WHITE PAPER:
THE SECURE CLOUD:
BEST PRACTICES FOR CLOUD ADOPTION

The Secure Cloud: Best Practices for Cloud Adoption

Where we are, where we're going, and how best practices can help enterprise IT buyers and service providers today

Confidence in a connected world. Symantec™

Executive summary

Cloud computing promises incredible benefits in terms of speed, flexibility, and cost. But many enterprises are dragging their feet, worried about security. Indeed, sharing data over vast networks outside the business's perimeter does raise big questions: Who has access to your data? How can you control it? How can you establish trust between users and the services with which they interact?

Bodies such as the Cloud Security Alliance (CSA), and providers such as Symantec, are working hard to put in place standards, specifications, and protocols for cloud computing, which will improve governance, simplify interoperability, and enforce security controls. Much important progress has been made, but there's a lot still to do. And the benefits of the cloud are such that you can't afford to sit and wait for standards to be completed, ratified, and enforced.

This paper outlines three best practices that you can follow today.

First, conduct a full risk assessment before you contract with any cloud provider. Look not just at the provider's security and compliance activities, but how stringently they apply their policies to their subcontractors, how easily you can migrate your data to another platform at the end of a contract, and how likely the provider is to drop offline or go bankrupt. Cloud standards bodies have already published frameworks and benchmarks you can use to conduct your assessment.

Second, look at how your own security works in a cloud environment. How comprehensive is your existing security capability? And can you adequately protect your data and your user identities beyond the perimeter? Techniques like authentication and encryption are vital.

Third, implement a strong ongoing governance framework. Gather information from providers and from your own systems, and monitor for security events and compliance with accepted best-practice and specific regulation/standards where appropriate. Check that your providers are fulfilling their SLAs and contracted obligations. And plan for how you'll respond to and remediate problems.

This three-part framework will serve you well, whatever the future holds. But there is a fourth stage we recommend, too: Get involved in how cloud security develops. It's a demanding and exciting time, and your input can help shape the future.

CONTENTS

About Symantec

Symantec has grown to become one of the world's leading Information security and information management companies.

We employ more than 18,500 people, including some of the brightest minds in security, operating in 48 countries around the world. Thanks to our significant investment in R&D, our participation in the leading research groups, and the unparalleled data we collect from our Global Intelligence Network, we have an unparalleled insight into the security and threat landscape that informs our unique perspective to help our customers get ahead and stay ahead.

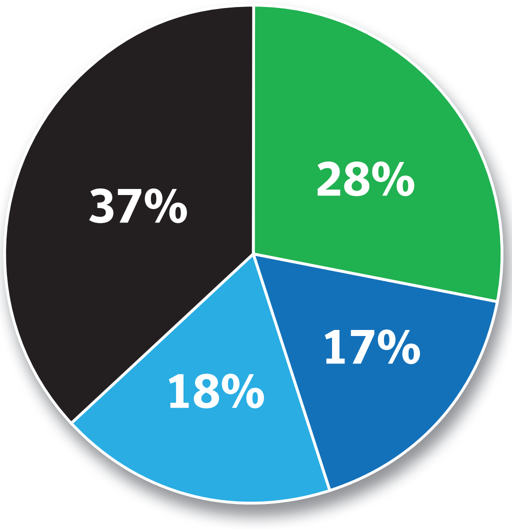
Symantec delivers unparalleled choice and flexibility in the adoption of market-leading solutions to secure and manage information in the cloud.

Today, Symantec.cloud has over 11 million security customers worldwide and Norton Data Services is the number one consumer backup provider in the world—serving more than 13 million subscribers and storing more than 70 petabytes of data. Symantec has the expertise to enable cloud infrastructures and provide hybrid solutions to enterprises as they transition to the cloud.

Cloud computing changes the game: A trillion-dollar opportunity

Cloud computing is a transformational new way of delivering and paying for IT services. It is revolutionizing delivery models, enabling companies to make step changes in IT agility, to re-engineer their business processes, and revolutionize forever the way that they use applications and interact with consumers and other companies.

In Europe, the Centre for Economics and Business Research has estimated that cloud computing could generate €763 billion ($1.05 trillion) and 2.4 million new jobs by 2015.[1]



- **New enterprise creation**
  Drastically reduced financial and logistical barriers to entry increase incentive to create new businesses, especially SMEs
- **Business development**
  Increased growth and profitability in new and existing revenue streams
- **Cost savings**
  Reduced administration and operational costs
- **Indirect gross value added**
  Faster deployment of new applications, increased competitiveness, reduced burden on IT systems and workers

In the United States, the government has put a major drive behind a “cloud first” strategy. In February 2011, the Obama administration announced that “the adoption of cloud computing will play a pivotal role in helping the government close the productivity gap between the public and private sectors.”[2] Governments around the world are making similar commitments.

And IDC estimates that over 20 percent of the typical enterprise IT budget will go on cloud computing by 2013,[3] with Saugatuck asserting that 65 percent of new workloads will be cloud-based by 2014.[4]

A focus on what’s valuable: information

What cloud is riding on is a whole new conception of computing that aligns IT much more closely with business value. Cloud makes it clear that value doesn’t come from the stacks of hardware and networks that make up the data center— it’s in the information that the hardware holds. Information is valuable and it needs to be secure and accessible.

> Value doesn’t come from the stacks of hardware and networks that make up the data center—it’s in the information that the hardware holds.

Despite all the momentum around cloud in the last few years, we're only seeing the tip of the iceberg in terms of use cases and potential benefits.

Many enterprises are today evaluating and considering what is known as *private cloud*. In reality, although the technology and payment terms have changed, private cloud services operate much like the traditional outsourcing model: Enterprises move services to a defined set of infrastructure at a single provider (possibility the internal IT department) with whom they have a consumption-based contract, and they let the provider manage the infrastructure efficiently. The relationship is still one-to-one and the technical architecture allows established infrastructure-based approaches to security to remain valid.

We've only just begun to realize the potential

As organizations become more comfortable with true, public cloud—where a provider's infrastructure is a resource shared by many clients—service provisioning can become truly information-centric, freed from today's infrastructure-centric legacy. Relationships between customers and providers become more dynamic and more automated: Enterprises contract with providers that offer them the best value for their computing, storage, or service needs, right then. Service providers in turn may subcontract instantly to infrastructure cloud providers for the lowest costs and best reliability. We swap being locked into inflexible relationships for a loose, ad hoc ecosystem of partners working together for brief periods.

It's a powerful vision. Public cloud computing will drive the efficiency gains that businesses are demanding. Eventually it may become the default mode of delivering what we call "computing." So what's holding organizations like yours back from making it real?

Security concerns threaten to constrain adoption of cloud computing

Security dominates concerns about cloud

You only have to look at the effects on customers when cloud providers experience downtime, contravene compliance requirements, or get hacked to understand why organizations are worried about cloud computing. In a 2010 survey, IDC found security to be the top concern in cloud computing among enterprise IT buyers.[5] And this concern essentially boils down to one underlying question: How can I let my data flow over networks, through organizations, and to devices outside of my infrastructure, between an exponentially increasing number of providers, without losing control and security?

How can I let my data flow over networks, through organizations, and to devices outside of my infrastructure, between an exponentially increasing number of providers, without losing control and security?

Security isn't the issue, trust is

Cloud computing doesn't need to be a threat to IT security; it can actually be part of the solution. The abstraction layer that cloud computing creates can actually improve visibility, a fundamental requirement for effective security. The challenge arises from lack of ownership and the corresponding concerns over lack of control.

- Infrastructure: How can you ensure that your infrastructure providers have appropriate security and disaster recovery policies and stick to them?
- Identity: How can you enforce rigorous authentication across multiple interconnected systems without adversely affecting flexibility and productivity?
- Information: How can you classify and protect sensitive information, and ensure compliance with policies and regulations?

Unless this issue of assuring control beyond the organization's perimeter gets resolved, cloud computing will struggle to deliver the benefits it promises: elasticity and cost savings that come from shared, virtualized infrastructures; applications that are architected in a multi-tenant manner; interactions that come from anywhere to access services over the Internet; and, in cloud 2.0, having a fluid, complex set of providers handling data. Only by reconciling agility and security will enterprises feel confident moving past the early steps of private cloud and low-risk, small-scale deployments.

There are already initiatives underway to help manage the security challenges that cloud has thrown up by defining secure infrastructure models, tackling the issue of trust between participants in cloud ecosystems, and bridging the gap between existing internal security standards and those governing off-premise services. These fall into two areas: certification and international standards.

Certification

Cloud requires a change of mindset. To realize the benefits of a virtualized environment, it's necessary to accept that perimeters become logical rather than physical, dynamic rather than fixed. Whereas in the past rights could be tied to a physical machine and its location, the policies and privileges assigned to a virtual machine must change when its workload does. Likewise, a user's access to information and applications shouldn't just depend on who they are, but also where they are, what device they are using, and how they are using the information. For example, their access to confidential information might be blocked if their location is not trusted, or if they are using an unsecured device.

As well as forcing a rethink of policies, cloud computing requires new tools and operating practices. Certification is a proven technique for establishing identity and trust and its role will become increasingly important as services move to the cloud. Certificates such as those provided by VeriSign® Authentication Services, now part of Symantec, help give companies and consumers the confidence to engage in communications and commerce online.

International standards

Standards are important because they allow interoperability, portability, and a simpler way to measure risk. But the task of any cloud computing security standard is ambitious. It needs to:

Manage how access rights and data governance policies get enforced across multiple systems from multiple providers, without inconveniencing users or automated transactions. The usual model for this is what's known as a "trust broker" or "federated identity," and it needs to be end-to-end and seamless from the user's perspective.

Facilitate and foster interoperability between different services to help promote the value of cloud computing to users and the communication of privilege and access rights between services. Interoperability is what enabled mobile communications to take off, and it can do the same for cloud.

Offer protection that's appropriate for context: including the nature of the request the user or machine is making, the importance of the data, the risks posed by the network and device doing the accessing, the user's privileges, and the risk profile of the provider. One size does not fit all.

Encompass nontechnical issues, like assessing vendor risk and viability, legal jurisdiction and compliance, which may vary from case to case.

Symantec is an active member and participant in the most important standards bodies to drive creation of these standards, and provides input into international regulation. Although there is plenty of work still to do, already several important results have been accomplished.

The CSA publishes a CloudAudit tool for assessing infrastructures; a governance, risk management, and compliance (GRC) stack for use in forming cloud service relationships; and publishes best practices, cloud metrics, and information on security controls.[6] Symantec solutions are built to a three-layer model in line with CSA best-practices, and we've published a detailed Technology Reference Model (see diagram) based on the CSA framework.

The U.S. National Institute of Science and Technology has published 24 use cases and a draft definition of cloud and security best practices, with a goal of creating minimal standards to promote truly interoperable clouds that use federated security and share core functionality to allow service and data portability.[7]

The Open Grid Forum has published several recommendations governing using authentication mechanisms, such as SAML, and secure communications in distributed computing environments.[8]

The Open Cloud Computing Interface (OCCI) is an actual production-ready set of specifications and API for remote-managing and monitoring IaaS, PaaS, and SaaS environments.[9]

The Storage Networking Industry Association runs a Cloud Storage Initiative covering relevant areas such as backup and restore and a cloud data management interface (CDMI) specification, which increases service portability by standardizing the service requirements of different data types through metadata.[10]

The Organization for the Advancement of Structured Information Standards has started an "identity in the cloud" technical committee to investigate gaps and new standards in identity management.[11]

The U.S. government has produced the Federal Risk and Authorization Management Program, which defines government requirements for cloud computing security controls, including vulnerability scanning, and incident monitoring, logging, and reporting.[12]

The Initiative for Open Authentication is developing identity management standards that could help promote the universal adoption of the strong authentication necessary to secure cloud-based services.

Through working with the standards bodies, Symantec has created a practical framework that can be used to help assure security of information on its journey to the cloud, as well as in the cloud. This framework, shown in the diagram below, addresses the critical security domains as identified by the CSA, across key layers in the cloud (Infrastructure as a Service, Platform as a Service and Software as a Service). It is capable of being adopted both by enterprises, and by cloud and communication service providers, to protect the flow of digital assets to, from, or in the cloud.

	Cloud Security Alliance Domains	Service	Platform	Infrastructure
Governing the Cloud	Governance and Enterprise Risk Management	Control Compliance Suite Data Loss Protection Altiris Patch Management Altiris ServiceDesk	Control Compliance Suite Data Loss Protection Altiris Patch Management Altiris ServiceDesk	Control Compliance Suite Data Loss Protection DeepSight Security Information Manager
	Legal and Electronic Discovery	Control Compliance Suite Data Loss Protection Enterprise Vault	Control Compliance Suite Data Loss Protection Enterprise Vault NetBackup Security Information Manager	Control Compliance Suite Data Loss Protection Enterprise Vault NetBackup Security Information Manager
	Compliance Audit	Data Loss Protection Control Compliance Suite Altiris	Control Compliance Suite Data Loss Protection Altiris NetBackup	Control Compliance Suite NetBackup Critical System Protection Security Information Manager
	Information Lifecycle Management	Control Compliance Suite Data Loss Protection Enterprise Vault NetBackup	Control Compliance Suite Data Loss Protection Enterprise Vault NetBackup	Control Compliance Suite Data Loss Protection Enterprise Vault NetBackup
	Portability and Interoperability			OpenStorage Standard
Operating the Cloud	Traditional Security, Business Continuity, and Disaster Recovery	Brightmail Enterprise Security/Network Access Control AntiVirus for Network Attached Storage NetBackup FileStore	Scan Engine Critical System Protection Brightmail Veritas Cluster Server One	Brightmail Enterprise Security/Network Access Control Critical System Protection AntiVirus for Network Attached Storage CommandCentral Storage FileStore/SF Veritas Cluster Server NetBackup Web Gateway Security Information Manager
	Data Center Operations	Control Compliance Suite Altiris Patch Management Altiris Service Desk	Control Compliance Suite Altiris Application Virtualization and Streaming	Control Compliance Suite CommandCentral Storage Altiris Storage Foundation Veritas Cluster Server
	Incident Response Notification Remediation	Control Compliance Suite Altiris	Control Compliance Suite Critical System Protection Altiris Patch Management Altiris ServiceDesk	Control Compliance Suite Enterprise Security Critical System Protection Security Information Manager Altiris Patch Management
	Application Security	Critical System Protection	Critical System Protection	
	Encryption and Key Management	Symantec Endpoint Encryption PGP Desktop Email PGP Whole Disk Encryption	PGP Key Management Server	Symantec Brightmail Gateway PGP Universal Gateway Email
	Identity and Access Management	VeriSign PGP Veritas Cluster Server TrustCenter	VeriSign TrustCenter	VeriSign
	Virtualization	Altiris Application Streaming Enterprise Security Critical System Protection	Altiris Application Virtualization Enterprise Security Critical System Protection NetBackup Veritas Cluster Server One	Enterprise Security Critical System Protection NetBackup Veritas Cluster Server One

What should you do today?

Immediate solution: effective best practices

You can't hold off embracing cloud until standards mature completely—your existing and emerging competitors aren't holding back and will soon be benefiting from the flexibility and efficiency that cloud can offer.

In the meantime, there are best practices you can follow that will help give you the control you need and deliver a level of security in the cloud similar to that which you get from traditional IT infrastructure. Importantly, these solutions are as much process and contract based as technical, because cloud is as much a shift in business and delivery models as it is a technical revolution.

A high-level roadmap to implement security best practice consists of the following phases:

- Conduct a full risk assessment
- Secure your own information and identities
- Implement a strong governance framework

Step one: Conduct a full risk assessment

Before contracting with a cloud provider, it's your responsibility to assess whether they meet your needs and your policies through a risk assessment. The risk assessment is your opportunity to bring transparency to the cloud, as a foundation for building trust. It's not just about evaluating how well the provider defends itself against external threats and examining the provider's proposed cloud SLA, it's also about assessing the risk that the provider itself poses to you. Choose your providers consistently by considering five areas:

1. Interoperability and portability: What data formats do providers use, what APIs? How can you get your data out? Does it support CDMI? Can you move virtual machines between providers? How can you move security configurations between providers? How can you make sure vendors delete your data once you move? These questions are important to ask before you adopt even cloud 1.0, but they're critical for enabling the agility of cloud 2.0 where portability is a cornerstone.

2. Compliance: Including whether providers can limit where data is stored for jurisdiction-specific compliance, and how they assure data privacy.

3. Vendor risk: In cloud, you're totally dependent on your provider to keep services working. What measures do providers use to assure services are available and high performing, and quickly elastic? What disaster-recovery measures do they use? How strong is their financial performance?

4. Supply chain and ecosystem: What policies do providers follow when subcontracting part of service delivery or using suppliers for infrastructure? How do they assess their risk, and what measures do they take to protect your data? This area will become vastly more important in cloud 2.0.

5. Infrastructure and operations quality: You're not running the infrastructure yourself—cloud should mean not having to worry about capacities and speeds, and most providers do this well. But you should satisfy yourself that your provider is making full use of security best practices, particularly as they relate to the unique structures of cloud infrastructure. For example, by logically separating data as part of multi-tenanted environments, securing application configurations that would otherwise be your responsibility, wiping storage before reallocating it to other shared service users, and securing virtualized environments. Don't forget business continuity measures and physical security, including staff security clearances. Physical security is often a compliance requirement too (for example in the Payment Card Industry Data Security Standard).

For now, properly conducting a risk assessment is a manual task that first requires you to understand your organization's appetite for risk and your protection needs, which may vary by application. If you can standardize your requirements into a minimum benchmark for different use cases, you can use it with all cloud providers to compare their responses. The risk-assessment phase should rapidly get more automated, which will be vital for cloud 2.0. The European Network and Information Security Agency has already published a Cloud Information Assurance Framework that provides 24 pages of questions about other operational areas for customers to ask their providers. The CSA's CloudAudit, Cloud Controls Matrix, GRC stack, and Consensus Assessments Initiative Questionnaire provide another foundation for providers and customers to align service capabilities against security requirements.

Ultimately, if your cloud provider won't tell you the information above, you can't be confident in deciding whether they can and will follow satisfactory processes. Don't trust a certification logo—verify their performance yourself.

Step two: Secure your own information and identities

If you're opting for PaaS or IaaS instead of SaaS, you'll be taking on more responsibility for things like secure application design. But you always have a responsibility to secure your own data and systems. Even though devices, networks, core infrastructure, and providers may be out of your control, your data and your users' interactions aren't.

Authentication is the first place to start. Limit user privileges, including the privileges of your administrators. Rogue admins are a big source of security breaches in the cloud, just as they are in traditional computing. Strong passwords are still important, even if you have limited user access rights and segregated systems. Two-factor authentication is better, and cloud-based strong authentication gives access to this extra layer of identity verification without the cost and management overhead of traditional implementations. Risk-based authentication balances security against ease of access, which is one goal of using the cloud. You can leverage single sign-on and federated identity systems to pass authentication details between trusted providers—SAML and OpenID are two options.

Encryption of your data in storage and in motion is a critical measure for guarding against threats from all sides, including from your providers' staff.

Endpoint security is still important, even if you don't control all the devices accessing a public cloud service. Firewalls, antivirus, VPN connections, and a strict patching policy are standard measures that you should continue to use as part of a "security in depth" strategy.

Step three: Implement a strong governance framework

Pie Chart 2: Are cloud computing services evaluated for security prior to deployment or engagement?

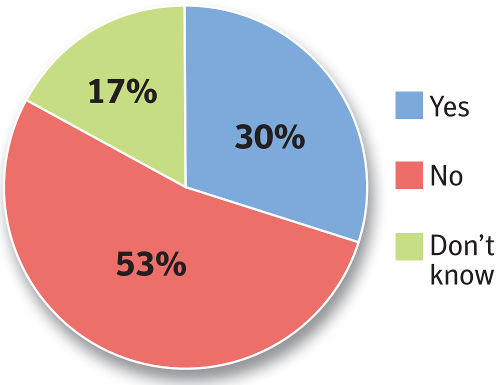


Table 2: If no, why does your organization permit cloud computing resources without vetting or evaluation for security?[13]

Not able to control users	76%
Not enough resources to conduct evaluation	50%
No one is in charge	44%
Not considered a priority	43%
Don't know	18%

There's no sense in asking lots of questions in your risk assessment phase, and implementing strong local security measures, if you fail to monitor how well your providers' security is working. Proper governance depends on accurate and complete data. To get this:

- Ensure your provider uses security information and event management to track and notify you of security events. The OCCI standard can give you remote monitoring if your provider supports it.
- Monitor your own log files for devices you control.
- Stipulate in your contracts that SLAs are paired with defined metrics and standards for what data your providers will give you.
- Centralize within your organization responsibility for selecting and working with cloud providers.
- Plan contingencies for what happens when a breach occurs or a provider fails. Test your plans when and where possible.
- Use the Security Content Automation Protocol to verify that your providers are using the secure configurations you defined in your risk assessment, possibly using the Open Checklist Interactive Language and the Open Checklist Reporting Language to automatically verify that policies are being followed.

Ready for whatever the future holds

With a robust risk-assessment process, set of security controls, and governance framework in place, you'll be both reducing risk as you take your first step into cloud, and at the forefront of capitalizing on emerging technologies and upcoming standards in cloud computing. This three-part approach to security is also forward compatible: It lets you evolve over time to maintain your protection without disruption, whatever the future holds.

Play your part in defining cloud security practices

At Symantec we have a long-term vision for solving the issue of securing the cloud—we call it O3. We believe the best way to secure the cloud is to get above it, to put in place not just technical solutions but a complete governance framework. And the important strategy is to follow the value—the data itself—which is exactly why enterprises started looking at cloud in the first place. The infrastructure is a distraction. First you need rules for how to control access to data by users, by machines, in locations and times, and by device types and networks: a policy engine. You need an authentication center or trust broker to verify and lock down that access whenever and wherever it's requested: a protection layer. And you need a pervasive monitoring layer so the people who govern data security can track data use in real time. This model is directly compatible with the best practices we've shared in this paper.

But cloud computing models, and their security implications, affect every enterprise. It shouldn't be left up to providers to work out security approaches, technologies, and best practices. Everyone, from governments to IT departments, security experts to users, network owners to service providers, should be involved to help specify what they need to make their jobs easier and to make their information more secure. Find out more about O3 by watching our webcast at http://go.symantec.com/rsa-2010-webcasts

To learn more and stay ahead, join us at www.symantec.com/cloud

Further reading

"Embracing clouds, avoiding storms" white paper:
http://go.symantec.com/embracing-clouds

Performing a thorough risk assessment

Symantec Foundation IT Risk Assessment:
http://go.symantec.com/sf-risk-assess

Securing data and users

Symantec's Approach to Pervasive Encryption:
http://go.symantec.com/pervasive-encryption

Implementing a strong governance framework

Presentations from Vision 2010 conference: Information Risk and Governance:
http://go.symantec.com/info-risk-gov

[1] http://uk.emc.com/about/news/press/uk/2011/02222011-01.htm

[2] http://www.cio.gov/pages.cfm/page/IT-Reform-Series-Federal-Cloud-Computing-Strategy-Published

[3] http://www.networkcomputing.com/cloud-computing/cloud-minuses-outweigh-pluses-for-businesses.php

[4] SIIA On Demand Europe London, UK, October 19, 2010

[5] http://www.networkcomputing.com/cloud-computing/cloud-minuses-outweigh-pluses-for-businesses.php

[6] http://www.cloudsecurityalliance.org/Research.html

[7] http://csrc.nist.gov/groups/SNS/cloud-computing/

[8] http://www.ogf.org/

[9] http://occi-wg.org/

[10] http://www.snia.org/cloud

[11] http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=id-cloud

[12] http://fedramp.gov

[13] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-ponemon_institute_flying_blind_in_the_cloud_WP.en-us.pdf

Confidence in a connected world. Symantec™