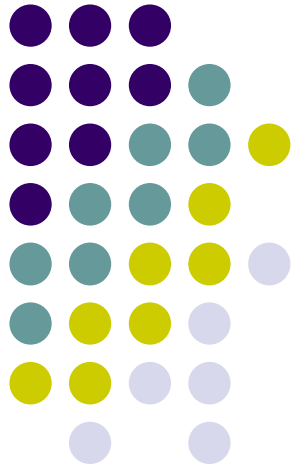
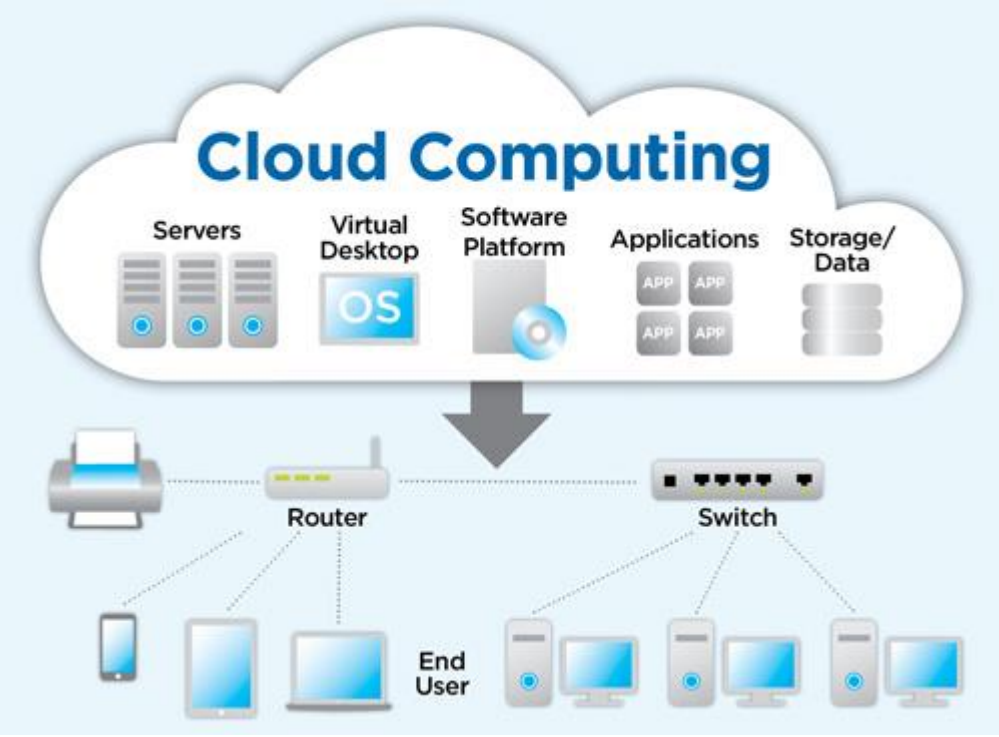
Cloud Computing

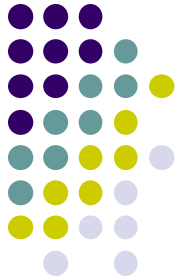


A Working Definition of Cloud Computing

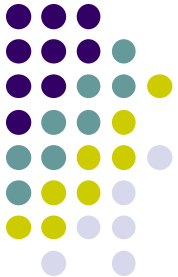
Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.



Objectives of Cloud Computing



- **Elasticity:** Ability to scale virtual machines resources up or down
- **On-demand usage:** Ability to add or delete computing power (CPU, memory), and storage according to demand
- **Pay-per-use:** Pay only for what you use
- **Multitenancy:** Ability to have multiple customers access their servers in the data center in an isolated manner



3 Cloud Service Models

- Cloud Software as a Service (SaaS)

  The **capability provided to the consumer is to use the provider's applications** running on a cloud infrastructure and accessible from various client devices through a thin client interface such as a Web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure, network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

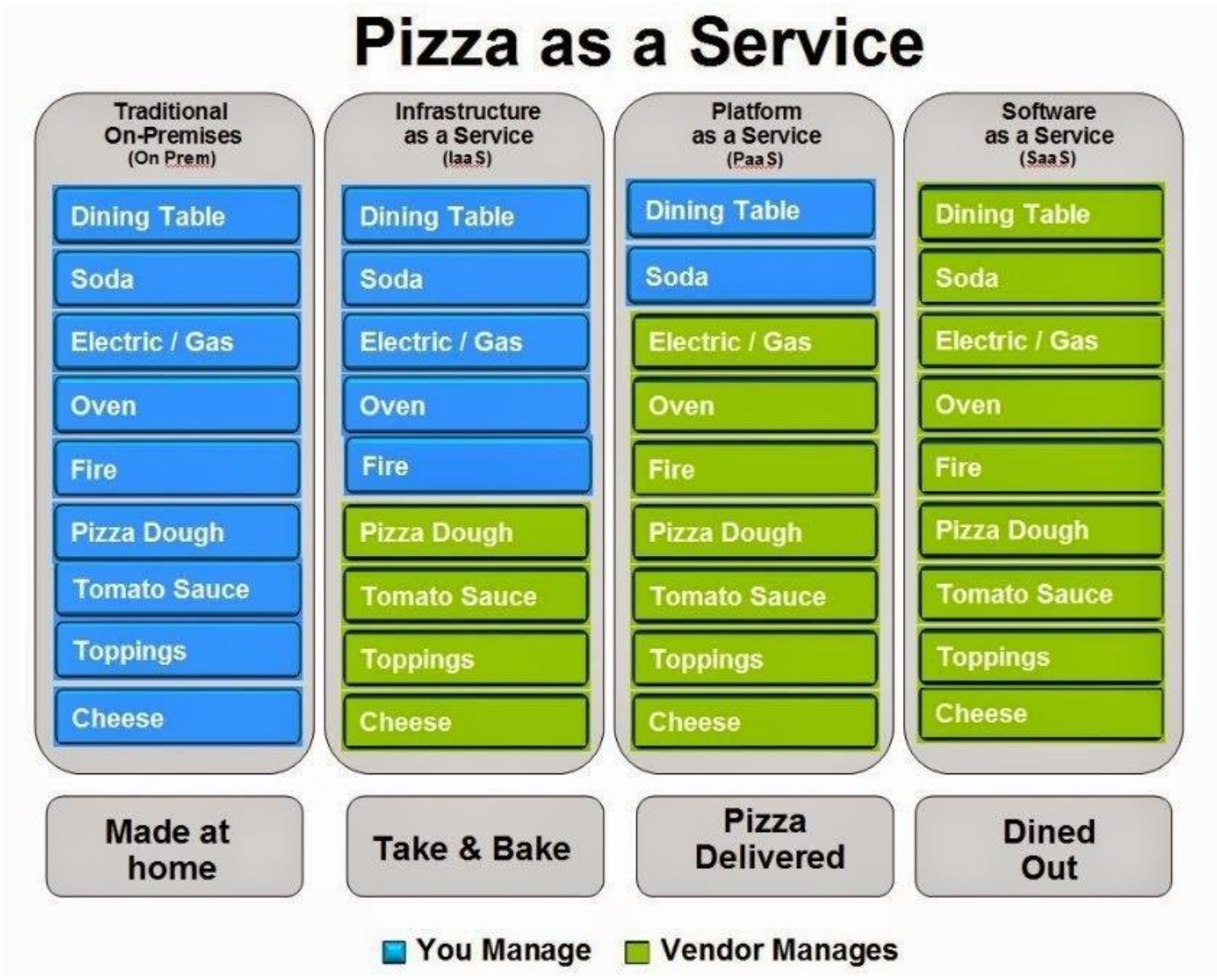
- Cloud Platform as a Service (PaaS)

  The **capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created applications using programming languages and tools supported by the provider** (e.g., Java, Python, .Net). The consumer does not manage or control the underlying cloud infrastructure, network, servers, operating systems, or storage, but the consumer has control over the deployed applications and possibly application hosting environment configurations.

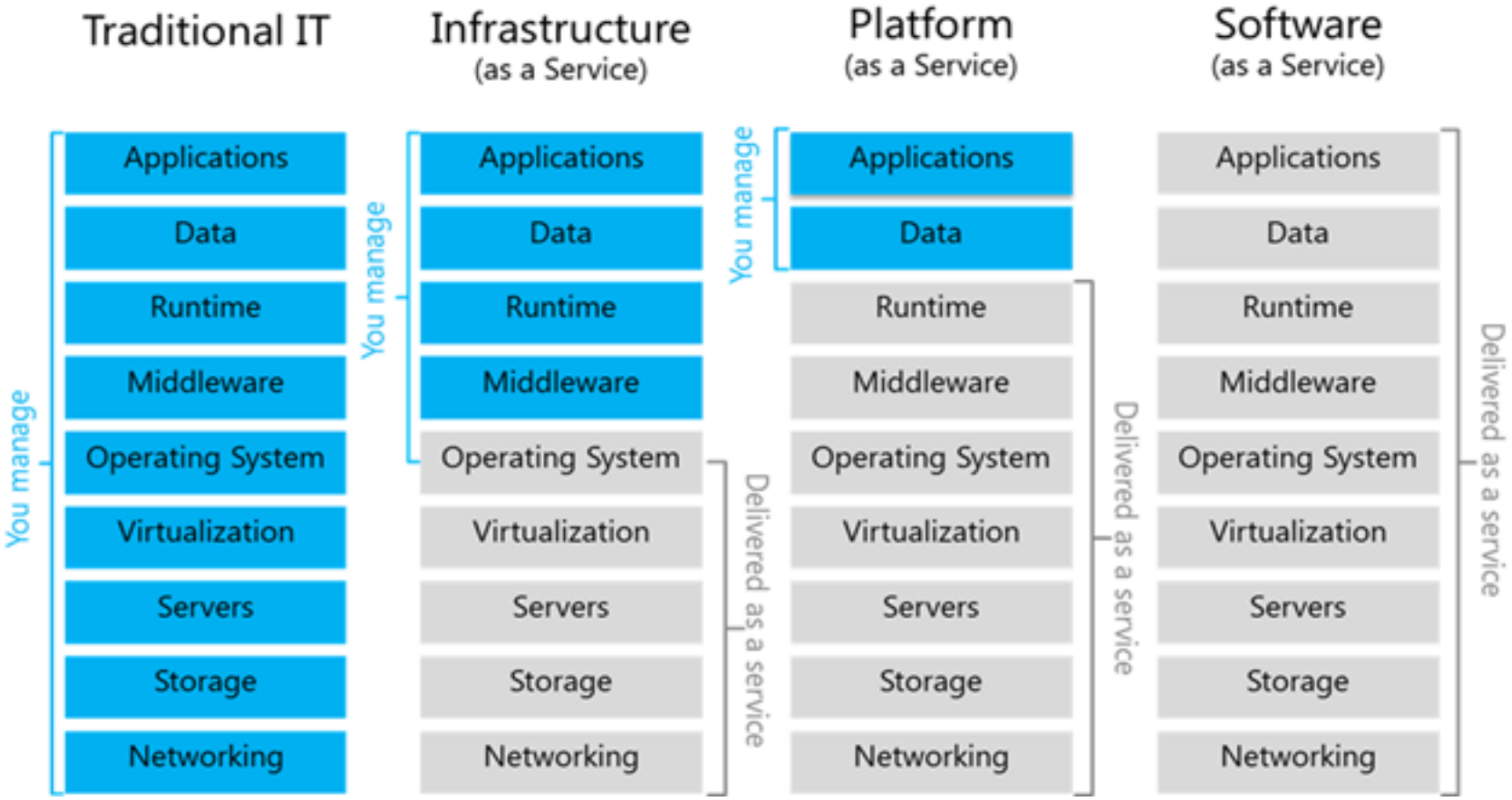
- Cloud Infrastructure as a Service (IaaS)

  The **capability provided to the consumer is to rent processing, storage, networks, and other fundamental computing resources** where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly select networking components (e.g., firewalls, load balancers).

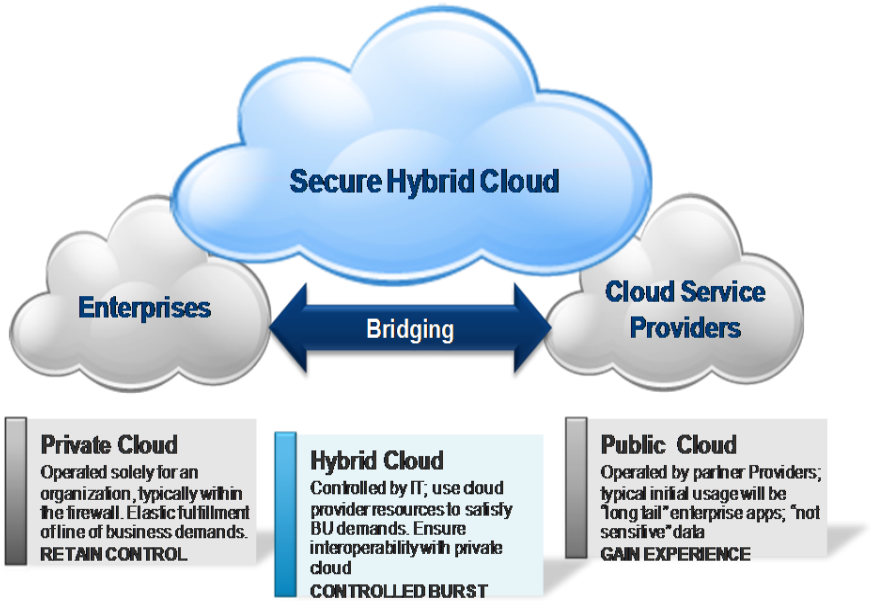
- To be considered "cloud" they must be deployed on top of cloud infrastructure that has the key characteristics


Pizza as a Service
Traditional On-Premises (On Prem)
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)
Software as a Service (SaaS)
Dining Table
Soda
Electric / Gas
Oven
Fire
Pizza Dough
Tomato Sauce
Toppings
Cheese
Made at home
Take & Bake
Pizza Delivered
Dined Out
You Manage
Vendor Manages

Saas, PaaS, IaaS



3 Cloud Deployment Models



- Private cloud

  The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

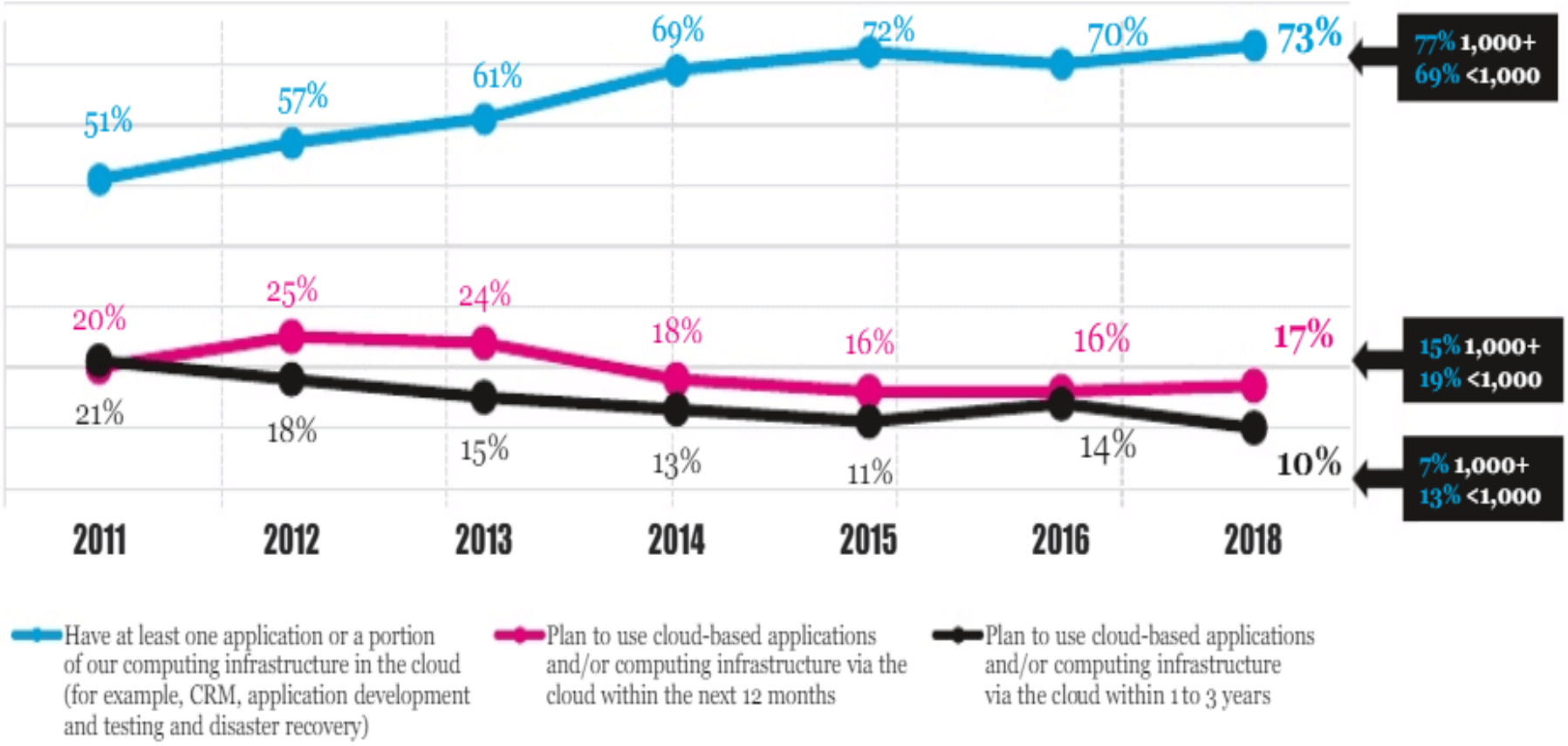
- Public cloud

  Mega-scale cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

- Hybrid cloud

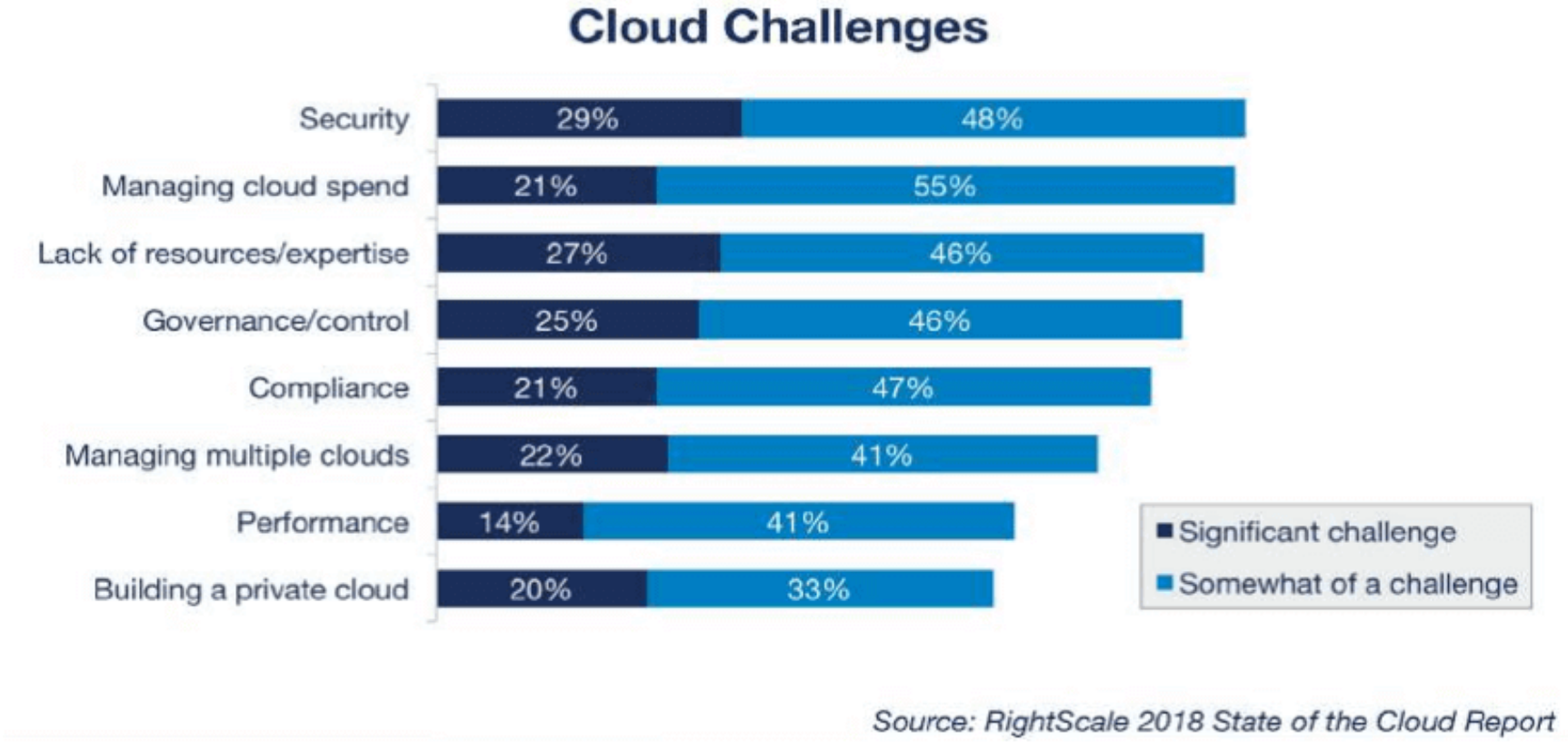
  The cloud infrastructure is a composition of two or more clouds (private or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability

Cloud Has Come of Age



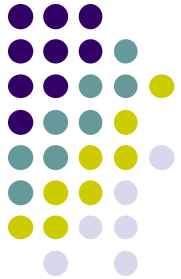
Q. What are your organization's plans with regard to utilizing computing infrastructure or applications via the cloud?

Security is the Major Issue



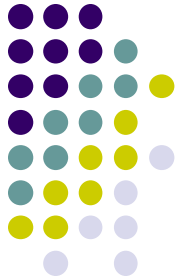
Source: RightScale 2018 State of the Cloud Report

Cloud Security Challenges



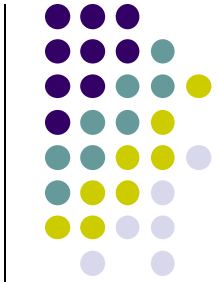
- Trusting vendor's security model
- Multi-tenancy (serves multiple tenants)
- Data ownership issues
- QoS guarantees
- Attraction to hackers (high-value target)
- Security of virtual OSs in the cloud
- Obtaining support from cloud vendor for security related investigations

Cloud Security Challenges



- Indirect administrator accountability
- Proprietary cloud vendor implementations can’t be examined
- Loss of physical control
- Possibility for massive outages

Cloud Security Advantages



- Shifting public data to a external cloud reduces the exposure of the internal sensitive data
- Dedicated Security Team
- Greater Investment in Security Infrastructure
- Cloud homogeneity makes security auditing/testing simpler
- Clouds enable automated security management and real-time detection of system tampering
- Rapid Re-Constitution of Services
- Redundancy / Disaster Recovery