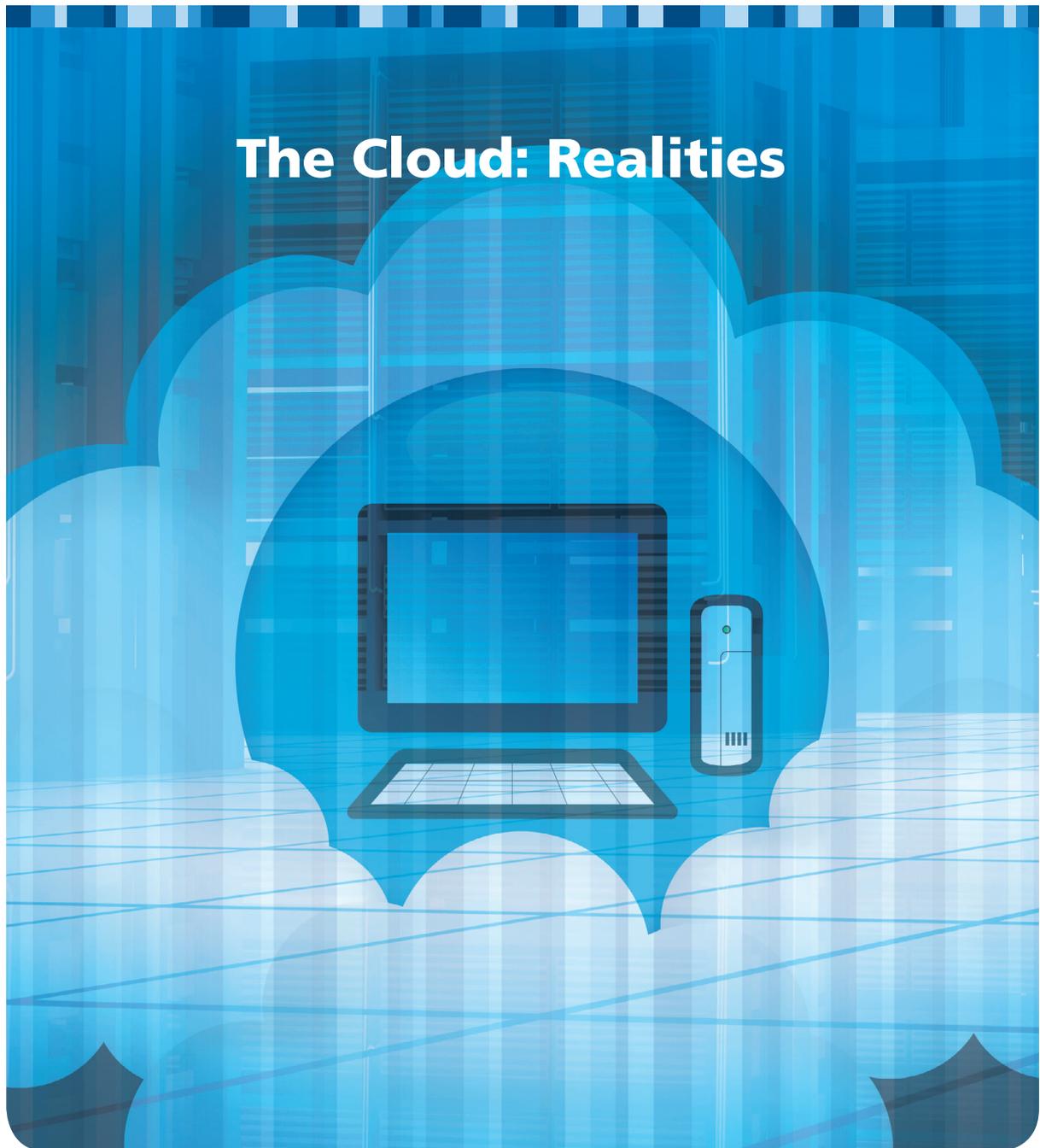




Global Knowledge®

Expert Reference Series of White Papers



info@globalknowledge.net

www.globalknowledge.net

Understanding Data Centers and Cloud Computing



Introduction

Today, cloud computing is a reality for many web users, whether they recognise it or not. Amazon, Google, and a host of other providers offer 24/7 services that many general Internet users access without serious security considerations. For companies from start-ups and small-to-mid-sized businesses (SMBs) to large enterprises, the case for moving business activities to the cloud is more complex. For example, there are certain applications that corporations would rather run on their own servers due to concerns about application and data control. Although the cloud is beyond the point of experimentation, organisations are just beginning to realise the true benefits.

Security

Since its development, unanswered questions remain in regards to how the cloud model will work with complex business-critical services, especially around issues of security. The degree of concern is related to the kind of cloud environment a company chooses: public or private. In terms of public clouds, the shared computing environment is unrestricted, allowing access to all individuals, companies, or other kinds of organisations. Fears in regards to adequate data security are compounded by issues related to compliance, governance, and reliability.

Key security issues relate to:

- **Data location:** processing and data storage can take place anywhere around the globe with legal jurisdiction implications
- **Data segregation:** content resides in shared environments where encryption methods and data protection can be ineffective
- **Recovery:** concerns exist in regards to data and application infrastructure replication and recovery
- **Investigation:** ever-changing hosts and data centers make data-breach inquiries difficult
- **Long-term data viability:** assurance that providers will maintain continued solvency and independence

Fail-Safe Reliability

Companies still face uncertain data stability when deciding to move operations to the cloud. Another area is related to compatibility issues. Moreover, uptime Service Level Agreements



(SLAs) that guarantee performance standards may also be ineffective. They can end up offering little in defining how to validate the SLA, unless procedures are clearly defined at the outset of the agreement.

The rapid rise of the use of cloud providers and the fact that many providers are still refining and testing their platforms means that outages will continue to occur, some having more impact than others. While high availability within a cloud infrastructure is desired, it may ultimately require customised back-end architectural modifications by customers to achieve.

Integration Factors

Business applications typically operate in silos, disconnected from each other. Therefore, integrating them with cloud-based services to achieve an end-to-end business process can be a costly and time-consuming task. Moreover, integration between on-premise and cloud applications is becoming increasingly complex as well as imperative.

Some organisations use hybrid combinations of Software-as-a-Service (SaaS)-based applications, hosted cloud platforms, and their own private cloud. As a result, batch uploads, read-only integration, and cloud silos are no longer adequate for gaining sufficient parity between the separate hosts. Organisations will face an increased need to mediate and monitor information flows between their internal infrastructure and external cloud services using simpler methodologies.

First Adopter Costs

Much of what we understand about the cloud's business-related effectiveness comes from the experiences of first adopters. For this sector, in some respects, the cloud is a commodity. It requires upfront capital and the capacity to weather a multitude of possible complications.

The up and downsides for these companies mean that the public cloud offers the potential for achieving early competitive advantage while also risking insolvency. Some of the challenges early adopters face:

- Manageability/reducing SaaS silos
- Lack of cloud security standards
- Creating a unified platform/cloud-to-cloud integration
- Confirming SLA guarantees
- Avoiding provider lock-in/flexible transitioning between providers

Conclusion

At the most fundamental level, cloud adoption requires that organisations and users learn to trust the cloud with their data. Cloud providers must continue to innovate and improve their data processing capabilities, and users need to accept the challenges and rewards that are part of any new technology adoption. Our current state of cloud computing has its basis in this process of evolution. Consequently, the cloud industry has emerged as an aggregator industry with enormous promise and equally large unseen risks.

The emergence of cloud computing offers a new opportunity to shape the relationship between those who use IT services and those who sell them. As the cloud matures and gains an increasing number of adherents, it requires increased levels of data protection and insurance from a range of threats. As with any evolving technology, today's businesses must understand how best to leverage the advantages that the cloud offers and guard against its deficiencies.

Learn More

Visit www.globalknowledge.net

