Stratecast A Division of FROST & SULLIVAN

Overcoming Obstacles to Cloud Computing

An Executive Brief Sponsored by IBM

February 2011

OVERCOMING OBSTACLES TO CLOUD COMPUTING

INTRODUCTION

Many businesses—in fact, the majority of businesses—approach cloud computing with the same skepticism as they would a get-rich-quick email or a miracle cure elixir. Sure, it sounds good: low costs, no capital investment, on-demand resources, unlimited scalability. But the risks—known, perceived, and suspected—often overshadow the benefits to the point where businesses are unwilling to make a move.

Yet, failing to incorporate cloud computing into the corporate data environment can bring its own pitfalls—pitfalls stemming from stretched budgets, insufficient staffing, and poor workload management. There may also be collateral damage to the reputation of the IT director who unilaterally decides *not* to participate in the hottest new technology trend since the mobile workforce. Certainly, few corporations want to explain to shareholders why they are refusing to adopt new, cost-saving technologies!

In reality, the cloud is neither a wonder drug nor a curse. Companies should neither hurtle unquestioningly toward the cloud nor bar the door. Instead, they should approach the cloud with the same clear-headed assessment used for other technology decisions—working to maximize the benefits while mitigating the risks.

In this paper, we look at the top concerns and perceived risks associated with cloud computing. We make recommendations to overcome these obstacles for enterprises who are considering getting started with cloud computing. And we show how enterprises can utilize solutions such as IBM's suite of cloud and security services to safely incorporate cloud computing into their data center strategies.

ONE CLOUD DOES NOT FIT ALL

The industry commonly refers to "the Cloud" as if it were an entity; a definable place or recognizable set of parameters. It's more useful to understand the cloud as a business model for distribution and consumption of computing resources. The business model virtualizes workloads on a shared infrastructure. The computing resources are available to users on-demand, via the Internet or other network connection. For enterprises, the cloud business model supports elasticity and flexibility for workloads, while minimizing capital investment and labor costs for hardware.

This definition of the cloud model has given rise to three variations:

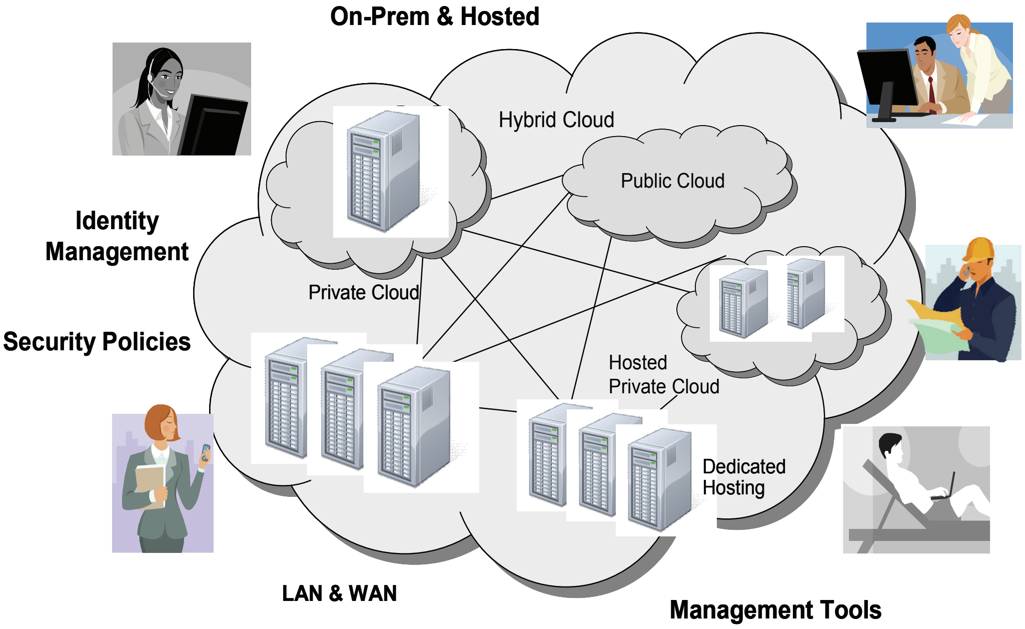
Public cloud: In the public cloud model, the infrastructure is hosted by a third-party provider and is shared among multiple customers. Each customer is charged for computing resources on a metered or pay-as-you-go basis.

Private cloud: In a private cloud, computing resources are dedicated to a single enterprise, with infrastructure shared exclusively among the enterprise's own applications. Private clouds may be hosted by a third-party provider, or built within a company's own data centers.

Hybrid cloud: A hybrid cloud configuration combines both public and private elements—on-premises and hosted—under a common management system. While this model has gained great interest among enterprises, surprisingly few cloud providers are equipped to support a true hybrid cloud. Unless the cloud resides solely in the provider's domain, incompatible delivery platforms and inflexible management systems are often unable to accommodate legacy systems and configurations that every enterprise data center contends with. (A notable exception is IBM, whose flexible cloud platform does support true hybrid clouds.)

For businesses, any or all of these cloud models may be appropriate additions to the data center environment—along with non-virtualized private data centers, co-location and dedicated hosting, and Software as a Service subscriptions. That means the average business is already or will soon be managing their workloads across a number of data center environments, as shown in Figure 1.

Figure 1
Multiple Data Center Environments Managed by Enterprises



Source: Stratecast

Just as there's more than one cloud delivery model, there is a broad variety of cloud services available. Without industry standards to guide them, cloud service providers are free to develop and deliver their services as they choose. Security, performance and availability service level agreements, and visibility and control over cloud workloads will vary dramatically by provider, as will price and terms (e.g., contract length, terms of disengagement). The wide variation is responsible, in part, for concerns about cloud adoption.

OBSTACLES TO CLOUD ADOPTION – AND HOW TO OVERCOME THEM

For all the hype about cloud computing over the last couple years, only about 20 percent of businesses have incorporated the business model into their data center strategies, according to a 2010 Frost & Sullivan survey. Considering the ease of entry and the promises of cost avoidance and savings, that is a low adoption rate. While businesses are interested in exploring cloud delivery models, many have serious concerns that are causing them to delay adoption.

While some of their concerns can be attributed to lack of education or fear of the unknown, by and large they are valid topics of discussion. Enterprises are wise to have a frank discussion of their concerns with their potential provider, and determine the best solution for each workload and data set.

In this section, we look at data from two recent user studies that explore the top concerns enterprises have about the cloud—the IBM 2010 Global Risk Survey (IBM), and the Frost & Sullivan 2010 Cloud End-User Survey (F&S). For each concern, we offer suggestions for addressing it with your provider.

1. Threat of Data Breach or Loss

How widespread is the concern? While unauthorized access to data is a threat that pervades every data center—hosted or self-managed—over half of enterprises believe that the cloud poses a particular risk to data security (F&S), with fully 77 percent expressing belief that it's harder to protect privacy in a cloud environment (IBM).

Is there reason for concern? The threat of unauthorized access magnifies in a shared environment, where isolation failures may cause data to be exposed to other tenants of the provider. In addition, the threat of damage from a malicious insider expands when "insiders" include employees of the provider. Furthermore, the web-based interface may prove a vulnerable entry point to sensitive data.

Addressing the concern – Enterprises should expect that their sensitive cloud workloads will have at least the same level of protection as their sensitive on-premises workloads; but for less sensitive workloads, they should avoid paying for excessive security. First, understand what base security solutions—e.g., firewalls—your provider has built into its cloud architecture, and what assurances it is willing to offer in the case of breaches or loss. Is it sufficient for the workloads you're planning to put into the cloud? Second, apply a strong user authentication scheme associated with your cloud workloads. Some cloud service providers, including IBM, offer optional security services that allow you to tailor the security solution to the workload.

2. Loss of Control

How widespread is the concern? 61 percent of IT decision-makers are concerned about handing their sensitive data over to third parties in a cloud environment (IBM).

Is there reason for concern? Although providers sometimes deride them as "server huggers," there's a lot more than stubborn territorialism behind this concern. In a cloud environment, enterprises rely on the provider's architecture to keep their workloads performing, the provider's processes for backup and recovery, and the provider's security framework to protect their data. Without visibility and control over where and how sensitive data is being handled, the enterprise is right to feel vulnerable.

Addressing the concern – This fear can only be mitigated by trust, and trust is earned by providers based on their track record of performance. Select a provider with a long history as a market leader. Look for the provider to share not just product descriptions, but details about how it operates. Finally, look for management tools that provide high levels of visibility into your cloud environment. For example, users of IBM's cloud services can utilize the company's robust Tivoli management system to manage all their IBM cloud and data center services, whether on-premises or hosted, private or public.

3. Application Performance

How widespread is the concern? 54 percent of enterprises express concern over performance of their cloud-based applications (F&S).

Is there reason for concern? Application performance can be attributed to many things, some of which are outside the control of the enterprise in a public cloud environment. The cloud provider is responsible for balancing workloads across the shared infrastructure, so that each workload has access to sufficient server resources. If the provider hasn't configured the servers appropriately, performance of one or all applications sharing server resources can suffer. Performance can also be negatively impacted by equipment or facility outages, as well as network bottlenecks.

Addressing the concern – Enterprises planning to host workloads that are latency-sensitive should discuss their expectations for end-to-end performance with their provider. While few (if any) public cloud offers include end-to-end application performance service level agreements, some providers will custom-configure a solution that meets specific workload needs, usually combining a private cloud with a private network configuration. For each workload, be sure to consider the provider's standard service assurances, as well as its history of meeting those commitments.

4. Vendor Lock-In

How widespread is the concern? With so much control ceded to the provider, it's no surprise that 50 percent of enterprises are concerned about being locked-in to a single cloud vendor (F&S).

Is there reason for concern? There are several reasons enterprises may be concerned about lock-in. Those who are looking to move or burst workloads among provider platforms may find it difficult to do so, since most cloud providers use proprietary platforms. Other enterprises are concerned about their lack of ability to move workloads and data between their legacy on-premises center and their cloud provider. Others are concerned about how a potential provider handles customer data after the contract is terminated, so that it is inaccessible to other tenants or unauthorized users.

Addressing the concern – Enterprises should understand the source of their concerns, and be able to address them openly with potential providers. Because there are currently no established standards governing cloud platforms, it's true that each provider has built its platform independently, with little interoperability. (The same is true of most private data centers and dedicated hosting.) Given that, enterprises that are looking for a short-term ability to burst into the cloud would do well to select a provider that offers the most flexible range of interoperable cloud offers today (for example, IBM's ability to seamlessly port workloads and data among private, public, and hybrid cloud environments). For long-term interoperability, select a vendor that is committed to pursuing open standards among cloud providers. To ensure your data and workloads are protected if your relationship is terminated, be sure your vendor details processes for disposition of customer data as part of the contract.

5. Regulatory Compliance

How widespread is the concern? 35 percent of enterprises are concerned about their ability to comply with local and national regulations in a public cloud environment, with the percentage skewing higher for heavily regulated industries like healthcare and financial services (F&S).

Is there reason for concern? Compliance is tricky, because regulations specifying the handling of sensitive data are numerous, change frequently, and vary across geographies. And it is always the enterprise—never the third-party host—that bears responsibility for assuring compliance. Furthermore, as a security measure, many cloud providers do not divulge where customer data is physically located; nor do they permit third-party audits.

Addressing the concern – As noted, one cloud does not fit all, and enterprises should talk to potential cloud providers to determine which cloud options will allow them to meet their compliance requirements for specific data. In some cases, where a public cloud option does not offer the necessary geographical guarantees or audit capabilities, you may opt for a private cloud, either hosted or on-premises. Or look for a provider that offers a hybrid option that will enable you to keep regulated data in a private cloud environment while the associated code is hosted in a public cloud. This option provides necessary compliance while also offering some of the cost and productivity benefits of a cloud environment.

6. Uptime/Resilience

How widespread is the concern? Enterprise IT departments are responsible for assuring that workloads and data are available to internal and external clients, and 34 percent of enterprises harbor concerns about uptime of applications in the cloud (F&S).

Is there reason for concern? When a business entrusts its workloads to a third-party provider, it is dependent on the provider's infrastructure architecture and its processes for continuity and failover, which may be less stringent than the enterprise's own plans. Furthermore, access to enterprise workloads can be impacted by other, unknown tenants that are sharing the infrastructure, as when servers are overloaded or network capacity is insufficient. Finally, enterprises need to be sure that their data is protected, in the production environment, storage, and archiving.

Addressing the concern – In the cloud, responsibility for workload uptime and data persistence falls largely in the domain of the provider. Therefore, it is important to understand the provider's infrastructure and architecture, as well as its policies and processes for managing availability of resources. Do the provider's data centers meet your needs for redundant infrastructure (e.g., access to redundant power sources or network routes)? Does the provider offer sufficient service level assurances for uptime? To support data persistence, look for a robust cloud offering specifically designed for storage; and ensure that the provider supports backup and synchronization (e.g., IBM's Information Protection Services).

7. Vendor Stability

How widespread is the concern? 34 percent of enterprises are concerned about the cloud provider's financial strength and overall track record of stability (IBM).

Is there reason for concern? If the cloud vendor experiences financial difficulties, it may defer server purchases, straining the shared capacity. If—heaven forbid—it should unexpectedly shutter its doors, the enterprise runs the risk of being unable to access its data. As with concerns about vendor lock-in, the enterprise faces the added risk of data persistence on the provider's hardware. Similarly, a vendor that is new to cloud or hosting services may decide to change strategic directions, also leaving your data vulnerable.

Addressing the concern – The solution to this concern isn't found in technology, but in due diligence. Spend time researching any vendor you are considering to host your cloud. Cloud services are just a few years old, so even the industry leaders have only been offering their cloud services for a few years, and new entrants appear regularly. Be sure your provider is established, with a strong financial position that will limit your risk. Ask whether the provider owns its own data centers or leases space from other providers. If they lease, that adds an additional level of vulnerability to your data, and will require you to perform the same due diligence on all subcontractors.

DEVELOPING AND EXECUTING A LOW-RISK CLOUD STRATEGY

For enterprises considering entry into the cloud, the best way to overcome concerns is not to address them one at a time, but instead to develop and execute a well-planned strategy. Most important, they need to select a cloud partner whose products and capabilities align with their needs and expectations.

In this section, we explore steps that enterprises can take to mitigate corporate risk as they introduce cloud computing into their environments, with particular focus on IBM's solutions.

Steps for Mitigating Cloud Risk

1. ***Develop a secure cloud strategy as part of your corporate data security strategy.*** Corporate data must be protected, regardless of where it resides and how it is managed—on-premises or remote; dedicated or shared; self-managed or third-party hosted. Best practices dictate that corporate security and IT work together to develop and implement a comprehensive approach that ensures security is built into the fabric of each data center environment, including cloud solutions.

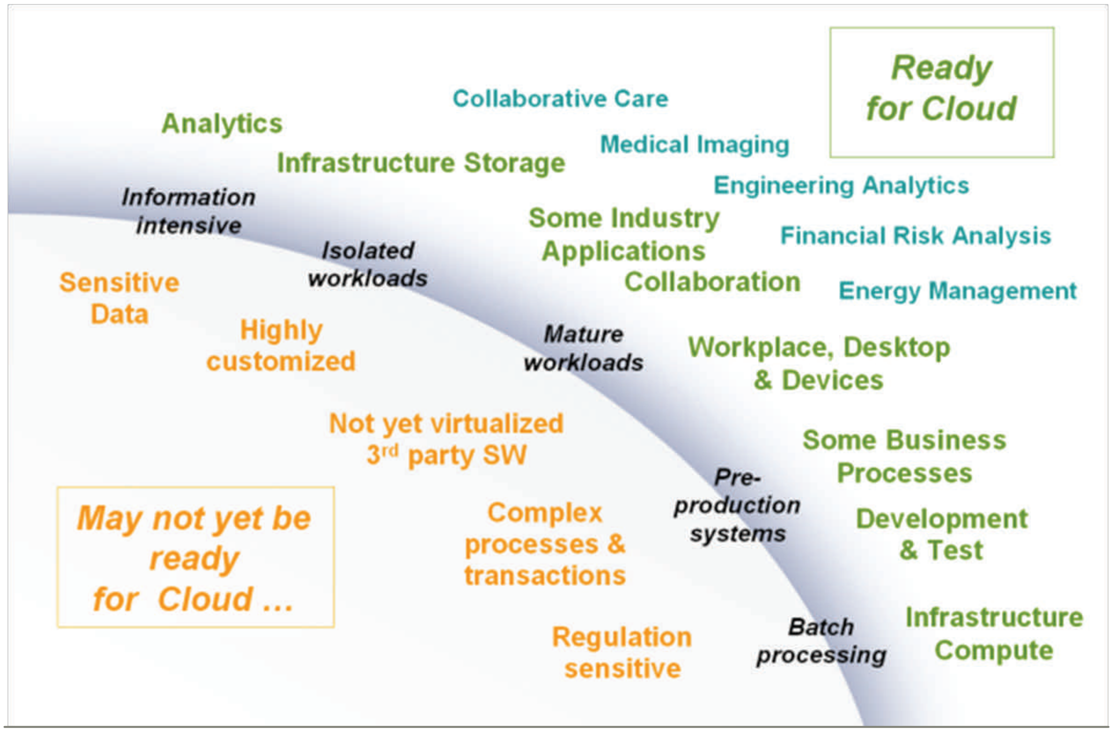
   Corporate security is complex and requires skills that are in limited supply. Few enterprises have in-house expertise required to address the critical challenges associated with securing data in the cloud. Therefore, enterprises are well advised to look for expert assistance in developing and implementing an effective security profile. To meet their needs, IBM has recently launched a series of initiatives aimed at bolstering cloud security for enterprises and providers. As a starting point, enterprises may refer to the IBM Cloud Security Guidance document, a comprehensive roadmap for enterprises and providers of cloud services. Furthermore, the company offers a range of professional services that can help an enterprise get started with the cloud, beginning with Security Consulting Services to help design a secure cloud strategy, and the IBM Cloud Security Assessment.

   To support their cloud workloads, enterprises can utilize IBM's extensive portfolio of security services, which includes services related to data protection (including intrusion detection and prevention, data loss protection, web and email security) as well as identity and authentication management (such as user authentication, single sign-on, and managed identity services). To ensure compliance, IBM provides visibility and reporting to support audits, as well as consulting and services related to specific regulations, e.g., PCI Assessment services. In addition, a new line of IBM managed security services supports cloud-based security services for all workloads.

2. ***Choose the right workloads to start in the cloud.*** For most enterprises, the decision to enter the cloud is not "all or nothing." Instead, they decide which and how many workloads to migrate first. In determining which of their workloads are good initial candidates for cloud computing, enterprises should first understand their own risk tolerance. Then they should assess each workload for requirements related to security, compliance, performance, and availability, as well as characteristics such

as complexity, customization, and collaboration requirements. In Figure 2, IBM illustrates a useful framework for assessing cloud-readiness.

Figure 2 – Characteristics to Assess Workloads for Cloud-Readiness



Source: IBM

But the complexity of the decision goes beyond "cloud or no cloud." As noted, there are multiple cloud environments for enterprises to choose from, including private, public (shared, third-party), and hybrid. Each workload should be further assessed for the appropriate cloud environment. As one of few cloud providers that has built expertise and services across the full range of cloud delivery options, IBM is well positioned to help enterprises assess their workloads. The company's cloud consulting services cover the broad scope of options to determine the best delivery model for each workload.

3. ***Understand your provider's cloud architecture.*** As noted, there are no industry standards or even common language associated with cloud services. Go beyond the marketing claims to probe the provider's physical architecture, standard security elements, and processes for deployment, backup and recovery, and data deletion. This is the time to "trust but verify."

IBM has built its own cloud service infrastructure, using what it calls the "Secure by Design" framework. This means that security has been architected into the fabric of the cloud platform, rather than "bolted on" later. For enterprises that utilize the IBM cloud, this platform enables the visibility they need to ensure the performance, availability, and security of their cloud workloads—through a single, simple user console. Furthermore, IBM cloud consultants apply the same "secure by design" framework in helping enterprise clients develop their own private clouds. As a result, IBM cloud clients are able to centrally manage their cloud workloads with an end-to-end view regardless of delivery option (private, public or hybrid)—thus ensuring consistent adherence to corporate data management policies across data center environments.

4. ***Ensure appropriate resilience and performance of workloads.*** The cloud model is inherently well-suited to workload resilience. Virtualization technology used in the cloud means that workloads can be easily moved among servers, within a data center or to another data center, with just a few keystrokes. Workloads can be replicated, many times over, and housed wherever sufficient capacity exists, anywhere in the world. It would be easy for an enterprise to mistakenly assume that all its cloud workloads are automatically and equally resilient.

   In fact, the resilience of a workload depends on a number of factors, some of which are in the hands of the cloud provider and others are the choice of the enterprise. The challenge for the enterprise is to determine what level of resilience is required for each cloud workload, and then understand whether the provider has offers that will meet those requirements.

   With over 150 secure data centers worldwide, IBM has both the physical infrastructure and processes in place to offer its cloud customers high levels of protection from equipment failures and power outages. In addition, the company offers a number of services and solutions to help enterprises implement appropriate levels of resilience for their workloads. The company recently launched an offer that provides managed backup and recovery for cloud-based workloads. In addition, IBM Resiliency Consulting Services and the Security Risk Assessment give clients the expert assistance they need to ensure high availability for their most critical workloads, while providing adequate protection for other workloads.

5. ***Ensure data persistence.*** With the exponential proliferation of data, on-demand cloud storage is a welcome solution for enterprises that are struggling to keep up with necessary increases in storage infrastructure. Unfortunately, many cloud storage solutions fall short when it comes to ensuring that data is always available when it is needed—and that it is stored securely and cost-effectively.

   IBM's suite of Information Protection Services offers a range of managed security services that can help ensure data persistence throughout the data lifecycle. Information Protection Services include data storage, synchronization, backup, archive, and restoral services across a variety of data center environments—on-premises or hosted, private or public cloud. As a result, enterprises can select the storage solution that makes most sense for each dataset, without compromising on availability, security, compliance, or cost.

6. ***Future-proof your cloud environment.*** Even when they're first starting out in the cloud, enterprises need to keep an eye on the future, when their needs may change. But because there are not yet industry-recognized standards for cloud services,

enterprises are challenged to determine which cloud provider platforms are the most flexible and open.

A leader in cloud services, IBM has built its service suite to support the range of data center environments that enterprises actually use. While most cloud providers do not support legacy private data centers or even allow migration from dedicated hosting services, IBM seamlessly supports the entire spectrum of delivery options (including private, hosted and cloud services) through it's robust, Tivoli-based Service Management System. This gives customers the flexibility to move workloads and data among environments, as their needs change. Furthermore, the company is taking a lead role in industry organizations that are working to develop standards for cloud platforms—standards that will make it easier for enterprises to move their workloads among cloud platforms.

Stratecast

The Last Word

There is no risk-free cloud—just as there's no risk-free private data center. For enterprises to benefit from the cost-efficiencies and flexibility of the cloud delivery model, they need to determine the level of risk that's acceptable for each workload, and to find a cloud partner they can trust to deliver what they need. Because cloud delivery models require enterprises to cede considerable control over their data to a third party, the choice of cloud partners is critically important to the ability to overcome obstacles.

In selecting a cloud provider, enterprises should consider the following:

- **Expertise:** Industry buzz and the low barrier to entry have led hundreds of businesses to tout themselves as cloud providers. Be sure your provider has a proven history of success, not just in one area of cloud computing, but in every area that's important to success: data center infrastructure, hosting, security, and applications
- **Flexibility:** The cloud is evolving, as are your needs. Be sure your provider supports multiple cloud delivery models, not just hosted options but also extending into your private data center.
- **Ease of implementation and management:** Cloud computing isn't a "set it and forget it" effort. Choose a provider that can help you assess your workloads; select the right workload for each environment; and provide visibility and management tools across all your data center environments to ensure optimal price-performance for all workloads.
- **Trust:** Ultimately, a successful cloud engagement is all about the relationship between the cloud provider and the client. Be sure to select a provider you can rely on to provide service assurance, now and in the future.

As a worldwide leader in the IT industry, IBM has drawn on its expertise in infrastructure and services to deliver a comprehensive portfolio of secure, cloud-based services. For enterprises that are just starting out in the cloud, IBM can help them develop and implement a secure, resilient cloud strategy that meets their needs while minimizing corporate risk.

Lynda Stadtmueller

Program Manager – Business Communication Services
Stratecast (a Division of Frost & Sullivan)
lstadtmueller@stratecast.com

Silicon Valley
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10, Suite 400,
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London
4, Grosvenor Gardens,
London SWIW ODH,UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost
myfrost@frost.com
http://www.frost.com

CONTACT US

Beijing
Bengaluru
Bogotá
Buenos Aires
Cape Town
Chennai
Delhi
Dubai
Frankfurt
Kolkata
Kuala Lumpur
London
Manhattan
Melbourne
Mexico City
Milan
Mumbai
Oxford
Palo Alto
Paris
Rockville Centre
San Antonio
São Paulo
Seoul
Shanghai
Singapore
Sydney
Tel Aviv
Tokyo
Toronto
Warsaw

ABOUT STRATECAST

Stratecast assists clients in achieving their strategic and growth objectives by providing critical, objective and accurate strategic insight on the global communications industry. As a division of Frost & Sullivan, Stratecast's strategic consulting and analysis services complement Frost & Sullivan's Market Engineering and Growth Partnership services. Stratecast's product line includes subscription-based recurring analysis programs focused on Business Communication Services (BCS), Consumer Communication Services (CCS), Communications Infrastructure and Convergence (CIC), OSS and BSS Global Competitive Strategies (OSSCS), and our weekly opinion editorial, Stratecast Perspectives and Insight for Executives (SPIE). Stratecast also produces research modules focused on a single research theme or technology area such as Connected Home (CH), MS and Service Delivery Platforms (IMS&SDP), Managed and Professional Services (M&PS), Mobility and Wireless (M&W), and Secure Networking (SN). Custom consulting engagements are available. Contact your Stratecast Account Executive for advice on the best collection of services for your growth needs.

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, enables clients to accelerate growth and achieve best-in-class positions in growth, innovation and leadership. The company's Growth Partnership Service provides the CEO and the CEO's Growth Team with disciplined research and best-practice models to drive the generation, evaluation, and implementation of powerful growth strategies. Frost & Sullivan leverages 50 years of experience in partnering with Global 1000 companies, emerging businesses and the investment community from more than 40 offices on six continents. To join our Growth Partnership, please visit http://www.frost.com.