# Cloud 2.0: Securing Trust to Survive the 'One-In-Five' CSP Shake-Out

Sponsored by Trend Micro


**October 2013**

STL Partners / Telco 2.0

contact@stlpartners.com

# Contents

## Figures

# Introduction: one in five Cloud providers will survive

The Cloud market is on the verge of the next wave of market penetration, yet it's likely that only one in five Cloud Service Providers (CSPs) in today's marketplace will still be around by 2017, as vendors fail or are swallowed up by aggressive competitors. So what do CSPs need to do to survive and prosper?

*This research was sponsored by Trend Micro but the analysis and recommendations represent STL Partners' independent view. STL Partners carried out an independent study based on in-depth interviews with 27 senior decision makers representing Cloud Service Providers and enterprises across Europe. These discussions explored from both perspectives cloud maturity, the barriers to adoption and how these might be overcome. The findings and observations are detailed in this three-part report, together with practical recommendations on how CSPs can address enterprise security concerns and ensure the sustainability of the cloud model itself.*

# Part 1: Cloud - coming of age or troubled adolescent?

While the concept of organising computing as a utility dates back to the 1960s, the cloud computing model as we know it today is built on the sub-classifications of Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

We've covered telcos' role in Cloud Services in depth in our Cloud research stream, and found that hype, hope and uncertainty have been notable features of the early stages of development of the market, with many optimistic forecasts of adoption being somewhat premature.

In terms of the adoption cycle adoption today, our analysis is that Cloud Services are on the brink of 'the chasm': well established among early adopters but less well known, trusted and used by the mass market segment of the enterprise market.

Building trust among new customer segments is the key to bridging this gap. For the industry it is a make or break point in terms of achieving scale. For CSPs, trust will be a key to survival and prosperity in the next phase of the market, enabling them to open up new opportunities and expand the amenable market, as well as to compete to retain and grow their individual market shares.

Many of the obstacles to and inhibitors of cloud adoption stem from customers' perceptions of product immaturity – "will it be safe and work how we want without too much hassle and commitment?" In this report we examine findings on the general inhibitors and drivers of adoption, and then those related to the main inhibitor, data security, and how they might be addressed.

## *Overcoming the obstacles*

Enterprise decision-makers in the study admitted to being deterred from the cloud by the prospect of migration, with the "enterprise/cloud barrier" perceived as a significant technical hurdle. While CSPs with enterprise-grade propositions have in place the business model, margins and consultative resources to offer customers an assisted journey to the cloud, standard public offerings are provided on a Do-It-Yourself basis.

However, data privacy and security remain the biggest inhibitors to cloud adoption among enterprises, due in no small part to a perceived loss of visibility and control. Recent headline-grabbing events relating to mass surveillance programmes such as PRISM have only served to feed these fears. As will be seen in this report, a lack of consistent industry standards, governance and even terminology heightens the confusion. Internal compliance procedures, often rooted in an out-dated "physical" mind-set, fail to reflect today's technological realty and the nature of potential threats.

According to the UK Department for Business Innovation & Skills, the *direct* cost of a security breach (any unauthorised access of data, applications, services, networks or devices) is around £65,000 for SMEs and £850,000 for larger enterprises. However, add to this financial penalties for failure to protect customer data, reputational damage, diminished goodwill and lost business, and the consequential losses can be enough to put a company out of business. It's little wonder some enterprises still regard cloud as a risk too far.

*"Enterprise adoption of cloud massively depends on industry – how risk-averse or security conscious they are."*

Lead, Secure Mobility, CSP

In reality, CSPs with a heritage in managed services and favourable economies of scale can typically match or better the security provisions of on-premise data centres. However, as "super enterprises" they present a larger and therefore more attractive target for malicious activity than a single business. There is simply no room for complacency.

CSPs must shift their view of security from a business inhibitor to a business enabler: crucial to maintaining and expanding the overall cloud market and confidence in the model by winning customer trust. This requires a fundamental rethink of compliance – both on the part of CSPs and enterprises – from a tick-box exercise to achieve lowest-cost perimeter protection to *cost effectively* meeting the rigorous demands of today's information-reliant enterprises.

*"A recent survey asked what was the single biggest benefit of cloud. Vendors talked about cloud bringing the lowest TCO, but enterprises said it's about speed to market, being able to switch on initiatives more quickly."*

Business Development Manager, CSP

Cloud services cannot be considered mature until enterprises en masse are prepared to entrust anything more than low-sensitivity data to third party CSPs. The more customer security breaches that occur, the more trust will be undermined, and the greater the risk of the cloud model imploding altogether.

## State of the nation

The journey to the cloud is often presented in the media as a matter of "when" rather than "if". However, while several CSPs in our study believed that the cloud model was starting to approach maturity, enterprise participants were more likely to contend that cloud was still at an experimental or "early adopter" stage.

The requirements of certain vertical markets were perceived by some respondents to make cloud a non-starter, for example, broadcasters that need to upload and download multi-terabyte sized media files, or low-latency trading environments in the financial sector. Similarly, the value of intellectual property was cited by pharmaceutical companies as justifying the retention of data in a private cloud or internal data centre *at any cost*.

*"Cloud providers need to be clearer about how they operate security and more open about what standards they adopt and use. You shouldn't have to pull teeth to get it."*

IT Security Manager, Public Sector

CSPs universally acknowledged that their toughest competitor continues to be enterprises' own in-house data centres. IT departments are accustomed to having control over their applications, services, servers, storage, network and security. While notionally, they accept they will have to be less "hands on" in the cloud, a lack of trust persists among many. This reticence was typically seen by CSPs as unwarranted fear and parochialism, yet many are still finding it a challenge to educate prospective customers and correct misconceptions. CSPs suggested that IT professionals may be as likely to voice support for the cloud as turkeys voting for Christmas. However, more enlightened IT functions have embraced the opportunity to evolve their remit to working *with* their CSP to monitor services against SLAs, enforce compliance requirements and investigate new technologies rather than maintaining the old.

For tentative enterprises, security is still seen as a barrier to, rather than an accelerant of, cloud adoption, and one of the most technically challenging issues for both IT and compliance owners. Enterprises that had advanced their cloud strategy testified that successful adoption relies on effective risk management when evaluating and engaging a cloud partner. Proponents of cloud solutions will need compelling proof points to win over their CISO, security team or compliance officer. However, due diligence is a lengthy and often convoluted process that should be taken into account by those drawn to the cloud model for the agility it promises.

*"I don't foresee a day when major corporations with intellectual property will be happy to concentrate in the hands of relatively few cloud providers, because it's a very attractive attack target."*

IT Security Manager, Enterprise

The majority of CSPs interviewed were relatively dismissive of customer security concerns, making the valid argument that their security provisions were at least equal to, if not better than, that of most enterprise data centres. However, as multiple companies concentrate their data into the hands of a few CSPs, the larger and more attractive those providers become to hackers as an attack target. Nonetheless, CSPs rarely offer any indemnification against hacking (aside from financial compensation for a breach of SLA) and SaaS providers tend to be more obscure than IaaS/PaaS providers in terms of the security of their operations. Further commercial concerns explored in this report relate to migration and punitive contractual lock-in. Enterprises need to feel that they can easily relocate services and data across the cloud boundary, whether back in house or to another provider. This creates the added challenge of being able to provide end-to-end audit continuity as well as in transit.

*"If you look at the big cloud players, they're already buying up the smaller ones, so there's a certain level of consolidation. We would be an acquirer, not the acquired."*

Senior Manager, CSP

There are currently around 800 cloud service providers (CSPs) in Europe. Something of a land grab is taking place as organisations whose heritage lies in software, telecoms and managed hosting are launching cloud-enabled services, primarily IaaS and SaaS.

However, "cloudwashing" – a combination of vendor obfuscation and hyperbole – is already slowing down the sales cycles at a time when greater transparency would be likely to lead to more proofs of concept, accelerated uptake and expansion of the overall market.

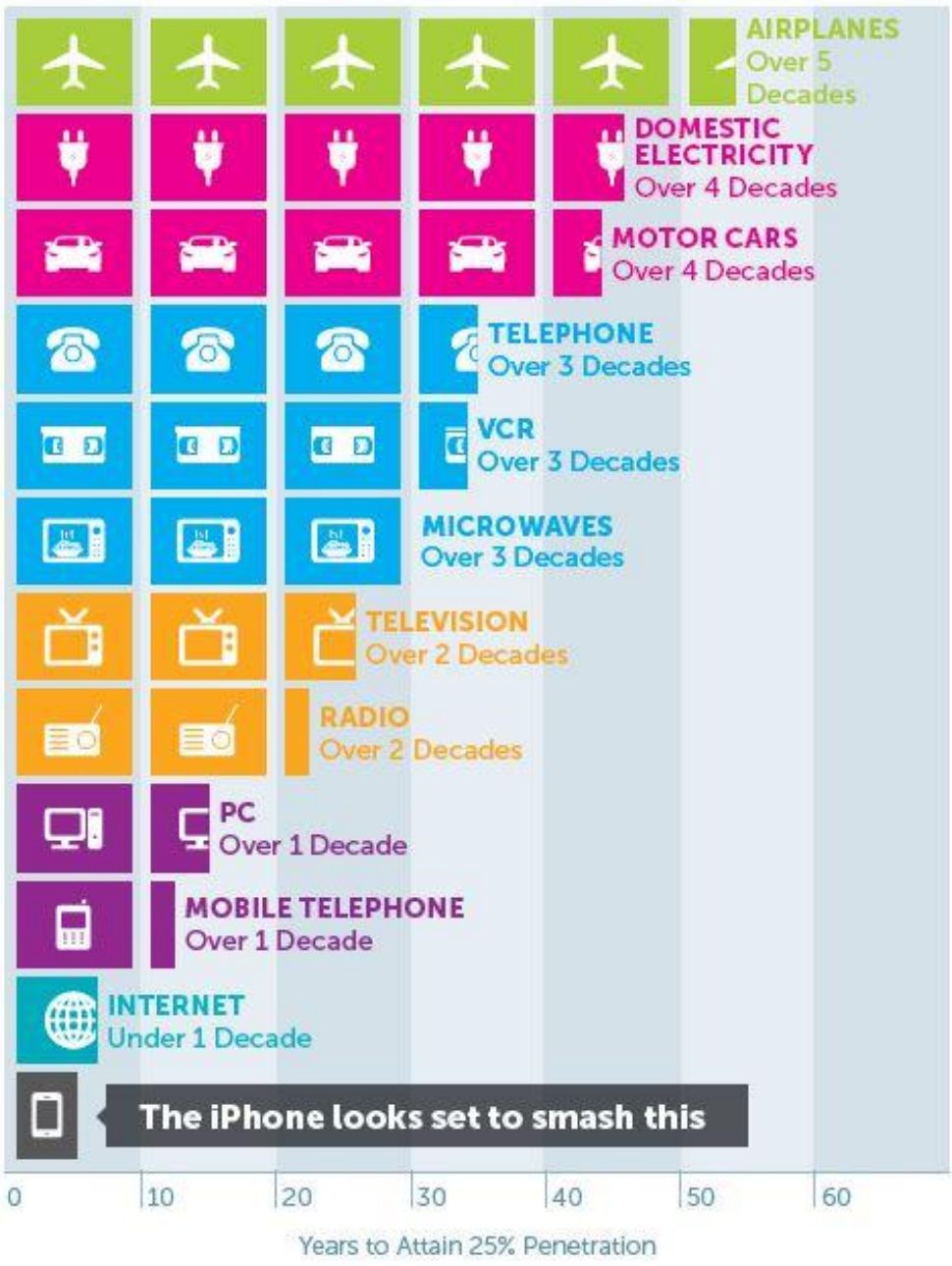
Turbulence in the macro economy is exacerbating the problem: business creation and destruction are among the most telling indicators of economic vitality. A landmark report from RSM[1] shows that the net rate of business creation (business births minus deaths) for the G7 countries was just 0.8% on a compound annual basis over the five-year period of the study. The BRICs, by contrast, show a net rate of business creation of 6.2% per annum – approximately eight times the G7 rate.

In parallel, the pace of technology success is accelerating[2]. Technologies are considered to have become "mainstream" once they have achieved 25% penetration. As cloud follows this same trajectory, with a rash of telcos, cable operators, data centre specialists and colocation providers entering the market, significant consolidation will be inevitable, since cloud economics are inextricably linked to scale.

[1] The Road to Recovery: Insights from an international comparative study of business 'birth' and 'death' rates, 2013

[2] P R Smith, 2010

**Figure 1 – Technology adoption rates**




Source: STL Partners

Lastly, customers are adapting and evolving faster than ever, due in no small part to the advent of social media and digital marketing practices, creating a hyper-competitive environment. As a by-product, the rate of business failure is rising. In the 1950s, two-thirds of the Fortune 500 companies failed. Throughout the 1980s, almost nine out of ten of the so-called "Excellent" companies went to the wall, and 98% of firms borne out of the "Dot Com" revolution in the late 1990s are not expected to survive.

As a result, STL Partners anticipates that by 2018, a combination of consolidation and natural wastage will leave only 160 CSPs in the marketplace – a survival rate of one in five.

## *Drivers of cloud adoption*

The business benefits of the cloud are well documented, so the main value drivers cited by participants in the study can be briefly summarised as follows:

**Figure 2 – Business and IT Drivers of cloud adoption**


*Source: STL Partners*

# *Inhibitors to cloud adoption*

*"IT Security Teams don't necessarily have time to keep up with technologies so even today there's a lot of ignorance around what's available."*

Business Development Manager, CSP

*"We try to educate our customers. With Amazon, you can do everything self-service, but now they're hiring sales and solution architects to go to customers and explain how cloud can help them."*

Head of Special Projects & Evangelisation, CSP

While discussions around cloud are ubiquitous, the model cannot be considered mature as long as it is still regarded by enterprise IT as a technical challenge to address, rather than a business asset to embrace. According to our study, cloud only appears to be well-understood among technical decision-makers, undermining its potential as a business enabler and innovation platform.

Enterprises face a disorientating array of terminology and service models – no two cloud providers are structured alike or define their propositions according to a common taxonomy. Lack of consistency and industry-wide standardisation in the semantic definition and implementation of cloud is undermining enterprise confidence. As a result, several mass-market infrastructure providers are now investing in sales and solution architects to educate enterprise prospects in how the cloud can address their needs.

The concerns raised by enterprises in the study can be categorised as follows:

- Migration / integration of cloud with internal systems
- Contractual lock-in and exit strategies
- Governance and compliance issues
- Supplier credibility and longevity
- Testing and assurance
- Security and data privacy (especially international)

## Cloud migration and integration with internal systems

If cloud is to deliver on its promise of agility and innovation, it needs robust governance in place to speed up the move from drawing board to deployment. With the exception of start-ups, most organisations realistically need a hybrid of private cloud, dedicated public cloud and shared public cloud, not to mention managed hosting and colocation of legacy systems that aren't suitable for migration or virtualisation. Not all CSPs are vendor-agnostic, and not all can or are willing to support a hybrid proposition.

Due to the fragmented nature of the cloud market, cloud brokerage – the aggregation, integration and customisation of services and solutions – presents a sizeable opportunity. A brokerage role may be provided in-house (as a subdivision of IT) or by a third party which may itself be a CSP, systems integrator or independent consultancy. Alternatively, there are a range of tools and management consoles that allow interoperability between private and public clouds – the best of which go beyond the operating infrastructure to provide an application-centric view across pooled storage and networking.

## Vendor lock-in and exit strategies

*"Our fears about cloud are what happens if we want to change service providers? It doesn't matter who you go with – you have the same problem everywhere."*

Head of IT Security, Public Sector

A significant deterrent to IaaS in particular expressed by enterprise decision-makers was contractual lock-in – the severity of which often appears to depend on the commercial model and cost base of the CSP. This issue only manifests once an enterprise has already satisfied itself the provider can be trusted with its data and is ready to do business.

## *Fine print*

*"Contracts are becoming more business-like than technology-driven – we're adapting our contract frameworks and risk profiling to deal with that level of service expectation."*

Head of IT Solutions, CSP

In the early stages of cloud, CSPs tended to offer standard contracts on a take-it-or-leave-it basis. However, a growing number of enterprise cloud providers are now willing to negotiate individual terms and conditions for mid-tier customers.

To avoid punitive vendor lock-in, enterprise decision-makers need to check the small print, paying special attention to liability for failures, stipulations in service level agreements, compatibility with EU data protection rules and any right of suppliers to alter the service without notice.

## *Standardisation*

*"The risk is that global players will dominate the market from a volume perspective and work at single-digit margins, but we can't afford to do that."*

Senior Manager, CSP

With the cloud market seemingly set to be rationalised through attrition and acquisition, some enterprise respondents voiced fears that the remaining dominant vendors may attempt to trap infrastructure customers with proprietary technology. This was of particular concern for smaller companies making opportunistic journeys into the cloud.

However, these fears may be misplaced: cloud should provide a highly standardised environment – after all, standardisation is what makes cloud economies attractive. Several established CSPs serving mid-tier and large enterprise customers described their cloud services as a set of building blocks that could be fitted together in any combination. While the modules are generic, it's the ability to combine them to meet customers' precise requirements, migrate at the customer's pace, and differentiate through the service wrap that enables the provider to stand out from the crowd. Where that degree of customisation isn't required, a Virtual Private Data Centre (VPDC) can offer low or no commitment, allowing customers to take full advantage of true switch-on, switch-off, pay-as-you-go services without penalty.

## *Exit Strategy*

*"With regard to vendor lock-in, we considered our way in and our way out."*

Head of IT Security, Public Sector

Cloud computing can also create external dependencies for an enterprise that heighten business risks. For example, if an enterprise puts its proverbial eggs in a single, mass-market CSP's basket, it may find itself backed into a corner if the provider decides to impose a blanket price increase overnight.

When investigating how to get into the cloud, enterprises should have a clear exit strategy in place before signing any contract. That means touching any proprietary or non-standard elements as lightly as possible, and understanding how data comes out, how much time is allowed, and the extent of the vendor's co-operation in making it happen. Those enterprises that encrypt their data in the cloud can ensure portability by retaining control of their encryption keys; in so doing, they can not only safeguard their data from third parties, but also avoid reliance on the CSP to unlock their data should they wish to switch to another provider or bring data back in house.

## Governance and compliance issues

*"PCI DSS states all cloud service providers and merchants should ensure contractual agreements – that means legal obligations mapped out clearly from the start, with a lot of focus on who does what job and ensuring it's done."*

Head of IT Solutions, CSP

Enterprises were almost unanimously dissatisfied with the vague or ambiguous contractual language typically employed by CSPs. Marketing materials and Service Level Agreements (SLAs) often make promises around availability, but are less keen to specify security benchmarks. A frequent complaint was that many cloud services claimed to be compliant with various regulations such as PCI DSS, HIPAA and HITECH. However, for many of these designations, there is no formal certification or stamp of approval.

Take PCI DSS, for example – the Payment Card Industry Data Security Standard. It offers a framework of specifications, tools, measurements and support resources to ensure the safe handling of cardholder data. But in a case of "whose data is it anyway?" *all* companies that process, store or transmit credit card information have to maintain a secure environment.

Cloud security is a shared responsibility between the CSP and its customers: if payment card data is stored, processed or transmitted in a cloud environment, PCI DSS will apply to that environment, and will typically require validation of both the CSP's infrastructure *and* the customer's usage of that environment. The allocation of responsibility between customer and CSP for managing security controls does not exempt the customer from the responsibility of ensuring that their cardholder data is properly secured.

Clear policies and procedures should be agreed between the enterprise and the CSP for all security requirements, with responsibilities for operation, management and reporting clearly defined and understood for each requirement. Governance, Risk and Compliance testing should list threats, vulnerabilities and risks associated with IaaS, PaaS and SaaS, and suggest controls assimilated from prevailing industry best practices in the absence of definitive standards.

## Supplier credibility and longevity

*"Customers are looking to out-task quite deeply: they want to hand over a suite of applications and say 'you are now solely responsible for performance, capacity and security of those applications'."*

Head of IT Solutions, CSP

Given that cloud is still seen as an emerging rather than established technology, enterprises looking to undertake a substantial commitment are cautious about the long-term viability of some CSPs. For many IT professionals, entrusting their infrastructure, applications and data to a faceless third party still feels like an act of faith when they are used to being able to walk down a corridor and inspect the tin at will.

While some cloud providers have sprung from a background in business continuity and disaster recovery, others have evolved or branched out from telcos. They have the advantage of existing data centres and customer relationships, and cloud is more or less a natural evolution of traditional managed hosting services, yet some telcos have yet to establish real credibility in the IT services market, especially for cloud delivery models.

A bigger concern to any prospective customer is CSPs that have seemingly come from nowhere, prompting questions such as

- Who are these people?
- Are they financially stable?
- Will their service "play nice" with my existing IT infrastructure and routines, or will I be expected to distort my way of life to fit theirs?
- Do they have experience of meeting the needs of peers in our industry, or organisations with?

- Who's responsible for what?
- Are they likely to fail or be swallowed up by a CSP we'd be reluctant to do business with

CSPs with a strong heritage and a substantial footprint of wholly-owned data centres (and often networks) are better placed to allay these fears with tangible proof points. But if opting for a provider with less in the way of provenance, its key once again that enterprises have a decent exit strategy in place and can reclaim their data swiftly if trouble looms.

## Testing and assurance

Unlike traditional performance testing, where scalability is limited to the number of users within the network, cloud offers almost unlimited scalability. Enterprises should therefore satisfy themselves that any application running on cloud infrastructure can submit to and pass the following:

- **Performance testing** – to measure response times and isolate issues related to specific steps or actions
- **Load testing** – to determine stability when supporting a user count in the hundreds, thousands or even millions
- **Stress testing** – to breaking point, perhaps three or more times the maximum expected usage
- **Capacity testing** – to determine maximum capacity for current or future hardware, bandwidth or other needs
- **Fail-over testing** – conducted under anticipated load with simulated component failure
- **Application security testing** – to determine whether the application is appropriate to migrate or design in the cloud, and establish any dependencies on other systems
- **Latency testing** – to measure the delay between action and response for any cloud delivered applications

That leaves the biggest challenges until last – security and data privacy – persistent concerns which are having such a detrimental effect on enterprise cloud adoption that they merit a section all to themselves.

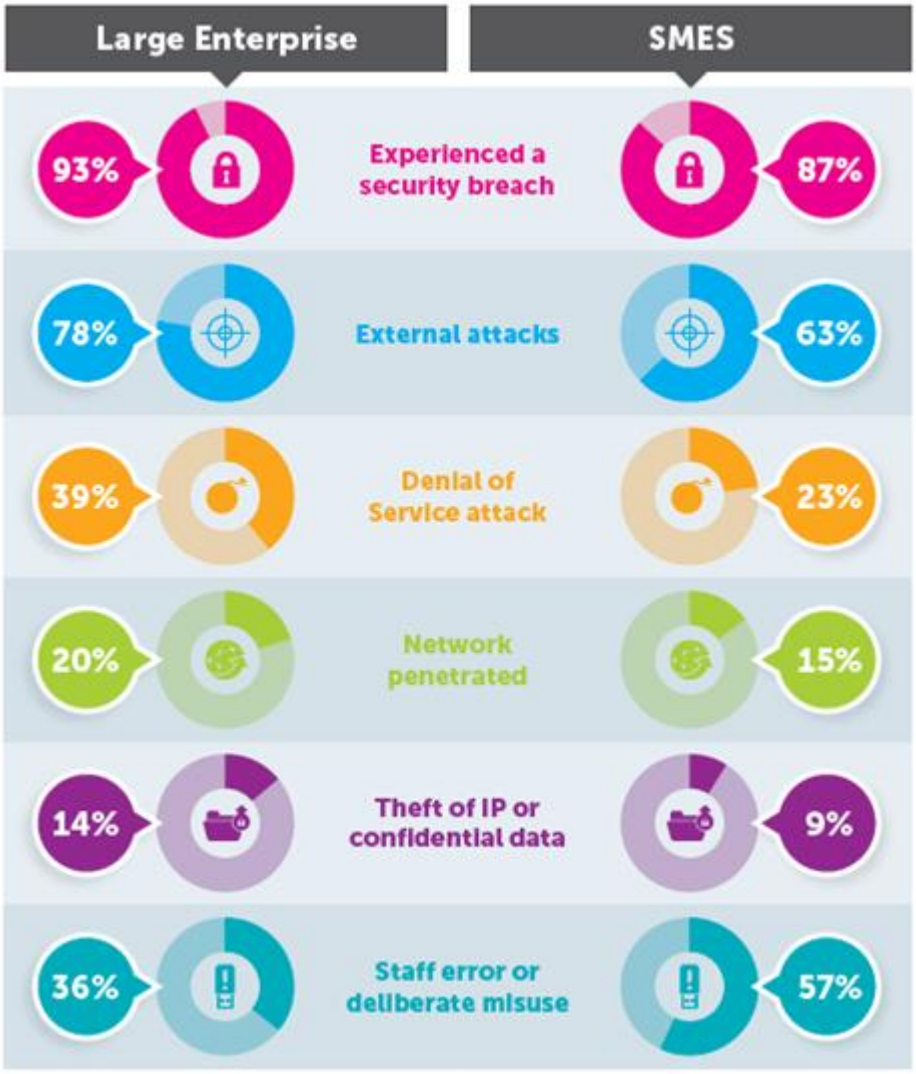
# Part 2: Cloud security and data privacy challenges

*"Years ago, people kept their money at home under the mattress because they didn't trust the banks not to get held up. It's the same thing with cloud computing."*

Head of Special Projects & Evangelisation, CSP

In any data centre, serious security breaches are usually due to multiple failures in technology, processes and people, rather than a single, isolated weakness. Security was deemed to be a particularly big barrier to cloud adoption by those enterprises whose dealings with the cloud were limited, as opposed to their more experienced peers.

**Figure 3 – Information security breaches 2013**




Source: Department for Business Innovation & Skills

Even for organisations well versed in outsourcing and offshoring, however, the cloud can throw up new security challenges. With new system architectures come new cyber-threats, so security mechanisms relied on in the past are unlikely to suffice now and into the future.

*"Anything over and above infrastructure, security is down to the customer to make sure whatever they provision to a cloud environment is secured."*

Head of Innovation, CSP

Recurring themes emerged when discussing privacy concerns around the cloud. An obvious source of anxiety was the increased risk of improper use and disclosure of personal information stored and accessible in multiple locations, by multiple parties, across multiple jurisdictions.

Hot on the heels of recent adverse media coverage, several enterprises expressed a fear of disclosure to foreign law enforcement or regulatory authorities, where data was stored and processed outside the home country of individuals from whom the information was collected.

Many were concerned about upholding their organisation's transparency obligations with regard to privacy and data protection practices, especially as the full picture of how and where data is stored, processed and shared would be more likely to be obscured in the cloud environment. Others highlighted the potential for a CSP failing to meet their organisation's data retention and destruction obligations.

In 2012, the Cloud Security Alliance launched a Privacy Level Agreement Working Group to help CSPs and enterprises navigate data privacy standards and support implementation of EU data protection requirements. But while this aims to provide an objective and comparable way for CSPs to communicate their personal data handling practices, it's an entirely voluntary arrangement.

## Physical security

Interestingly, when discussing security, many CSPs spoke almost exclusively about physical rather than logical security. A level of complacency was evident in assuming that the security box could be ticked through the use of intruder prevention measures, while hacking was only mentioned as an afterthought or considered to be an occupational hazard.

## Data residency and jurisdiction

Geospatial risks are a growing concern. Many enterprise-grade cloud services allow enterprises to specify a location for data hosting when setting up the service. Organisations writing data to mass-market cloud-based storage, on the other hand, may not know where their data resides or have any influence over its location – one of the biggest fears around cloud adoption.

Identifying all the jurisdictions that apply is not a simple process. There's the country within which the enterprise is headquartered, the country in which the CSP is headquartered, and the country in which the data centre actually resides. Reputable CSPs tend to be well aware of the issue and offer customers a choice of geographical nodes for their data.

*"Security is customers' biggest fear. One bank in Germany ruled out a web conferencing provider because it was a US company, subject to the Patriot Act, and they didn't want conversations being monitored."*

Director of Innovation & Prototyping, CSP

In our study, enterprise decision-makers expressed uncertainty around what would happen in the event that national legislation applicable to the CSP (although not their own business) compelled the provider to hand over data to third parties. The Patriot Act in particular was singled out by multiple respondents, although in reality, other governments have just as much access as the US for national security or law enforcement reasons. In order to subpoena records, the US Government must still obtain a court order, which the judge should only issue if records sought are "relevant" to authorised investigations to protect against terrorism or other clandestine activities. But when the finer points of law can come down to semantics, who determines relevance?

The recent revelations about PRISM and similar security programmes have served to make US data centres a no-go area for many European enterprises. However, it's worth noting that EU CSPs are also subject to compliance requests from other countries under Mutual Legal Assistance Treaties.

*"Recent events will drive encryption for purposes of data sovereignty not just privacy."*

Information Security Specialist, CSP

Full disk encryption has been shown to be highly effective, leading law enforcement and federal agencies in the US to complain that they are unable to retrieve encrypted data in criminal investigations.

## Compliance and audit

*"We think about contract obligations, give the customer an approach to manage data, and check the controls every month. We have strong SLAs that can be audited by the customer's internal team, all included in the service."*

Head of IT Solutions, CSP

Compliance doesn't equal security: it only attests to the state of security at a specific moment in time. Some compliance requirements are no longer fit for purpose, having failed to keep pace with technological development – for example, to physically locate data on a specific piece of hardware and associate all physical procedures relating to access to that hardware.

Several CSPs interviewed were more than happy to offer prospective customers a guided tour of their data centre facilities, yet only one explicitly stated they allowed their systems and processes to be audited by a third party. However, it would remain to be seen whether the scope of this invitation was restricted to an examination of the CSP's policies and procedures, rather than a rigorous evaluation of the implementation's effectiveness, or whether the customer could carry any evidence discovered of non-compliance off the CSP's premises.

*"We map our procedures to the customer's, and we create an overarching governance, risk and compliance policy that both organisations can clearly understand."*

Head of IT Solutions, CSP

For enterprises embarking on a cloud partnership, a copy of the CSP's ISO 27001 certification isn't sufficient evidence of compliance. What's more, a compliant provider doesn't automatically make for a compliant customer: the enterprise is still responsible for ensuring the CSP maintains regulatory controls, while maintaining compliance for any of its in-house IT operations that connect to the cloud service.

The CSP should be able to demonstrate a customer's environment is segmented from other tenants' in the equivalent to physical network separation, with each organisation working with a customised virtual application instance. Additionally, but less commonly available in practice, vendors should be able to provide real-time event analysis and reporting to demonstrate their ability to respond to information security threats in a timely, effective manner and ensure internal policy enforcement. The task of protecting the organisation can become complex and unwieldy without automated tools to help identify patterns, filter, clean and analyse the data that forms the context of an attack.

## Encryption

*"Your most effective security is encryption within the third party environment, but key management and ownership should stay with the data owner, not the cloud provider."*

Innovation Specialist, CSP

Encryption is among the more mature and readily available security controls in cloud computing today. Once data is encrypted, criminals can't sell it, and if it goes missing, companies are generally protected from disclosure requirements.

As such, it can compensate for a litany of security issues, from a bad firewall to a determined hacker or a lost laptop. However, encryption keys and management rights must also be orchestrated and secured, otherwise the protection afforded by encryption will go straight out the window in the event that an external party is compromised.

The majority of small-scale data breaches tend to be caused by mundane events through employee negligence – such as loss or theft of a device that contains corporate data – rather than wilful or malicious acts. With increasing mobilisation, any device that leaves the organisation needs to be protected with more than just a password. Most organisations formulate policies for securing mobile devices, but paradoxically lack the tools to enforce them. Further, often overlooked complications include enterprise data at rest, such as back-up tapes in storage, and removable media, such as USB drives, which similarly need to be encrypted.

If the CSP offers software-based full disk encryption, this service expediently ticks a box in as much as the data is unreadable, while allowing enterprises to take advantage of cloud economics. But relying exclusively on the cloud partner also carries a number of risks.

- The CSP could be compelled to hand over encryption keys to Governments without the enterprise being aware
- Having a CSP as the custodian of both the encryption keys and encrypted data does not provide adequate segregation of duties
- If the enterprise customer wishes to leave for another a vendor or to bring data back in-house, it could find itself locked in

*"If you use a third party encryption product and manage the keys, you can be relatively certain you won't be locked in from an encryption perspective."*

Head of Strategy, CSP

These concerns can be addressed by ensuring the enterprise retains custody of the encryption keys. While this liberates an enterprise to take up a competitor's cloud offer or bring data back in house, this is in fact a positive differentiator as customer loyalty is not won through 'Stockholm Syndrome' – trying to secure customers' loyalty by holding them captive.

The CSP, meanwhile, should also be able to offer written assurances around centralised policy management and granular device control and data management, to prevent embarrassing, high-profile leakage of corporate information through human error and oversight.

## Identity and Access Management

As the recent Wikileaks scandal will attest, the biggest threats to information security often come from within.

Cloud environments pose unique access control challenges through a combination of multi-tenancy, architectural diversity and large scale. Depending on the service model, while applications and associated infrastructure may be under the control of the CSP, the enterprise is still responsible for identity and access management (IAM). The enterprise must be able to handle its own provisioning and de-provisioning of user access rights and automate the administration of user accounts. It also needs to be able to track who has accessed what data in the cloud to demonstrate compliance with internal and regulatory policies.

*"We ensured cloud met both in-house and regulatory requirements and that risks fell within our internal appetite."*

IT Security Manager, Enterprise

Many access control techniques were designed for enterprise data centres and are poorly suited to cloud environments. It can be costly and time-consuming to implement a typical old-school IAM system, which invariably lacks the flexibility to handle new business processes or applications outside the enterprise firewall, such as SaaS.

As software vendors continue to transition features and functions as well as data into the cloud, identity management as a service (IDaaS) is emerging in the form of authentication infrastructure that resides in the cloud. It offers all of the usual benefits associated with cloud – reduced on site infrastructure, easier management and a broader range of integration options. But it poses risks and challenges, too. The biggest is how to manage privileged access to virtual machines provisioned on an IaaS platform. Processes that were previously behind a firewall become exposed to the internet. It involves entrusting a highly critical business function to a third party, with little or no insight into their processes or background checks on personnel. And of course identity is the key component of regulatory compliance – providing access to the right data starts with restricting access to the right people.

As a result, enterprises may be reluctant to outsource control of the IAM function to cloud vendors without a high level of assurance around the CSP's confidentiality, business continuity and longevity.

## *Shared resources and data segregation*

*"We have three flavours of cloud – completely shared or public; isolated, where the customer environment is dedicated at blade level but they share the network and storage areas to keep costs down; and fully dedicated – if the customer wants an environment to support IL3."*

Head of IT Solutions, CSP

In the public cloud model, enterprise data is often stored and processed in a shared environment in order to derive the economies of scale that make cloud so appealing. Most mass-market CSPs interviewed dismissed multi-tenancy as "not a major concern" for enterprise customers, believing it was an accepted trade-off as part and parcel of the cloud model. However, these assertions didn't take account of the type of tenants that might be expected to be neighbours – consumer, SOHO, growing business, mid-market enterprise, corporate – or the difference between SaaS and IaaS/PaaS customer demands. Enterprise-grade service providers, on the other hand, were able to offer greater assurances that all tenants on shared infrastructure would be like-minded organisations with a common requirement for security, rather than start-ups, cyber criminals or threat actors.

There is also something of a misconception among enterprises that private clouds are inherently a safer bet, although in reality, the security challenges, threats and requirements are more or less identical. A private cloud that lacks the appropriate security measures is just as vulnerable to threats and, if anything, enterprises may have an over-reliance on a single perimeter to protect a private cloud.

Enterprises need to review a public cloud vendor's architecture to ensure proper data segregation is available and that data leak protection measures are in place. They should also satisfy themselves as to the whereabouts and measures surrounding back-ups and archives.

## Security incident management

*"My concern with SLAs is that if your provider fails to live up to it, what do you get in return? Probably some usage credits, but is that really what you want if they've failed you? We need to think a little more radically about what kind of sanctions are in place."*

Head of Innovation, CSP

Unsurprisingly, both CSP and enterprise participants interviewed were a little evasive about whether they had suffered a data breach. Perhaps more worryingly, many admitted being unaware – some assumed a security incident was inevitable in the course of modern business, while others couldn't state with any confidence that they had definitely not been breached at some point.

Of greater concern is what happens in the event of a breach: while many CSPs felt these provisions were adequately covered in their SLAs, enterprises typically disagreed. Few providers were confident they had a defined policy for incident management – one that clearly stated who (provider or customer) defines an incident, how incidents are categorised, who is supposed to do what and to what level, who will check and how, what will be reported to whom, in what format and when.

Neither should enterprises assume that CSPs can provide forensic investigations into inappropriate or illegal activities, or preserve the scene of the crime, since most in the study did not support such measures. Only larger, more established CSPs had internal forensics capability or partnered with a security specialist to provide "ghost-hunting" and remediation.

## Continuity services

Protecting organisations from unplanned downtime relies on building redundancy and diversity directly into business continuity and disaster recovery systems. Business systems need to be able to run on a number of different infrastructures, whether public or private clouds, and switch between them (fail over) quickly and efficiently. This requires a combination of redundancy in design with automation in the cloud management layer.

Solutions for resilient design are almost as many and varied as the software components they use, so their efficacy boils down to how the architecture is operated. If a given cloud resource goes down – from a disk drive to an entire geographical region – the crucial test is how seamlessly it can fail over to keep operations up and running.

*"It's a joint responsibility to ensure all layers of the stack are secure. The provider can't secure the full stack without customer co-operation."*

Global Business Development, CSP

As a rule of thumb, the greater the level of automation employed, the better the operational excellence of the CSP. However, to keep enterprises within their comfort zone requires visibility into all infrastructures through a 'single pane of glass' or management console. The same automation and control that gives organisations the ability to scale up or down to align with fluctuating demand should also let them migrate entire server deployments to a new infrastructure if disaster strikes.

## Data disposal

Failure to dispose properly of customer data can lead to serious breaches of data protection and privacy problems for CSPs, not to mention compliance issues. While a traditionally outsourced data centre provider will typically commit to destroying data at the

end of a contract and confirm destruction in writing, that type of policy is rare for SaaS providers. While the storage architecture for most SaaS services means data from erstwhile customers will be quickly overwritten and virtually impossible to recover, there is little or no convention surrounding the treatment of former customers' data on back-up media.

Anecdotally, enterprises mentioned notable instances of discovering data on storage that has not been properly sanitised. Not all CSPs are happy to physically destroy physical storage media in a way that renders them unreadable – such as shredding or melting – due to the economies of maintaining a fully-flexible resource pool. Once again, encryption goes a long way to addressing the concern of data falling into the wrong hands.

## Cloud provider assessment

Generic lack of trust was acknowledged by both enterprises and CSPs as a significant barrier to cloud adoption – with lack of transparency cited by enterprises as the main culprit. Of course, no enterprises should be placing high-criticality data into a cloud service without undergoing a thorough, in-depth assessment of requirements and provider risks.

*"We did a lot of work around information security, ensuring the service provider had controls in place that were as tight as our own."*

IT Security Manager, Enterprise

Many CSPs claimed to be very open in sharing their security controls with prospective customers. But the reality is that it's very time-consuming for enterprises to audition multiple providers, request and review these controls and document them for comparison. Several CSPs admitted they would require a signed NDA with the customer before sharing such controls.

## Industry standards and codes of practice

This brings us neatly to industry standards – or lack thereof. Both enterprises and CSPs in the study lamented the lack of industry standardisation and defined certification. The cloud industry is still evolving frameworks to answer customers' questions of what security protocols are in place and how well they're performing – activity which is being championed by the Cloud Industry Forum (CIF).

*"There's a great comic strip that says 'There are fourteen different standards out there. We need to create a fifteenth to unify them'."*

Chief Technology Officer, CSP

Many CSPs cited the SAS 70 (latterly ISAE 3402) attestation standard as evidence of their security protocols. However, the significance of this has been extended beyond its original remit: the certification was originally designed to audit corporate compliance with financial reporting rules and, as such, doesn't adequately address threat assessments. Moreover, it's a snapshot in time, not an ongoing performance measure. For these reasons, enterprises can't place too much emphasis on SAS 70 / ISAE 3402 certification, or even ISO 27001[3] information security management certification, but should rely instead on self-assessments and agreed auditing procedures[4]

[3] See http://www.iso.org/iso/catalogue_detail?csnumber=42103 for more information on ISO standards

[4] The Statement on Auditing Standards (SAS) 70 is being replaced by SSAE 16. See www.aicpa.org for more details.

*"Industry codes of practice and standards are not adequate by any stretch of the imagination."*

IT Security Manager, Public Sector

*"There's good work being done by the Cloud Security Alliance in terms of recommendations and guidelines for governance and compliance."*

Chief Researcher (Security), CSP

The Cloud Security Alliance (CSA) has developed a standard known as the Cloud Control Matrix, which describes over a dozen areas of cloud infrastructure including risk management, security and compliance measures around government and legal regulations and hardware architecture. However, although the standard defines hundreds of criteria, it doesn't dictate implementation. Further standards bodies with names that read like leftover tiles in Scrabble – NIST, IEEE and ENISA – have all individually published guidelines or checklists around security or interoperability, creating a patchwork landscape of recommendations.

In 2011, the CSA created a public cloud provider registry called 'STAR' (Security, Trust and Assurance Registry). This allows CSPs to submit self-assessment reports that document compliance with CSA published best practices. It is intended to represent a major leap forward in industry transparency, encouraging CSPs to make security capabilities a market differentiator. Open to all CSPs, the CSA has seen tremendous growth in terms of major cloud players. Nevertheless, some of the market leaders are dragging their feet, claiming it will open them up to competitor scrutiny or malicious attention. The CSA contests this, stating that all information collected is:

> *"intended to allow a provider to document its security practices without going into a level of detail that would expose sensitive information. For example, a provider will likely document whether or not they regularly perform application layer penetration testing but would not likely publish detailed results of web scanning tools."*

Ultimately, STAR will only become meaningful if critical mass is achieved. This will require enterprise buyers to demand participation by CSPs as a gold standard of integrity.

## Migration strategy

The migration of enterprise systems is a dilemma many companies wrestle with. Mass-market cloud infrastructure providers typically provide little or nothing in the way of assisted migration. The study revealed their customers tended to use the cloud as a dev and test sandbox. Consequently, these vendors were more likely to describe the cloud as being in the experimental or early adopter phase of maturity than those offering enterprise-grade IaaS propositions, who professed to adopt a more consultative approach. Many revealed they included change management or migration support as part of their presales process, together with bolt-on, chargeable professional services.

They were typically able to advise which legacy applications would be unsuitable for the cloud, such transaction-intensive, ultra-low latency or network-intensive applications or ageing, proprietary "green screen" applications. However, few had the automated server migration tools in place to forklift the entire stack to the cloud seamlessly; fewer still had a defined process for enforcing data encryption in motion and at rest, or securing key management during migration and with hybrid deployments.

## Customer visibility

Enterprises are long accustomed to investing in the people, processes and controls they need to satisfy themselves that they can adequately insulate their business against technology risks. The cloud delivery model requires they cede much of the control over risk mitigation and management to a third party.

CSPs generally use self-assessments based on arbitrary frameworks, certifications and SLAs that spell out their own obligations but don't necessarily include customer-centric monitoring. However, more sophisticated cloud services tend to come with a portal – a single console that allows customers to manage their accounts, gain visibility into resources and monitor deployment alterations. Notwithstanding, very few include sufficiently "beefy" feature sets that would give customers unwavering confidence in their cloud provider's security posture.

# Part 3: Improving your 'security posture'

Marketing-savvy cloud providers should be eager to improve their 'security posture' (their overall plan and approach to security) and use it as a vehicle to drive enterprise adoption of cloud-delivered products and services. It is STL Partners' recommendation that CSPs reframe their perception of security not only as a competitive differentiator, but also as a means to ensure their survival into 2018 and beyond.

## *The ethos, tools and know-how needed to win customers' trust*

*"You should be putting in encryption to a relevant level, dedicated firewall, identity and access management, monitoring your joiners, losers and movers, hardening of devices… Whatever you're doing in any environment on whoever's site, you should do that."*

Head of IT Solutions, CSP

Information security is a highly specialised and potentially resource-intensive and costly undertaking – one that requires the tools, skills and knowhow to identify and combat continuously evolving threats. For enterprise data centres and CSPs alike, the increasing frequency and sophistication of cyber-attacks means not just keeping the enemy out but also safeguarding business-critical applications and data within.

Enterprise security has traditionally been applied at the network perimeter. But in today's world, borderless networks can connect multiple types of users with enterprise private data centres and other cloud-based resources. Some types of transactions – for example a remote worker accessing Salesforce.com – may not even pass through the corporate network or scanning systems at all.

Integrating security as standard into their core offering can help CSPs to inspire confidence among enterprise customers. This can be achieved by building security solutions into automated provisioning tools, including the self-service customer portals used to select services and deploy virtual machines. Additionally, this harmonisation can help to avoid potential conflicts between multiple security solutions running in a shared environment. Reciprocally, enterprises can benefit by reducing, or even eliminating altogether, the on-premise security systems they currently have to maintain.

## *The Four Levels of Cloud Security*

Taking a "hard shell, soft centre" approach to security is no longer enough. A vigorous security posture requires a combination of adaptive security solutions to provide robust and risk-appropriate, cloud-scale defences *at every layer* – from the perimeter, through the network to the data centre, and ultimately around the data itself – while controlling the cost of compliance.

- **At the perimeter,** CSPs should deploy an appropriate combination of firewall, anti-malware, email, mobile and mobile file security solutions.

- **At the network layer**, data packets should be scrutinised to identify unauthorised data, without redirecting or altering it. When new threats are detected, a new rule set should be generated and looped back to the perimeter to reinforce the first line of defence.

- **At the data centre level,** on physical, virtual or hybrid servers, tools should span anti-malware, intrusion detection and prevention, firewall, web reputation, integrity monitoring and log inspection, to safeguard virtual machines. Virtual patching can enable CSPs to reduce the operational overheads of responding to zero day threats (attacks that exploit previously unknown vulnerabilities).

- **Around the data itself**, encryption needs to be supported on a volume (partitioned) basis for greater reliability and to enable the economies of scale that make the business case stack up for CSPs and enterprises alike. A combination of location-awareness and the ability to locate encryption keys with the enterprise or with a third party assures enterprises of data privacy, no matter where the data resides and even in the event of seizure.

### Figure 4 – The four levels of Cloud security


Source: Trend Micro and STL Partners

Security solutions should be rapid to implement and provided on a manageable OPEX basis to offer a cost-effective, scalable and proven means for CSPs to reduce the likelihood and impact of a security breach.

CSPs additionally need to consider how they can support a considered and painless cloud migration strategy. For example, comprehensive auditing capabilities can assist

the seamless transfer of customer workloads from the customer's current environment to the cloud.

By being able to proactively and tangibly demonstrate these capabilities to prospects, CSPs can radically differentiate their offerings in a highly contested marketplace and promote a sustainable enterprise cloud model that withstands anything the enemy can throw at it.

A 360 degree approach should harness a combination of measures, outlined as follows:

**Figure 5 – A 360 Degree Framework for Cloud Security**

| What? | How? | Why? |
|---|---|---|
| **Adaptive threat protection** | | |
| Advanced Persistent Threats (APTs) and targeted attacks have clearly proven their ability to evade conventional security defences, to remain undetected for extended periods, and to ex-filtrate corporate data and intellectual property. In recognition, it's recommended that enterprises redefine security due diligence to embrace specialised threat detection technology and a proactive process of real-time threat management. | ▶ Evasive threats are identified and detected in in real-time by monitoring the environment for malicious content, communication or behaviour.<br>▶ Analysis and actionable intelligence enables identification, remediation and defence against targeted attacks. | ▶ Enterprises gain visibility across the computing environment, shortening the time to attack discovery and allowing a sufficiently early response to prevent damage.<br>▶ Minimises the likelihood of successful APT intrusion and reduces the risk and impact of APT attacks.<br>▶ Counters attacks with a custom defence. |
| **Comprehensive server security** | | |
| VM-aware security increases cloud computing efficiency without sacrificing performance, and increases VM density, simplifying and streamlining patching, and making public cloud management easier. | ▶ Agentless and agent-based protection, including anti-malware, intrusion detection to maximise Virtual Desktop Infrastructure security and performance.<br>▶ Allows the enterprise to run the same security software in the public cloud environment and data centre, administered from a central console.<br>▶ Permits an unprecedented level of visibility across the evolving computing environment. | ▶ Data in the private, public or hybrid cloud can be encrypted and controlled and server access validated.<br>▶ Better protection, less administrative complexity and improved performance. |

| What? | How? | Why? |
|---|---|---|
| **Server security for cloud or hybrid environments** | | |
| Prevents damage from infection, identity theft, data loss, network downtime, lost productivity and compliance violations from device to cloud. | ▶ Cloud-based threat intelligence.<br>▶ Integrated data loss /theft prevention and security.<br>▶ Virtual patching to provide immediate protection. | ▶ Breaks the infection chain by blocking access to malicious files or websites.<br>▶ Improved virtualisation cost performance without compromising security.<br>▶ Reduced business risk and cost of breach disclosure, reduced operational cost and IT management workload.<br>▶ Eliminates the need for emergency patching, frequent patch cycles and downtime.<br>▶ Faster scanning leads to a transparent user experience and by freeing up memory, has less of an impact on productivity.<br>▶ Extends the life of legacy systems and applications. |
| **Data encryption and key management** | | |
| Cloud customers may not always know where their data is or who can access it, so encryption is vital. Data protection should be provided for public and private clouds and virtual environments, *and* meet regulatory compliance requirements. | ▶ The customer is charged with encryption and remote cipher key management, so they can specify when and where information is accessed according to a policy.<br>▶ Offers unique server authentication to ensure only authorised virtual machines receive keys. | ▶ The CSP gives the customer control of the encryption keys, so they have the freedom to encrypt data the cloud or even move data between cloud vendors. |

| What? | How? | Why? |
|---|---|---|
| | | ▶ Enables data protection in private and public clouds and promotes safe storage recycling by rendering any data remnants indecipherable.<br>▶ Facilitates internal governance and regulatory compliance. |
| **Mail server security from spam to APTs** | | |
| As more than 90% of Advanced Persistent Threats (APTs) start with a spear phishing email (targeted at a specific company), CSPs need to block targeted attacks, spam, phishing and malware. | ▶ Use big data analytics and predictive technology to correlate file, web and email reputation data in real-time.<br>▶ Check for malicious links within the body and known/unknown exploits in attachments like PDFs and MS Office docs.<br>▶ Integrate with Data Loss Prevention to identify sensitive data throughout the mail store and control ingoing/outgoing email. | ▶ Reduces the risk of spam, phishing and targeted attacks and allows sensitive messages to be quickly found, traced and destroyed<br>▶ Enables compliance personnel to centrally manage DLP policies and violations.<br>▶ Reduces administration time and effort with support for Exchange in virtual environments. |
| **Endpoint Security** | | |
| With a growing number of endpoints connecting to the corporate network – including devices belonging to contractors, temporary workers and visitors – enterprises need to be free to embrace a Bring Your Own Device (BYOD) strategy without increasing their risk exposure. | ▶ Mobile Device Management<br>▶ Mobile Device Security<br>▶ Mobile Application Management | ▶ Allows administrators to see the number, types, and configuration of devices accessing corporate resources and enforce polices across those devices.<br>▶ Reduced operational costs thanks to centralised visibility and control of device management, app |

| What? | How? | Why? |
| --- | --- | --- |
| | ▶ Cloud-based access to files from anywhere, anytime, on any device, with secure synchronisation and collaboration | management, security and data protection from a single platform.<br>▶ Improves employee productivity and flexibility in terms of the range of devices they can use to access work applications and data.<br>▶ Pushes productive apps and blacklists unproductive ones.<br>▶ Enforces policies for data access and protection with passwords, data encryption and remote lock-and-wipe.<br>▶ Ensures proper device configurations and adds protection to reduce the risk of compromised devices. |

Source: STL Partners

# Key take-aways for Cloud Services Providers

Cloud security requires a trinity of management, technology and operation. Enterprises just starting out on their journey to the cloud increasingly expect CSPs to be able to satisfy four fundamental lines of enquiry:

1. Where is my data?
2. How will my cloud integrate with in-house IT?
3. What security issues will my cloud service pose?
4. What is my exit strategy?

By employing multiple layers of defence and robust architecture, CSPs can win the confidence of enterprises with:

- **Control enforcement** – embedded directly into the infrastructure
- **Control management** – with centralised provisioning and monitoring of security controls, while allowing enterprises to autonomously enforce policy for sensitive data and manage authentication requests and encryption keys
- **Security management** – with a combination of managed events and alerts, remediation as necessary, and any prevailing regulations and standards mapped to policies with continuous verification of compliance

The commercial models that characterise cloud services shouldn't have any bearing on the level of security. Equally, no single security method will provide a panacea for all security risks and threats, so it's likely that enterprises will compartmentalise their cloud infrastructure and applications, and opt instead to apply specific controls based on the criticality and business value of the applications and data in question.

CSPs should, however, be encouraged by the knowledge that enterprises which have already overcome the hurdles of security and trust are able to focus on interoperability – joining up the services of multiple service providers to create the best of all worlds.

# About STL Partners

STL Partners has been at the forefront of the field of business model innovation and analysis in telecoms, media and technology (TMT) since 2006. In particular, the Telco 2.0 Initiative has focused on the opportunities for growth through new telecoms business models, and through its New Digital Economics Executive Brainstorms it has been working on cross-TMT business model opportunities in Telco 2.0, Digital Entertainment, M2M and the Internet of Things, Cloud 2.0 and Digital Commerce 2.0.

To get in touch, please call +44 (0) 247 5003 or email contact@stlpartners.com.

# About Trend Micro

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative security solutions for consumers, businesses and governments protect information on mobile devices, endpoints, gateways, servers and the cloud. For more information, visit www.trendmicro.co.uk