White Paper

McAfee

Cloud Computing: Risks and Rewards

Helping government agencies make informed decisions about cloud computing

Table of Contents

From the 1990s to present day, the evolution of in-the-cloud services and virtualization has enabled companies and governments to do more with fewer resources and greater efficiency. This paper examines the security implications of today's cloud computing options for your government business, and provides insight into services available from McAfee for those government agencies who ultimately decide to leverage the benefits of cloud computing.

Background

A key development in the evolution to cloud computing has been the virtualization of server infrastructure. Moving this virtualization to "the cloud," third-party service providers can virtualize resources for *multiple* tenants across an entire infrastructure. As it has for enterprises, virtualization enables service providers to maximize the efficiency of large servers and processing power, and it enables these providers to serve many more clients using a fraction of the computer hardware that a non-virtualized environment would require. In essence, virtualization gives service providers *economies of scale*—making it possible for them to offer hardware, networks, software applications, and support at a lower operational cost than their clients could achieve by building that infrastructure themselves. In fact, the ability of service providers to create a profitable business based on offering their clients inexpensive computing power "in the cloud" is a key factor driving the success and popularity of cloud computing.

Seeing the potential for government and business benefits, cloud computing service providers have increasingly offered the market complementary options:

- *Infrastructure-as-a-Service* enables government agencies to cost effectively "lease" the network—data center space, servers, disk space—and scale as needed without spending on the hardware up front.
- *Software-as-a-Service* allows government agencies to outsource applications or functionality that leverage a service provider's deployment and management expertise and hardware investment.
- *Platform-as-a-Service* provides government agencies with a "rented" development platform for building new applications.

"For the U.S. government, cloud computing could be an easy way to deal with urgent and important issues, such as upgrading the federal and state technology infrastructure without costly upgrades."

—Om Malik, "Can the U.S. Government Help Cloud Computing Reach a Tipping Point?" July 23, 2009[1]

Benefits of Cloud Computing

Governments and businesses alike have considered cloud computing as a panacea of sorts to address needed cost improvements in the current fiscal times, and longer-term cost reduction measures. But there are more than cost improvements. All of the cloud service models share several benefits:

- As with virtualization, fewer resources are required to run the hardware and software that the agency needs to support its operations.
- Organizations can choose what they need, when they need it, and only for as long as they need it. Access to cloud-based applications can easily be limited to only specific users for a specific duration, as opposed to costly licensing of the applications per seat regardless of time of use.
- Agencies can scale capacity up or down without having to lock into software licensing and hardware capital expenditures.
- Staff and other users need only a web browser to leverage in-cloud applications, which greatly simplifies deployment within the agency.
- Agencies can avoid or reduce the need for application-specific expertise and capital expenditures to run the applications on their network.

Cost Reductions: Not the Only Consideration

Clearly there can be solid financial reasons for government organizations to consider cloud computing. Due to the fiscally challenging economic climate and trend to tighter budgets, as well as a shortage of staff to administer and manage software, many IT departments (in both public and private sectors) have already delayed some technology purchases. But cost is not the only consideration.

McAfee®

1. http://gigaom.com/2009/07/23/vivek-kundra-us-cio-on-cloud-computing/

While IT budgets have been shrinking, security concerns are actually growing. Security threats, for example, are on the rise, according to indications from McAfee's own research (which detected 1.5 million malware attacks in 2008). So in these fiscally lean times in which government agencies are asked to do much more with far fewer resources, it is important not to overlook the security implications of IT spending decisions. While investigating low-cost operational models, government agencies would be well advised to also give serious consideration to data security.

Best Practices for Security and Privacy

As with any decision to outsource, the decision to leverage cloud computing is one that should be made with considerations for best practices in security and privacy. Cloud computing alters the risk landscape in areas such as confidentiality, privacy, integrity, regulatory compliance, availability, and e-discovery. This is particularly true for those leveraging the cloud to store sensitive data such as customer records, employee records, financial data, and other data that is regulated or that should otherwise be strongly protected. Organizations must also realize that the incentives for attackers are higher when a greater amount of data of value is stored in one location; it makes for a more lucrative target. Therefore, it is important to ensure that proper security assurances are in place.

"Personal information, be it biographical, biological, genealogical, historical, transactional, locational, relational, computational, vocational or reputational, is the stuff that makes up our modern identity. It must be managed responsibly. When it is not, accountability is undermined and confidence in our evolving information society is eroded."

—Ann Cavoukian, Ph.D. (Information and Privacy Commissioner of Ontario), "Privacy in the Cloud"[2]

- *Consider the type of data you're moving to the cloud*
  You must begin by weighing the risks and benefits for storing various forms of data in the cloud if you intend to use the cloud in this way. Perhaps you want to take advantage of the benefits of cloud computing but only for the least sensitive data, while retaining the most sensitive data on your own network and under your own control. Start with a full understanding of the types of data you retain today, where you retain that data, and how, so that you also understand how your risks will change as you change the location and control of your data.
- *Understand the "people, process, technology" model for your service provider*
  You will need to do greater due diligence in understanding the people, process, technology model of your provider so that you can evaluate how that compares to your own. Some questions to consider:
  - » What security and privacy best practices does your provider follow?
  - » Does your provider follow an international framework such as ISO 17799 for its security operations?
  - » What is the training your provider requires of those running the network and touching the data?
  - » What, if any, background checks are required of the provider's operators?
  - » Does the provider use behavioral analysis tools that trigger alarms when unplanned or non-compliant changes are made?
  - » How does the provider handle vulnerabilities and alerts?
  - » What is the provider's patch management strategy?
  - » How does the provider approach privacy of customer data? Do they espouse a framework of privacy principles? (Models for privacy practices include the Generally Accepted Privacy Principles from the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA), and the Government of Ontario's new PrivacybyDesign™ privacy principles.)
  - » How do you get your data to and from the provider?
  - » Can you access mission-critical or real-time data instantly, at any time?
  - » What is the best way to secure the clients being used to access the data or the data now resident on the client's machine?
- *Review security, breach, and uptime accountability*
  As with any outsourcing arrangement, there must be clear accountability to the security of your data—from the confidentiality, to the integrity, to the availability of that data. The legal contracts should clearly stipulate your desires with regard to accountability and the level of accountability with which you are most comfortable, particularly in regard to regulated data. If the country and state in which you operate or conduct business have clear data breach laws, for example, all aspects of the data breach and reporting responsibility should be clearly understood by all parties, and the actions to be taken by each party—and when—should be documented.

2. http://www.ipc.on.ca/images/Resources/privacyintheclouds.pdf

If you are using a service provider in another country, you must understand that country's obligations and ability to enforce those obligations relative to the country or state for whose data you are accountable.

As with traditional outsourcing arrangements, you should be very familiar with the contractual uptime requirements and understand how they will impact your business as it relates to the type of data being stored in the cloud. What are your provider's service-level agreements (SLAs) and how do you affectively manage them? Keeping your own customer in mind, how do you guarantee availability?

- *Choose a model (infrastructure, software, or platform)*
  Armed with the information from your due diligence, you're then in a better position to weigh the risks and rewards of each model (Infrastructure-as-a-Service, Platform-as-a-Service, or Software-as-a-Service) and understand how each model could benefit your government agency. Each will have different implications for your security and privacy needs, but security must be an absolute baseline consideration, whichever model you select.

McAfee Security Expertise for the Cloud

If the number of decision points and amount of due diligence seems daunting, the good news is that you are not alone in determining the best practices that suit your environment, the regulatory practices you must consider for a cloud computing service model, and other concerns. McAfee Foundstone® Professional Services offers expert services and education to help organizations continuously and measurably protect their most important assets from the most critical threats. Through a strategic approach to security—including the challenges of virtualization—our team of Foundstone security experts identify and implement the right balance of people, process, and technology to manage digital risk and leverage security investments more effectively. Our team consists of recognized security experts and authors who have broad security experience with multinational corporations, the public sector, and the U.S. military.

Understanding what your provider uses to provide you with baseline security for your cloud services is part of the due diligence process that McAfee advocates to all customers considering in-the-cloud services. To make the process easier for government agencies, McAfee Foundstone Professional Services team provides two important services.

McAfee Foundstone Cloud Computing Readiness Check and Security Assessment

McAfee's Foundstone Cloud Computing Readiness Check provides expert assistance in designing, implementing, and assessing a cloud solution that meets the security requirements of your organization.

The Foundstone Cloud Computing Security Assessment is available to both customers of cloud computing services and providers of such services. This helps your agency in two ways: You get assistance in the vetting process; and if you're considering a provider that has taken the McAfee Security Assessment, you can request the provider's security assessment report.

For cloud computing customers, McAfee can assess your solution as implemented in the new cloud environment to verify that it is implemented at the appropriate level of security. McAfee consultants will create a custom methodology tailored to your unique needs. For service providers, McAfee can assess physical security and application security and provide a letter of attestation regarding the provider's level of security. McAfee's approach to the assessment includes:

- *Architecture and Design Assessment:* McAfee consultants assess things like network topology, data storage and operation, trust boundaries, and administrative controls.
- *Cloud Infrastructure Security Assessment:* McAfee consultants assess the logical network, applications, and services hosted in the cloud, including assessments of application or products, firewall, and remote access.
- *Governance, Policies, and Procedures Review:* The policies, procedures, and regulations followed by the cloud vendor may not be consistent with the requirements and expectations of your organization. For that reason, McAfee consultants compare the vendor's policies and procedures against industry best practices and regulatory compliance requirements specific to your organization. Based on the results,

policies, procedures, and SLAs can be developed to bridge the gaps identified. The areas covered include but are not limited to legal contract and SLA review, e-discovery and information management, compliance and audit, and incident response and forensics.

Foundstone's cloud computing services cover all the major cloud computing architectures: Infrastructure-as-a-Service, Platform-as-a-Service, and Software-as-a-Service. The Foundstone Professional Services team consists of recognized security experts and authors with broad security experience with multinational corporations, the public sector, and the US military. Solution briefs with details of the Foundstone Readiness Check and Foundstone Secuirity Assessment are available.

McAfee: Protecting VMware environments

If your service provider takes advantage of the VMware environment, you can be confident in the knowledge that McAfee protects VMware environments in several ways:

- McAfee VirusScan® Enterprise for Offline Virtual Images 2.0 uses VMware VMSafe technology to provide scanning of VMware's offline virtual images; Citrix support is available as well.
- McAfee Total Protection for Virtualization includes McAfee VirusScan Enterprise for Offline Virtual Images and other endpoint protection solutions.
- Traditional McAfee solutions such as McAfee Vulnerability Manager, McAfee Policy Auditor, and McAfee Network Security solutions protect VMware solutions.
- Partner solutions from Catbird (sold through the Security Innovation Alliance Sales Teaming program) monitor traffic among virtual machines on a single physical system.
- Virtual firewall appliances can be installed as virtual machines and use VMware technology.
- McAfee Foundstone Virtual Infrastructure Security Assessment services provide secure architecture and deployment services for VMware.

McAfee Software as a Service offerings

With McAfee's recent acquisition of MX Logic, McAfee offers the most comprehensive cloud-based security portfolio in the industry—one that combines leading McAfee Global Threat Intelligence technologies with Security-as-a-Service solutions. McAfee's Software-as-a-Service portfolio leverages our global threat expertise with the experience of securing global enterprises and medium-sized businesses. As noted, the combination of tight budgets, a shortage of IT staff, and increasing security threats are reasons why McAfee's Security-as-a-Service may be an appropriate consideration for your IT requirements. As with any of the software experts in the Software-as-a-Service model, McAfee develops our own software; therefore we have the knowledge and capacity to run it more efficiently for you. That allows government organizations to focus on securing their government assets, rather than managing security installations, patches, and upgrades or developing security expertise in-house.

The McAfee Security SaaS portfolio includes:

- *McAfee Total Protection Service:* Delivers one integrated endpoint, email, and web security solution that protects desktops, servers, and other devices against viruses, spyware, spam, hackers, vulnerabilities and web threats—all managed online with McAfee SecurityCenter.
- *McAfee Email Security Service:* Stops email-borne attacks and spam before they reach your network and enforces outbound email policies to prevent sensitive data leaks.
- *McAfee Web Protection Service:* Stops malware and other web-borne threats, using URL filtering and McAfee TrustedSource™ reputation-based security technology to enforce security policies in real time.
- *McAfee Vulnerability Assessment SaaS:* Provides accurate vulnerability scanning and actionable reporting to confirm the security of an organization's web applications and network perimeter.
- *McAfee PCI Certification Service:* Scans web applications and provides remediation assistance and reporting to help merchants successfully satisfy Payment Card Industry security compliance demands.
- *McAfee Partner Security Service Program:* Provides value-added partners with a toolkit in the form of an online Partner SecurityDashboard that allows MSPs, MSSPs, and other service providers to deliver managed services based on McAfee Security SaaS technology.

"We view McAfee as the leading dedicated security company and pioneer in Security-as-a-Service. We will now be even better equipped to help our customers address the complex challenges associated with blocking spam, phishing scams, viruses in the cloud, and enforcing email policies to prevent sensitive data leaks."

—John Street,
Chairman and CEO,
MX Logic

With the MX Logic portfolio, McAfee offers comprehensive web and email defense, disaster recovery options, and email archiving to the already broad set of delivery options. Today, MX Logic protects 40,000 customers with more than four million end users. Data centers in Asia Pacific, EMEA, Japan, and the United States protect a geographically dispersed customer base with the capacity to expand into global markets and support our customers' global network needs.

Fed by McAfee's Global Threat Intelligence, the only collective threat intelligence in the market, McAfee arms its Software-as-a-Service offering with the benefit of up-to-date threat analysis. McAfee monitors 50 million enterprise nodes and 100 million consumer nodes in its collection of intelligence. Our Global Threat Intelligence includes:

- *Malware research:* 50,000 samples/day
- *Email research:* Approximately 10 million spam emails per day
- *Web security research:* Rated over 21 million sites, covering 95% of the Internet

Summary

Ultimately, the best decision you can make with regard to cloud computing will be based on both your current operating model and the balance of risks vs. rewards that such a service model can provide your government agency. Organizations such as critical infrastructure providers, all levels of government, financial services, and those in other industries that are already lucrative targets for would-be attackers should take particular heed of the processes and best practices advocated. But no corporation or government agency is immune. Ensuring that you have established a baseline of best practices for all of your security and privacy regulations and non-regulatory obligations to your customers, citizens, and employees is a fundamental step in the right direction. With this baseline, you are ready to consider the many benefits of cloud computing in a model that best meets the needs of your government agency.

McAfee®

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

7036wp_dtp_cloud-computing_0909_ETMG