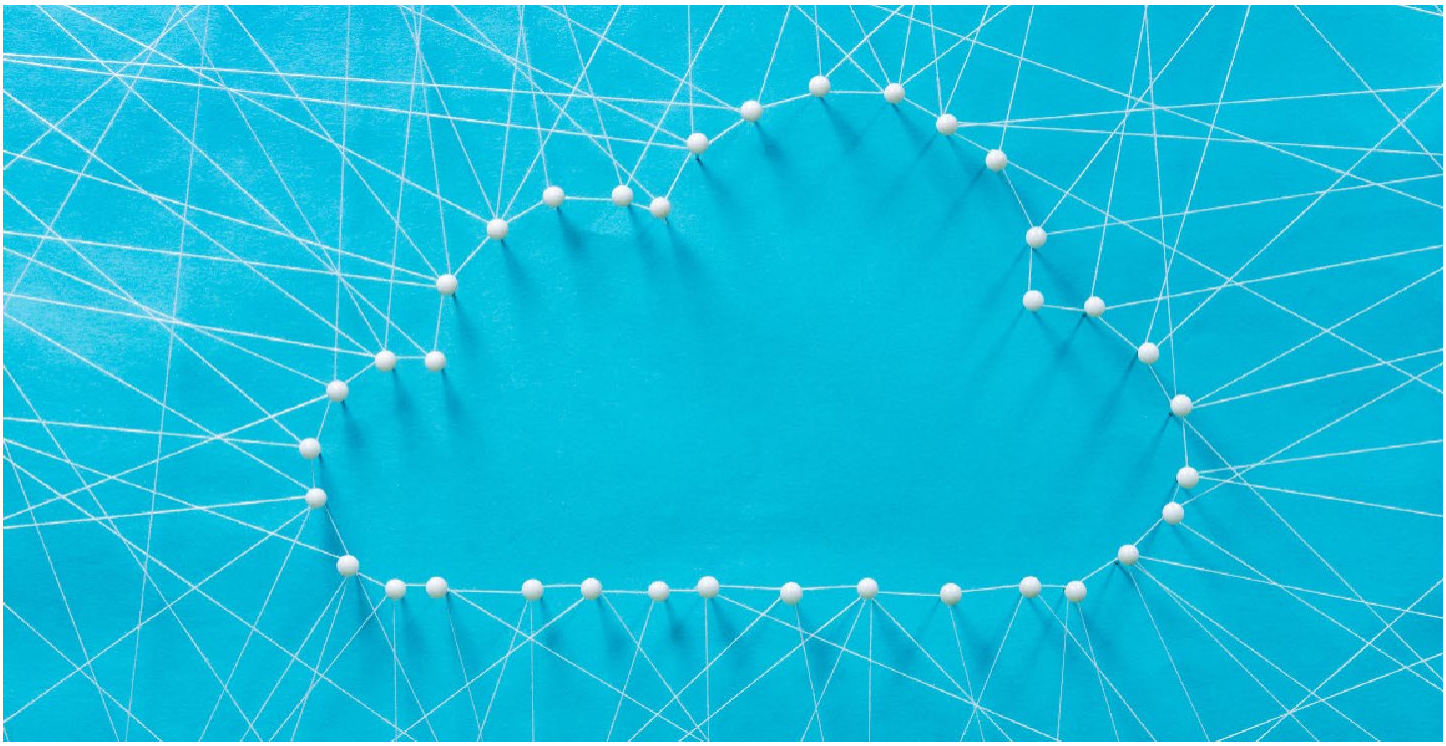
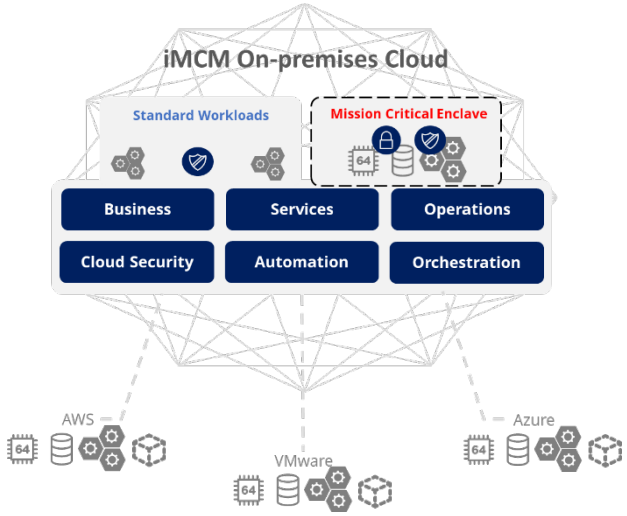
Deloitte.



Integrated Multi-Cloud Management Solution Architecture

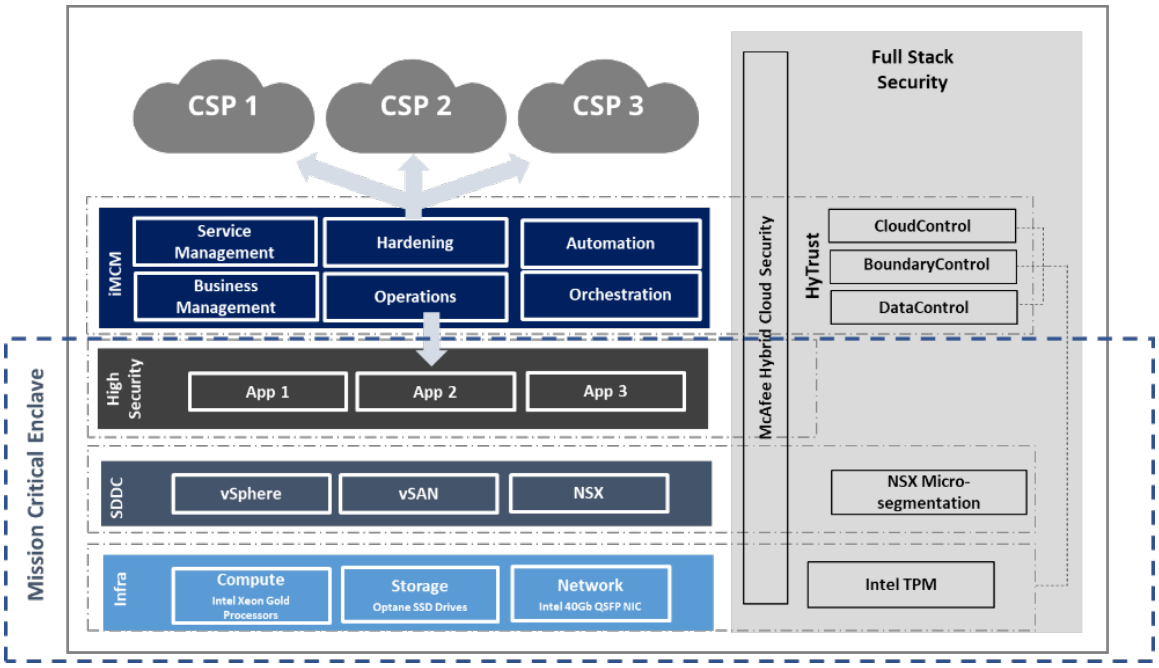
Introduction

Hybrid Cloud environments consisting of on-premise private cloud and rapidly adopted external public cloud services are becoming broadly implemented in the federal government space. Even as the transition to innovative but external cloud services accelerates, there is a demand to provide similar agile, elastic, reusable, and high-performance services for mission critical workloads running in highly secure environments within government data centers. Additionally, federal IT leaders are under tremendous pressure to respond to these rapidly expanding technical challenges and comply with a growing and evolving set of mandates, including cloud policies that address significant concerns, such as regulatory compliance, risk, and security. Deloitte, leveraging an ecosystem of leading technologies, has developed an integrated multi-cloud management (iMCM) solution where application workloads can be deployed to external clouds or on-premise environments based on requirements and best-fit, but managed through a common and standardized management plane. This allows for the application of standardized policy, processes and governance across multiple cloud environments to help maintain compliance with evolving federal mandates. Our multi-cloud solution can enable quicker deployments, accelerate security accreditation, and streamline the use of cloud services to help deliver the most value to any IT organization. The on-premise solution consists of two workload-specific compute clusters.



Overview of the Hybrid Cloud Mission Critical Enclave Architecture

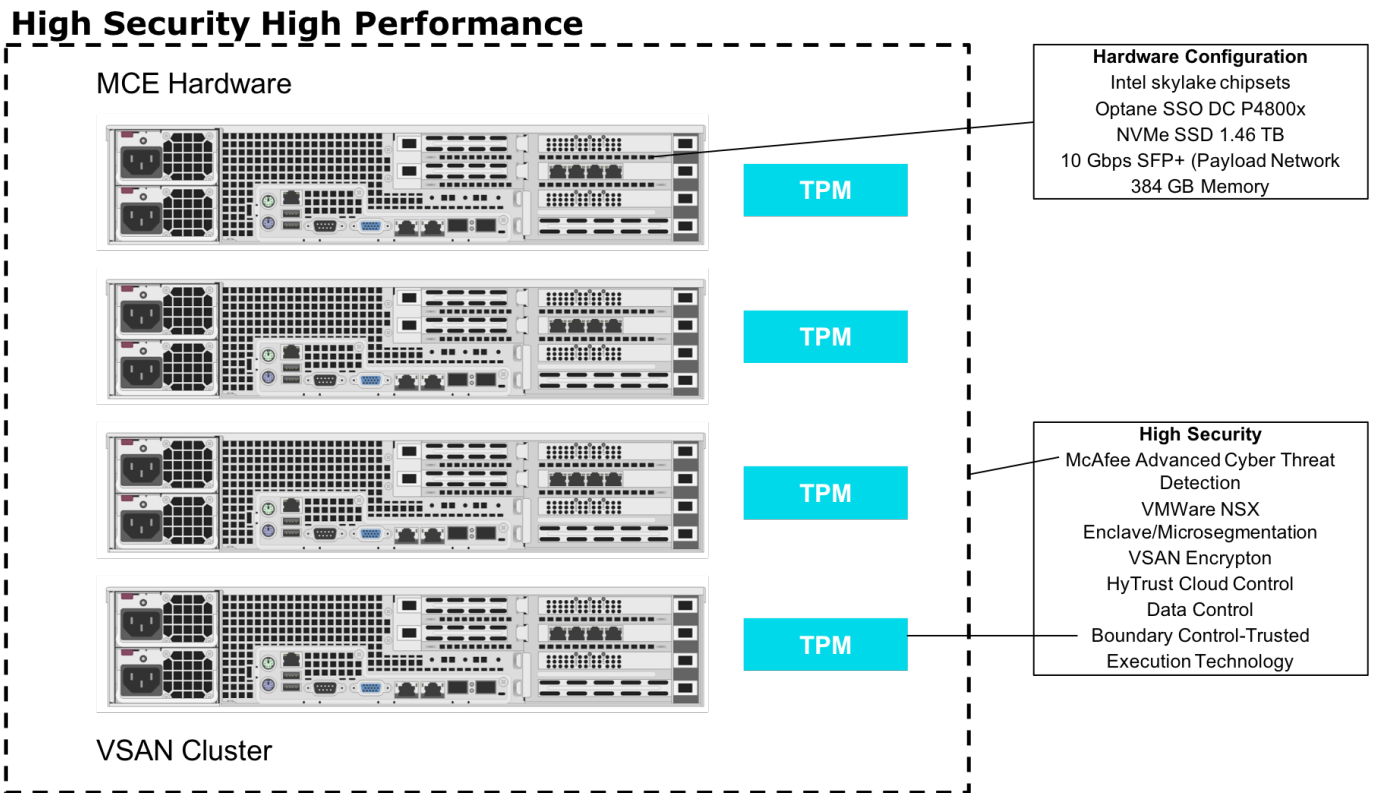
The Hybrid Integrated Multi Cloud Management solution coupled with the Mission Critical Enclave (MCE) capability offers performance, security, and operability by integrating advanced hardware and software components from IT market leaders with the industry knowledge of professional services. Deloitte has developed and benchmarked the Hybrid Integrated Multi Cloud Management solution described below and as such we are including the specific technologies to provide context to that baseline. The four layers of the iMCM MCE core stack, depicted below, are further explained in the following sections.



Infrastructure

The infrastructure layer, containing the compute, storage, and network components of the Hybrid Cloud MCE, leverages the following readily available hardware selections:

Component	Description
Dell PowerEdge R640 Rack Mounted Servers	Enables dense scale-out data center computing and storage through a dual-socket platform that also provides embedded diagnostics and SupportAssist. In the reference configuration, each server has been configured with 6 – 1.46TB high performance NVMe SSDs and 2 – 350GB state-of-the-art Optane drives for superior performance.
Intel Xeon Gold 5115 Processor	Provides Intel's advanced hardware-enhanced reliability, availability and serviceability (Advanced RAS) and is highly scalable to support a wide range of existing workloads for a modern hybrid cloud business strategy. Built on 14 nm process technology and configured with 10 cores/20 threads per socket for increased performance, the Intel Xeon Gold 5115 has a Processor Base Frequency (Clock speed) of 2.40 GHz with capability to reach 3.2GHz at Max Turbo Frequency.
Intel Trusted Platform Module (TPM)	Enables secure system start-up processes and is leveraged by Intel TXT to store measurements (hash of components) of the platform. The advanced features of TPM enable the measurement, storage, encryption and reporting of the current state of the platform data.
Intel 40Gbps Quad Small Form-factor Pluggable (QSFP)	Enables inter-server connectivity required for vSAN operations. Each server is equipped with 2 QSFP ports which provide high availability and allow for multi-pathing.
Intel Optane SSD DC P4800X	Supports the storage tier with dual cards and features 3D XPoint memory media, which utilizes the property- change of the memory material itself, to store the data and when coupled with Intel-developed controller and firmware, helps take SSD performance to the next level.



SDDC

The Software Defined Data Center (SDDC) layer on top of the infrastructure provides abstraction between the operating system, applications, and hardware. While traditional storage and network implementations require complex, proprietary, costly infrastructure and labor resources with often difficult to find skill-sets, SDDC enables organizations to simplify the management of their compute, storage and network through the following solutions:

- vSphere provides a powerful, flexible, and secure foundation for business agility that can accelerate the digital transformation to hybrid cloud and success in the digital economy. It helps run, manage, connect and secure applications in a common operating environment across the hybrid cloud. With vSphere, iMCM can support new workloads and use cases while keeping pace with the growing needs and complexity of infrastructure.

- vSAN delivers flash-optimized, secure shared storage with the simplicity of a VMware vSphere-native experience for all critical virtualized workloads. vSAN 6.7 is architected for the hybrid cloud with operational efficiencies that reduce time to value through an intuitive user interface and provide consistent application performance and availability through advanced self-healing and proactive support insights. Seamless integration with VMware's complete SDDC stack and leading hybrid cloud offerings makes it one of the most complete platform for virtual machines—whether running business-critical databases, virtual desktops or next-generation applications.

- NSX is the network virtualization platform for the SDDC, delivering networking and security entirely in software, abstracted from the underlying physical infrastructure. NSX Data Center enables the Virtual Cloud Network, providing pervasive, end-to-end connectivity and security for apps and data through micro segmentation and policy-based network configurations.

iMCM

The Multi-Cloud Management stack consists of several integrated layers, each one providing a specific set of capabilities, which are complementary to the overall solution. These solution layers work in conjunction with the orchestration platform and the hardening environment to deliver iMCM's value. Each solution layer is summarized in the points below:

- The Business Management layer facilitates informed decision making. This layer includes the tool set that provides transparency and control over the costs and quality of IT services, enabling the decision makers to align IT with the mission by comparing the costs of workloads between the private cloud and multiple public clouds.
- The Service Management layer provides a common unified portal to allow users with role-based authorization to request IT Services across clouds. It includes a workflow management and automation capability to implement a service catalog and governance that spans the entire multi-cloud operational environment in a manner that is streamlined for the user.
- The Operational Management layer offers a single pane of glass command and control panel, which provides operations staff cloud administration, performance monitoring/tuning, risk mitigation, and troubleshooting capabilities.
- The Automation layer provides consistent deployment and management of IT services while reducing manual processes and helping to limit human error and ensure compliance with policies. Automation enables significant operational efficiencies by reclaiming inactive resources that may be repurposed to other applications based on dynamic mission demands.
- The Orchestration platform enables the automation of complex IT tasks to adapt and extend service delivery and operational management across clouds. The orchestration platform is the engine by which the Automation and Operational Management layers provide deployment, remediation and adherence to industry- standards and/or organizational policies. Additionally, it includes the ability to automate and orchestrate with PaaS, SaaS, and Serverless/Containers/Microservices.
- Hardening and Security Management for the Hybrid Cloud Mission Critical Enclave is implemented through a suite of leading technical products that can effectively meet agency hardening guidelines and control requirements and enables strong security management for workloads in both public and private clouds. These management techniques leverage best practices in Cloud Business Management, Data Encryption/management, Privileged Account Management, Password Vaulting, and Cross-cloud security threat detection and mitigation to provide effective security in an elastic environment, multi-cloud ecosystem.

Mission Critical Enclave Security

Deloitte's Multi-Cloud Management enforces control and governance from the physical hardware up through the application software, and several layers in between them:

- Intel's Trusted Platform Module securely stores keys, passwords and digital certificates in onboard microcontrollers and Trusted Execution Technology is a hardware extension that attests application authenticity and protects against software-based attacks while protecting the confidentiality and integrity of data stored and created on servers.
- Software Defined Networking implements VLANs and microsegmentation along with selective firewalling of data transiting networks internally as well as externally. Additionally, all traffic is secured with encryption keys and authorized certificates both internally between servers, and externally thru encrypted VPNs to any CSP extension, and resources therein.
- Virtualization host servers are built hardened and protected with an audited, rotated, single-use strong password control system for access. Operating System Virtual Machine gold images are built and deployed to DISA STIG specification.
- Compute Workloads are provisioned automatically to a Zero-Trust model, adhering to appropriate placement and access policies are restricted or allowed, as necessary.
- Notable iMCM product suites that actively govern security policies are HyTrust Boundary Control and an enterprise-class security suite (such as McAfee EPO, Microsoft ASM, of or Symantec SEP solutions) covering Cloud Security, Data Protection and Encryption, Endpoint Protection all managed through automated orchestration.
- Software-Defined Data Center operational maintenance is controlled by a dedicated Lifecycle Manager which keeps all virtual infrastructure components up to date, patched, and interoperable by its compatibility matrix.
- Cloud Native Platform as a Service lays groundwork for agile containerized applications and services lending itself to additionally resilient and granular affinity and anti-affinity policy control.
- Compliance is monitored constantly with multiple tools in both Security and Operational modules with ability to programmatically quarantine misaligned resources and remove threats.
- Data Protection is maintained though server and storage clustering, hardware and/or software backup appliance technology, virtualization data protection and replication of defined application groups to accommodate desired Disaster Recovery and Business Continuity RTO/RPO policies.

Advanced Security through Threat Identification and Protection

Deloitte's Multi-Cloud Management is designed to provide defense across the multiple layers of the mission critical enclave, securing from the hypervisor (SDDC) all the way through the application layer. Described below are the advanced threat defense suite of products that were utilized as part of our benchmarking. Our approach to providing advanced security is technology agnostic and Deloitte would tailor this solution to reflect the client's choice of security providers as part of their existing and planned system architecture.

Security Feature	Description
Centralized Management Console	Component for supporting products within the installation, software management and deployment, and reporting. The console managed the systems topography and is required to support the data center infrastructure.
Network Security Platform	Provides network security management and protection for the enclave. This component combines intelligent threat prevention at the network layer and extends it beyond intrusion, matching signatures with layered signature-less and emulation technologies.
Cloud Security Component	Allows the discovery, import, management and securing of all cloud-based infrastructure such as AWS, Azure, and VMWare vCenter. Offers improved visibility and control to address the unique requirements of public cloud server security.
Advanced Threat Protection	This component goes beyond traditional sandboxes to deliver broader protection and expose evasive, well-hidden attacks. Drawing on the tight integration from the network to the endpoint, it instantly shares information across the environment to accelerate threat investigation and protect the mission.
Threat Intelligence Sharing Network	Enables collective learning across the defense fabric to neutralize emerging threats more quickly.
Policy Auditor	Provides the tool for compliance auditing and reporting on the asset portfolio, vulnerabilities, and configurations of the enclave.
Data Loss Prevention ("DLP") Platform	Suite of products designed to protect various data types as they move through the network. The platform consists of: • DLP Endpoint – Centrally managed policies to control the use and transfer of sensitive data and provide detailed forensic reports. • Device Control – Comprehensive device management to help control and block the exfiltration of confidential data through removable storage or similar means. • DLP Discovery – Performs file scans and collection jobs to search endpoints, servers, Box, SharePoint, and database repositories to identify and protect sensitive data. • DLP Prevent – Works with web proxies and mail transport servers to protect web and email traffic. • DLP Monitor – Passively scans unencrypted network traffic for potential data loss incidents.

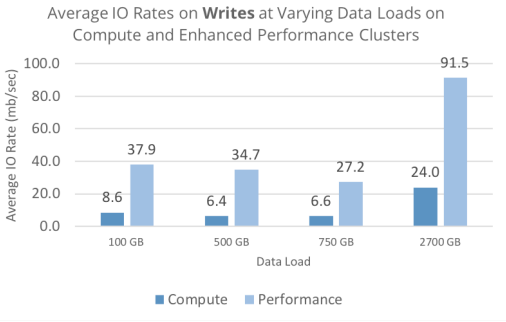
Benchmarking Performance

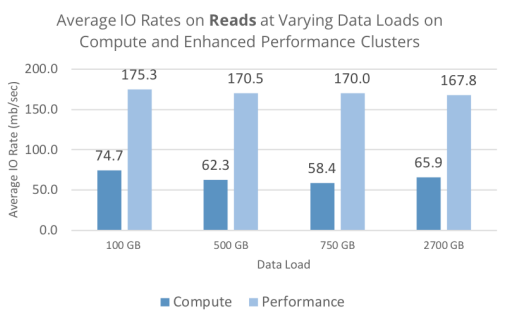
The advanced performance capabilities of the hybrid cloud MCE have positioned it to be a preferred solution for compute and IO-intensive critical workloads. Whether running advanced analytics on extremely large data sets or enabling security-driven workloads to get cloud-like performance in on-premise environments, the hybrid cloud MCE can perform at the highest tier. For example, our tests using a high-performance compute cluster of Dell EMC and Intel technologies previously mentioned demonstrated significant performance improvement over a standard compute cluster when running benchmarking stress tests using tools like TestDFSIO, Teragen and Terasort. The findings below further support the hybrid cloud MCE's compute performance:

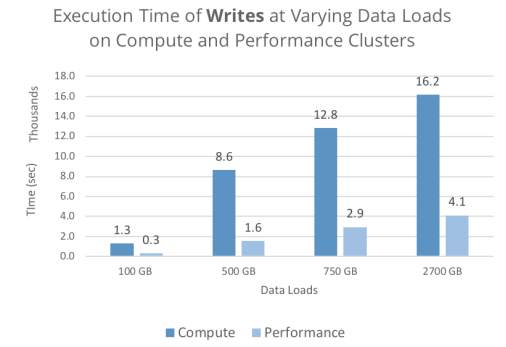
TeraSort Hadoop Benchmark Test: Performance Cluster wrote data to disk 3.5 times faster and sorted the data 2.5 times faster than the Standard Compute Cluster

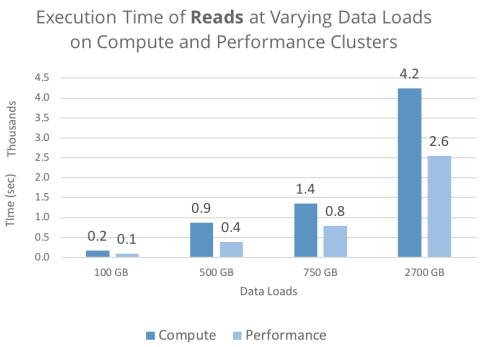
TestDFSIO Test: Throughput increased 4 to 5 times when writing to disk and 2 times when reading at varying data loads on the performance cluster. The Average IO found from the TestDFSIO test also showed that writing to disk increased 4 to 5 times and disk reads increased 2 times on the performance cluster at varying data loads and a replication factor of 3.

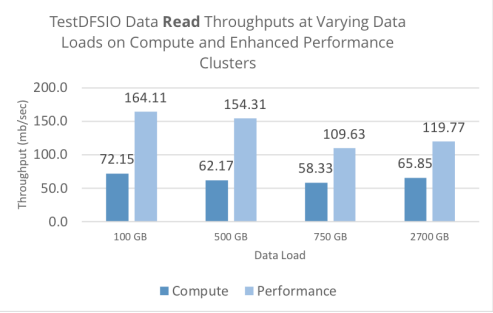
These diagnostic evaluations illustrate that any IO intensive workload, like aggregating data received from in-field IoT devices and then storing the continuous data stream prior to running analytics tools, such as Hive or Spark, should be targeted towards the MCE high-performance compute cluster. With this ability, predictive analytics can identify and remediate issues prior to failure and disruption to services. The figures summarize test results.

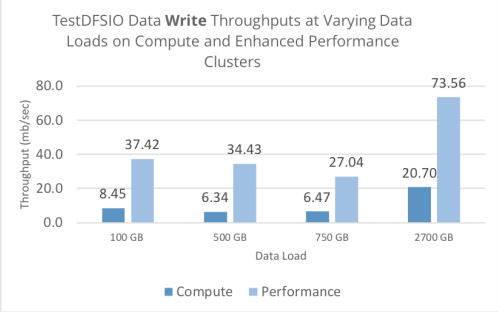












Conclusion

The iMCM solution features a robust hybrid framework that provides a flexible multi-cloud management toolset, including a service and organizational component that delivers capabilities across on-premise and public infrastructure. Through iMCM, disparate cloud ecosystems are tied together into one common cloud management solution to deliver a comprehensive view and maintain operational control of resources and workloads running across multiple cloud service providers. The iMCM Mission Critical Enclave is the vital component of the solution that enables customers to run highly secure and highly compute and IO intensive workloads on premises while achieving exceptional performance results. As the above performance benchmarking results demonstrate, the MCE based on this reference architecture can provide significant mission benefits for processing of very large datasets and high intensity analytics in very secure environments. With Hybrid iMCM, IT organizations can view and manage IT workloads across cloud providers and on- premise environments to achieve cost, security, and performance

benefits.

Let's Talk

Reach out to our team to request a demo and learn more about how iMCM MCE can help you transform your organization.

Contacts:

Doug Bourgeois
Managing Director
Deloitte Consulting LLP
dbourgeois@deloitte.com
+1.571.814.7157

Sean VanDruff
Senior Technology Fellow
Deloitte Consulting LLP
svandruff@deloitte.com
+1.215.446.4314

Thomas Henry
Senior Manager
Deloitte Consulting LLP
thhenry@deloitte.com