Infosys cobalt

WHITE PAPER

CYBERSECURITY CONSIDERATIONS IN THE CLOUD ENVIRONMENT

Abstract

There is a saying "Enough is Enough!". The recent cyber-attacks on various large and complex organizations in the world have proved that "Enough is NOT Enough". Cybersecurity is an ever-growing challenge that one needs to address on an ongoing basis.

With the invention of Cloud technology in the last decade, more and more organizations are migrating their workloads and offering services to their customers through it. The many reasons why organizations are opting to deploy their workloads in the cloud are ease of deployment, consumption-based payment model, global connectivity, almost 100% availability, scalability, and elasticity. While all these benefits can be reaped at the click of a mouse button, an organization's data and applications are exposed to a very complex environment with increased dependency on the service provider. Many cloud service providers claim to provide better security than the on-premise solution; however, that comes with a lot of conditions and constraints that organizations need to understand in terms of responsibilities and ownerships.

This paper attempts to provide a view on the security aspects for the cloud that can help organizations while they move their workloads in the cloud and create a secure design for a hybrid environment (on-premise and cloud/ public-private cloud). They can easily maintain a secured environment so that information security and privacy aspects adhere to legal or regulatory compliance requirements on an ongoing basis.

Infosys®
Navigate your next

Introduction

Cloud services are complex in nature due to various deployment and service models, underlying platforms, compatibility considerations of various applications and platforms, and also due to distributed roles and responsibilities between the service provider and organizations in the context of design, implementation, and maintenance of a secure environment.

There are various similarities and differences when it comes to information security in the cloud as against on-premise solutions.The below diagrams shows some of these aspects.

Similarities

- Traditional network, host, database, application security controls are still applicable in cloud environments such as hardening standards, network segmentation, OWASP top 10 for applications
- Physical and environmental security controls are applicable to cloud data centers
- Industry specific compliance, standard and regulatory requirements are still applicable in the cloud such as SOX, PCI-DSS, HIPAA and GDPR
- Except for federated IDAM other user authentication and authorization, password policy, multifactor authentication controls remain the same

Differences

- Security is a shared responsibility between the cloud service provider and the organzation. For on-premise it is completely owned by the client
- Depending on the type of cloud service and delivery model chosen by the organization, ownership of security controls is determined. For on-premise security controls are competely managed by the organization
- Because of multitenancy in the public cloud, the service provider has to ensure proper logical isolation of each organization's data, network, and has to maintain privacy. For on-premise such complexity does not exist
- There is a need for appropriate agreements with the CSP for forensic investigation and access to third-party investigation agencies for any security incident.There is no such need for any agreement as the organization itself is hosting and managing the environment for on-premise solutions
- Key management on cloud is complex as compared to on-premise
  Issues like cross border data transfer in public cloud and lack of control over data location do not exist for on-premise data center
- IDAM solution in cloud is more complex than on-premise and may need federation

As we see that there are very subtle differences with regards to security in the cloud environment as against the local on-premise environment, there are also many similarities between on-premise and cloud. The basics of security and data privacy remain the same. Security best practices such as the principle of least privileges, defense in depth, minimizing the footprint to reduce the exposure, security hardening the OS, network, applications, and databases, maintaining robust security monitoring and incident management processes, ensuring skilled professionals are deployed, constant vigilance towards 'zero-day' attacks and ability to respond to new threats in the ever-changing threat landscape are some of the must-have characteristics of a healthy solution.

Irrespective of the service or deployment model chosen by an organization, the cloud service provider is always responsible to maintain security and availability of the underlying backbone infrastructure such as hardware and host OS platforms, physical and environmental security, network security, and physical and logical access to this infrastructure.

Cybersecurity challenges in cloud environment

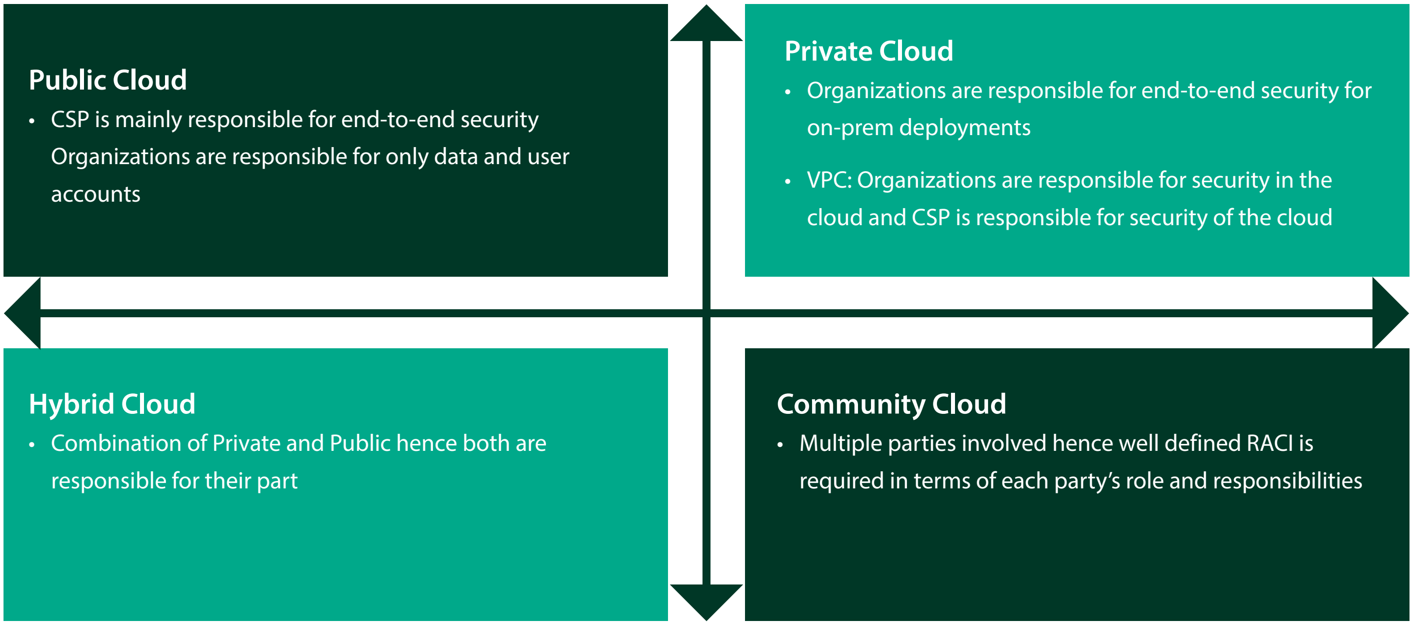
Prior to the advent of cloud, organizations' IT perimeters were well defined in terms of their data centers and locations. Now organizations need to extend their security policies to cloud environments in addition to their on-premise workloads. Although advanced, the cloud technology brings in several challenges to an organization that include:

- Maintaining the security posture
- Maintaining and managing IDAM solution to cater to authentication and authorization needs of the on-premise and on-cloud workloads
- Designing and implementing various security controls
- Maintaining roles and responsibilities in the context of shared responsibility model
- Centralized dashboards and reporting for security metrics
- Ensuring legal, regulatory, and other compliance requirements are met

These challenges are in fact opportunities for hackers. The cloud service provider carves out a network segment generally called the Virtual Private Cloud, creates an account for the organization, and provides administrative access. Beyond that, the organization must manage all security requirements within its network segment. This includes designing and deploying endpoint security solutions, security monitoring and incident management solution, enforcing security policies, designing and deploying firewalls, intrusion prevention solutions, and implementing data encryption and access control solutions to name a few. Each of these solutions bring complexity in terms of reporting and dashboard analysis, integration and consolidation with on-premise instances. Despite having robust information security policies and procedures, many organizations fail to consistently demonstrate effective implementation.

When it comes to designing, implementing, maintaining, monitoring, managing and improvising various security controls in the cloud, one needs to consider the boundaries defined by deployment and service models. Stated below are the cybersecurity considerations with respect to:

Cloud Deployment Models



Public Cloud

- CSP is mainly responsible for end-to-end security Organizations are responsible for only data and user accounts

Private Cloud

- Organizations are responsible for end-to-end security for on-prem deployments
- VPC: Organizations are responsible for security in the cloud and CSP is responsible for security of the cloud

Hybrid Cloud

- Combination of Private and Public hence both are responsible for their part

Community Cloud

- Multiple parties involved hence well defined RACI is required in terms of each party's role and responsibilities

Cloud Service Models and Corresponding Control Ownership

3 main service models are very commonly used and those are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

SaaS

- CSP is responsible for security up to the application layer Organization is responsible for the data and account management

PaaS

- CSP is responsible for Host OS, Guest OS, and underlying network and physical security
- Organization is responsible for the application platform, data security, and accounts management

IaaS

- CSP is responsible for the Host OS and underlying network and physical security
- Organization is responsible for the guest OS, platform, data, applications security, and the account management

Cybersecurity in the cloud is not just an IT problem, it is a business problem as an attack can cause immense damage to the business including financial loss, loss of reputation, adverse impact on repeat business, possible legal penalties, etc. it is therefore required to be looked at holistically.

People, Process and Technology

People

- Shadow IT
- Lethargic responses
- Skill shortages
- Increased attrition rates
- Communication gaps between Cloud, on-prem SPOCs and SMEs

Process

- Lack of Governance
- Inadequate policies and procedures
- Lack of central dashboards and reports
- Inadequate SLA's
- Poor change and configuration management
- Improper contractual terms and conditions
- Inadequate backup policy

Techlology

- EOL/EOS Platforms
- Delayed Patching
- Poor detection and response time
- Omission of security incidents due to improper triggers
- Ever changing technology and threat landscape
- Non-Traceability of VMs
- Improper configuration

Legal and Data Privacy Requirements

One of the most important aspects of cybersecurity and data privacy in the cloud environment is legal and jurisdictional compliance requirements. This is mainly important from a data privacy and access requirements perspective especially due to the global nature of the cloud. As cloud service providers create zones and regions to ensure that the required service is always available and that the service performance is improved for request from any corner of the world, they cross various local, regional and international boundaries. Due to this, the data that resides in respective geographical areas are subject to local jurisdictions and organizations need to be completely aware of this to ensure end-customer data privacy requirements are always met irrespective of the deployment or service model chosen. This comes with only a few exceptions such as data extradition is required by the government authorities against a warrant, or the data is required to be shared with a third party that is doing a forensic investigation with necessary approvals. The Cloud service provider, therefore, needs to ensure that such clauses are included in the service contract while offering the services to its customers.

Key Recommendations

The recent successful ransomware attacks on many reputed and large organizations have proved that even the organizations that follow a very systematic and planned approach towards cybersecurity are vulnerable to such attacks. Attackers have successfully exploited control weaknesses. It is therefore worth introspecting the overall approach towards information security management in the context of the cloud environment.

Attackers have massively focused on RDP infrastructure after COVID 19, given that almost all the organizations have mandatorily asked their staff to work from home.

Below are some of the recommendations that can provide some help to the organizations in terms of reducing the possibility of falling prey to such attacks in the future.

Area	Challenges/Threats	Recommendations
Security Standards and frameworks	• How do we extend on-premise ISO 27001 compliance to the cloud? • Which security frameworks to follow?	• ISO 27017 provides clauses specific to the cloud environment. • ISO 27018 provides controls specific to PII information in Public Cloud environments.
Pre-Deployment	• A new environment with unknown variables • The possible omission of security requirements	• Risk-based approach for requirements finalization, high-level, and low-level design • Conduct risk assessments at regular intervals • Identify risks on processes, architecture design and on the assets in the given business context, and IT environment
Infrastructure Security	• Use of weak protocols, unplanned changes to device configurations, unneeded services, ports and protocols, lack of security baseline, lack of asset classification	• Accurate asset inventory • Well established security baselines for each of the network, database, host, and application platforms • Use of international best practices such as CIS (Center for information security) security benchmarks
People	• Untrained/unskilled staff • Errors and mistakes for various device configurations • Improper understanding of roles and responsibilities • Phishing attacks • Uncontrolled access on end- user systems (laptops, desktops, and mobile devices)	• Mandatory training and certification • Well defined SOPs • Peer reviews • Change log reviews • Internal audits • Continuous training for all the staff on phishing attacks, do's, and don'ts • Automate disablement of user accounts if found compromised by phishing or by spammers • Enforce centralized policies on end-user systems with well-defined access rights to prevent download on any unauthorized software through the internet or USB devices
Security incident management	• Delay in identification and resolution of the incident • Improper root cause analysis • Intractability of VMs • False-positive events • Zero-day vulnerabilities	• Well defined security incident management procedure • Detailed roles and responsibilities for incident management • Auto-discovery tools and accurate and up to date asset inventory • Feedback mechanism for fine-tuning SIEM solution for continuous improvement. • Automate incident detection, alerting, and response wherever possible • Use built-in tools and capabilities provided by the CSP such as DDOS prevention, security logging, and monitoring
User Management	• Weak passwords • Dormant Accounts • Excessive privilege. • Improper role definitions • Multiple identity management solutions • Intractability and unaccountability of administrative changes • Use of shared admin accounts • Weak processes for joiners and leavers • Uncontrolled vendor/third party access	• Strict enforcement of strong password policy with consistent deployment across all the environments • Regular internal audits and peer reviews. • Well established SOPs for account administration and management • Two-factor authentication and well-documented change management process • Change log enabled and audited at regular intervals • Logs are securely stored and protected from unauthorized access • Vendor/Third-party audits at regular intervals • Use automated methods to disable dormant accounts, notify the use of admin accounts, disable accounts on last working day for the employees
Connectivity to cloud	• Insecure connectivity to a cloud environment • Use of weak encryption protocols • Unpatched perimeter devices and servers	• Ensure regular patching of jump hosts, RDS servers • Strictly control access, remote access servers by using two-factor authentications • Configure RDP over VPN • Use strong encryption algorithms • Renew expired PKI certificates on public-facing infrastructure • Use DNSSEC instead of DNS • Harden DNS servers and ensure that insecure zone transfers are not possible • Implement IPS and other DDOS protecting appliances
Legacy Systems	• Systems and devices cannot be patched • Lack of vendor support	• Identify and isolate such systems from other business-critical systems if they can't be replaced immediately • Extend vendor contracts to get better support • Explore the possibility of virtual patching • Enable compensatory controls such as SIEM • Continuously monitor activities on EOL/EOS systems • Plan to replace such EOL/EOS systems

Conclusion

Benefits provided by cloud environments can only be reaped if proper precautions and security measures are taken. The cloud environment is very similar to the on-premise environment when it comes to server, network, data, application, and other security aspects. It is therefore necessary to extend your on-premise security policies to the cloud environment and integrate them for centralized security dashboard and reporting.

Time and again it is proven that the weakest link in security is people working and having access to the environment. Insider threat is difficult to detect and is more dangerous. Hackers are constantly inspecting your network using automated scripts and even very sophisticated mechanisms such as 'Ransomware as a Service'. Maintaining secure infrastructure is the responsibility of everyone in the organization. Continuous efforts are required for identifying and remediating risks proactively, following security best practices, configuring all the systems and devices based on industry standards such as CIS, OWASP, SANS, NIST.

References

1. https://www.cisecurity.org/benchmark/amazon_web_services/

2. https://www.cisecurity.org/benchmark/azure/

3. https://owasp.org/www-project-top-ten/

4. https://www.nist.gov/cyberframework/risk-management-framework

5. https://www.enisa.europa.eu/publications/security-framework-for-governmental-clouds/at_download/fullReport

About the Author

Vijay Mahajani

Cyber Security Unit as a Principal Consultant, Infosys

Vijay Mahajani has over 22 years of experience in IT that includes designing, implementing secure networks and systems, conducting security audits and risk assessments on cloud and On-Prem systems. He is working with Infosys, Cyber Security Unit as a Principal Consultant for the past 3.5 years. He has successfully completed various consulting engagements in the USA, UK, Australia, Middle East, and other parts of the world for SOX, ISO 27001, Business continuity management, and information security risk assessments. He has also pioneered efforts to develop various templates for GDPR, SOX, and ISO 27001 implementations and develop tools to measure the maturity of an organization based on various standard and compliance requirements.

He has achieved various certifications in past such as CCNA, MSCE+I, CNI, CISA, ITIL v3, BS 25999, ISO 27001:2005 LA and at present maintaining CCSP, ISO 27001:2013 LA and CISSP certificates.

For more information, contact askus@infosys.com

Infosys®
Navigate your next