Why Cloud Smart Over Cloud First

Cloud Repatriation for U.S. Federal and DoD

DELL Technologies
Position Paper

Cloud Solution Guidance

Contents

DELL Technologies
Position Paper

Cloud Solution Guidance

Overview

The U.S. Federal Government and DoD have been evaluating and pursuing cloud-based solutions to support their goals of decreasing IT costs and meeting various agency mandates for cloud adoption. Early exploration of cloud focused primarily on public cloud solutions as the panacea to the challenge around reducing US Federal and DoD footprints, establish predictable costs, and measurable outcomes. With the evolution of technology and learning from the limitations of early Cloud First approaches a more diverse approach to workload placement has been established.

The Initial Challenges of Cloud First

In the early days of cloud technology pursuits, the various U.S. Federal Government and DoD mandates did not provide direction on what data or applications should be moved to the public cloud. When a Cloud First model appeared around 2010 it was a step forward, but many providers still didn't have the right solutions for the government customer. There was a strong push for adoption based on the promise of lower costs with simplified administration and access. The initial challenges of Cloud First dealt with the capability of public cloud providers to provide the necessary security controls and certifications needed to host the various classifications of data that are designated by the U.S. Federal Government and DoD. As cloud efforts were planned and pursued other disadvantages of Cloud First became evident. Vendor lock-in, limited data controls, limited to no flexibility in operational models, bandwidth requirements, and cost over-runs all bubbled to the top during deployments in scenarios.

By the numbers:

- U.S. Federal spending on Cloud rose to $6.6 BN in 2020
- Federal spending on cloud is projected to rise to 7.8 BN by 2022
- Cloud cost overruns are expected to impact 60% of on-premise budgets by 2024
- Cloud costs management is the biggest concern on running cloud big data technologies and applications

Evolution to Cloud Smart

The Department of Homeland Security (DHS) in partnership with the American Technology Council (ATC) presented a report to the President of the United States that outlined the shortcomings of the legacy Cloud First Strategy and recommended the pursuit of a Cloud Smart policy in 2017. The report recommended redefining Cloud Computing to include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The report also provided guidance on the use of private, hybrid, and multi-cloud operational models alignment to the characteristics that best suit the mission needs of the organization.

Cloud Smart is an enabler for Cloud Repatriation. Cloud repatriation provides greater flexibility to run workloads in the most appropriate cloud (public, private or hybrid). It is the recognition of the public cloud as another tool to enable the enterprise architectures to support the U.S. Federal and DoD missions.

Cloud Solution Guidance

How Dell Technologies Interprets Cloud Smart

Dell Technologies believes the answer to Cloud Smart for the U.S. Federal Government and DoD is a multi-cloud solution. It's crucial to align hybrid and private cloud solutions to the right missions and operational environments.

Public Cloud

Public cloud can be an integral part of a Cloud Smart strategy. The key to success is to abandon the old philosophy that migrating everything into the public cloud will drive efficiencies and to leverage its positive capabilities appropriately to support your enterprise infrastructure planning.

Key values for public cloud include:

- Global reach and resilience
- Extensive marketplace of services and capabilities
- Self-service
- Chargeback/show back
- Highly scalable
- Effective for low access data storage
- Ability to consume as a service

Key risk considerations for public cloud include:

- Possible inability to control where data will be located geographically
- Restrictive contract terms
- Vendor lock-in
- Possible high costs for high data access and data manipulation
    - This can be a considerable cost and risk for organizations that want to leverage data for image processing, AI/ML development, and other big data projects

Private Cloud

Establishing Private Cloud services within an organization with the goals of consolidating infrastructure and reducing overhead is another piece of the cloud strategy that organizations should leverage. Private clouds can on premises or in co-location facilities and be managed internally or by 3rd parties.

Key values of private cloud include:

- Customization to develop the cloud platform that best suits the mission requirements
- Security control; the solution can live within the organization's existing IT infrastructure
- 2-4x lower cost

Key risk consideration for private cloud:

- Cost controls are the primary challenge as the organization must cover the development and deployment costs up front. This risk can be offset through various financing models.
- IT overhead costs to manage and maintain the expertise to manage and operate the infrastructure. This risk can be offset via managed services solutions.
- Scaling to meet spikes in resource demands can be challenging if not pre-planned.

Hybrid Cloud

A Hybrid Cloud allows organizations to leverage the benefits of both public and private cloud while offsetting risks through appropriate workload assessment and placement.

- Leverage secure workloads in the private cloud while leveraging the public cloud for lower value data to balance costs versus security considerations.
- Leverage the public cloud infrastructure for its global reach to enhance mission capabilities while using private cloud in remote/edge scenarios to ensure mission function on the ground.
- Leverage the capability to develop once and run anywhere applications that have capability to run in private and public cloud arenas allowing developers and their missions to take full advantage of data where it is the most cost effective.
- Process data at the edge in private cloud scenarios and leverage the public cloud to transfer back results and findings to cut down on bandwidth requirements.

The key goals for a hybrid cloud solution are the capabilities to manage data, services, and applications under a connected management framework.

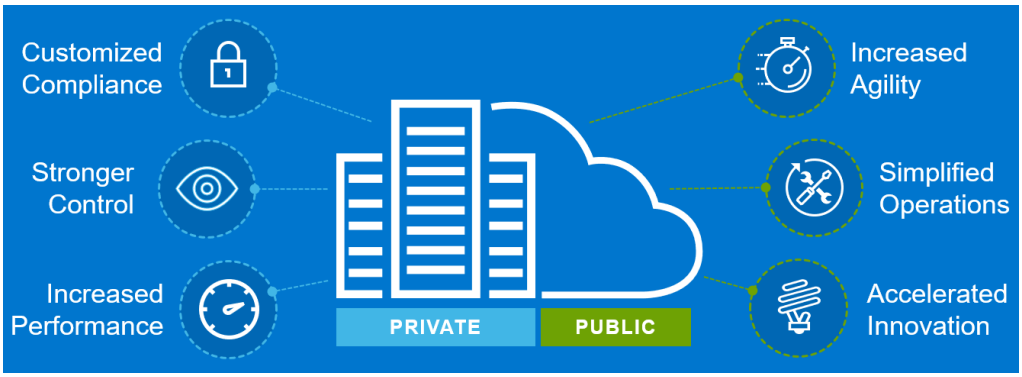

Figure 1 Balancing Private and Public Cloud

Workload Placement

The key to understanding workload placement is to understand that cloud is not a place, it is an operating model. This allows the organization to continually assess the best operating model for changing mission goals.

Assessment of workload placement focuses on ensuring the operating model will meet the infrastructure and deployment options that meet the mission requirements.

- Start by determining and assessing where each workload will work best.
- Optimize each workload by matching it to the infrastructure that best meets requirements
- Dell Technologies' hybrid cloud offers the opportunity for customers to manage their entire infrastructure through a single pane of glass. This approach provides workload agility—the ability to flexibly and seamlessly move workloads between environments.

Workload optimization depends on having the right options available at the right time, by making them quickly available based on changing operational factors.

Cloud Smart delivers an intelligent, dynamic, requirements-driven approach to cloud.

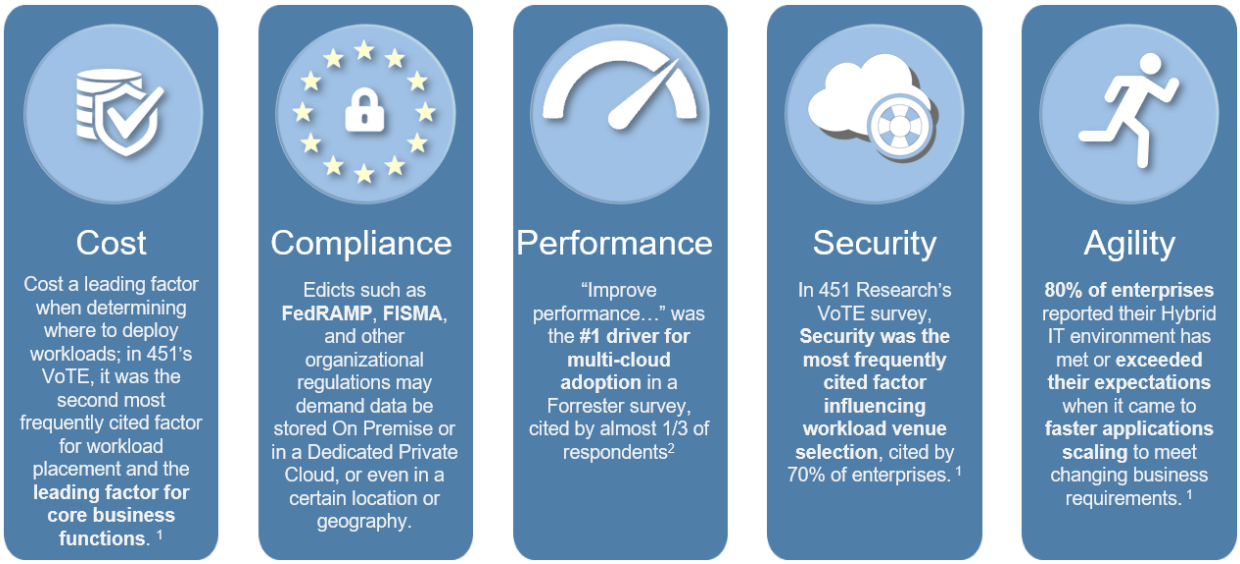

Figure 2: Key Considerations for Workload Placement

Dell Technologies Delivering Cloud Smart in Federal

Dell Technologies is uniquely positioned to help organizations with their cloud journey. Dell Technologies solutions span every section of the technology stack, with support options available every step of the way, and with a broad community of cloud partners to help build exactly what is required.

Dell Technologies Agile Multi-Cloud

The key to a successful multi-cloud approach is establishing an agile service-delivery architecture and set of data services to provide consistent capabilities across a choice of endpoints spanning hybrid multi-cloud environments.

Dell Technologies has developed a 7-layer approach to drive a consistent cloud operating model.

- Service Management: Capability for people or software to place requests for IT services via APIs or web services.
- Business Operations/Management: Process and governance model to establish policy driven rules engine to ensure security, support for outcome goals, and alerting.
- Automation and Orchestration: These elements work together to execute and deliver the requirements of the infrastructure across the multi-cloud environment. This could include resource provisioning, expansion, or retraction.
- Cloud enabled compute, network, storage: The infrastructure must deliver API driven, cloud enabled compute, network and storage resources. Their robust sets of "APIs" turn infrastructure into code controlled by the cloud management platform in a programmatic fashion.

Controlling the cloud management layers is critical to maintaining the capability to avoid vendor lock-in for public cloud elements in a multi-cloud approach.

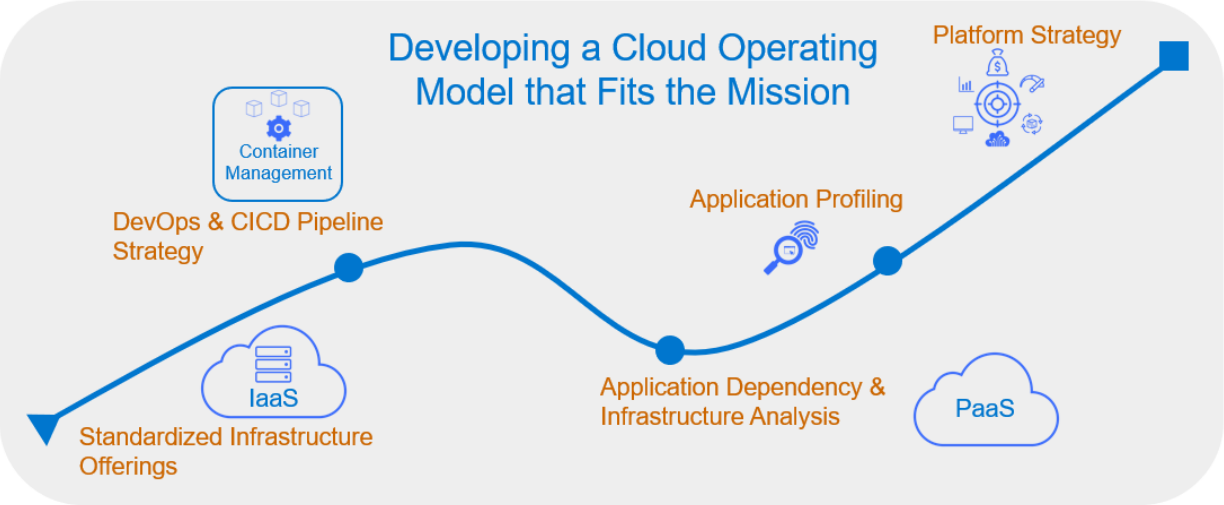

Figure 3 Cloud Operating Model

The Bones of a Successful Multi-Cloud Architecture

Dell Technologies has partnered with VMware to deliver industry leading cloud management software for both traditional and cloud native application. VMware is the dominant platform for traditional 3-layer applications, delivering the industry's best infrastructure as a service platform for the majority of business applications.

With its Cloud Foundry and Kubernetes offerings, Pivotal is the industry leader in delivering a development and deployment platform designed for the latest cloud-native containerized and function-based applications. In addition, Pivotal Labs educates customers on how to build and deploy these next-generation applications to get the most business value.

For the vast majority of organizations, VMware and Pivotal deliver the best cloud experience, and both invest in partnerships to ensure the deepest integration across the cloud landscape.

For example, in combination with Dell EMC's hardware platforms, Dell Technologies provides integrated infrastructure services and solutions for Private cloud deployments, and Dell Technologies also partners broadly across the enterprise cloud and public cloud vendors.

That same Dell EMC hardware and VMware and Pivotal software stack runs in thousands of global leading enterprise-class clouds, that carry specific SLAs or vertical specific services that your industry may need. Dell Technologies continues to partner at every level with all of the major public cloud players.

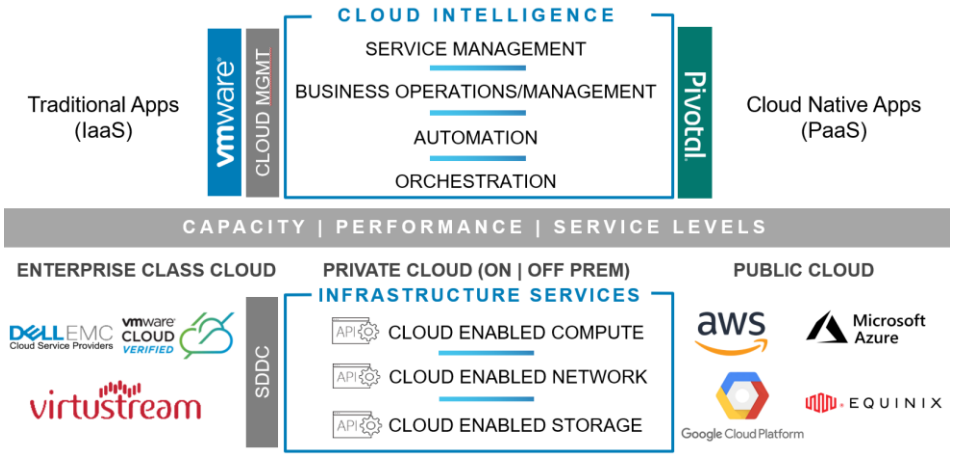

Figure 4 Supporting the 7 Layers for Agile Multi-Cloud

Services and Lifecycle to Support a Data Fabric Vision

A critical element in starting or assessing where an organization is in their cloud journey is Lifecycle Services. Dell Technologies has the breadth and expertise to deliver this vision to any organization through a single relationship.

Dell Technologies has support teams that are dedicated to helping organizations implement, adopt and scale cloud.

Dell Technologies has an established partnership ecosystem, including AWS, Google Cloud, Azure, Equinix, and more than 4,200 other cloud partners across 120 nations, that helps provide a frictionless hybrid and multi-cloud cloud experience.

Dell Technologies prioritizes sustainability, particularly with the new APEX Cloud service. Dell Technologies will recycle or re-use 95% of APEX infrastructure, sanitizing and remarketing technology that can be recovered, and recycling (in an environmentally friendly and compliant manner) that which cannot be redistributed. Dell Technologies has also achieved an ISO 14001 certification for environmental management

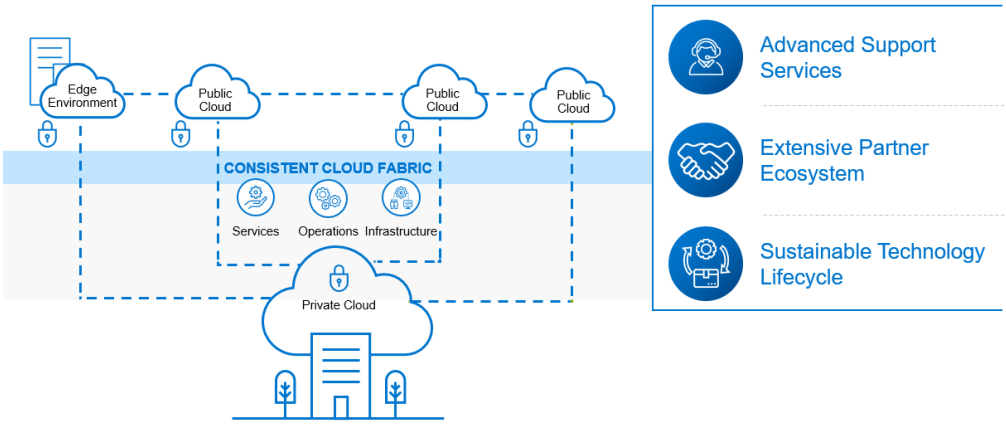

Figure 5 Lifecyle Support for Multi-Cloud

The Edge is Critical in Multi-Cloud

U.S. Federal and DoD agencies have an ever-expanding challenge to meet IoT and Edge mission requirements. Dell Technologies views the IoT ecosystem as comprising edge, distributed core and cloud, which function as zones of intelligence that perform analytics while it matters, where it matters, with the edge being closest to the things or data sources and performing real-time decisions.

- Private Cloud: On-prem (or co-location) and ingesting and processing massive amounts of edge data for both near real time sophisticated decision making as well as machine learning to train and optimize edge models
- Public Cloud: Off-prem and integrating IoT data with massive data sets, including business applications and other clouds, to perform deep learning for strategic insights that improve the overall performance of the IoT ecosystem over time.
- Edge: Could be isolated, possibly low-latency, bandwidth-restrained capabilities closer to the point of service delivery.

As data moves through this ecosystem of Edge, Private Cloud and Public Cloud, Dell Technologies sees it all working together as a virtuous cycle, delivering continuously better outcomes for your agency, as data flows in from the Edge through to the Private Cloud and Public Cloud, and new models get pushed back out.

Figure 6 Spectrum of the Edge

The Private Cloud provides powerful compute, networking, and storage for rapid, sophisticated decision-making. A distributed-core approach places enterprise-class, data-center-level compute, storage, and networking close to the data source. This approach decreases the volume of data that needs to traverse through the cloud and back to the data center. The result is faster mission-critical response at the edge with increased security of data, and decreased exposure to transport bandwidth costs and limitations.

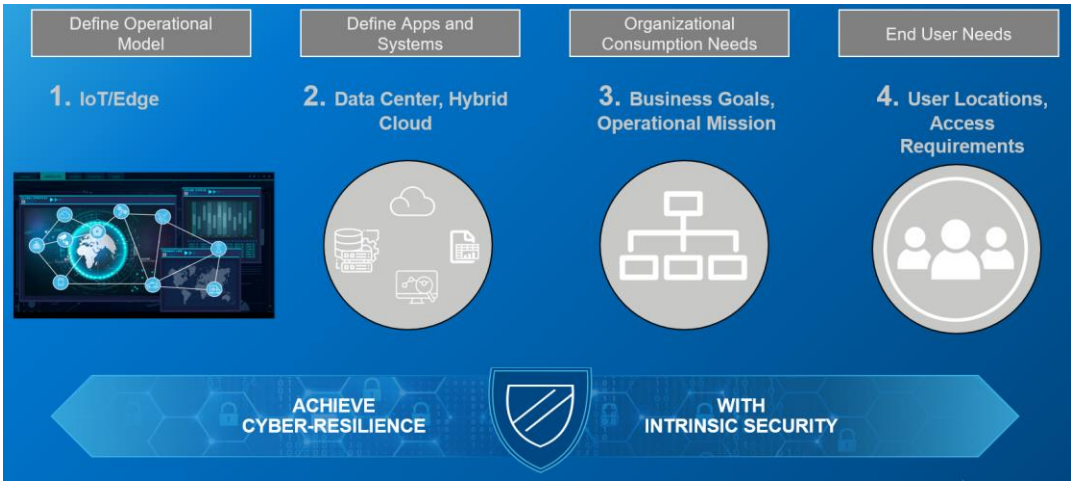

Figure 7 Full Solution Edge to Cloud Approach

Dell Technologies Approach to Zero Trust

Due to the increases in ransomware, security vulnerability exploitations, and supply chain attacks there is a renewed interest in Zero Trust Principles for cybersecurity. There are a number of US Federal and DoD directives on the topic, as well as the National Institute of Standards and Technology (NIST) reference architecture. This enables organizations re-assess their current approach and application of Zero Trust Principles. The challenge is how to fully understand where they are in their journey and whether their current cybersecurity framework roadmaps will help them achieve the best outcomes.

How Dell Technologies Looks at the Zero Trust Model

Dell Technologies leverages the NIST Special Publication 800-207: Zero Trust Architecture tenets.

- All data sources and computing services are considered resources
- All communication is secured regardless of network location
- Access to individual enterprise resource is granted on a per-session basis
- Access to resources is determined by dynamic policy
- The enterprise monitors and measures the integrity and security posture of all owned and associated assets
- All resource authentication and authorization are dynamic and strictly enforced before access is permitted
- The enterprise collects as much information as possible related to the current state of assets and uses it to improve its security posture

The Dell Technologies 7 Pillars of Zero Trust

Dell Technologies has developed a derivative model from the NIST SP 800-207 model. The goal of the model is to make it easier for cybersecurity leaders to assess their current cybersecurity framework and explain to others how Zero Trust Principles enhance the security model.

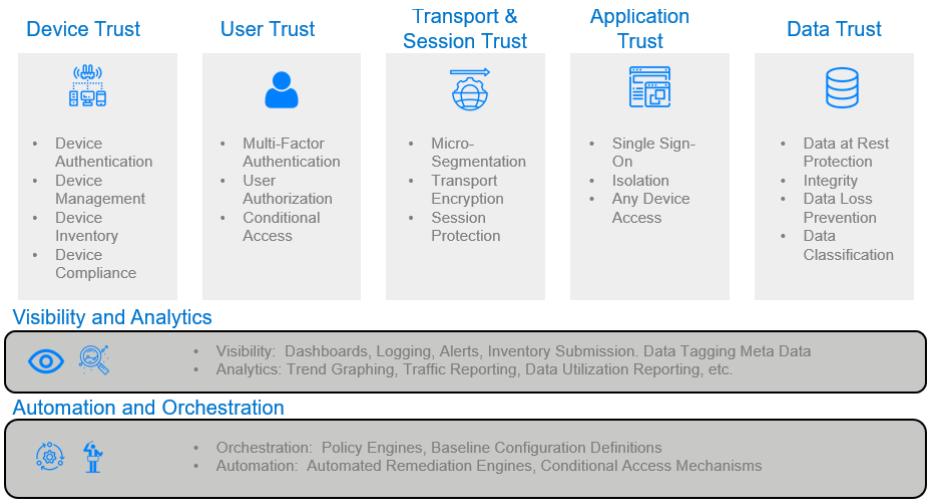

Figure 8 The 7 Pillars of Zero Trust

The 7-Pillars are set out in a manner that allow for the visualization of distinct assets and communication flows.

Device Trust: Defined as any physical device within the enterprise. Examples would include end user devices (smart phones, tablets, laptops, etc.), data center devices (servers, storage, network switches, etc.) IoT devices (sensors, cameras, kiosks, etc.).

User Trust: Defined as end user, administrator, and service level accounts.

Transport/Session Trust: Defined as the communication path utilized to move into, across, and out of an enterprise network.

Application Trust: Defined as both local and cloud applications that enter, work within, or leave the network for data access.

Data Trust: Defined by the organization as key assets used to execute the function and mission of the organization that can be held within the enterprise and extended into cloud services.

Visibility and Analytics: Defined by the resources from the 5-Pillars that should be enabled, to the fullest extent, to allow for analysis of the secure state and function of the pillar definition.

Automation and Orchestration: Defined through the use of the visibility and analytics output to perform policy enforcement, baseline configuration definitions, automated remediation, and conditional access models.

Zero Trust in a Multi-Cloud Environment

The key elements to a successful deployment of a Zero Trust principled architecture approach are data governance and identity and credentialing access management.

Data governance is a data management concept that references an organization's ability to ensure the quality of data throughout its lifecycle. The key focus areas of data governance include availability, usability, consistency, data security. Agencies should also establish accountability processes in case of poor-quality data is input into the system, creating a negative effect across the organization.

Identity Credential and Access Management (ICAM) comprises the tools, policies and systems that allow an organization to manage, monitor and secure access to protected resources.

A multi-cloud environment with a properly developed Zero Trust principle security model enhances the capability of ICAM and data governance by limiting the unnecessary transfer of data throughout the enterprise when personnel or support applications require direct access. Data can be acted on, access-controlled, and governed based on where it is in the overall infrastructure. This approach allows for the movement of only the data needed to drive the mission outcome. Examples could include processing IoT sensor alert and metrics data at the edge and sending the results back to the cloud for AI/ML analysis. Sending all of the sensor data without filter creates another potential point of failure because of the increased risk across numerous transport layers.

Dell Technologies Cloud to Edge Ecosystem

The old Cloud First thinking drove a lot of single-threaded cloud provider solutions. It is now clear in the Cloud Smart approach that the world is a multi-cloud environment. Dell Technologies has developed partnerships that are critical to providing Federal and DoD organization with the best opportunities to succeed, no matter where their data resides.

How Dell Technologies can help with the multi-cloud journey:

- Helping organization identify the best on- or off-premises solutions for each workload
- Identifying CSP Partners that can deliver more than a thousand as-a-Service offerings powered by Dell Technologies
- Ensure flexibility to provision, scale up, and scale down application resources
- Maintain choice to manage and move workloads
- Provide choice across Infrastructure, Software and Applications, Data Protection, Security, Desktop, Big Data, Development Platforms and other solutions

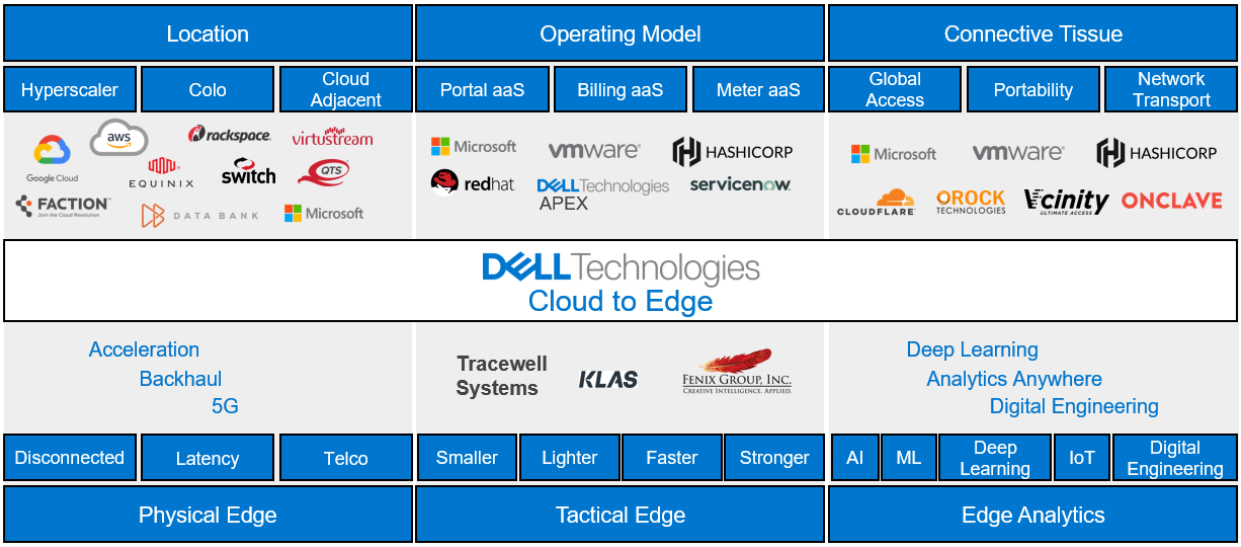

Figure 9 Cloud Edge Ecosystem

Conclusion

Dell Technologies believes that Cloud Smart means agencies must consider how to use their current resources effectively. Cloud Smart is about a holistic approach that considers where data is produced, what the customer wants to do with the data, and how that data is served to the people who need it to be successful. Dell Technologies can work with customers to help equip agencies with the tools and knowledge they need to make these decisions for themselves, rather than a one-size-fits-all approach.

With Dell Technologies capabilities to help organizations understand modern technologies and practices, they will be able to harness new capabilities and expand existing abilities to enable their mission and deliver services to the public faster. To make this shift, instead of "buy before build", agencies will need to move to "solve before buy," addressing their service needs, fundamental requirements, and gaps in processes and skillsets before starting on a new procurement. By rationalizing their application portfolios regularly, agencies can continue to make modernization progress while targets move with the ever-changing technology landscape.

References:

- CIO.Gov Cloud Smart Strategy, https://cloud.cio.gov/strategy/
- Federal Cloud Spending 2020, Federal Cloud Spending Rose to $6.6 Billion, Despite Slowing Growth Rate – MeriTalk
- Projected Federal Spending on Cloud, [Free Summary] Federal Cloud Computing Market, 2020-2022 (deltek.com)
- Cloud Cost Overruns, Cloud Migration Costs and Avoiding Overspend (gartner.com)
- Cloud Cost concerns, https://www.prnewswire.com/news-releases/new-survey-reveals-one-third-of-businesses-are-exceeding-their-cloud-budgets-by-as-much-as-40-percent-301216394.html