DHS Cloud Service

By: Saketh Lakshmanan, Christian Domacena, Rafael Simioni

Benefits of Cloud Computing

Reduced IT Cost

- Most cloud computing services offers Pay-as-you-go structure
- No new hardware necessary
- Reduce energy cost
- Servers and other hardware upgrade or repairs are handled by the vendors.
- Eliminates Redundancies

Flexibility

- Can handle fluctuating demands
- Resolves data-storage issues
- Security features
- Variety of tool selection that fit a company’s needs

Strategic Value

- Teams can collaborate from widespread locations
- Competitive Advantage
- Automatic Software Updates

Efficiency

- Accessible to anyone from anyone with a device connected to the internet
- Loss prevention
- Speed to market

Risks of Cloud Computing

Confidentiality

- Sensitive data are handled and transmitted between two or more parties.
- Ownership claim

Availability

- Service disruption

Compatibility

- Change in service
- Return on investment

Cloud Computing Types

Public

- Cloud infrastructure available for the all of public over the internet
- Owned by cloud service providers
- Individual organizations using it do not have private access

Private

- Privately owned by a single organization
- Can be managed by a third party or the organization itself
- Has a data center that is on-premises

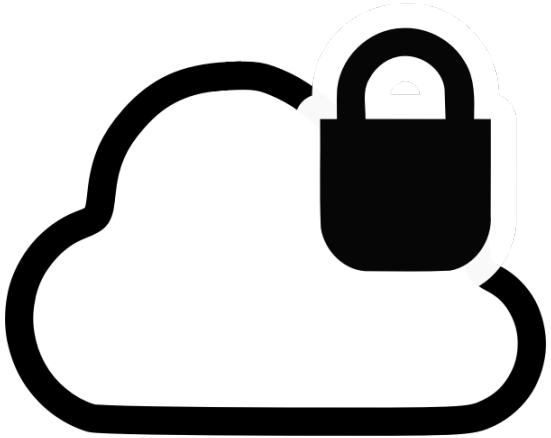
Hybrid

- Combination of a public and private cloud
- Organization has data centers on-premises as well as public clouds to mix and match

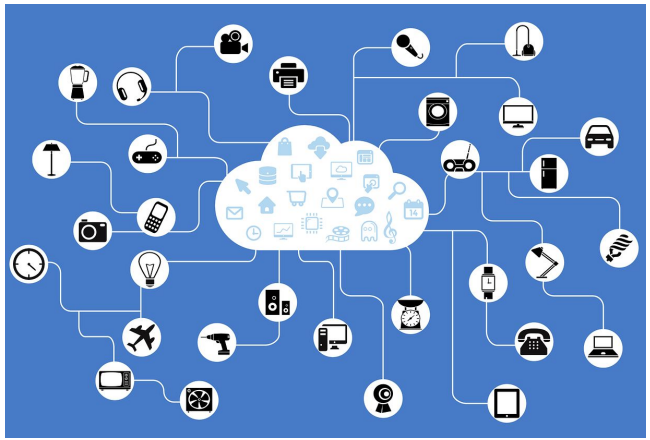
Building Cloud Service at DHS

- We are trying to provide public and private cloud offerings, so essentially a hybrid system

- Private Cloud offerings
  - For sensitive but unclassified information



- Public Cloud offerings
  - For non-sensitive information



Development and Test as a Service (DTaaS)

- Mobility
- Increase productivity
- Less onboarding time
- Fully managed teams

Infrastructure as a Service (IaaS)

- Provides storage, backup, and recovery.
- High-performance computing
- DHS does need to provide maintenance to their hardware. All the troubleshooting and upgrades are handled by the service provider
- Disaster Recovery

Email as a Service (EaaS)

- Service to ensure the privacy of incoming and outgoing emails sent by or to the Department of Homeland Security
- Will be used across Headquarters and Federal Emergency Management Agency (FEMA).
- Expected to have at least 100,000 users DHS-wide on this service

SharePoint as a Service (SHPTaaS)

- Service to help different organizations across the DHS share online resources easier and more securely

- Organizations using it will be the Headquarters and United States Citizenship and Immigration Services

- Expected to have at least 90,000 users

Authentication as a Service (AuthaaS)

- Fully automated lifecycle administration of users, permissions and tokens
- Automated threshold and event-based alerts
- No hardware requirements
- Various 2FA authentication methods to choose from.
- Customizable security policies

Case and Relationship Management as a Service (CRMaaS)

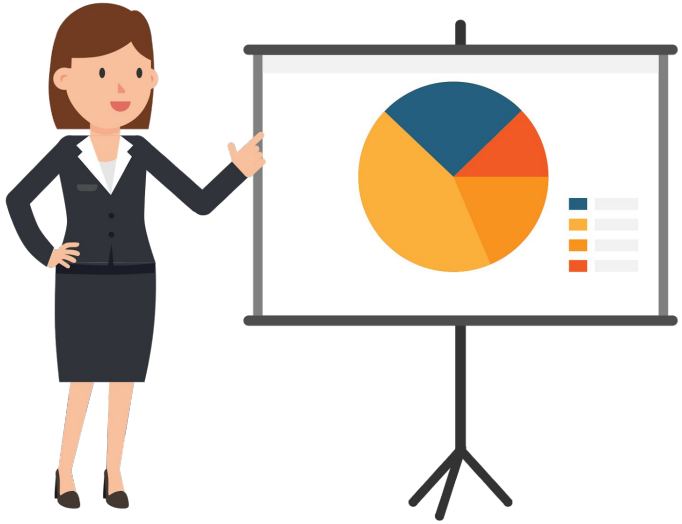
- Leverages Enterprise License Agreements (ELA)
- Improve case workflows
- Better Customer Relationship Management or CRM
- Provide regulations tracking service

WorkPlace as a Service (WPaaS)

- Enabling a mobile workforce is important
- Will provide mobile services for DHS users nationwide like
  - virtual desktop,
  - remote access
- The expectation is that the service reduces yearly expenditures on traditional desktop and laptops

Project Server as a Service (PSaaS)

- A management service to help publish project schedules that can be easily shared across offices and divisions
- Improves the standardization of project management
- Supports the efforts to improve the management of both IT and non-IT programs



Business Intelligence as a Service (BIaaS)

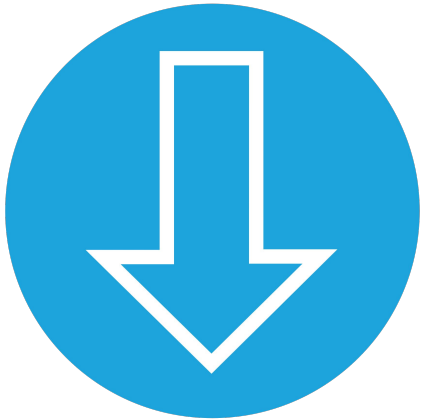
- Offers Data & Model optimization
- Deploy analytics tool
- Organize and plan dev sprints as needed for progress and scale
- Security & Usage Monitoring

Identity Proofing as a Service (IDPaaS)

- Provide an extra layer of protection for user accounts
- Ensures whoever is logging into the account is actually the user
- Can immediately stop most attacks that are especially prevalent in government sectors
  - Phishing
  - Social engineering
  - Credential theft

Enterprise Content Delivery as a Service (ECDaaS)

- Caching content as close to the end user as possible
  - Speeds up and improves the overall experience for the end user
  - Helps to reduce bottlenecks when serving content
- Can use private, isolated infrastructure
  - Needed for handling sensitive data
- Provides extra security where needed
  - Access control
  - DDoS protection



Web Content Management as a Service (WCMaaS)

- Ability to manage content anywhere
- Less configuration time
- Hosting and domain management are mostly included in the service.
- SEO optimized

Conclusion

- Cloud-first is very popular
- Offloads tasks such as hardware maintenance resulting in decreased maintenance costs
- Easily scalable depending on needs and/or current load for further cost savings
  - No need to physically provision or deprovision hardware
- Move the edge further closer to the end user
  - Improves overall performance and experience

References

https://www.dhs.gov/news/2011/10/05/testimony-richard-spires-chief-information-officer-house-committee-homeland-security

https://www.ibm.com/cloud/learn/iaas