BeyondTrust

>>> Discover Gaps in Your Cloud Security Coverage

Cloud Service Provider Assessment Questionnaire

Cloud provider choices are important.

Evaluate your options with security as priority #1.

Selecting a cloud service provider (CSP) is a weighty decision. Your CSPs may be responsible for everything from your organization's entire cloud foundation to the key services on which your business and users depend.

A Step-by-Step Cloud Service Provider Evaluation

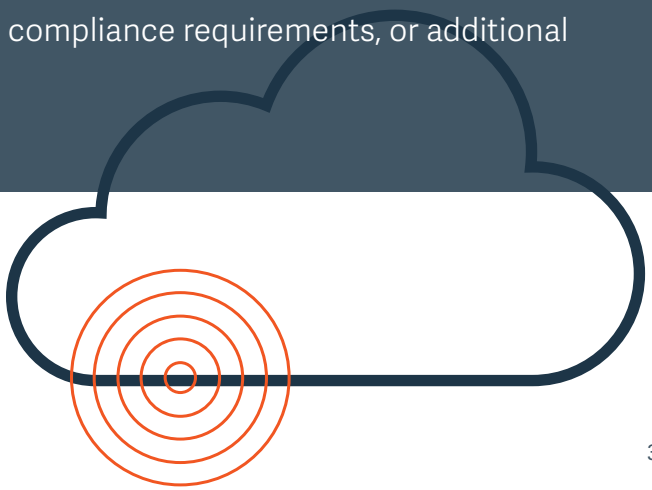
Utilize this cloud service provider questionnaire to assess the security posture cloud providers should be maintaining to keep pace with evolving cyberthreats and cloud security best practices.

There are many attributes that you may consider when selecting a particular cloud vendor, and the criteria vary based on each use case.

The questions and verification steps in this document are designed specifically to evaluate the security foundation of any cloud service provider you are considering, and so you may proactively identify any security control gaps that may require mitigation upfront.

Disclaimer. Please Note:

If a cloud service provider fails to meet some of these criteria, it is not always grounds for dismissal. Instead, consider implementing your own security controls to mitigate risks, or leverage a third-party solution to fill any gaps. You can use these questions to start a conversation with your CSPs to better understand each other's requirements and capabilities around security and compliance. This is not a comprehensive list by any means; your organization's requirements will vary based on industry, compliance requirements, or additional initiatives, like HIPAA or GDPR.



	Questions to Ask	Next Verification Steps	Comments
1	Are cloud provider root or administrator accounts used to manage all accounts and instances?	Access the administrative account and verify access and visibility to all accounts and instances.	
2	Are different accounts required for the different development stages, such as dev, staging, or production?	Access the cloud management console and determine if there are separate roles by default for different development stages.	
3	Are dedicated accounts being used for security audit and logging functions?	Access the cloud management console and navigate to the security section for logging and audit reports. Verify role-based access can be applied.	
4	Are shared email aliases/groups being used for the root account per each instance?	Access the cloud management console for the cloud service provider and navigate to the identity, account, and profile sections. Verify that a common email can be applied to all root accounts for notifications, and other email accounts can be added to notify owners.	
5	Does each root account have multi-factor authentication (MFA) enabled?	Access the cloud management console for the cloud service provider and verify root and all other administrative accounts have MFA enabled.	
6	Has the root account been used in the last 7 days?	Access the cloud management console and create an alert or execute a report to verify root accounts are not being used for daily activity.	
7	Have encryption at rest features been implemented for all data stores?	Within the management console, verify that encryption is enabled and applied to all types using the organization's standardized compliance regulations.	
8	Has volume encryption been implemented for volumes and snapshots?	In the management view for volumes or snapshots, verify the encryption status of each volume. This should be displayed as an attribute for each selection.	
9	Is SAML-based single sign-on (SSO) being used for identity and access management?	Verify SSO is enabled via SAML and denied for direct access to the services and management console.	
10	Are there any identities configured with console access?	Verify no users have unauthorized console access by viewing role-based access of identities or executing a report.	
11	Have any identities or accounts been granted access keys configured for programmatic access?	Verify no users have API access by viewing role-based access of identities, or executing a report, verify no users have API access. This should be limited to machine-to-machine identities only.	
12	Have any identities or accounts been granted access keys that have not been used in the last 90 days (or less)?	Create an alert or execute a report to verify that no identities or accounts have been stale for longer than 90 days in the cloud management console.	

	Questions to Ask	Next Verification Steps	Comments
13	Are all relational database service (RDS) instances using identity-based authentication for access?	Verify that database access is only granted via identity-based accounts in the cloud management console.	
14	Does the cloud service provider support third-party secret and credential storage from a privileged access management vendor?	Confirm providers have secrets and credential storage integration with a third-party privileged access management vendor.	
15	Do any security groups permit non-HTTP service access from the Internet?	Confirm that services for management, remote access, APIs, etc., are disabled from Internet access, and all private access is encrypted.	
16	Are private subnets used for internal servers, databases, and other resources?	Confirm that management and database access is private and locked down via VPC.	
17	Are all RDS instances in private subnets, and not publicly accessible?	Access the cloud management console to verify that relational database services are bound to internal addresses exclusively.	
18	Are security groups for outbound network access implemented for each VPC?	Access the cloud management console to confirm that VPC services are locked down for private and public access.	
19	For AWS only: Are any S3 buckets permitting open access permissions or allowing access to any authenticated AWS user? Are block public access settings enabled for all S3 buckets?	Enter the cloud management console and select the Trusted Advisor service. Once the page is updated, it will show the Amazon S3 Bucket Permissions action, which will detail S3 buckets that permit open access.	
20	Are cloud service providers enabled in all active and applicable regions?	Confirm that services are only available in desired regions. Disable any region for which the business is not ready to service yet.	
21	Are activity logging, data events, and access and authentication logs enabled for all instances and services?	Confirm that logging is enabled to provide forensics for daily operations. All collected data should be centralized using a cloud-native or SIEM tools.	
22	Have incident response plans been created and tested?	Obtain confirmation that the cloud service provider has an incident response plan in place and that it has been tested.	
23	Verify backup procedures and recovery service level agreements (SLAs) from each cloud provider.	Confirm backup solutions are implemented and tested.	
24	Are instances patched using system manager or another solution at a regular cadence?	Confirm that patch management solutions are implemented for all instances.	
25	Are all hosted servers and databases accessed through a secure remote access solution?	Confirm that internal servers and databases are only accessed using a bastion host, or other secure remote access solution. Default access via RDP, VNC, and SSH should never be publicly used.	

Noticing gaps in security coverage? BeyondTrust can help.

Cloud service providers place a high focus on securing public cloud infrastructure. However, customers share responsibility for securing the applications they choose to host in the cloud.

For these scenarios, **BeyondTrust's Privileged Access Management solutions** are built to quickly implement enterprise cloud security best practices. Reliably address gaps around privileges, identities, access controls, remote access, monitoring, and auditing with BeyondTrust.

Customers use BeyondTrust PAM to:

- Discover, onboard, and manage cloud computing instances, assets, accounts, and credentials
- Enforce least privilege and just-in-time access for cloud/multicloud infrastructure
- Right-size cloud entitlements
- Centrally manage remote access with a single, cross-cloud, VPN-less bastion host
- Manage, monitor, and audit every session involving privileged access

Learn more about BeyondTrust PAM for Cloud Security

Contact Us Today