RISK INSIGHTS
Expert Information Security Services

Public Cloud Security Control Requirements for SMB's

Overview

Risk Insights has identified 39 key security requirements for organizations wishing to leverage public cloud computing services for sensitive data transactions. These requirements are intended to serve as a starting point and organizations may need to develop deeper controls in some areas based upon their unique business risks. For questions or comments about these requirements, we can be reached at info@riskinsights.net.

Categories	Description of Security Category
Data Protection	Cloud accessible services are available to store sensitive and restricted data at rest via encryption within the public hosting environment.
Governance	Clear standards and guidelines are in place to indicate what types of projects are available for public cloud hosting. In addition, specific processes are implemented to ensure that cloud usage patterns are aligned with company policy.
Platform Integrity	A robust compute, storage and network security foundation is in place within the public cloud. This foundation is used to verify that our offerings and services are operating within a secure environment.
Access Control	Processes for access provisioning, permissions management and change are in place for AWS environment. The scope of access management security strategy includes: AWS platform (i.e. AWS console and service API's) as well as compute and storage instances.
Key Management	To accompany the data protection strategy, robust key management protocols are in place to support the protection of data within the public cloud.
Situational Awareness	Near real-time capabilities are in place to adequately capture the state of the public cloud configuration and to monitor drift from expected standards.
Vulnerability Management	Services to continuously assess and track the remediation of OS and App level cloud vulnerabilities in order to reduce the probability of a system compromise within the cloud.
Detection and Containment	Technical capabilities with supporting processes that enable the company to detect patterns indicative of abuse or compromise against company services.

Security Guidance for Public Clouds

Cloud security controls are the "how" or best practices. They are best depicted as the "minimal security bar" to be in place to secure company data and assets in public cloud.

Cloud Security Controls	Short Name	Description	Implementer
Governance	GO-1	An independent security assessment will be conducted against the Public Cloud technical architecture and operational processes. Issues identified during the course of the assessment will be tracked and remediated.	
Governance	GO-2	During the on-boarding process, end-users will be required to submit the following security related information regarding their offering: - Project Name - Project Owner - Type(s) of data being used - If the system will be Internet facing or internal facing	
Governance	GO-03	Security training will be required prior to obtaining full public cloud access	
Governance	GO-05	Requests for public cloud hosting will be submitted to an cross-organizational approval party to verify that the requested use case conforms with company policy.	
Platform Integrity	SI-01	Available AMI choices for Full Public cloud users will be limited to AMI's that have been approved by the security group.	
Platform Integrity	SI-02	Security patches for Public Cloud instances will be maintained according to the company's vulnerability management SLA's:	
Platform Integrity	SI-03	The baseline AMI's will include a forensics agent	
Platform Integrity	SI-04	The baseline AMI's will include an anti-virus agent	
Platform Integrity	SI-05	Security approval is required for the addition of new software packages on public cloud instances	
Platform Integrity	SI-06	Monitoring utilities will alert on changes to critical system files, libraries, and services	
Platform Integrity	SI-07	Automated mechanisms are in place to detect instances that are not compliant with the Platform Integrity conditions: side channel account, AV agent, forensics agent, etc.	
Access Control	AC-01	Access to the AWS master account will be managed by the company's access control team.	
Access Control	AC-03	A side-channel account for monitoring/security/management will be incorporated into the baseline AMI	
Access Control	AC-04	AWS IAM roles will be defined for the following minimum roles types: - Project Super Administrator - Project Developer - Project Network Administrator - Project Systems Administrator	
Access Control	AC-04	Multi-factor authentication will be enabled for the master AWS account	

Cloud Security Controls	Short Name	Description	Implementer
Access Control	AC-05	Separate security groups (firewall) will be defined for the following environments (at a minimum): - Public facing (HTTP/HTTPS allowed in) - Non-Public (Access from Public over TBD ports) - Sensitive (Access from Non-Public over TBD ports) - Security Service Enclave (Access to/from other zones over TBD ports)	
Access Control	AC-06	Local account (instance level) access for production instances will be managed by the company's access control team.	
Access Control	AC-07	Network access to public cloud instances will be restricted to company network egress points (IP's)	
Access Control	AC-08	Access to console administration accounts will be managed by the company's account provisioning process.	
Access Control	AC-09	Automated mechanisms are in place to detect, change and revoke user permissions on the AWS control plane as well as EC2 instances.	
Access Control	AC-10	Changes to the AWS security groups (firewall) will require formal change approval	
Access Control	AC-11	Changes to the AWS security groups (firewall) will be performed only by authorized personnel who possess the appropriate role permissions.	
Access Control	AC-12	AWS console user accounts will consist of the employees company email address	
Access Control	AC-13	Automated audit processes will be implemented to detect AWS accounts that are in place for non-employees	
Key Management	KM-01	Key management API's for key creation, revocation and authenticated access will be accessible within a cloud suitable form factor	
Key Management	KM-02	AWS access keys will be stored within a secure key repository.	
Key Management	KM-03	Encryption keys for client side S3 encryption will be stored within a secure key repository	
Situational Awareness	SA-01	On-demand cloud metadata is available to provide a report of the following information: - Asset IP addresses - AMI details - AMI requestor - AMI image type - AMI creation date - Corresponding project	
Situational Awareness	SA-02	Local EC2 instance logs are sent to a central, cloud accessible logging service	
Situational Awareness	SA-03	Cloud collected log information is forwarded over to a central security event collection and analysis system.	
Situational Awareness	SA-04	The security team (security operations center) is Amazon's primary escalation point of contact for security issues detected via Amazon's in-house tools.	
Situational Awareness	SA-05	Offering specific vulnerability information is available in an end-user view within the hosting portal.	

Cloud Security Controls	Short Name	Description	Implementer
Vulnerability Management	VM-01	All, active public cloud IP addresses are scanned for infrastructure and application related vulnerabilities according to the security team's standard scanning SLA	
Vulnerability Management	VM-02	An automated data service is in place to automatically maintain/sync active instance IP address information with the infrastructure and application security scanning services	
Data Protection	DP-01	All service calls between AWS and the company will be transmitted over secure transport methods (i.e. SSL, TLS)	

Cloud Security Threat Model

Security Threats	Risk Impact	Control Strategies (Mitigation)
Exploitation of cloud resources by a malicious actor **Breakdown** • Application layer compromise • OS layer compromise • Content delivery corruption • Storage compromise	• Cloud compute instances • Content delivery services • Cloud storage services (S3, EBS)	• Vulnerability management • Situational awareness
Regulatory/audit findings with regards to data use in the cloud	• Cloud compute instances • Content storage services	• Data sensitivity based hosting criteria • Data encryption
Denial of service	• Cloud compute instances	TBD
Post-compromise, covert channels	• Cloud compute instances	• Platform Integrity monitoring • HIDS/HIPS?
Unauthorized access (via accounts)	Unauthorized access (via accounts)	• Access management processes and auditing • Secure key storage/access