Managed Services for a Hybrid Infrastructure

By Bogdan Udrea

April 2016

Acknowledge the change

IT infrastructures using private and public clouds are gaining momentum. While the hybrid cloud market is expected to reach its full potential within the next few years, enterprises across industries are exploring various models of infrastructure as a service (IaaS) to store less-critical workloads, expand disaster recovery capabilities or deal with compute capacity spikes with cloud bursting for their dedicated infrastructure.

When moving to IaaS, platform-as-a-service (PaaS) and software-as-a-service (SaaS) models, internal IT teams as well as managed services providers (MSPs) need to undergo a major change, which impacts the support structure, underlying processes, and utilized tool sets and technologies.

Such a drastic change comes with challenges, driven by the need to continuously support two different worlds for production environments that span multiple mediums:

- **A well-established, physical infrastructure:** Structured around clear layers of responsibility — from physical data center facilities, network and storage, to application layers
- **A new infrastructure model powered by private and public clouds:** Where segments of the environment are controlled and managed by third-party, everything-as-a-service (XaaS) providers

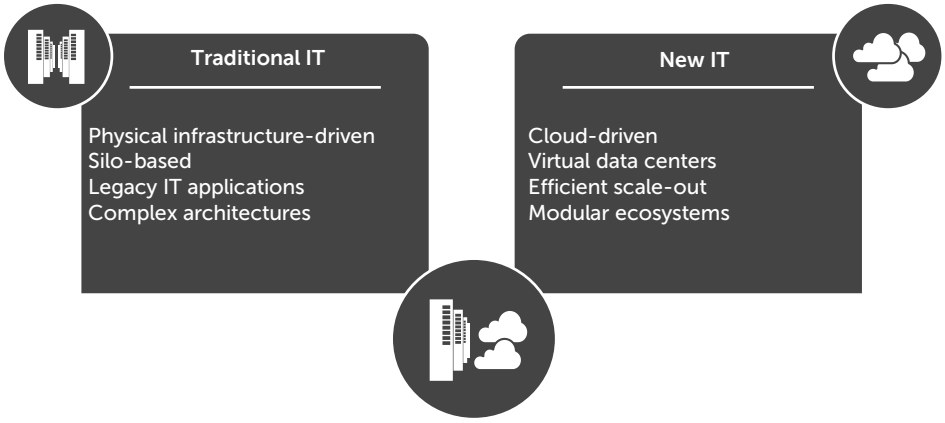

Figure 1. Bi-modal IT scope of control and management

In this white paper, we provide an overview of changes to consider to overcome these challenges, whether your organization is supported by internal IT, an outsourced service provider, or a hybrid model of internal and external IT. The best practices we offer in this paper are based on our own transformational journey from a traditional IT outsourcing provider to an agile, bi-modal IT support provider that deploys, manages and continuously evolves all layers of a hybrid infrastructure.

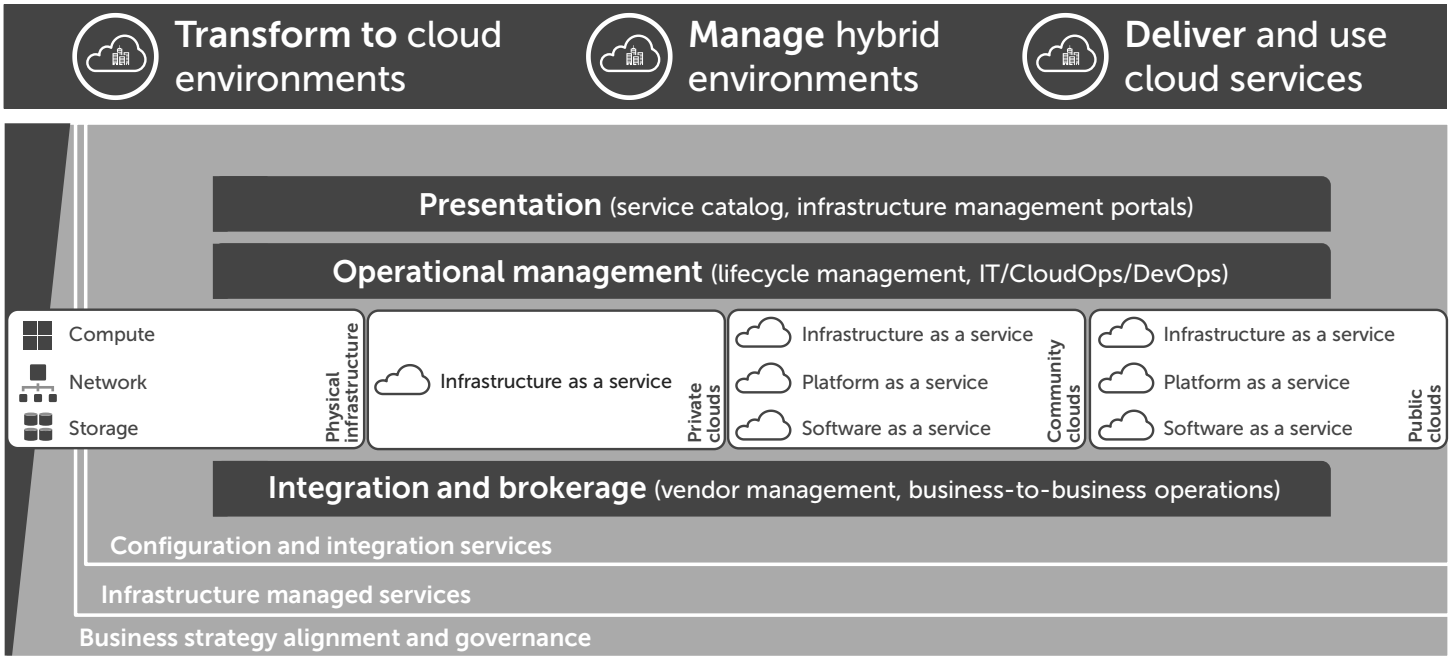

Figure 2. Construction of hybrid infrastructure management

Adopt and operationalize

Typically, IT Infrastructure Library (ITIL)-aligned support models followed a tiered structure, with three to four layers determined by the complexity of the managed environments and siloed or driven by towers and technologies.

From tier 1 support for proactive or reactive operational-level activities, to a tier 3 or 4 level that enabled complex administration and engineering activities, this model provided end-to-end, technology-based service support with matured intra- and cross-tower processes. But with infrastructures for testing, development and production environments spanning physical and virtual data centers, this tower-based, technology-driven support model needed to converge into a fluid and flexible construct.

Based on an agile design, a bi-modal IT service delivery model supports hardware-driven infrastructures as well as cloud-enabled data centers — without adding complex layers and duplicating resources. This model is also built around tiers of support:

- **Tier 1** maintains the first level of infrastructure services delivery, and is typically built above the service-desk/help-desk level. Always-on, cross-skilled, and operating in micro-technology hubs or sub-ecosystems, this tier enables streamlined communication and collaboration to provide quicker issue resolution, data gathering and issue documentation, symptoms analysis, and overall incident remediation based on clearly defined escalation procedures and a cross-technology knowledge base.
- **Tier 2** is designed as a cross-skilled, hybrid model that takes advantage of multi-vendor support capabilities. It comprises a more granular layer of complementary technology ecosystems based on skill sets and operational support abilities. Ensuring there are no fixed or enforced technology skill-set boundaries, support resources are logically grouped into evolving hubs that allow them to grow within and outside of the logical ecosystem. In addition to complementary technologies, this tier provides the enterprise access to administrators with hardware and software expertise across both physical and virtual data centers.
- **Tier 3 and additional tiers** cater to vendor-specific technologies without enforcing or utilizing a complete cross-skilled model. This design ensures that resources continue to provide expert-level support for legacy, tower-based infrastructures as well as virtual and cloud-based environments.

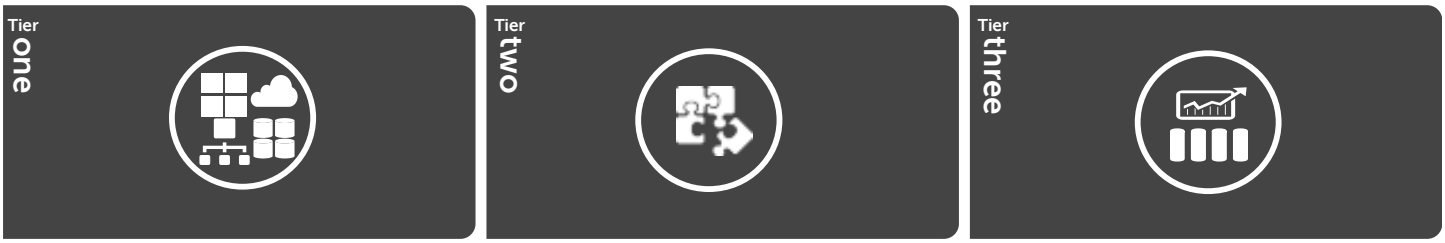

Figure 3. Redesign of support model tiers

Manage and control

As part of the overall transformation program, it is important to consider the processes required to manage and control a continuously evolving infrastructure. Processes need to adapt with an organization's dynamic IT environment — from a siloed/linear approach, to processes that streamline and improve intra- and inter-ecosystem engagement, as well as drive better vendor management and collaboration for enhanced IaaS, PaaS and SaaS usage.

To highlight the overall challenge, for example, process blueprints for core ITIL processes, such as incident, request and change management, need to support the provisioning, troubleshooting and modifications of workloads or services across a complex, hybrid infrastructure. This drives the adoption and implementation of a micro-services approach, which accommodates continuously changing components/flows, such as streamlining support of request management processes across legacy and dedicated infrastructures, as well as public/private cloud deployments.

This micro-services approach defines integration points of process components, and enables operational efficiency and decision making for hybrid infrastructure scenarios. This approach — driven by changes in infrastructure consumption models — helps optimize or change one component of the process (such as including a new IaaS vendor), while maintaining integration points and not disrupting the rest of the process flow. The addition of a circuit-type model to this approach ensures that new process paths become available, and that old paths are immediately closed based on infrastructure type and potential changes in support requirements.

Additionally, the adoption of service integration and management (SIAM) methodologies helps transform core process management functions regarding vendor management. Integrating SIAM into the operational support process transforms the overall vendor engagement model from an escalation management and ticket-transfer function to a complete, multi-vendor management practice. Governed by availability and performance measurements, the SIAM layer allows the enterprise to take advantage of and manage an integrated set of XaaS providers.

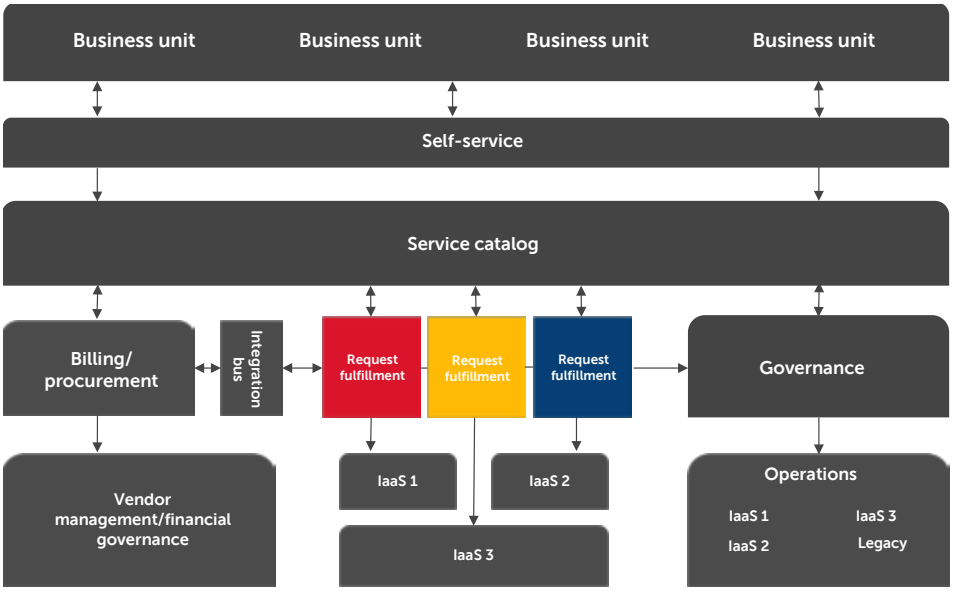

Figure 4. Micro-services approach to service management processes

Monitor and enable lifecycle management

Tool sets that support service delivery play an important role in enabling the transformation process and managing a hybrid infrastructure. As the scope of support begins to span various environments — from dedicated, on-premises infrastructures to hosted private and public clouds — the tools, technologies and associated reference architectures have to be built and integrated in a modular manner.

A key element of the hybrid infrastructure is the monitoring and lifecycle management layer, which monitors all IT services layers across physical and cloud data centers. This provides a single-pane-of-glass interface across business applications (synthetic and real transactions), platforms (databases, middleware, OS and virtualization) and physical infrastructures (server, network and storage). The layer also enables accurate measurement of service delivery, which allows internal and external IT to understand and support a continuously scaling-up, scaling-out and scaling-down infrastructure.

Another element to keep in mind is IT service management (ITSM), which is the core of any enterprise's tools and technology reference architecture. While acting as a process management platform, ITSM offers a centralized service catalog and service request management catalog that provides a unified, single point of entry into the infrastructure.

ITSM redesign and deployment principles need to provide the ability to measure service delivery against business results rather than by tower or technology. Business-aligned ITSM platforms offer an end-to-end view of the closed-loop connection between IT organizations and multiple providers, while also providing the insight required to enforce predetermined performance and response objectives. And having a mature event management and correlation engine to act as the integration layer between monitoring and management tool sets and the ITSM platform helps reduce false monitoring alerts for environments that are no longer limited by physical boundaries.

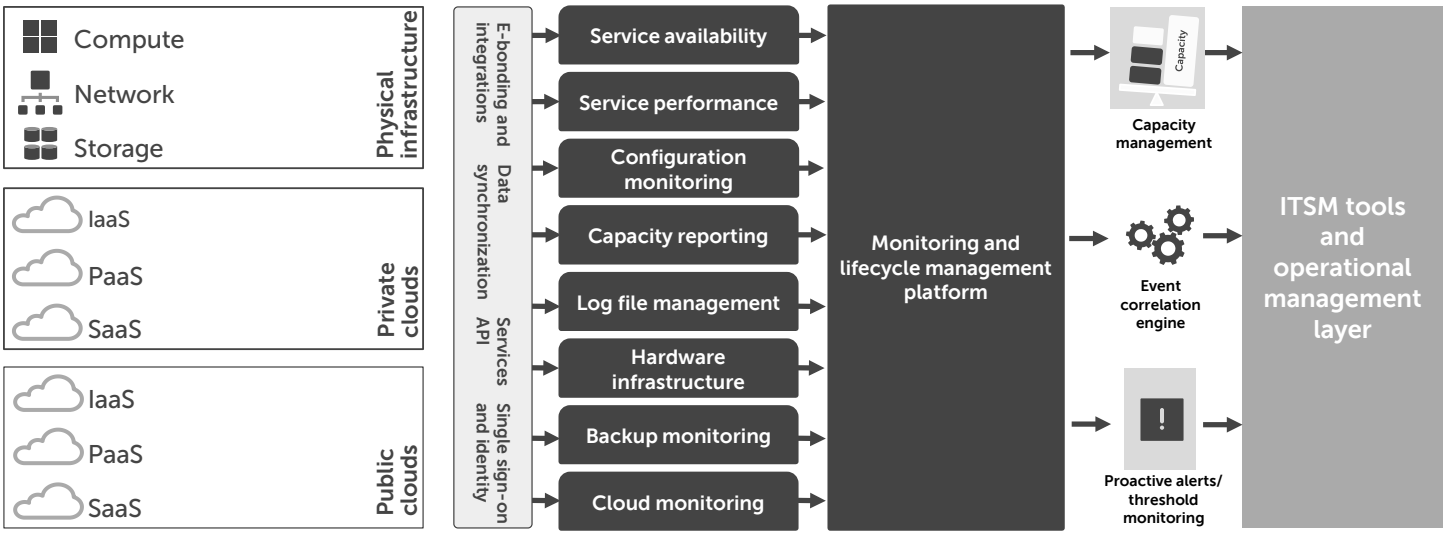

Figure 5. Operational monitoring workflow

Automate and orchestrate

Manual monitoring and management aren't adequate for supporting a hybrid infrastructure. Covering the lifecycle of infrastructure management services, a comprehensive automation and orchestration architecture and framework are designed as a repeatable, modular and truly holistic solution that addresses various automation needs. The architecture and framework use a systematic approach built on the simple principle that any repetitive IT task or process can and should be automated using one or multiple layers within the construct:

- **IT service support process automation:** Automates common and repeatable ITSM processes, and links into various infrastructure components and business systems. This layer aims to improve service levels and process compliance, enable cross-functional efficiencies and provide an improved experience when end users and business interact with IT.
- **IT operations automation:** Operates either as runbook/task automation or as monitoring-level automation. It is initially implemented to manage independent infrastructure elements and provide quick incident remediation or request fulfillment for discrete components. As the footprint of infrastructure elements increases, overarching workload orchestration is gradually rolled out through dynamic integrations between various automated tasks and ITSM.
- **Provisioning and release automation:** Enables service efficiency and addresses multiple infrastructure support components such as requests, provisioning, development and operations, in addition to compliance and configuration management. Closely aligned with and connected to the infrastructure technology stack, this layer relies on platform-agnostic enablers (including cloud management and provisioning tool sets or configuration management automation and control such as Puppet) or vendor-specific technologies such as VMware vRealize or Microsoft System Center Orchestrator suites.

Enabling these layers and their underlying technologies in a hybrid infrastructure deployment allows enterprises to realize the benefits of service automation across the entire lifecycle. This design goes beyond pure IT processes or components automation and expands into overall business and IT integration. It also provides the flexibility to introduce a specific task into the right layer of automation, delivered by the right tool.

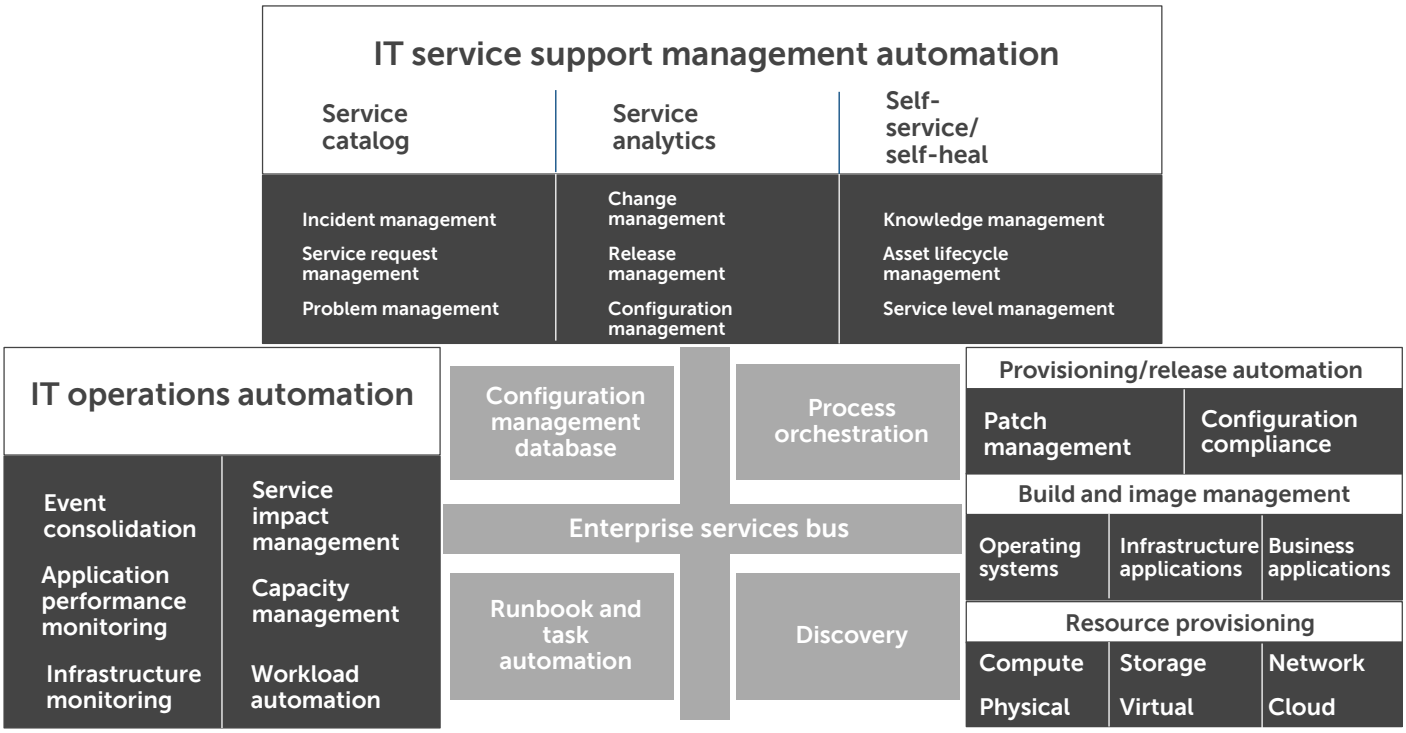

Figure 6. Automation layers enable hybrid infrastructure management orchestration

Secure

While organizations adopt private and public clouds for critical workloads and applications, security becomes a shared responsibility between cloud providers, cloud tenants and the service provider — with each retaining the level of control at specific layers. This model adds to the challenge as enterprises move away from traditional infrastructure environments. To address the dynamic demands of a hybrid infrastructure model, the security services structure needs to be flexible to adopt new data center and services models, while providing the peace of mind that enterprises are looking for.

Combining the tools and integration points that are controlled and managed by internal IT, external IT or third-party providers, the XaaS security models need to provide identical regulatory controls (such as for the Health Insurance Portability and Accountability Act and Payment Card Industry) under the hypervisor levels. This ensures that all current security controls are expanded and effectively managed in the new infrastructure.

Some of the core functions remain unchanged. For example, the tool sets, technologies and associated processes for endpoint security currently used for on-premises infrastructure management can also be used for cloud deployment and management. This allows immediate and natural expansion of additional policies and procedures into the IaaS environment by either utilizing

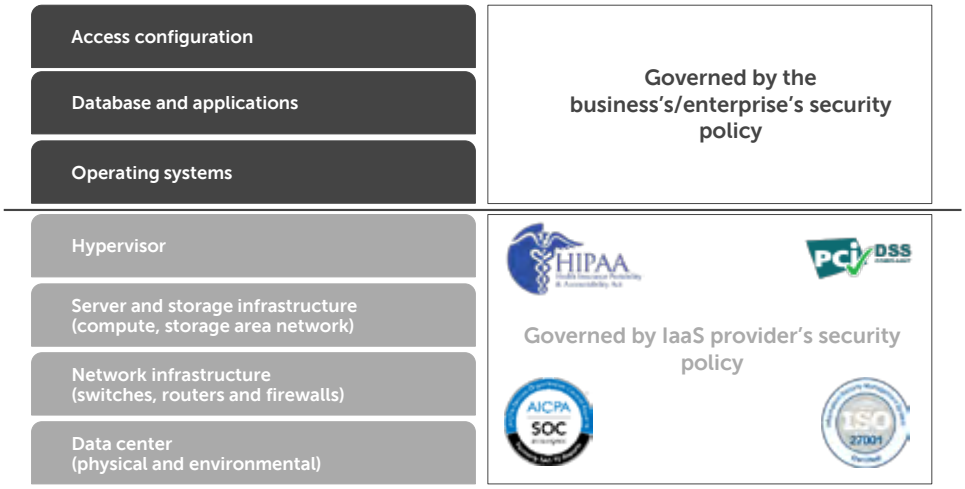

Figure 7. IaaS security and compliance scope

available licensing models of various cloud marketplaces or deploying the same set of tools and technologies on provisioned workloads.

However, the functions — which are now a shared responsibility or are no longer under the full support and control of internal or external IT — are changing. For example, security controls and management below the hypervisor layer in an externally provided IaaS model now become part of the vendor management model and its associated processes. Such controls don't need end-to-end management (across tools, processes and people) from the enterprise and the managed security service provider (MSSP), but require continuous monitoring and regular compliance validation driven by the enterprise and IaaS providers.

Subsequently, the security advisory and consultancy model also undergoes a change. Not constrained by physical data center boundaries, enterprises require dedicated security experts, such as information security managers and architects, to help with their overall infrastructure adoption decision-making process. They provide guidance and detailed security considerations on the inclusion and implementation of various XaaS models by recommending profiles and associated vendors that are best suited for the enterprise. This offers insight into whether the chosen XaaS models enable adequate expansion and management of security policies into the new environment, which allows the business to understand, anticipate and drive strategies to secure assets hosted on cloud infrastructures.

Evolve

Cloud adoption and evolving infrastructures are driving enterprises to adopt new methodologies, such as DevOps, which were difficult to deploy and manage in a hardware-driven data center. The single-pane-of-glass view across all service layers, the accelerated feedback chain, the flexible continual service improvement function, and the ability to roll out and roll back immediately make it easy to operationalize an agile deployment and management methodology without compromising reliability, availability, performance and security.

Realize the benefits of a fully managed hybrid infrastructure with Dell

For organizations beginning to explore cloud solutions as an alternative infrastructure model or already expanding into XaaS models, Dell helps maximize the transformational investment. Having successfully implemented a hybrid infrastructure within our technology ecosystem and with multiple customers, we understand the building blocks from the ground up. Tailored to specific industries and technology environments, our tools and processes are modular, time-tested and adaptable to meet dynamic business requirements. With an end-to-end portfolio of products, technologies and services, we support an organization's cloud enablement program lifecycle in complete alignment with their business objectives.

Taking advantage of our transformed delivery methodology, Centers of Excellence, research and development labs, and newly redesigned governance models, our integrated technology solutions portfolio also includes a holistic set of hybrid infrastructure building blocks. Dell, as an end-to-end solutions provider, delivers a range of management services for hybrid infrastructure deployment in addition to tested and certified next-generation data center technologies to support an organization's transformational journey toward XaaS.

Our transformation model provides a wide range of business-aligned IT services to help enterprises continuously evolve and maximize the value of on-premises IT and private and public cloud consumptions.

Whether considering cloud services or in the process of migrating infrastructure elements to the cloud, organizations need a partner with the insights and experience to confidently make this transformation. Dell has a wide range of engineered technology solutions — private and hybrid clouds, hosted and fully managed IaaS, cloud brokerage, security management and services integration functions — to holistically transform and manage a bi-modal IT for mid-market and large enterprises.

Our end-to-end cloud infrastructure and management solutions help enterprises accelerate the implementation of hybrid clouds to enhance productivity, enable operational efficiencies with better deployment choices, and gain control with policy-based governance to meet security and compliance needs. Organizations can take advantage of our technology innovations, extensive partner ecosystem and depth of experience in enterprise service delivery to accelerate their journey to the cloud and drive value for their business.

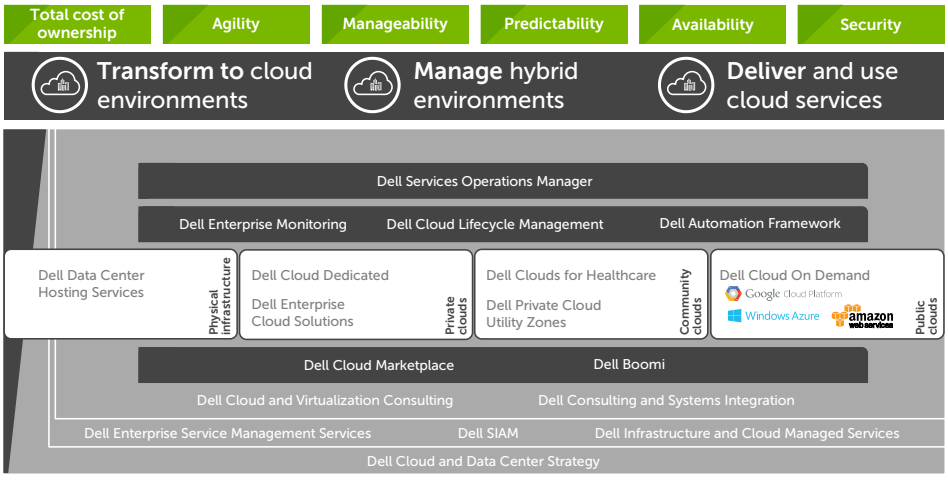

Figure 8. Dell's end-to-end solution for hybrid infrastructure management

For more information about our service offerings, visit dell.com/managedservices or contact a Dell representative.

April 2016 | D722 Managed Services for a Hybrid Infrastructure.indd | Rev. 1.0