Security in the Cloud: A Checklist for Cloud Buyers

Security is at the top of every IT professional's list.[1] Despite years of cloud maturation and examples of highly sensitive and regulated workloads, security remains one of the top reasons companies don't move specific workloads to the cloud, especially in highly regulated industries.[2] Naturally, it remains one of the top criteria IT decision makers and IT pros look at when evaluating cloud providers.[3]

aws

For some, however, cloud security continues to remain largely misunderstood—and certainly underestimated.[4] In fact, Gartner predicts that through 2020, public cloud infrastructure as a service (IaaS) workloads will suffer at least 60% fewer security incidents than those in traditional data centers.[4] Their conclusion? The security provided by major cloud providers is as good as or better than most enterprise data centers, so this concern should no longer be considered a legitimate road-block to cloud adoption.

So, how do you go about ensuring that your cloud services provider has the industry-leading security coverage you need?

We've outlined ten checklist items that can help you evaluate the options when purchasing cloud resources.

AT-A-GLANCE: Cloud Security Checklist

- ☐ Infrastructure Security
- ☐ DDoS Protection and Response
- ☐ Data Encryption
- ☐ Deployment and Configuration Security
- ☐ Security Monitoring and Logging
- ☐ Identity and Access Control
- ☐ Regulatory Compliance
- ☐ Simulation Testing
- ☐ Support for Third-Party Security Solutions
- ☐ Support and Security Services

The provider you choose likely operates under a “shared responsibility” model that gives both parties responsibility for specific security items. It’s important to clarify the security role of each party to understand your organization’s roles and responsibilities. Let’s start with the most fundamental layer in our checklist—infrastructure security.

Infrastructure Security

To enhance your existing security controls, your cloud services provider should not only give you the capability to quickly create virtual private networks, but they should also provide you with full control over each private network. For example, can you select your own internal classless interdomain routing (CIDR) range, create both publicly routed and privately routed subnets, as well as define your network egress paths? Can you use both IPv4 and IPv6 in your network for easy access to resources and applications?

Also check for security features such as stateful packet filters, web application firewalls (WAF), and network access control lists (NACLs) that can assist with inbound and outbound filtering at the instance level and subnet level. In addition, do you have the ability to launch dedicated servers on dedicated hardware for further isolation?

Finally, can you connect your network to both the Internet and your corporate data center? Can you connect privately to other networks as needed to share resources? Your connectivity options should allow private or dedicated connections from your office or on-premises environment, and encryption with Transport Layer Security (TLS) for data in transit across all services.

Can you connect your network to both the Internet and your corporate data center?

What about protecting your environment from increasingly large-scale network attacks such as a distributed denial of service attack (DDoS)?

DDoS Protection and Response

Your cloud services provider should offer automatic responses to DDoS attacks—at both the infrastructure layer and the application layer—to help minimize the time to mitigate and reduce the impact of an attack.

For example, at the infrastructure layer, your cloud service should provide you with the ability to automatically scale to absorb large and unexpected volumes of traffic, by either horizontal or vertical scaling. Likewise, network capacity and input/output (I/O) should be able to automatically scale to accommodate larger volumes of traffic. In addition, scalable load balancing should be available to distribute excess traffic across multiple back-end instances.

At the application layer, your cloud service should allow you to automatically close connections from slow-reading or slow-writing attackers. When you can accurately identify the IP addresses participating in the attack, you should be able to block those source IP addresses with a network access control list or firewall. You may also want a provider that allows you to set a threshold for the number of requests your web application can serve, and automatically block any additional requests if a bot or crawler exceeds that limit. In conjunction with your own network observations, does the provider offer hourly third-party IP reputation lists for blocking known bad actors?

For more advanced DDoS protection, your cloud service should help you to obfuscate resources in order to reduce the attack surface. For example, they can provide an application programming interface (API) to act as a “front door” to your applications, obfuscating other components of your application from the public and helping to prevent those resources from being targeted by a DDoS attack.

If your cloud service accepts only well-formed connections, that may also help prevent many common DDoS attacks like synchronization (SYN) floods and User Datagram Protocol (UDP) reflection attacks.

How do you ensure that only authorized persons or services can read and access sensitive information? You want to make sure your cloud provider gives you strong encryption and easy access to it.

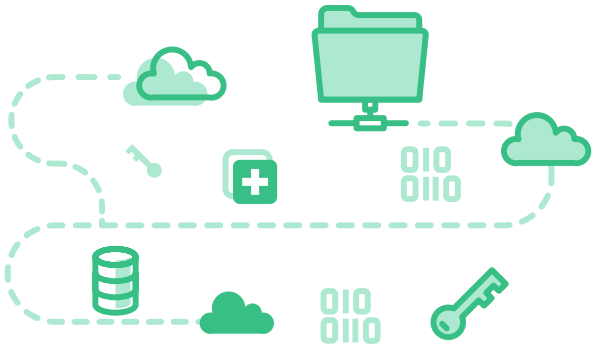
Data Encryption

Your cloud services provider should offer the option for data encryption to protect data in storage and databases, regardless of which database platform you're using.

Flexible key management options should allow you to choose whether to have the encryption keys managed by the cloud services provider or to self-manage your own key infrastructure. In either case, dedicated, hardware-based cryptographic key storage should be provided, allowing you to strengthen your existing compliance capabilities.

Ideally, your cloud service will provide APIs that allow you to integrate your own encryption and data protection features with any of the services you develop or deploy in the cloud environment.

Dedicated, hardware-based cryptographic key storage should be provided, allowing you to strengthen your existing compliance capabilities.



Automation is critical to any organization, large or small. You should quickly be able to leverage deployment tools to aid in your build process and to ensure that policy and governance controls are always deployed.

Deployment and Configuration Security

Your cloud services provider should offer tools and templates to facilitate your creation and decommissioning of cloud resources, as well as inventory and configuration management tools that allow you to track and manage changes to your cloud resources over time.

Template definitions and management tools in particular can be used to help organizations create standardized, preconfigured cloud environments in keeping with industry security standards.

Your cloud services provider should also offer security assessment services that can automatically evaluate deployed cloud applications for security vulnerabilities or deviations from configuration best practices, including identifying impacted networks, operating systems, and attached storage.

In addition, your provider should provide you with tools that can help with data loss prevention (DLP) and alert you when critical files are accessed within your cloud environment.

Your provider should provide you with tools that can help with data loss prevention (DLP) and alert you when critical files are accessed within your cloud environment.

A critical function of every security solution is the ability to support monitoring, automated alerting, and robust logging features. Your log files should be stored in a durable storage that prevents unauthorized access and encryption. For added control, you should look for a provider that gives you options for write once, read many (WORM) archives for long-term data holds for compliance or legal requirements.

Security Monitoring and Logging

Your cloud services provider should provide proactive security monitoring and logging as part of their shared services model. Monitoring capabilities can increase your visibility, sending alert notifications when specific events occur or thresholds are exceeded. These features let you spot issues before they impact the business, helping to reduce risk and improve the security posture of your environment.

In addition, flexible log aggregation options can help organizations facilitate security investigations as well as compliance reporting. You may even want your cloud service to provide clear visibility into API calls, including what calls were made, who made them, when they were made, and from where they were made.

According to Gartner, by 2018, 60% of enterprises that implement appropriate cloud visibility and control tools will experience one-third fewer security failures.[4] Gartner recommends that organizations investigate cloud-aware tools to improve visibility, so that day-to-day security operations rest with the infrastructure and operations (I&O) and security teams instead of with developers.

60% of enterprises that implement appropriate cloud visibility and control tools will experience one-third fewer security failures.[4]

Identity and access controls are critical to ensuring that only authorized users, groups, or applications can access internal resources. Your provider should give you granular access to identity solutions but also allow you to integrate with federated logins from solutions like OAuth, SAML, LDAP, or ADFS.

Identity and Access Control

Your cloud services provider should offer capabilities to define, enforce, and manage least privilege user access policies for all cloud services. These critical identity and access management features should give you the option to define individual user accounts with permissions across cloud resources and to implement multi-factor authentication for privileged accounts—including options for hardware-based authentication.

Ideally, identity and access management will be integrated across all services, as well as providing the ability to use APIs to integrate with your own applications or services. You may also want your cloud solution to provide a directory service enabling you to integrate and federate with corporate directories, to reduce administrative overhead and improve the end-user experience.

Your provider should also offer you the ability to provision short-lived credentials for external parties like contractors or authorized third parties without the need to create long-lived credentials. Integration with OAuth can also be leveraged to reduce the burden of managing identity authorization and validation systems altogether.

Your provider should also offer you the ability to provision short-lived credentials for external parties like contractors or authorized third parties without the need to create long-lived credentials.

Many organizations are now required to follow certain guidelines for regulatory compliance frameworks such as PCI, ISO 27001, HIPAA, FISMA, and CJIS. Your cloud services provider should provide you with the capabilities to meet these regulatory requirements.

Regulatory Compliance

Your cloud services provider should be able to help you meet your compliance requirements, whether that means:

- Carrying specific certifications such as Federal Information Processing Standards (FIPS), International Organization for Standardization (ISO), or Payment Card Industry Data Security Standard (PCI DSS)
- Providing support for specific security and privacy laws and regulations such as Family Educational Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH) Act, or the European Union (EU) Data Protection Directive
- Supporting specific frameworks such as EU-US Privacy Shield, Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST), Personal Health Records (PHR), or others that may be relevant to your industry

Cloud computing does reduce the overall security scope, and it does require customers to manage some of the computing stack in a shared-responsibility model. This is a good opportunity for new types of approaches and new method adoption to protect information.[4]

It's important to clarify with your cloud services provider who is responsible for which components of compliance and security. Although the specific methods may be different, organizations should retain control of the security they choose to implement to protect their own content, platform, applications, systems, and networks, the same as they would in an onsite data center. Finally, find out what compliance reporting and audit support options are available, and who has access to the audit trail.

Organizations must test their security controls and growth assumptions for unforeseen events. Your cloud provider should provide you with information on acceptable use and allow common security testing techniques such as port scans and penetration testing tools.

Simulation Testing

Your cloud services provider should allow you to run your own vulnerability scans, penetration tests, disaster recovery simulations, and other critical simulated events without generating security violations or setting off network abuse alerts. Due to the nature of these security-related testing activities, they can create conditions that would normally violate a cloud service provider's acceptable use policies. But these activities are an important part of an organization's security approach, and it's important that they can be authorized to be performed fully and on schedule—whether by your organization or by an approved third party—in order to help reduce operational risk.

Your cloud services provider should allow you to run your own vulnerability scans, penetration tests, disaster recovery simulations, and other critical simulated events without generating security violations or setting off network abuse alerts.

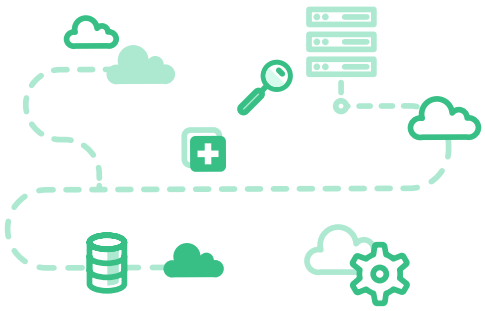
Your cloud provider should allow you to access third-party tools and services to help you gain better insight and access to your environment. A good cloud provider will have a marketplace with many offerings and solution providers.

Support for Third-Party Security Solutions

Your cloud services provider should allow you to use third-party solutions to enhance specific aspects of your security strategy, including infrastructure security, access and control, logging and monitoring, configuration and vulnerability analysis, data protection, and other aspects of cloud security where a third-party solution helps enable a comprehensive security architecture.

At a minimum, your cloud services provider should enable you to use industry-leading offerings that are equivalent to or better than your existing third-party security solutions and that complement the provider's existing cloud security services. And you should be able to integrate these solutions with the controls you're using on-premises to help ensure a seamless experience across your cloud and on-premises environments.

At a minimum, your cloud services provider should enable you to use industry-leading offerings that are equivalent to or better than your existing third-party security solutions.



It's important that your cloud provider have options for 24x7 support with SLA-backed response windows. Your provider should have in-house subject matter experts who can guide you to better understand your requirements and options on the platform.

Support and Security Services

Your cloud services provider should be able to help fill any gaps you may have in terms of cloud security expertise and provide comprehensive support for your cloud implementation with optional services. Your organization may need a little extra support or expertise to help define your security architecture based on your workloads and compliance requirements. They should provide guidance on how to provision your resources using industry security best practices and to help identify and close potential security vulnerabilities in your cloud implementation. Your cloud provider should help you detect and respond to security issues quickly, and help you meet your regulatory compliance needs. Essentially, you'll want a cloud services provider that can provide end-to-end support and security services.

Your cloud provider should help you detect and respond to security issues quickly.

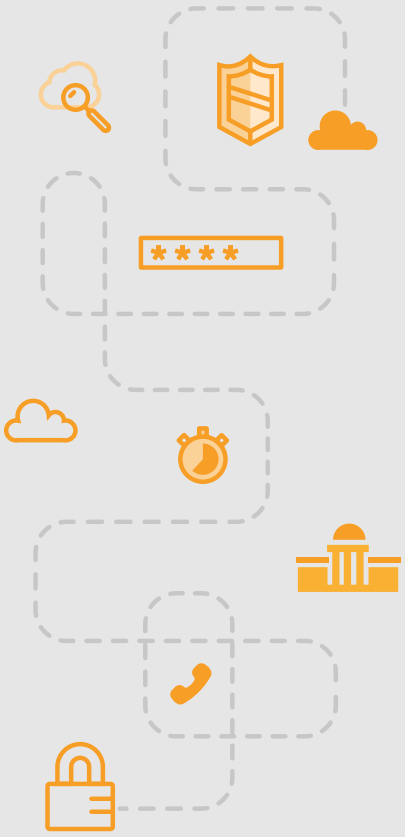
Amazon Web Services at Your Service

With security as our top priority, Amazon Web Services (AWS) protects millions of active customers around the world. Our customers represent diverse industries with a wide range of use cases, including large enterprises, start-ups, educational institutions, and government organizations. The scale and global reach of these customers gives us broad visibility and deep perspective on cloud security, knowledge which we rapidly reinvest back into our industry leading infrastructure and services.

As an AWS customer, regardless of your size or investment, you inherit all the benefits of our experience including best practices developed around our security policies, architecture, and operational processes tested against the strict standards and compliance requirements of third-party assurance frameworks.

We depend on the same infrastructure and security services that we provide you, and can help you simplify meeting your own security and regulatory requirements, as we have done for customers around the world.

To learn more about the security features of Amazon Web Services, visit our security website.



Visit our security website

Sources:

1 "The 2017 State of IT," *Spiceworks*, 2016. https://www.spiceworks.com/marketing/state-of-it/report/

2 "Six reasons why companies hang on to their data centers," *ZDNet*, May 1, 2017. http://www.zdnet.com/article/six-reasons-why-companies-hang-on-to-their-data-centers/

3 "Diving into IT Cloud Services," *Spiceworks,* 2016. https://www.spiceworks.com/marketing/reports/it-cloud-services/

4 "Is the Cloud Secure?" *Gartner*, January 23, 2017. http://www.gartner.com/smarterwithgartner/is-the-cloud-secure/