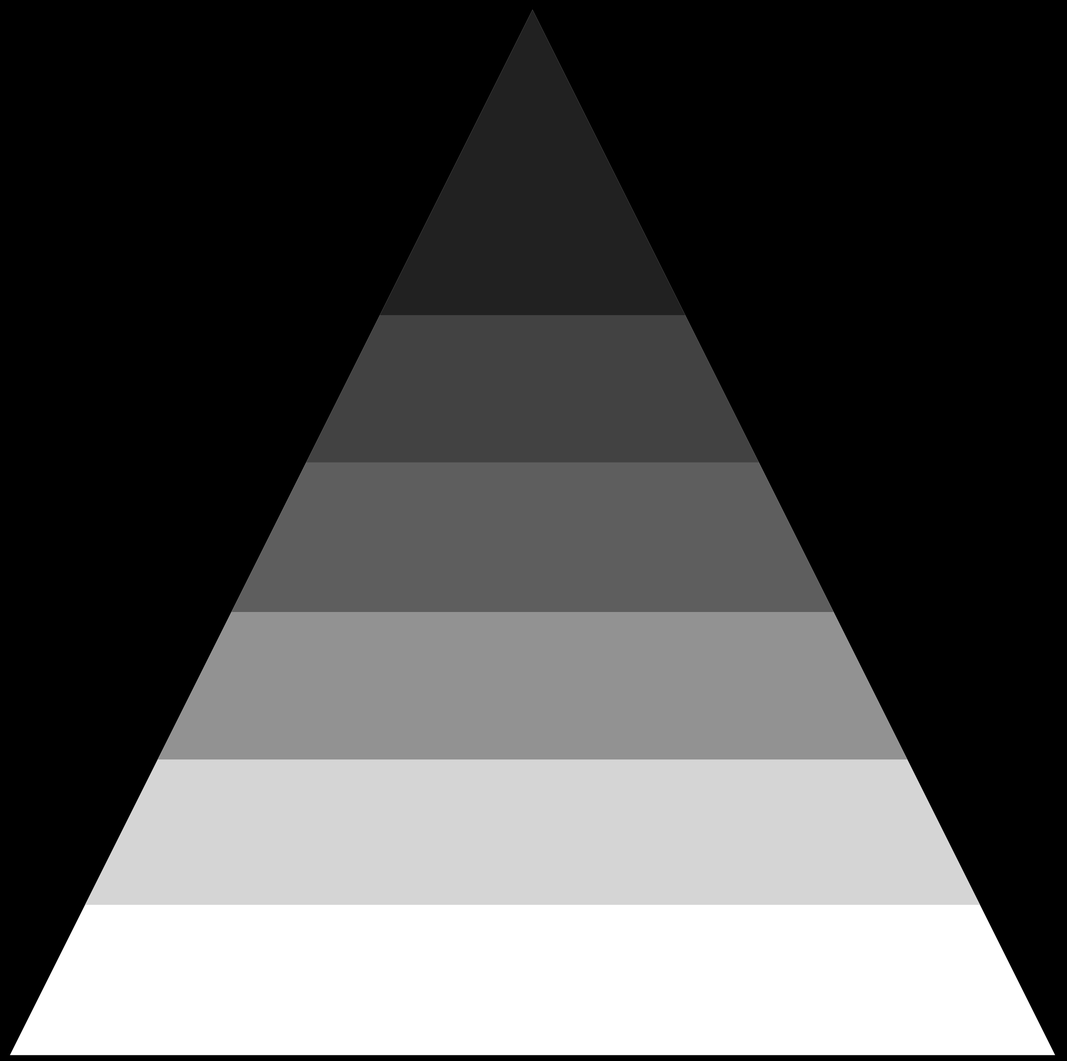
Operating system

Hosting infrastructure

Network infrastructure

Datacentre

Enterprise



Applications

Network controls

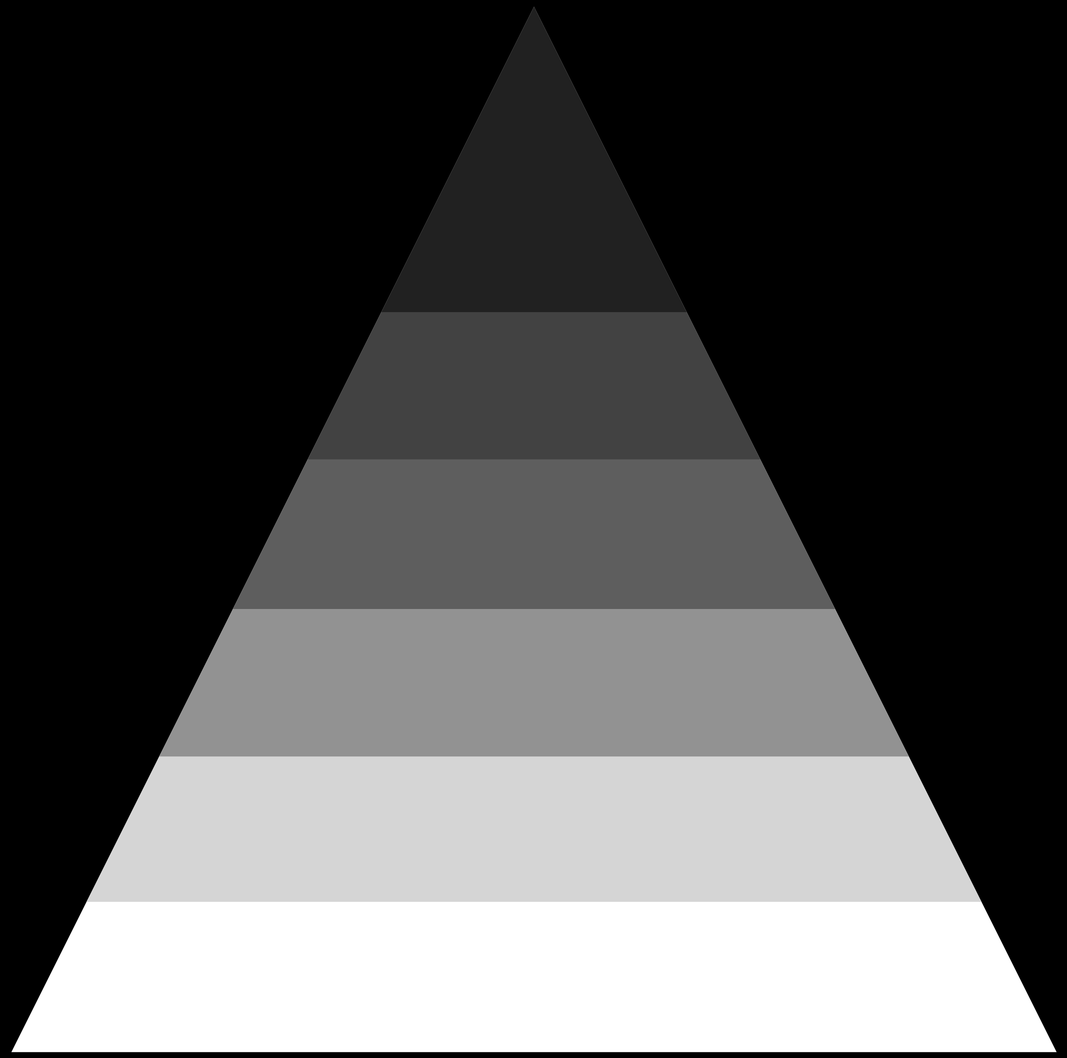
Operating system

Hosting infrastructure

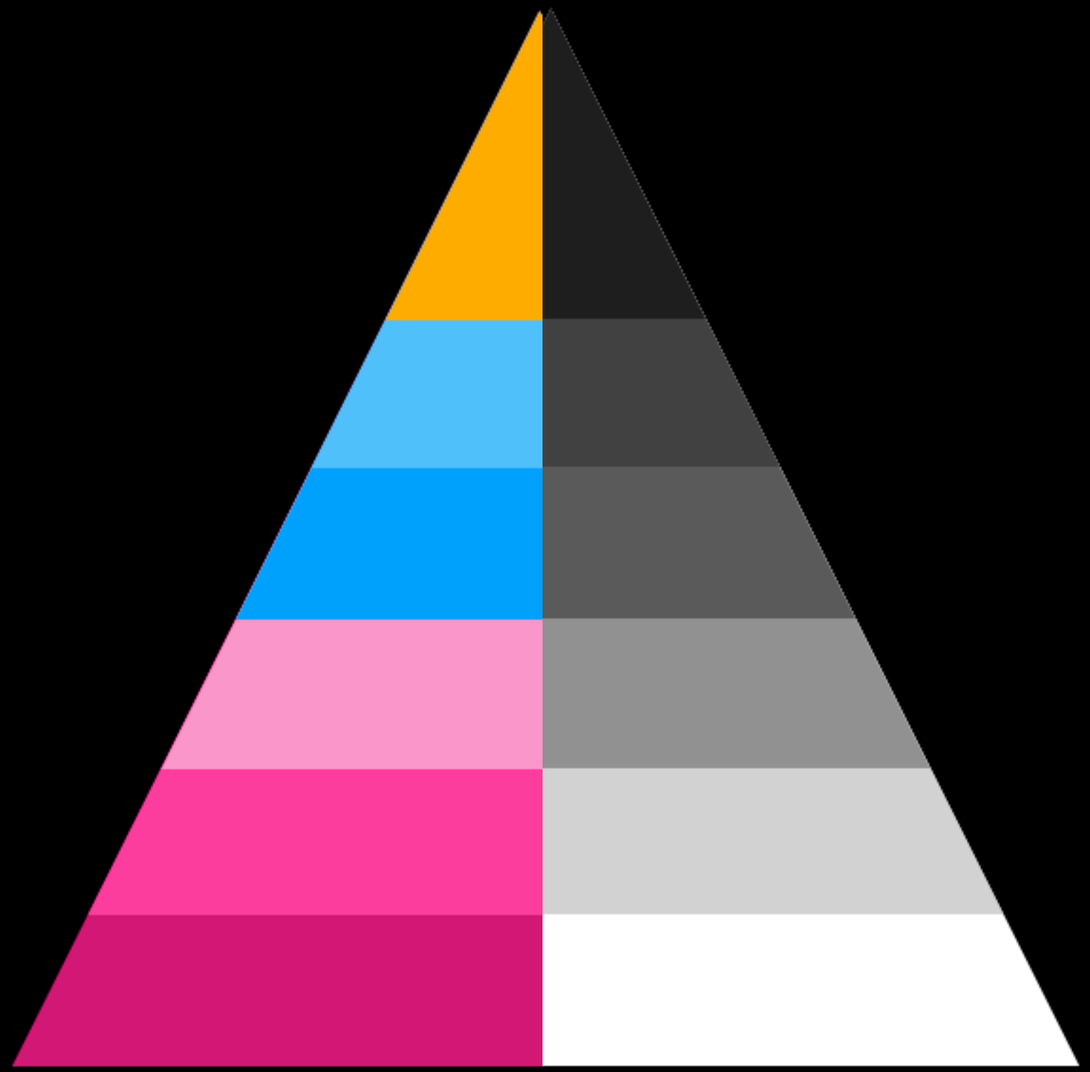
Network infrastructure

Datacentre

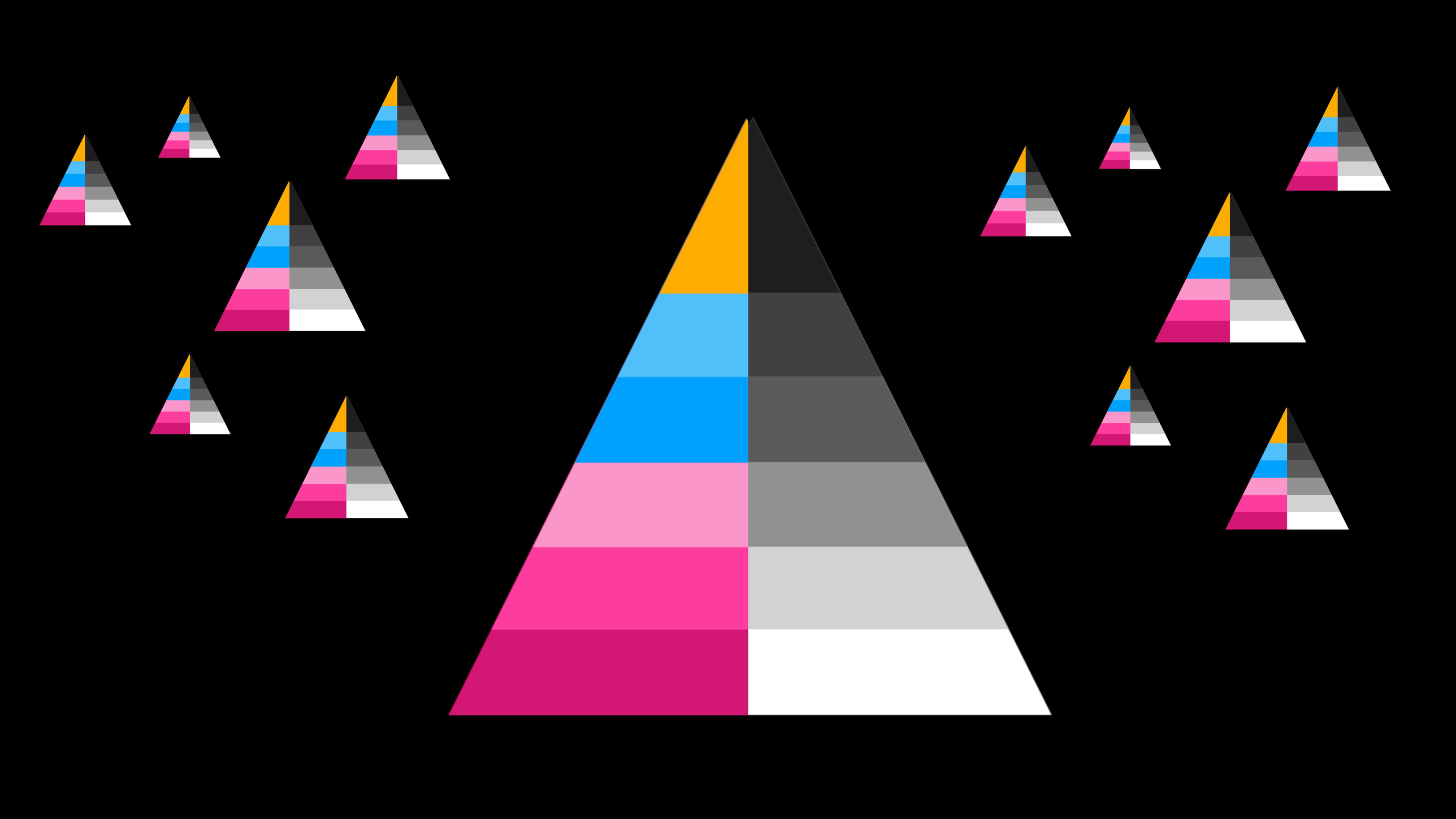
Enterprise

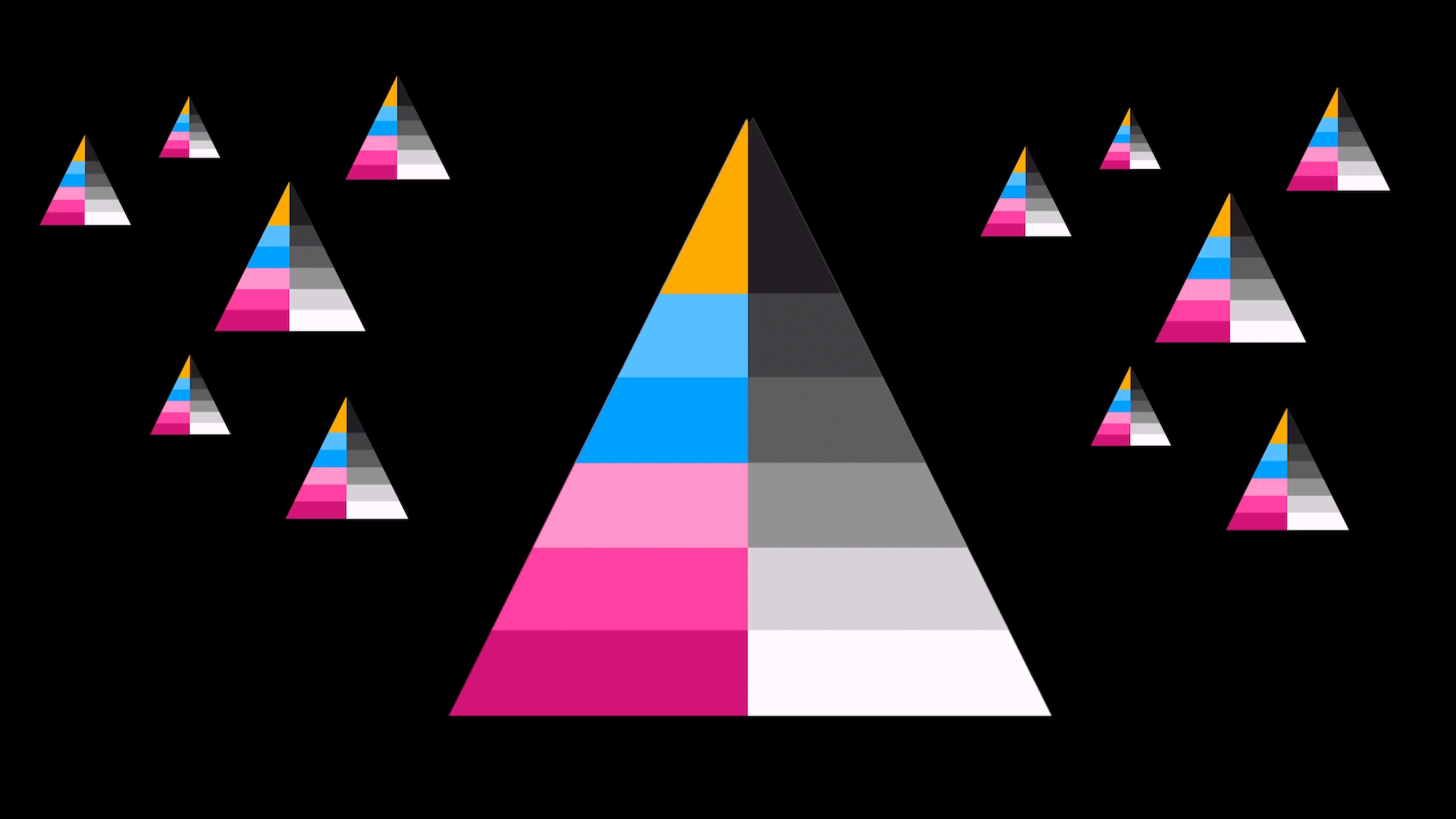


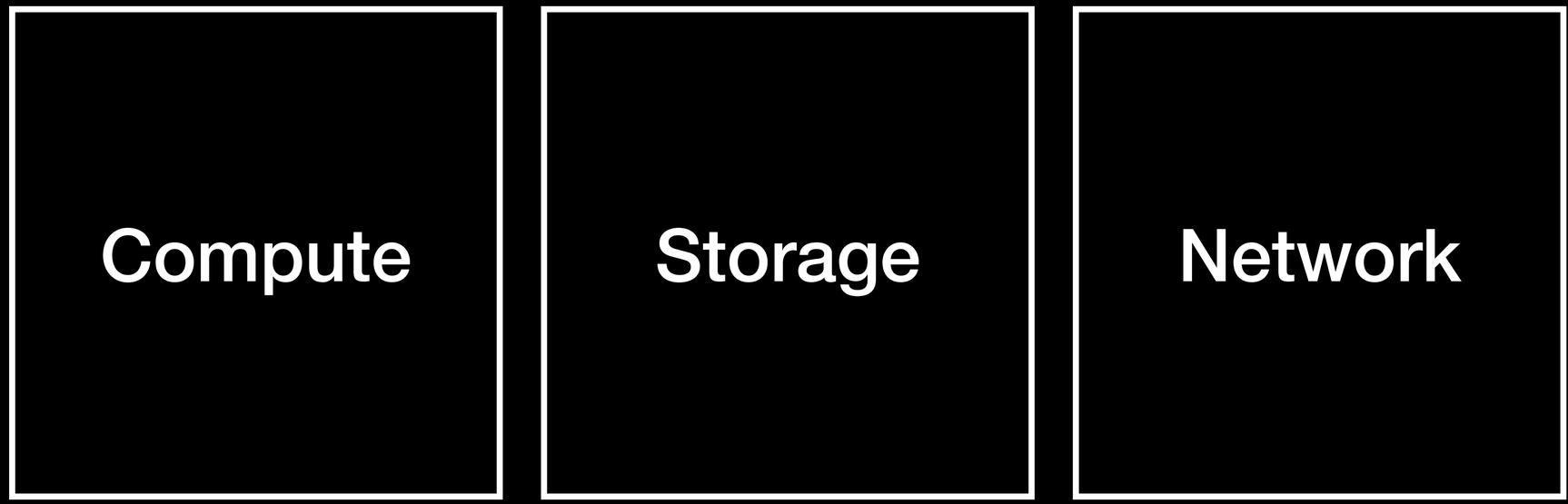
Cloud Provider



Enterprise






Compute
Storage
Network


Compute
Storage
Network

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:

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:

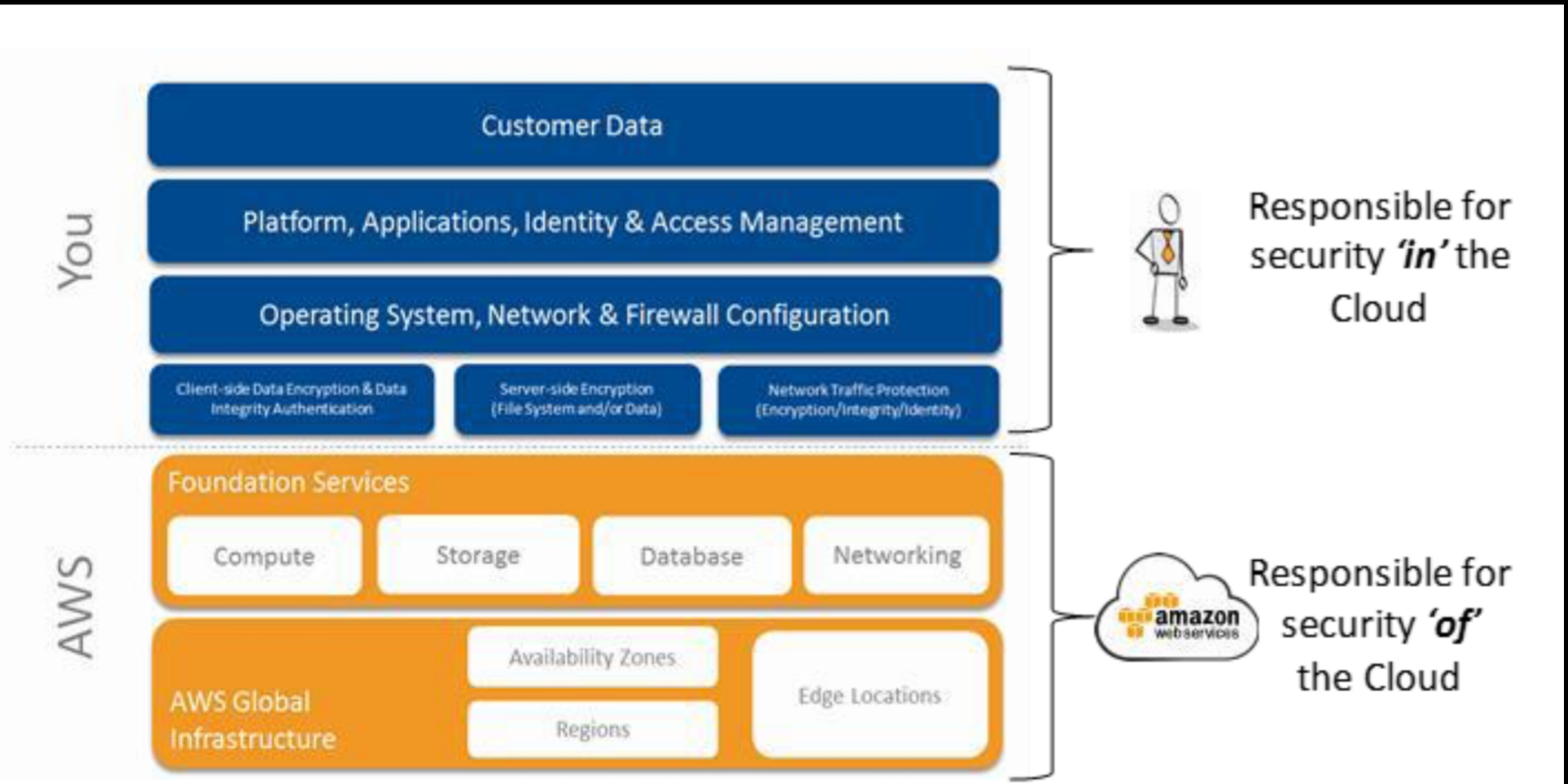


Figure 1 – Security Model

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.

Service models

Architecture