Cloud Security Considerations for the 2017 Enterprise

Cloud and DevOps Consulting Services Director:
Janaki Jayachandran

Authored by:
Kaviarasan Selvaraj
Marketing Manager

Rajkumar Murugesan
Cloud Consultant

aspire SYSTEMS
attention. always.

CONTENTS

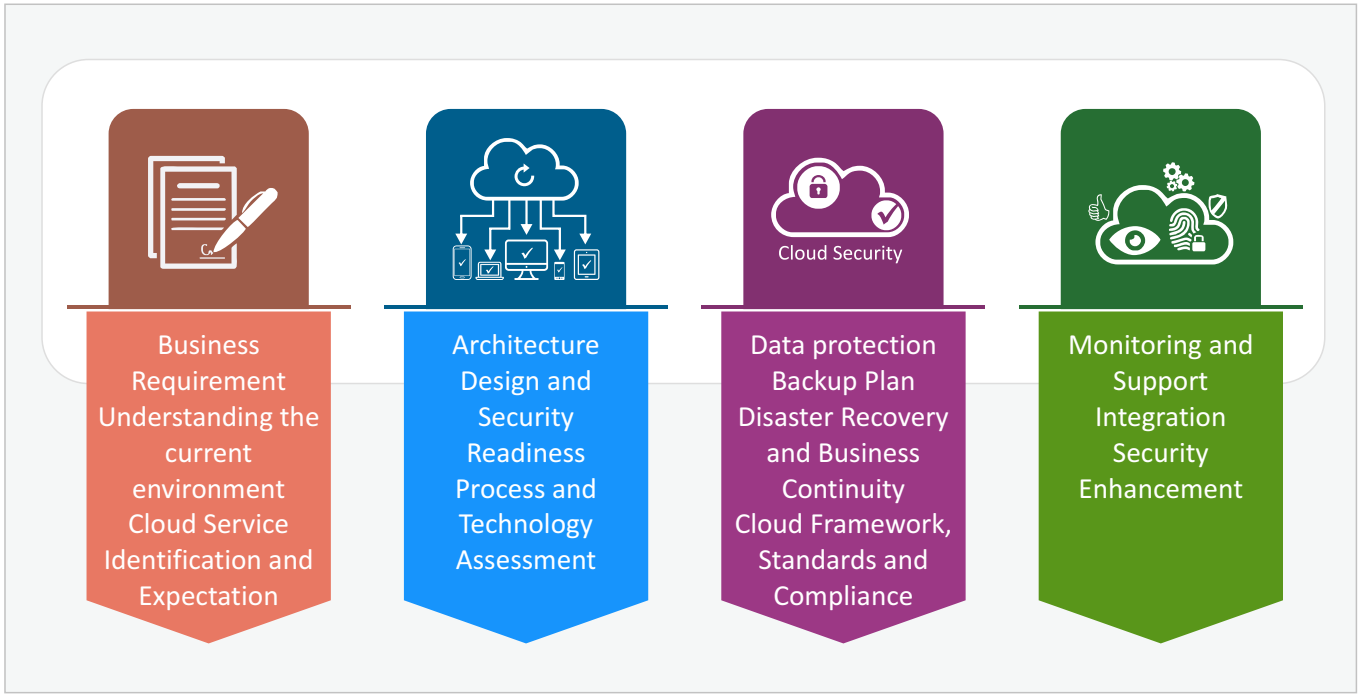
- How do you perform Security assessment for Cloud Readiness?
- Security Areas to be considered for protecting the customer information
- Data Classification
- Data Security
  - Security breaches and vulnerabilities
  - Counter measures
- Vulnerability Assessment and Penetration testing
- Intrusion Prevention System
- Host-Based and Network based Intrusion Detection
- Data Backups
- Cloud Data, Load balancer and Disaster Recovery
- Security standards and certifications
- Auditable Standards
- Cloud Monitoring and Support
- Conclusion

How do you perform Security assessment for Cloud Readiness?

In today's technology world, most of the enterprises are now focusing on how cloud is secure or not, how cloud is safer than on premise. Whilst customers, employees and intellectual property data of companies contend that it is the least safe place to store the data, depending upon the organization's business needs one or more compliance requirements are necessary to follow.

In fact, Gartner predicts that, through 2020, 95 percent of cloud security failures will be the customer's fault.

We have increasingly used computers to get hold, process and transfer our personal data and consequently, it's important to secure and protect the customer, employee, and intellectual property data of companies in an environment that is prone to security threats.



As cloud computing has become more widely accepted, number of information security concerns has been raised. Below areas will help guide you in assessing a prospective cloud vendor and to provide an overview of cloud security in each area.

"Organizations are increasingly focusing on detection and response, because taking a preventive approach has not been successful in blocking malicious attacks," said Elizabeth Kim, senior research analyst at Gartner.

Cloud Security Considerations for the 2017 Enterprise

75%

of security leaders expect their cloud security budget to increase dramatically over the next 3-5 years.

88%

of security leaders surveyed say their organizations are now moving to the cloud.

44%

of security leaders said that they expect a major cloud provider to suffer a significant security breach in the future.

Organizations should abide Regulatory Compliance and Certifications for complying with local, state, national, and foreign laws, including those related to data privacy and transmission of personal data, even when a service provider holds their data.

Security Areas to be considered for protecting the customer information

Security Areas Considered for Cloud	Objective
Data Classification	Documents are classified as Confidential, Public, Customer and internal purpose with proper naming convention
Physical Security and Data governance	Physical security to be taken care of by Cloud provider and needs to be reviewed from time to time while Data governance is managed by various assessments
Federation Solution Identification and Access control for Applications, Server and Network	Building strong authentication by way of a two factor authentication system, by adding another layer of security when users are connecting via public or private mode. Access control, firewall allow only authorized IP addresses and ports and RBA (Role based Access control) for Application, Sever, Network console. Ensure the active distributed Denial of Service [DDoS] Protection in place so that you can ward off attacks; with strong DDoS protection you can prevent external attacks that may block users from accessing cloud infrastructure.
Encryption and Application Security	The way data is encrypted can also increase the level of security. By enabling WAF (Web Application Firewall) encryption is enhanced on DB and Application Level
Password protection and policy	Policy needs to be approved, enabled in all servers and sent for review
Data Retention Policy	Data Retention policy that needs to be followed for defined months

Security Areas Considered for Cloud	Objective
Data Loss Protection	Define strategy for making sure that end users do not send sensitive or critical information outside the corporate network. Accidental data deletion or overwriting can cause the permanent loss of data/files in the same way as similar malicious behavior. Having adequate off-site backups can prevent organizations from irreparable damage caused by data loss threats.
Geographic Rules	Applying Geo Rules for unwanted access to the site
Readiness Training	Documenting necessary training in order to follow the Information Security Policy
Monitoring and Support	Cloud monitoring, incident response and support are important considerations as well. Defining these procedures in place will clearly delineate the shared responsibilities between you (the customer) and the cloud service provider

Data Classification

Documents that are classified in the Cloud help to identify the confidential document which has customer specific information, financial and legal risk, general to the public and internal purpose applied in the document from a business perspective. An organization must understand the specific types of data that it holds so that Document controls can be customized for its specific business needs.

Additionally, it is helpful to assess the risk of the relevant data types that need to be identified. Examples of considerations for assessing the risk of each data type include:

1. Whether the data is protected by regulations
2. Relative value of internal data (e.g., board papers versus financial information of Enterprise/corporate customer)
3. Direct impact to customers, business partners and their employees
4. Potential impact on brand and reputation
5. Potential loss of competitive advantage in the market

Data Security

Security breaches and vulnerabilities

In December 2010, Honda - a multinational motor company based out of Japan, experienced a data breach that affected 2.2 million customers. Customer names, email address, vehicle identification numbers (VINs), and access credentials for a Honda portal were stolen from the database. The database, however, was not within Honda's infrastructure. All these sensitive information was stolen from a cloud-based marketing service provider that Honda did business with.

One year ago, cloud storage provider Dropbox pushed a code change that eliminated the password authentication system required to access users' stored data, rendering any data from any account accessible to anyone who wanted to access it. In addition, Dropbox drew criticism for maintaining control of users' encryption keys; potentially making accounts and data susceptible to compromise should those keys fall into the wrong hands.

Counter measures

There are some cloud services that provide local encryption and decryption of your files in addition to storage and backup. It means that the service takes care of both encrypting your files on your own computer and storing them safely on the cloud.

Multi-tenancy is a key feature of Cloud that enables multiple customers to share one physical instance of the Cloud IT Infrastructure while isolating each customer tenant's application data. Encryption of Data in Transit (Network Security) allows Users access Cloud via the Internet protected by Secure Socket Layer version 3 (SSL v3) or Transport Layer Security (TLS).

If you're using an HSM (Hardware Security Modules), the goal is for the key to stay inside the HSM, and never leave. One common way to accomplish this is to store a key-encryption-key (KEK) in the HSM, and encrypted data-encryption-key(s) (DEK) elsewhere. In the case of Azure Key Vault, these could be retrievable secrets. AWS has similar security measures to protect your keys. When you need to use a DEK, you pass it in to the HSM, where it is decrypted using the KEK, and returned to you.

It is recommended that you deploy data protection and privacy controls supporting the laws of the various data protection authorities under whose jurisdiction you may fall.

Vulnerability Assessment and Penetration testing

Vulnerability assessments and penetration testing of the Cloud network infrastructure are also evaluated and conducted on a regular basis by both internal resources and external third-party vendors/tools like Veracode (A Global leader in Gartner Magic Quadrant for 3rd year running), Rapid 7, Qualys and Tenable.

Intrusion Prevention System

Intrusion Prevention systems monitor network traffic and are used to identify potential threats and respond to them swiftly, with their ability to identify suspicious activity, log it, attempt to block the activity so as to take immediate action after reporting. IPS can be either be hardware or software programs, generally it sits in line with the network and watches the network traffic as packets flow through it. Selecting top tools from large groups of open source or enterprise projects was very difficult as the tool selection varies based on requirements. However I have selected the most popular tools to scan for intrusion detection and prevention on security at each level, the following are some of the tools that provide IPS/IDS:Snort (Open source), OSSEC (Open source), Suricata, Bro IDS, Security Onion and OpenWIPS-ng.

Host-Based and Network based Intrusion Detection

Host-Based Intrusion Detection System (HIDS) server protection, plus a host of leading antivirus, anti-hacking, and vulnerability detection software that runs on a daily/weekly/monthly or need basis.

Network based IDS (NIDS) sits behind the firewall, on the demilitarized zone (DMZ) or the private network and sniff packets in promiscuous mode invisible to the attacker. It monitors and analyzes packets and can use anomaly or misuse detection techniques. While the firewall screens out unwanted traffic, the NIDS will alert as to what is "leaking" through the firewall. NIDS needs to keep up with the high volume of traffic or else it could miss attacks. High speed is also essential for low latency. Thus, it's usually available as dedicated hardware appliances.

Data Backups

Statistical pattern analytics evidence the existence of relationships where explicit relations are either weak or missing, statistically comparing performance patterns to identify common behaviors and therefore, implicit relationships.

> Gartner states that by 2020, 30% of organizations will leverage backup for more than just operational recovery (e.g., disaster recovery, test/ development, DevOps, etc.), up from less than 10% at the beginning of 2016. By 2018, 70% of business and application owners will have more self-service control over their data protection services, up from 30% today; and by 2020, over 40% of organizations will supplant long-term backup with archiving systems — up from 20% in 2015

Cloud master production database is replicated in real-time to a slave database maintained in the Cloud. A full backup is taken from this slave database each day and stored in the cloud. Cloud database backup policy requires database backups and transaction logs to be implemented so that a database may be recovered with the loss of as few committed transactions as is commercially practicable.

Transaction logs are retained until there are two backups of the data after the last entry in the transaction log. Database backups of systems that implement interfaces must be available as long as necessary to support the interfacing systems. This period will vary by system.

Backups of the database and transaction logs are encrypted for any database which contains customer data. In the database layer, we should focus to control for activity monitoring and blocking, data change logging, and auditing on its databases and all stored data are encrypted with AES at a minimum of 128 bits. All changes to data are logged in encrypted and unalterable log files with a variety of attributes.

Commvault is the top-ranked enterprise backup solutions research from Gartner 2016, other than that Veeam, EMC, IBM and Veritas technologies are major players in backup solutions.

Cloud Data, Load balancer and Disaster Recovery

Cloud warrants its service to its standard Service Level Agreement (SLA). The SLA includes a Disaster Recovery (DR) plan for the Cloud Production Service with a Recovery Time Objective (RTO) of 12 hours and a Recovery Point Objective (RPO) of one hour. The Recovery Time Objective is measured from the time the Cloud Production Service becomes unavailable until it is available again.

The Recovery Point Objective is measured from the time the first transaction is lost until the Cloud Production Service became unavailable. To ensure Cloud maintains these SLA commitments, Cloud maintains a DR environment with a complete replication of the production environment. In the event of an unscheduled outage where the outage is estimated to be greater than a predefined duration, Cloud executes its DR plan. The MSSQL database is replicated to the DR data center, new cloud instances are started in the DR data center which is in the cloud, and customers are redirected to the DR data center. The DR Plan is tested at least every six months.

Cloud enables automatic load balancing functionality in the cloud which allows distributing incoming application traffic in multiple instances of the cloud. It also achieves fault tolerance in the applications and seamlessly provides required amount of load balancing capacity needed to route application traffic.

Security standards and certifications

Enabling security standards which makes the environment most confidential in line with global security standards and certification security standards is based on the strict UK BS10012 standards for data privacy and the ISO27002 framework for security standards and the UK BS10012 standards have been adopted by Germany to govern its data privacy standards. We have to make with most confidential and global standards in place:

- EU Directive 95/46/EC (also known as the Data Protection Directive)
- Payment Card Industry Data Security Standard (PCI DSS)
- ISO27002, BS10012, SSAE-16 SOC2
- ASIO-4, FIPS 140-2 level 3 certification
- U.S. government FISMA accreditation (OPM/DHS/NTIS)
- Safe Harbor certification

Auditable Standards

- SOC 1 - Covers control objectives relevant to customers' internal control over financial reporting.
- ISO 27001:2005 Certification
- ISO 27001 is a standard for Information Security Management Systems (ISMS), published in 2005 by the International Organization for Standardization (ISO). It is a standards-based approach to security and is supported internationally by members of the ISO and is commonly used in Europe and around the world. The ISO standard is unique in that it is an international standard with predefined security clauses, objectives, and controls as opposed to the US SOC/SSAE 16 audits which are certified against service provider defined controls.
- Security Policies based on ISO 27002
- SSAE16-SOC2 auditing twice a year
- Safe Harbor Privacy Policy sets forth the privacy principles that the Companies follow with respect to personal information transferred from the European Union (EU) to the United States. The Companies will use personal information only in ways that are compatible with the purposes for which it was collected or subsequently authorized by the individual. The Companies will take reasonable steps to ensure that personal information is relevant to its intended use, accurate, complete, and current.

- Active Protection
- OWASP conform development
- Daily Application Penetration Testing
- Daily PCI-DSS Penetration Testing
- Monthly Infrastructure Penetration Test

Cloud Monitoring and Support

Spending on public cloud services will reach $204 billion in 2016, a 16.5% increase from 2015 revenue, according to Gartner. Consequently, more companies are trying to extend their performance management systems to the public cloud – a change that complicates end-to-end performance management

So monitoring is one of the key challenges in Cloud computing and it may be another reason, as organizations struggle to maintain visibility when transactions move off-site. Public cloud performance monitoring tools, however, can help overcome these challenges.

Security monitoring techniques using intrusion detection, network flow analysis tools, and host-based agents are common in internal data centers. However, ensuring systems are properly monitored in the cloud is a different story. In many cases, cloud providers may not allow or support advanced monitoring technologies or processes, although some may offer this as a service like Real-time alerts and Historical/custom reports on availability, SLA, response time, and detailed application performance allow to insure cloud-based services are being delivered reliably and efficiently as local services, and to hold cloud providers accountable as per the service-level agreements.

Health checks of instances on portals which are spun on different cloud platforms can be performed. Comprehensive approach and support through ITSM tool, prioritizing the tickets, quick call resolution, single pane of glass to have a single control point to manage their applications across clouds. Cloud providers offers cloud monitoring services to see the resource availability, performance and track metrics like AWS Cloud watch, Azure Application Insights and Google stack-driver monitoring.

You can have a try with some tools; many come with free trials and demos so it will give you a feel as to what to look for. If you're having AWS cloud then, you can just use what comes with it. Many vendors will give the impression that CloudWatch doesn't even exist so that they can sell their own tools.

Amazon CloudWatch is a very competent tool from AWS. It enables customers to monitor EC2 instances and Elastic Load Balancers in real-time. BMC Cloud Lifecycle Management is a hybrid (public/private) cloud management platform that allows you to get up and running quickly with simple, out-of-the-box use cases, and also supports more complex, production-class cloud environments. It supports different cloud infrastructure options such as AWS, Azure, OpenStack, VMware vCloud Director etc, and monitoring via CA NimSOft, SolarWinds Cloud Monitoring Tool, Zenoss Cloud Monitoring, RevealCloud by CopperEgg and Nagios. Best practices are to use one tool at a time and see how it fits your organizational needs.

Conclusion

The entire assessment focus is towards appropriate security measures and procedures at different levels within your IT environment; starting from choosing the cloud service provider to data protection, business risks, regulatory compliance requirements, continual monitoring and support. Place in your agreement with the cloud application vendor incentives and penalties to support your specific technical requirements and risk tolerance, expectations for their native controls, geographical diversity and additional efforts to which the vendor has committed. Have a defined plan for periodic health checks, risk assessments and a futuristic plan. These are some of the best practices and guidelines to perform security assessment for cloud readiness in your IT environment.

SINGAPORE +65 3163 3050 | NORTH AMERICA +1 630 368 0970 | EUROPE +44 203 170 6115 | INDIA +91 44 6740 4000 | MIDDLE EAST +971 50 658 8831

For more info contact info@aspiresys.com or visit www.aspiresys.com