How Cloud is Transforming Business
(and What Your Organization Should Do About It)

WHITE PAPER

Cloud computing is a fact of life for all enterprises—and not just for the IT organization. Cloud is now a business platform more than just a technology solution, involving and affecting people, processes and applications. This is changing the roles, priorities and mandates across the entire organization. For IT organizations, cloud brings dramatic impacts, particularly in three major areas: security, cloud-native applications and core business applications.

Organizations of all sizes and types are embracing digital transformation as an essential, strategic business imperative. But the challenging question for those enterprises is "what do we do to transform?"

Cloud computing is a key enabler of digital transformation. By now, the many benefits of cloud architectures—increased agility, nearly unlimited scalability, more efficient use of resources, end-user self-service and better utilization of IT staff—are well understood in IT departments, corner offices and boardrooms. As a result, cloud computing is now an IT market juggernaut. Organizations are projected to spend an eye-popping $390 billion on cloud hardware, software and services—yes, billion with a "b"—by 2020[1], and spending on cloud will grow more than 6 times faster the rate of overall IT spending by 2020.[2]

Cloud computing is now an essential ingredient for all organizations' business strategy—not just their IT operations. Cloud computing is the next business platform on which all businesses will execute rapid customized delivery of new products and services in both B2B and consumer markets, and all organizations will need to harness cloud to be successful.

1 "The changing faces of the cloud," Bain & Company, January 2017

2 "The Salesforce economy," IDC, September 2016

DELL EMC | intel

TechTarget | Custom Media

However, cloud doesn't just mean public cloud. In fact, most successful organizations are leveraging multiple cloud solutions from multiple cloud providers. It is now a multi-cloud world. The implications of the rapid and inexorable shift to a multi-cloud reality are still emerging, causing the potential for confusion and uncertainty over the best way to leverage various cloud environments to transform IT, to drive competitive differentiation, enhance customer satisfaction and unlock business value.

In this paper we explore how multi-cloud is accelerating digital transformation. We will outline the implications and provide recommendations in three key areas where all organizations will need to develop new strategies and tactics for success. First, security strategies will need to be modernized as IT will be operating outside traditional data center boundaries in a multi-cloud environment. Second, investment must be prioritized for new "cloud-native" application architectures to create innovative software. And finally, organizations can capture efficiencies with Infrastructure-as-a-Service [IaaS] to streamline the operation and management of existing applications so that resources saved can be reallocated to innovation.

How cloud is accelerating digital transformation: Make cloud your new business platform

Organizations across any size, geography, industry and business model are increasingly adopting multiple clouds, making it the modus operandi for digital transformation. More specifically, organizations are pursuing a multi-cloud strategy where combinations of cloud solutions are used to accommodate the needs of traditional and cloud-native workloads. Multi-cloud is the tactic to speed development of new ways of doing business and for making existing operations more efficient.

"The cloud tipping point is a nexus between the past and the future, just like the PC, x86 and TCP/IP were," noted cloud industry analyst and visionary Bernard Golden. "They became the foundation upon which IT operated. Cloud is the next one, and it will be just as dominant as they were."[3]

To create new ways of doing business, IT and business leaders need to transform their organization from operating traditional, siloed infrastructure to focus on building software that delivers innovative new business capabilities. Adopting IaaS automates operations and reduces specialization by abstracting the infrastructure. Leveraging a cloud-native platform accelerates new application development and delivery and empowers development teams to focus on coding, and on transitioning into DevOps and Agile development methods.

Gaining the biggest possible advantage from cloud requires having the flexibility to deploy a workload where it makes the most sense. IT and business leaders alike should leverage multiple clouds in all their forms—public, private, hybrid, on-premises and managed/hosted—as options for workload deployment. To do so, it's important to ensure that your multi-cloud strategy supports mixed deployment models and application portability. It is essential to avoid choices that lock a workload into a specific cloud: public cloud lock-in is a real and highly problematic scenario.

By adopting a multi-cloud strategy to create flexible application deployment models, improve IT resource allocation and utilization, your organization takes a giant step into the new reality of digital transformation, and you will create a powerful new engine to drive forward all aspects of your business.

Multi-cloud is the new business platform. Now, the $64,000 question: What should you do about it?

What it means: Security becomes a shared responsibility

It's impossible to talk about adoption of multiple clouds without considering a modernized strategy for security.

"Modernized" is the operative word here as concerns about cloud security have shifted dramatically in recent years.

3 "Cloud Computing Hits a Tipping Point," BernardGolden.com, June 2017

Not that long ago, security was the most-often-cited concern of IT and business executives when they considered public clouds—because of the perceived loss of control once data leaves the glass house of the traditional on-premises infrastructure. Public cloud service providers, meanwhile, have made massive investments in security infrastructure to demonstrate to customers that they are up to the task when it comes to protecting valuable data. In fact, global spending on cloud security solutions is expected to jump more than 25% on a compound annual basis between now and 2022, when it is projected to reach $12.7 billion.[4]

While security remains a key area of focus, customer concerns have largely shifted from "is cloud safe?" to recognizing that an organization's most mission-critical data increasingly is located in multiple clouds—and must continue to be protected at all costs. Cloud service providers and their customers are collaborating to handle security challenges for data, applications and services in the cloud. These include securing the edge for both traditional, corporate-owned endpoints and other third-party endpoints, as well as aligning cloud security models with risk mitigation and compliance requirements.

In order to execute a shared-responsibility model that spans multiple clouds, organizations should take several important steps:

- **Enhance existing multi-layered security postures.**
  - Start with the hardware layer. Today's cutting-edge hyper-converged platforms powered by Dell EMC PowerEdge servers and Intel® Xeon® Scalable Processors come with sophisticated new security features, such as cryptographically trusted booting for end-to-end server and data center security, system lockdown to protect against malicious or intended changes and system erase to easily retire or repurpose servers by wiping data—securely and quickly—from drives and embedded non-volatile memory.
  - Integrate new application security-as-a-service technologies. These technologies develop contextual intelligence to understand how applications

are supposed to work and continually monitor for changes to the intended state that indicate a threat. When a threat is detected, automated responses remediate application behaviors.

  - Adopt an integrated cloud platform designed and engineered to be supported as a single system. This approach reduces the security attack surface and ensures all system components are kept up to date.
  - Consider working with experienced third-party security experts, whose technical and business consultants have seen security vulnerabilities in countless forms and have advised clients accordingly. Security in multi-cloud environments should be extended with complementary capabilities from third parties and trusted partners.
- **Build a shared responsibility model to extend your security posture into the public cloud.**
  - Your security model will need to connect and integrate with outside agencies such as cloud service providers. In this new model, service providers handle much of the basic functionality such as physical security, while customers handle access/identity management, Active Directory integration and other capabilities. This shared responsibility model takes advantage of each party's strengths and experiences in the compliance area for regulations such as PCI, HIPAA and GDPR, and a number of cross-industry requirements for data protection, privacy and governance.

4 "Cloud security market by service type and service model," MarketsandMarkets, April 2017

- **Network security models need to change to a software-defined architecture.**
  - Software-defined networks offer more flexible and dynamic network security configurations, which are powered by robust policy engines that can migrate security policies with workloads and their associated virtual machines and/or containers across hosts and clouds. Software-based network micro-segmentation can define workload-specific networks and limit the avenues an attacker can take to explore the environment and sniff out information to steal.

What it means: Cloud-native is the next architecture for applications.

New cloud-native architectures enable software-driven innovation and rich customer experiences that are at the core of the digital economy. Cloud-native accelerates software innovation by dramatically shortening release cycle times for new software features. Cloud-native software is a key method by which organizations will find ways to reach new markets and disrupt existing markets in the digital economy.

Cloud-native development systems are guided by the 12-factor application methodology—a set of principles for building software-as-a-service (SaaS) applications that leverage micro-services and containers. This new architectural approach to code development goes hand in hand with new processes for deployment and managing software. The traditional waterfall methodology has given way to agile development methods and software is delivered continuously into production via automated testing and deployment toolchains. In this new world, the traditional separation of development and operations teams and processes is eliminated to create integrated software product teams that are responsible for the entire software lifecycle.

In order to take full advantage of the accelerating move to cloud-native applications, organizations should:

- **Focus development programs on an industry-standard platform to create maximum flexibility.** In the multi-cloud world, new applications should be cloud-native. Cloud-native platforms provide an end-to-end development environment that accelerates code writing, enables reliable application scaling and delivers "security by default." Typically in these platforms, tool chain integrations are pre-wired to speed development and delivery, thus improving time to value and ease of adoption.
- **Develop with an optimized platform supported as an integrated system.** The choice of a cloud-native platform is key because it provides a layer of abstraction that allows development teams to focus on creating innovative software. Adopt an integrated cloud-native platform. This eliminates the overhead for creating, managing and maintaining the development environment and ultimately creates time-to-value and operational benefits over manual do-it-yourself approaches. Additionally, choose a cloud-native platform that supports application portability between multiple public and private clouds. This will maximize your flexibility in deployment options across various public clouds.
- **Bear in mind.** Developing cloud-native applications within proprietary public cloud "as-a-service" environments tends to tie the application and its associated data to that cloud environment. If you do chose to develop in these environments you are likely going to reduce your flexibility for moving applications, which can drive up cost and complexity.

What it means: Core business applications—optimize with IaaS

Most organizations have an existing portfolio of traditional applications that must be optimized for maximum efficiency. Decisions must be made for what applications should be migrated to cloud-native models, transferred to SaaS, left as is or "re-platformed" to new, more efficient IaaS environments.

Some existing systems—traditional applications and systems of record—will continue to reside on-premises. There are numerous important reasons why this is the case; for instance, performance requirements and service-level agreements, cost and complexity for migration, network latency concerns or because of business risks due to data sovereignty, security or intellectual property concerns.

To optimize traditional applications with IaaS, organizations should:

- **Consider extending your virtualization strategy.** Implement IaaS via private cloud to gain efficiencies for existing applications and operations. With private cloud IaaS, you can continue to leverage your existing data center and application investments, and then create bridges to public cloud where appropriate.
- **Streamline on-premises infrastructure with converged and hyper-converged platforms.** Powered by latest Intel Xeon Scalable Processors, Dell EMC PowerEdge server platforms provide streamlined management, improved density, lower operating costs and a reduced data center footprint. This all contributes to making IT more efficient, and supporting IT's imperative to move up the value chain and become a source of innovation rather than a classic cost center.
- **Deploy an integrated IaaS system. Building an IaaS system is complex.** Engineering, installing, integrating, configuring and testing cloud software with hyper-converged platforms and software development environments is time-consuming and error prone. Precious internal human resources are better focused on higher-value projects than on the undifferentiated heavy lifting of racking hardware and installing, patching and updating software. Leverage integrated IaaS systems that are managed and scaled as a single integrated system. This will enable faster cycles of continuous innovation.

How Dell Technologies facilitates cloud-driven digital transformation

Making a safe, secure and successful journey to a multi-cloud reality requires smart planning, detailed execution and a partnership with an organization with a keen technical eye and a savvy business sense. Increasingly, organizations in all industries and geographies are turning to Dell Technologies to provide both the cloud-centric tools and the business acumen necessary to develop, deploy and even manage applications and systems in a cloud-first business model.

Dell Technologies offers broad and deep solutions that align with the recommendations made within this paper:

Make cloud your new business platform

Leveraging the cloud to turn the idea of digital transformation into a reality requires working with a partner that has a true portfolio of cloud-centric solutions, and a proven track record of helping organizations navigate that journey to the cloud. Dell Technologies' industry-leading hardware, software, services, and solutions—including integrated IaaS and cloud-native platforms, and security technologies and services—provide a comprehensive approach to implementing a multi-cloud strategy.

Cloud-native is the next architecture for all new applications

Pivotal Cloud Foundry and Pivotal-powered Cloud Solutions are Dell Technologies' answers to customers' needs for applications designed first and foremost for the cloud.

In addition, Dell EMC Cloud for Microsoft Azure Stack is an on-premises cloud platform for delivering infrastructure and platform-as-a-service with a consistent Azure experience. Access, create and share application services securely in Azure public cloud and Azure Stack for both traditional and cloud-native applications.

Developed in partnership by VMware, Pivotal and Google, the VMware Pivotal Container Service (PKS) is built on the Kubernetes open-source platform for developing, scaling and management of cloud-native container environments.

Security becomes shared

Combining the shared-responsibility model discussed earlier with these and other security solutions, Dell Technologies offers customers the confidence of a secure framework that scales as more and more customer applications, data and services move to the cloud.

With VMware NSX, organizations are creating entire networks in software and embedding them in the hypervisor layer, abstracted from the underlying physical hardware. All network components can be provisioned in minutes, without the need to modify applications. VMware App Defense is optimized for securing applications in virtualized or cloud environments, while integrating with third-party solutions for improved application visibility and response orchestration.

Dell EMC IaaS and cloud-native platforms are more secure than do-it-yourself configurations. They are built on known secure infrastructure configurations that are supported, patched and updated as an integrated system to reduce vulnerabilities and mitigate advanced persistent threats.

Dell SecureWorks provides intelligence-driven information security solutions to help organizations of all sizes prevent, detect, respond to and predict cyberattacks.

Dell EMC PowerEdge servers powered by Intel Xeon Scalable Processors are designed with rapidly evolving cloud security requirements and fast-changing compliance regulations in mind. These platforms embed new hardware and system-level security features to protect the infrastructure.

System Lockdown prevents configuration changes that create security vulnerabilities and expose sensitive data. SecureBoot, BIOS recovery capabilities and signed firmware provide enhanced protection against attacks.

By delivering security in hardware, software and services, Dell layers in protection across the full infrastructure stack so no one point of failure can compromise critical data.

Optimize with IaaS

In the real world, organizations demand a mixed portfolio of solutions for cloud, on-premises and hybrid environments. Dell provides an array of options that meet the diverse needs of organizations, each with different areas of emphasis for cloud-based applications and workloads.

These include Dell Technologies' VMware-powered cloud solutions and VMware Cloud on AWS solutions. VMware-powered cloud solutions are turnkey engineered IaaS systems built using Dell EMC converged and hyper-converged infrastructure that enable organizations to automate the delivery of traditional enterprise applications through a self-service catalog. VMware Cloud on AWS is an on-demand service that runs applications across vSphere-based cloud environments with access to a broad range of AWS services; it is optimized to run on dedicated, elastic, bare-metal AWS infrastructure. Virtustream Enterprise Cloud is purpose-built to run the most complex, mission-critical intensive applications with application-level SLAs and integrated security and compliance. Virtustream also offers services for managing all or part of your cloud and information infrastructure.

Cloud Infrastructure Matters: Dell EMC PowerEdge Servers, Powered by Intel Xeon Scalable Processors.

Dell EMC's newest server lineup, 14th-generation PowerEdge servers, are optimized for organizations looking to swing not just their IT operations, but also their business foundation, to the cloud.

Powered by Intel Xeon Scalable Processors, Dell EMC PowerEdge servers accelerate database performance, reduce latency, speed live migration of virtual machines and improve storage performance. The state-of-the-art Intel processors are critical ingredients in the new servers' enhanced, integrated security features. And the Xeon processors deliver 27% more CPU cores and 50% greater memory bandwidth, which speeds execution of mission-critical applications and workloads.

The path forward

As a core element of digital transformation, executing on your multi-cloud strategy no longer is an option—certainly not for any organization that needs to move faster, use human capital more strategically, stretch tight budgets and deliver new business products and services rapidly.

Your journey to a multi-cloud reality needs to be based on sound strategy and meticulous execution of tactics for enhancing security, building cloud-native applications with an integrated cloud-native platform, and optimizing traditional business applications with IaaS. Organizations that put these three elements at the heart of their multi-cloud strategy stand the best chance for leveraging the many benefits of various clouds to drive digital transformation and achieve their most important business goals.

IT and business leaders should look for an experienced partner both for developing their multi-cloud strategy and for deploying the right tools and services to help business users take advantage of all the cloud has to offer. Dell Technologies provides a broad and deep portfolio of integrated cloud platforms, security technologies and services, optimized around the three pillars highlighted in this paper.

For more information on how Dell Technologies can help you navigate your journey to the cloud, please visit www.delltechnologies.com.