[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@1dd1031b47814fe9ad56a53e0179c11b?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view#main)

ref <https://kinsta.com/blog/cloud-security/>

**A Comprehensive Guide to Cloud Security in 2021 (Risks, Best Practices, Certifications)**

[Edward Jones](https://kinsta.com/blog/author/edwardjones/), March 25, 2021



Cloud security encompasses the technologies, controls, processes, and policies which combine to protect your cloud-based systems, data, and infrastructure. It is a sub-domain of computer security and more broadly, information security.

It is a shared responsibility between you and your cloud service provider. You implement a cloud security strategy to protect your data, adhere to regulatory compliance, and protect [your customers’ privacy](https://kinsta.com/knowledgebase/woocommerce-ssl/). Which in turn protects you from the reputational, financial, and legal ramifications of data breaches and data loss.

Cloud Security Shared Responsibility Model (Image source: Synopsys)

Cloud security is a critical requirement for all organizations. Especially with the latest [research from (ISC)2](https://www.isc2.org/Resource-Center/Reports/Cloud-Security-Report) reporting 93% of organizations are moderately or extremely concerned about cloud security, and one in four organizations confirming a cloud security incident in the past 12 months.

In this article, we will create a comprehensive guide to cloud security. You’ll explore the security risks of moving to the cloud, understand why cloud security is required, and discover cloud security best practices. We’ll also cover topics like how to assess a cloud service provider’s security and identify the certifications and training to improve your cloud security.

Let’s begin.

**Table of Contents**

1. [How does Cloud Security Work?](https://kinsta.com/blog/cloud-security/#how-does-cloud-security-work)
2. [7 Security Risks of Cloud Computing](https://kinsta.com/blog/cloud-security/#7-security-risks-of-cloud-computing)
3. [Why Cloud Security is Required](https://kinsta.com/blog/cloud-security/#why-cloud-security-is-required)
4. [Best Practices for Cloud Security](https://kinsta.com/blog/cloud-security/#best-practices-for-cloud-security)
5. [Top 10 Security Checklist Recommendations for Cloud Customers](https://kinsta.com/blog/cloud-security/#top-10-security-checklist-recommendations-for-cloud-customers)
6. [What is the Cloud Security Alliance?](https://kinsta.com/blog/cloud-security/#what-is-the-cloud-security-alliance)
7. [What is Kaspersky Security Cloud?](https://kinsta.com/blog/cloud-security/#what-is-kaspersky-security-cloud)
8. [What is a Cloud Access Security Broker (CASB)?](https://kinsta.com/blog/cloud-security/#what-is-a-cloud-access-security-broker-casb)
9. [A Look at the Top 10 Cloud Security Certifications in 2021](https://kinsta.com/blog/cloud-security/#a-look-at-the-top-10-cloud-security-certifications-in-2021)

**How does Cloud Security Work?**

Cloud security is a complex interaction of technologies, controls, processes, and policies. A practice that is highly personalized to your organization’s unique requirements.

As such, there’s no single explanation that encompasses how cloud security ‘works’.

A Model for Securing Cloud Workloads (Image source: HyTrust)

Thankfully, there are a widely established set of strategies and tools you can use to achieve a robust cloud security setup, these include:

**Identity and Access Management**

All companies should have an [Identity and Access Management (IAM) system](https://www.csoonline.com/article/2120384/what-is-iam-identity-and-access-management-explained.html)to control access to information. Your cloud provider will either integrate directly with your IAM or offer their own in-built system. An IAM combines multi-factor authentication and user access policies, helping you control who has access to your applications and data, what they can access, and what they can do to your data.

**Physical Security**

[Physical security](https://www.ibm.com/blogs/cloud-computing/2012/02/22/cloud-physical-security-considerations/) is another pillar of cloud security. It is a combination of measures to prevent direct access and disruption of hardware housed in your cloud provider’s datacenter. Physical security includes controlling direct access with security doors, uninterrupted power supplies, CCTV, alarms, air and particle filtration, fire protection, and more.

**Threat Intelligence, Monitoring, and Prevention**

[Threat Intelligence](https://www.forcepoint.com/cyber-edu/threat-intelligence), [Intrusion Detection Systems (IDS)](https://www.barracuda.com/glossary/intrusion-detection-system), and [Intrusion Prevention Systems (IPS)](https://www.forcepoint.com/cyber-edu/intrusion-prevention-system-ips)form the backbone of cloud security. Threat Intelligence and IDS tools deliver functionality to [identify attackers](https://kinsta.com/blog/what-is-a-ddos-attack/) who are currently targeting your systems or will be a future threat. IPS tools implement functionality to mitigate an attack and alert you to its occurrence so you can also respond.

**Encryption**

Using cloud technology, you are sending data to and from the cloud provider’s platform, often storing it within their infrastructure. [Encryption](https://searchsecurity.techtarget.com/definition/encryption) is another layer of [cloud security to protect your data assets](https://kinsta.com/secure-wordpress-hosting/), by encoding them when at rest and in transit. This ensures the data is near impossible to decipher without a decryption key that only you have access to.

**Cloud Vulnerability and Penetration Testing**

Another practice to maintain and improve cloud security is [vulnerability and penetration testing](https://www.hitachi-systems-security.com/blog/penetration-testing-vs-vulnerability-assessment/). These practices involve you – or your provider – attacking your own cloud infrastructure to i[dentify any potential weaknesses or exploits](https://kinsta.com/knowledgebase/disclose-security-vulnerability/). You can then implement solutions to patch these vulnerabilities and improve your security stance.

**Micro-Segmentation**

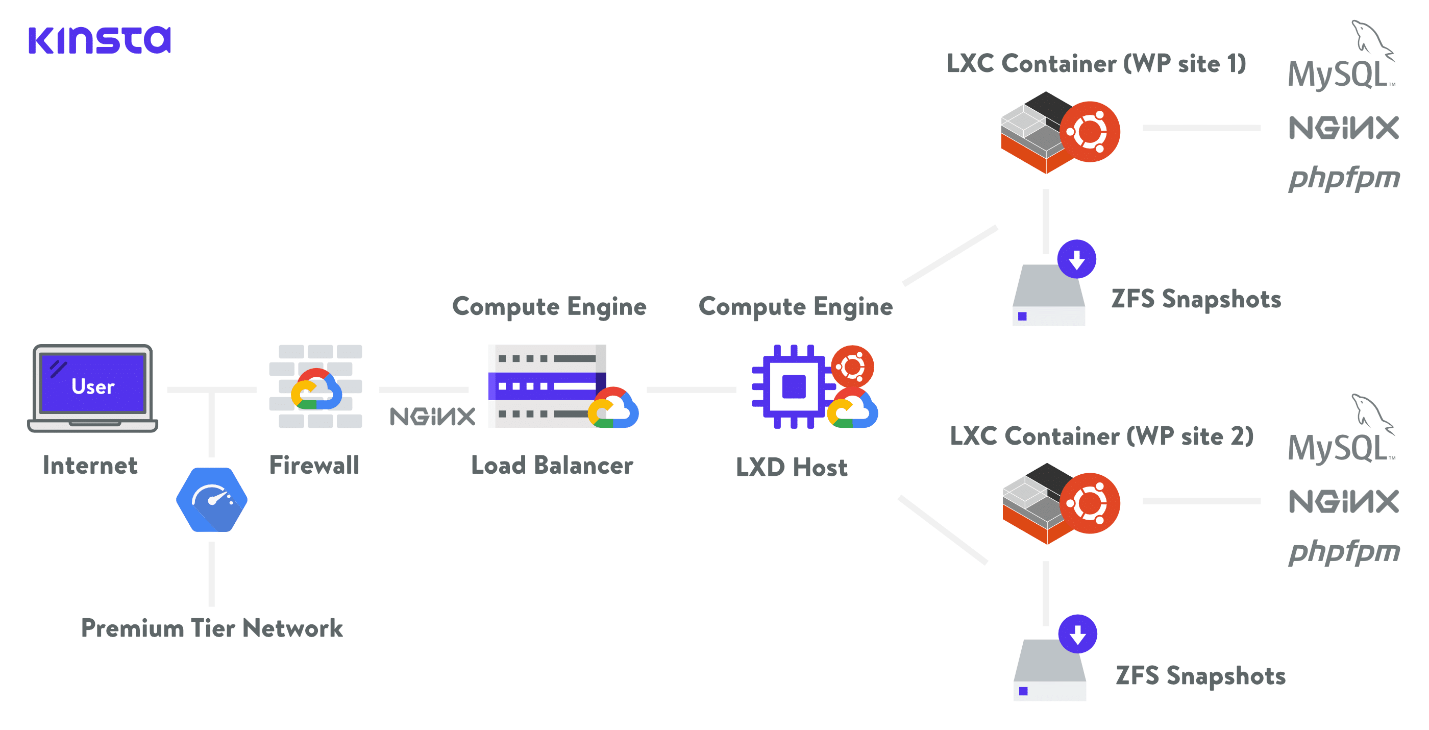
[Micro-segmentation](https://www.networkworld.com/article/3247672/what-is-microsegmentation-how-getting-granular-improves-network-security.html) is increasingly common in implementing cloud security. It is the practice of dividing your cloud deployment into distinct security segments, right down to the individual workload level.

By isolating individual workloads, you can apply flexible security policies to minimize any damage an attacker could cause, should they gain access.

**Next-Generation Firewalls**

[Next-Generation firewalls](https://digitalguardian.com/blog/what-next-generation-firewall-learn-about-differences-between-ngfw-and-traditional-firewalls) are another piece of the cloud security puzzle. They protect your workloads using [traditional firewal](https://kinsta.com/blog/what-is-a-firewall/)l functionality and newer advanced features. Traditional firewall protection includes packet filtering, stateful inspection, proxying, IP blocking, [domain name blocking](https://kinsta.com/blog/how-to-block-a-website-on-chrome/), and port blocking.

Next-generation firewalls add in an intrusion prevention system, deep packet inspection, application control, and analysis of encrypted traffic to provide comprehensive threat detection and prevention.



Kinsta hosting architecture

Here at Kinsta, we secure all WordPress websites behind the [Google Cloud Platform (GCP) Firewall](https://kinsta.com/feature-updates/auto-db-optimize/#now-secured-behind-google-cloud-platform-firewall). Offering state-of-the-art protection and the ability to integrate closer with other GCP security solutions.

[Security is a concern for all businesses that, if neglected, can significantly impact the reputation and bottom line. Check out the 7 security risks of cloud computing ⛈⚙️CLICK TO TWEET](https://twitter.com/intent/tweet?url=https%3A%2F%2Fbit.ly%2F3eVqCxj&via=kinsta&text=Security+is+a+concern+for+all+businesses+that%2C+if+neglected%2C+can+significantly+impact+the+reputation+and+bottom+line.+Check+out+the+7+security+risks+of+cloud+computing+%E2%9B%88%E2%9A%99%EF%B8%8F&hashtags=security%2Cwebhost)

**7 Security Risks of Cloud Computing**

Whether or not you’re operating in the cloud, [security is a concern](https://kinsta.com/blog/is-wordpress-secure/) for all businesses. You will face risks such as [denial of service](https://kinsta.com/blog/ddos-attack/), [malware](https://kinsta.com/knowledgebase/wordpress-malware-removal/), [SQL injection](https://kinsta.com/blog/sql-injection/), data breaches, and data loss. All of which can significantly impact the reputation and bottom line of your business.

When you move to the cloud you introduce a new set of risks and change the nature of others. **That doesn’t mean cloud computing is not secure**. In fact, many cloud providers introduce access to highly sophisticated security tools and resources you couldn’t otherwise access.

It simply means you need to be aware of the change in risks in order to mitigate them. So, let’s take a look at the unique security risks of cloud computing.

1. [Loss of Visibility](https://kinsta.com/blog/cloud-security/#1-loss-of-visibility)
2. [Compliance Violations](https://kinsta.com/blog/cloud-security/#2-compliance-violations)
3. [Lack of Cloud Security Strategy and Architecture](https://kinsta.com/blog/cloud-security/#3-lack-of-cloud-security-strategy-and-architecture)
4. [Insider Threats](https://kinsta.com/blog/cloud-security/#4-insider-threats)
5. [Contractual Breaches](https://kinsta.com/blog/cloud-security/#5-contractual-breaches)
6. [Insecure Application User Interface (API)](https://kinsta.com/blog/cloud-security/#6-insecure-application-user-interface-api)
7. [Misconfiguration of Cloud Services](https://kinsta.com/blog/cloud-security/#7-misconfiguration-of-cloud-services)

**1. Loss of Visibility**

Most companies will access a range of cloud services through multiple devices, departments, and [geographies](https://kinsta.com/knowledgebase/best-data-center/). This kind of complexity in a cloud computing setup – without the appropriate tools in place – can cause you to lose visibility of access to your infrastructure.

Without the correct processes in place, you can lose sight of who is using your cloud services. Including what data they are accessing, uploading and downloading.

If you can’t see it, you can’t protect it. Increasing the risk of data breach and data loss.

**2. Compliance Violations**

With the increase in regulatory control, you likely need to [adhere to a range of stringent compliance requirements](https://kinsta.com/blog/wordpress-ccpa-compliance/). When moving to the cloud, you introduce the risk of [compliance violations](https://kinsta.com/blog/wordpress-gdpr-compliance/) if you are not careful.

Many of these regulations require your company to know where your data is, who has access to it, how it is processed, and how it is protected. Other regulations require that your cloud provider holds certain compliance credentials.

A careless transfer of data to the cloud, or moving to the wrong provider, can put your organization in a state of non-compliance. Introducing potentially serious legal and financial repercussions.

**3. Lack of Cloud Security Strategy and Architecture**

This a cloud security risk that you can easily avoid, but many don’t. In their haste to [migrate systems and data to the cloud](https://kinsta.com/blog/cloud-market-share/#why-businesses-are-moving-to-the-cloud), many organizations become operational long before the security systems and strategies are in place to protect their infrastructure.

Here at Kinsta, we understand the importance of a security-first mindset when moving to cloud. That’s why [Kinsta provides free WordPress migrations](https://kinsta.com/knowledgebase/wordpress-migrations/) to ensure your transition to the cloud is both secure and avoids prolonged [downtimes](https://kinsta.com/blog/migrate-wordpress-site/).

Make sure you implement a security strategy and infrastructure designed for cloud to go live inline with your systems and data.

**4. Insider Threats**

Your trusted employees, contractors, and business partners can be some of your biggest security risks. These insider threats don’t need to have malicious intent to cause damage to your business. In fact, the majority of insider incidents stem from a lack of training or negligence.

While you currently face this issue, moving to the cloud changes the risk. You [hand control of your data to your cloud service provider](https://kinsta.com/knowledgebase/hosted-data-transfer/) and introduce a new layer of insider threat from the provider’s employees.

**5. Contractual Breaches**

Any contractual partnerships you have will include restrictions on how any shared data is used, how it is stored, and who is authorized to access it. Your employees unwittingly moving restricted data into a cloud service without authorization could create a breach of contract which could lead to legal action.

Make sure you read your cloud providers’ [terms and conditions](https://kinsta.com/legal/terms-service/). Even if you have authorization to move data to the cloud, some service providers include the right to share any data uploaded into their infrastructure. Through ignorance, you could unintentionally breach a non-disclosure agreement.

**6. Insecure Application User Interface (API)**

When operating systems in a cloud infrastructure, you might [use an API to implement control](https://kinsta.com/blog/wordpress-rest-api/). Any API built into your web or mobile applications can offer access internally by staff or externally by consumers.

It is external-facing APIs that can introduce a cloud security risk. Any insecure external API is a gateway offering unauthorized access by cybercriminals looking to steal data and manipulate services.

The most prominent example of an insecure external API is the [Facebook – Cambridge Analytica Scandal](https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html). Facebook’s insecure external API gifted Cambridge Analytica deep access to Facebook user data.

**7. Misconfiguration of Cloud Services**

Misconfiguration of cloud services is another potential cloud security risk. With the increased range and complexity of services, this is a growing issue. Misconfiguration of cloud services can cause data to be publicly exposed, manipulated, or even deleted.

Common causes include keeping [default security and access management settings](https://kinsta.com/blog/wordpress-security/#clever-passwords) for highly sensitive data. Others include mismatched access management giving unauthorized individuals access, and mangled data access where confidential data is left open without the need for authorization.

**Why Cloud Security is Required**

The [mass adoption of cloud technology](https://kinsta.com/blog/cloud-market-share/) combined with an ever-increasing volume and sophistication of cyber threats is what drives the need for cloud security. Reflecting on the security risks of adopting cloud technology – outlined above – failure to mitigate them can come with significant implications.

But it’s not all negative, cloud security can also offer significant benefits. Let’s explore why cloud security is a critical requirement.

1. [Cyber Security Threats Continue to Increase](https://kinsta.com/blog/cloud-security/#cyber-security-threats-continue-to-increase)
2. [Preventing Data Breaches and Data Loss](https://kinsta.com/blog/cloud-security/#preventing-data-breaches-and-data-loss)
3. [Avoid Compliance Violations](https://kinsta.com/blog/cloud-security/#avoid-compliance-violations)
4. [Maintaining Business Continuity](https://kinsta.com/blog/cloud-security/#maintaining-business-continuity)
5. [Cloud Security Benefits](https://kinsta.com/blog/cloud-security/#cloud-security-benefits)
6. [Choose a Trusted Provider](https://kinsta.com/blog/cloud-security/#choose-a-trusted-provider)

**Cyber Security Threats Continue to Increase**

A driving force for secure cloud practices is the ever-increasing threat from cybercriminals – both in volume and sophistication. To quantify the threat, a [Cloud Security Report](https://www.isc2.org/Resource-Center/Reports/Cloud-Security-Report) from (ISC)2 found that 28% of businesses experienced a cloud security incident 2019. With the [UK Government also reporting](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf) 32% of UK businesses experiencing an attack on the systems in the past 12 months.

**Preventing Data Breaches and Data Loss**

A consequence of these increased cyber threats is the acceleration in frequency and volume of data breaches and data loss. In the first 6 months of 2019 alone, the [Emerging Threat Report from Norton](https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html) outlined that more than 4 billion records were breached.

A loss or breach of data breaches can have significant legal, financial, and reputational implications. IBM now estimates the average cost of a data breach at US$3.92 million in its [latest report](https://www.ibm.com/security/data-breach).

**Avoid Compliance Violations**

We’ve already mentioned how cloud security carries the risk of compliance violations. To demonstrate the implications of non-compliance, you need only observe Germany’s federal privacy watchdog who recently handed 1&1 Telecommunications a €9.55 million fine for violating the [EU’s General Data Protection Regulation (GDPR)](https://kinsta.com/blog/wordpress-gdpr-compliance/).

**Maintaining Business Continuity**

[Good cloud security](https://kinsta.com/blog/managed-wordpress-hosting-in-the-google-cloud/#a-leap-forward-in-hosting-environments) helps maintain your business continuity. Protecting against threats like a denial-of-service attack ([DDoS attack](https://kinsta.com/blog/what-is-a-ddos-attack/)). Unplanned outages and system [downtime](https://kinsta.com/blog/migrate-wordpress-site/) interrupt your business continuity and impact your bottom line. A [Gartner research study](http://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/) estimates this downtime cost at an average of US$5600 per minute.

**Cloud Security Benefits**

Beyond threat protection and avoiding the consequences of poor practice, cloud security offers benefits that make it a **requirement for businesses**. These include:

1. Centralized Security

In the same way cloud computing centralizes applications and data, **cloud security centralizes protection**. Helping you to improve visibility, implement controls, and better protect against attacks. It also improves your business continuity and disaster recovery having it all in one place.

Info

Kinsta offers a [security guarantee](https://kinsta.com/knowledgebase/security-guarantee/) with each plan and, in case something bad happens, security specialists will fix your site.

2. Reduced Cost

A reputable cloud service provider will offer in-built hardware and software dedicated to securing your applications and data around the clock. This eliminates the need for significant financial investment in your own setup.

3. Reduced Administration

Moving to the cloud introduces a shared responsibility model for security. This can provide a significant reduction in the amount of time and resource invested into administering security. The cloud service provider will take on responsibility for securing their infrastructure – and you – across storage, compute, networking, and physical infrastructure.

4. Increased Reliability

A leading cloud service provider will offer cutting edge cloud security hardware and software that you can rely on. You will gain access to a continuous service where your users can securely access data and applications from anywhere, on any device.

**Best Practices for Cloud Security**

When moving your systems to the cloud, many security [processes and best practices remain the same](https://kinsta.com/blog/wordpress-security/). However, you will encounter a new set of challenges that you will be required to overcome in order to maintain the security of your cloud-based systems and data.

To help you with this challenge, we’ve compiled a series of **security best practices for cloud-based deployments**.

[Cloud security is a sub-domain of computer security and, more broadly, information security. Check out these best practices for cloud-based deployments! ☁️🔐CLICK TO TWEET](https://twitter.com/intent/tweet?url=https%3A%2F%2Fbit.ly%2F3eVqCxj&via=kinsta&text=Cloud+security+is+a+sub-domain+of+computer+security+and%2C+more+broadly%2C+information+security.+Check+out+these+best+practices+for+cloud-based+deployments%21+%E2%98%81%EF%B8%8F%F0%9F%94%90&hashtags=security%2Cdata)

**Choose a Trusted Provider**

The foundation of cloud security best practice is built on selecting a trusted service provider. You want to partner with a cloud provider who delivers the best in-built security protocols and conforms to the highest levels of industry best practice.

A service provider who extends a marketplace of partners and solutions to you in order to further enhance the security of your deployment.

The mark of a trusted provider is reflected in the range of security compliance and certifications they hold. Something any good provider will make publicly available. For example, all leading providers like [Amazon Web Services](https://aws.amazon.com/compliance/programs/), [Alibaba Cloud](https://www.alibabacloud.com/trust-center), [Google Cloud](https://cloud.google.com/security/compliance/) (which powers Kinsta), and [Azure](https://azure.microsoft.com/en-gb/overview/trusted-cloud/compliance/) offer transparent access where you can confirm their security compliance and certifications.

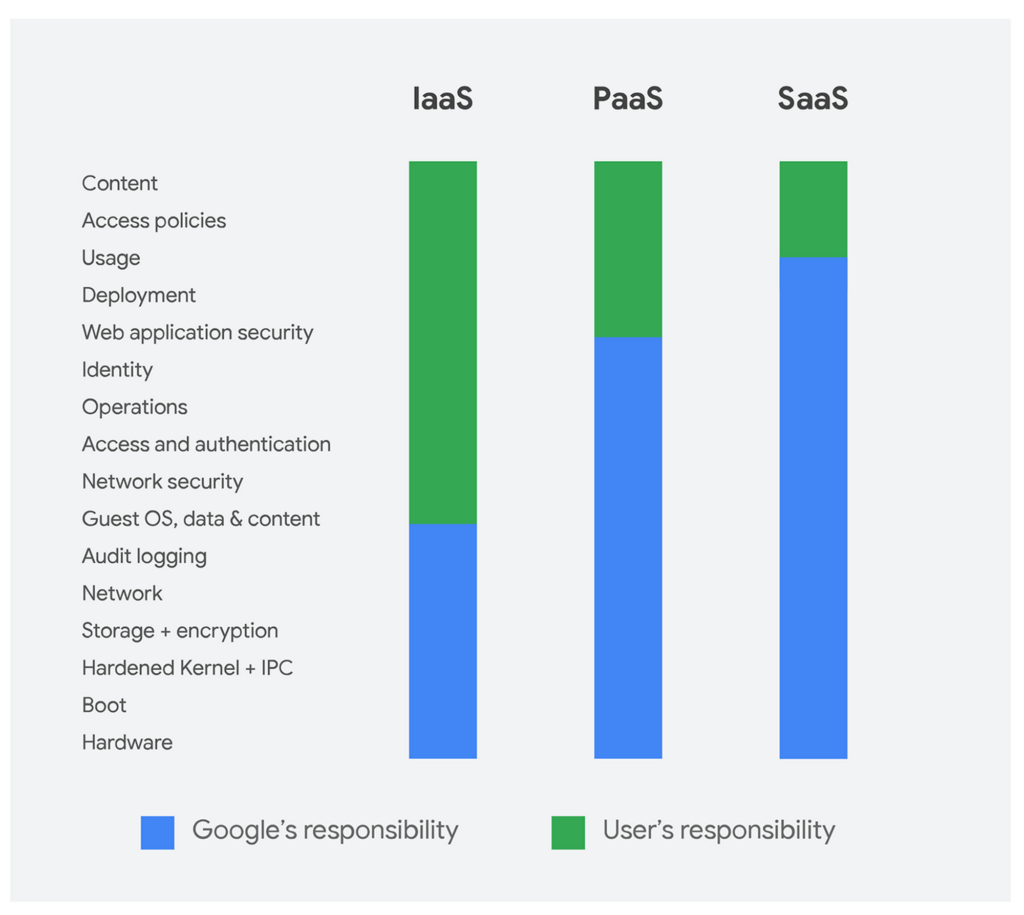
Beyond this, there are many factors that go into selecting a trusted provider. We cover this later in the article with a top 10 checklist for assessing the security of any cloud provider.

**Understand Your Shared Responsibility Model**

When [partnering with a cloud service provider](https://kinsta.com/blog/google-cloud-hosting/), and you move your systems and data to the cloud, you enter into a partnership of shared responsibility for security implementation.

A critical part of best practice involves reviewing and understand your shared responsibility. Discovering which security tasks will remain with you and which tasks will now be handled by the provider.

This is a sliding scale depending on whether you’re opting for Software as a Service ([SaaS](https://kinsta.com/blog/cloud-market-share/#software-as-a-service-saas)), Platform as a Service ([PaaS](https://kinsta.com/blog/what-is-paas/)), Infrastructure as a Service ([IaaS](https://kinsta.com/blog/what-is-iaas/)), or in an on-premises datacenter.

[](https://kinsta.com/wp-content/uploads/2020/01/Google-Cloud-Platform-Shared-Responsibility-Matrix.png)

Google Cloud Platform Shared Responsibility Model

Leading cloud service providers like [AWS](https://aws.amazon.com/compliance/shared-responsibility-model/), [Azure](https://gallery.technet.microsoft.com/Shared-Responsibilities-81d0ff91), [Google Cloud Platform](https://cloud.google.com/blog/products/containers-kubernetes/exploring-container-security-the-shared-responsibility-model-in-gke-container-security-shared-responsibility-model-gke), and [Alibaba Cloud](https://files.alicdn.com/tpsservice/8943876c3b1dd53c97a323659e4f679f.pdf?spm=a2c63.o282931.879956.3.5bbf639dVoklbR&file=8943876c3b1dd53c97a323659e4f679f.pdf) publish what is known as a shared responsibility model for security. Ensuring transparency and clarity. Make sure you review your cloud service providers shared responsibility model.

**Review Your Cloud Provider Contracts and SLAs**

You might not think of reviewing your cloud contracts and SLAs as part of security best practice, you should. SLA and cloud service contracts are only a guarantee of service and recourse in the event of an incident.

There is a lot more included in the terms and conditions, annexes, and appendices that can impact your security. A contract can mean the difference between your cloud service provider being responsible for your data and owning it.

According to the [McAfee 2019 Cloud Adoption and Risk Report](https://www.mcafee.com/enterprise/en-us/solutions/lp/cloud-adoption-risk.html), 62.7% of cloud providers don’t specify that customer data is owned by the customer. This creates a legal grey area where a provider could claim ownership of all your uploaded data.

Check who owns the data and what happens to it if you terminate your services. Also, seek clarity on whether the provider is required to offer visibility into any security events and responses.

If you’re unhappy with elements of the contract, try to negotiate. If any are non-negotiable, you need to determine if agreeing is an acceptable risk to the business. If not, you’ll need to seek out alternative options to mitigate the risk through encryption, monitoring, or even an alternative provider.

**Train Your Users**

Your users are the first line of defense in secure cloud computing. Their knowledge and application of security practices can be the difference between protecting your system or opening a door for cyber attacks.

As a best practice, make sure you train all your users – staff and stakeholders – who access your systems in secure cloud practices. Make them aware of how to spot malware, identify [phishing emails](https://kinsta.com/blog/email-deliverability-manager/), and the risks of insecure practices.

For more advanced users – such as administrators – directly involved in implementing cloud security, consider industry-specific training and certification. You’ll find a series of recommended cloud security certifications and training later in the guide.

**Control User Access**

Implementing tight control of [user access](https://kinsta.com/knowledgebase/mykinsta-user-roles/) through policies is another cloud security best practice. Helping you to manage the users that are attempting to access your cloud services.

You should start from a place of zero trust, only affording users access to the systems and data they require, nothing more. To avoid complexity when implementing policies, create well-defined groups with assigned roles to only grant access to chosen resources. You can then [add users directly to groups](https://kinsta.com/blog/manage-users-hosting-account/), rather than customizing access for each individual user.

**Secure Your User Endpoints**

Another element of cloud security best practice is to secure your user endpoints. The majority of users will access your cloud services through web browsers. It’s therefore critical you introduce advanced client-side security to keep your users’ browsers up-to-date and protected from exploits.

You should also consider implementing an endpoint security solution to protect your end-user devices. Vital with the explosion of [mobile devices](https://kinsta.com/blog/web-design-best-practices/#mobile-responsiveness) and [remote working](https://kinsta.com/blog/working-remotely/), where users are increasingly accessing cloud services through devices not owned by the company.

Look for a solution that includes firewalls, antivirus, and internet security tools, mobile device security, and intrusion detection tools.

**Maintain Visibility of Your Cloud Services**

The use of cloud services can be diverse and fleeting. Many organizations use multiple cloud services across a range of providers and geographies. With research suggesting cloud resources have an average lifespan of 2 hours.

This kind of behavior creates blind spots in your cloud environment. If you can’t see it, you can’t secure it.

Make sure you implement a cloud security solution that offers visibility of your entire ecosystem. You can then monitor and protect cloud usage across all your disparate resources, projects and regions through one single portal. This visibility will help you implement granular security policies and mitigate a wide range of risks.

**Implement Encryption**

[Encryption of your data is a security best practice](https://kinsta.com/knowledgebase/how-ssl-works/) regardless of location, critical once you move to the cloud. Using cloud services, you expose your data to increased risk by storing it on a third-party platform and sending it back and forth between your network and the cloud service.

Ensure you implement the highest levels of encryption for data both in transit and at rest. You should also consider using your own encryption solutions before uploading data to the cloud, using your own encryption keys to maintain full control.

A cloud provider might offer built-in encryption services to protect your data from outside parties, but it affords them access to your encryption keys.

Kinsta operates a [fully encrypted approach](https://kinsta.com/secure-wordpress-hosting/) to further protect its secure WordPress hosting solutions. This means we don’t support FTP connections, only encrypted [SFTP](https://kinsta.com/knowledgebase/how-to-use-sftp/) and [SSH connections](https://kinsta.com/blog/how-to-use-ssh/) (here’s the difference between [FTP and SFTP](https://kinsta.com/knowledgebase/ftp-vs-sftp/)).

**Implement a Strong Password Security Policy**

A strong password security policy is best practice regardless of the service you are accessing. Implementing the strongest policy possible is an important element in preventing unauthorized access.

As a minimum requirement, all passwords should require one upper-case letter, one lower-case letter, one number, one symbol, and a minimum of 14 characters. Enforce that users update their password every 90 days and set it so the system remembers the last 24 passwords.

A password policy like this will stop users from creating simple passwords, across multiple devices, and defend against most brute force attacks.

As an additional layer of security best practice and protection, you should also implement [multi-factor authentication](https://kinsta.com/feature-updates/two-factor-authentication-2fa-mykinsta/). Requiring the user to add two – or more – pieces of evidence to authenticate their identity.

**Use a Cloud Access Security Broker (CASB)**

The use of a CASB is fast becoming a central tool to implement cloud security best practice. It’s software sitting between you and your cloud service provider(s) to extend your security controls into the cloud.

A CASB offers you a sophisticated cloud security toolset to provide visibility of your cloud ecosystem, enforce data security policies, implement threat identification and protection, and maintain compliance.

You can discover more about how a CASB works later in the guide, including a list of the top 5 CASB providers.

**Top 10 Security Checklist Recommendations for Cloud Customers**

When migrating to the cloud and selecting a service provider, one of the most important factors you should consider is security. You’ll be sharing and/or storing company data with your chosen service provider.

You need to be confident your data is secure. There are countless security factors to consider, from shared responsibility to whether the provider’s security standards are up to scratch. This can be a daunting process, especially if you’re not a security expert.

[Security should never be neglected! Get this checklist of the top 10 security aspects when evaluating a cloud service provider 📌🔐CLICK TO TWEET](https://twitter.com/intent/tweet?url=https%3A%2F%2Fbit.ly%2F3eVqCxj&via=kinsta&text=Security+should+never+be+neglected%21+Get+this+checklist+of+the+top+10+security+aspects+when+evaluating+a+cloud+service+provider+%F0%9F%93%8C%F0%9F%94%90&hashtags=security%2Ccloud)

To help we’ve compiled a top 10 security checklist when evaluating a cloud service provider.

1. [Protection of Data in Transit and Data at Rest](https://kinsta.com/blog/cloud-security/#1-protection-of-data-in-transit-and-data-at-rest)
2. [Asset Protection](https://kinsta.com/blog/cloud-security/#2-asset-protection)
3. [Visibility and Control](https://kinsta.com/blog/cloud-security/#3-visibility-and-control)
4. [Trusted Security Marketplace and Partner Network](https://kinsta.com/blog/cloud-security/#4-trusted-security-marketplace-and-partner-network)
5. [Secure User Management](https://kinsta.com/blog/cloud-security/#5-secure-user-management)
6. [Compliance and Security Integration](https://kinsta.com/blog/cloud-security/#6-compliance-and-security-integration)
7. [Identity and Authentication](https://kinsta.com/blog/cloud-security/#7-identity-and-authentication)
8. [Operational Security](https://kinsta.com/blog/cloud-security/#8-operational-security)
9. [Personnel Security](https://kinsta.com/blog/cloud-security/#9-personnel-security)
10. [Secure Use of the Service](https://kinsta.com/blog/cloud-security/#10-secure-use-of-the-service)

**1. Protection of Data in Transit and Data at Rest**

When moving to a cloud service, a key element of security is the protection of data in transit between you (the end-user) and the provider. This is a two-fold responsibility for both you and the provider. You’ll need network protection to prevent the interception of data and encryption to prevent an attacker from reading any data should it be intercepted.

Look for a service provider who offers you a set of tools to [help you easily encrypt your data in transit and at rest](https://kinsta.com/knowledgebase/how-to-install-ssl-certificate/). This will ensure the same level of protection for any internal data transit within the cloud service provider, or transit between the cloud service provider and other services where APIs may be exposed.

**2. Asset Protection**

When selecting a cloud service provider, you need to understand the physical location of where your data is stored, processed and managed. This is especially important following the implementation of government and industry [regulations like GDPR](https://kinsta.com/blog/wordpress-gdpr-compliance/).

To ensure your assets are protected a good provider will have advanced physical protection in their data center to defend your data from unauthorized access. They will also ensure your data assets are erased before any resources are re-provisioned or disposed of to prevent it from falling into the wrong hands.

**3. Visibility and Control**

A key factor in security is the ability to see and control your own data. A good service provider will offer you a solution that provides full visibility of your data and who is accessing it, regardless of where it is and where you are.

Your provider should offer [activity monitoring](https://kinsta.com/blog/wordpress-activity-log/) so you can discover changes to configuration and security across your ecosystem. As well as supporting compliance with the integration of new and existing solutions.

**4. Trusted Security Marketplace and Partner Network**

Securing your cloud deployment will take more than one solution or partner. A good cloud service provider will make it easy for you to find and connect with different partners and solutions through a marketplace.

Look for a provider with a marketplace offering a curated network of [trusted partners with a proven security track record](https://kinsta.com/blog/ddos-attack/). The marketplace should also offer security solutions that provide one-click deployment and are complementary in securing your data whether operating in a public, private, or hybrid cloud deployment.

**5. Secure User Management**

A good cloud service provider will offer tools that enable secure management of users. This will help prevent unauthorized access to management interfaces and procedures to ensure applications, data and resources are not compromised.

The cloud provider should also offer functionality to implement security protocols that separate users and prevent any malicious (or compromised) user affecting the services and data of another.

**6. Compliance and Security Integration**

When considering a cloud service provider, security and compliance go hand in hand. They should meet global compliance requirements that are validated by a third-party organization. You want a cloud service provider who follows industry best practice for cloud security and ideally holds a recognized certification.

The Cloud Security Alliance’s Security, Trust, and Assurance Registry (STAR) program is a good indicator. Also, if you’re operating in a highly regulated industry – where HIPPA, PCI-DSS, and [GDPR](https://kinsta.com/blog/wordpress-gdpr-compliance/) might apply – you’ll also need to identify a provider with industry-specific certification.

To ensure your compliance efforts are both cost-effective and efficient, the cloud service provider should offer you the ability to inherit their security controls into your own compliance and certification programs.

**7. Identity and Authentication**

Your cloud provider should ensure access to any service interface is limited to authorized and authenticated individuals only.

When looking at providers, you want a service offering identity and authentication features including username and password, two-factor authentication, [TLS client certificates](https://kinsta.com/blog/tls-1-3/) and identity federation with your existing identity provider.

You also want the ability to restrict access to a dedicated line, enterprise, or community network. A good provider only delivers authentication through secure channels – [like HTTPS](https://kinsta.com/blog/http-to-https/) – to avoid interception.

Make sure to avoid services with weak authentication practices. This will expose your systems to unauthorized access leading to data theft, changes to your service, or a denial of service. Also avoid authentication over email, HTTP, or telephone.

Top of Form

Bottom of Form

**Want to know how we increased our traffic over 1000%?**

Join 20,000+ others who get our weekly newsletter with insider WordPress tips!

[Subscribe Now](https://kinsta.com/blog/cloud-security/#newsletter)

These are extremely vulnerable to social engineering and interception of identity and authentication credentials.

**8. Operational Security**

When selecting a cloud service, look for a provider who implements strong operational security to detect and prevent attacks. This should cover four core elements:

Configuration and Change Management

You want a provider who offers transparency in the assets that make up the service, including any configurations or dependencies. They should inform you of any changes to the service which might affect security to ensure vulnerabilities don’t occur.

Vulnerability Management

Your provider should have a vulnerability management process to detect and mitigate any new threats to their service. You should be kept informed of these threats, their severity and the planned threat mitigation timeline which includes resolution.

Protective Monitoring

Any provider worth their salt will have advanced monitoring tools to identify any attack, misuse or malfunction of the service. They will take quick and decisive action to address any incidents – keeping you informed of the outcome.

At Kinsta, we pride ourselves on delivering [the highest operational security standards for WordPress hosting](https://kinsta.com/secure-wordpress-hosting/) solutions. This includes implementing the latest security updates, continuous uptime monitoring, [automatic backups](https://kinsta.com/knowledgebase/wordpress-backups/), and active and passive measures to stop any attack in its tracks.

Bottom line: your site is monitored and secured 24/7.

Incident Management

Your ideal provider will have a pre-planned incident management [process in place for common types of attacks](https://kinsta.com/knowledgebase/security-guarantee/). They will be ready to deploy this process in response to any attack.

There will be a clear contact route to you to report any incidents, with an acceptable timescale and format in place.

**9. Personnel Security**

You need a cloud service provider whose personnel you can trust, as they will have access to your systems and data. Your chosen cloud service provider will have a rigorous and transparent security screening process in place.

They should be able to verify their personnel’s identity, right to work, and check for any unspent criminal convictions. Ideally, you want them to conform to your countries locally established screening standard, such as [BS 7858:2019 for the UK](https://standardsdevelopment.bsigroup.com/projects/2018-02194) or completion of [form I-9 in the US](https://www.uscis.gov/i-9).

In addition to screening, you want a service provider who ensures their personnel understand their inherent security responsibilities and undergo regular training. They should also have a policy to minimize the number of people who have access to and can affect your services.

**10. Secure Use of the Service**

You can choose a cloud provider with cutting edge security and still experience a breach through poor use of the service. It’s important to understand where security responsibilities lie when using the service.

Your level of responsibility will be influenced by your cloud deployment model, how you use any services and the built-in features of any individual service.

For example, you have significant security responsibilities with IaaS. Deploying a compute instance, responsibility would fall to you to install a modern operating system, configure security, and ensure ongoing patches and maintenance. The same is true of any application you deploy on that instance.

So, make sure you understand the security requirements of your chosen service and any security configuration options available to you. Ensure you also educate your staff in secure use of your chosen services.

**What is the Cloud Security Alliance?**

When we look at the [cloud computing industry](https://kinsta.com/blog/cloud-market-share/#platform-as-a-service-paas), it’s a disparate market without a central governing body where businesses can go for guidance. This can be frustrating, especially when approaching challenges like cloud security.

Thankfully, in the place of governing bodies, there are a number of organizations that dedicate themselves to supporting the industry. The Cloud Security Alliance is one such organization.

Cloud Security Alliance Logo

The [Cloud Security Alliance (CSA)](https://cloudsecurityalliance.org/) is a non-profit organization dedicated to developing and raising awareness of best practices to maintain a secure cloud computing environment.

It is a membership organization offering the industry cloud-specific security guidance in the form of education, research, events, and products. This guidance is harnessed directly from the combined subject matter expertise of industry practitioners, [associations](https://kinsta.com/blog/wordpress-for-nonprofits/), governments, and the CSA’s individual and corporate members.

To give you a better understanding of the Cloud Security Alliance, let’s take a closer look at how they support the industry.

**Membership**

The CSA is built on the foundation of its members. Joining the CSA as a member opens a range of different benefits depending on whether you’re an individual, enterprise, or solution provider.

Primarily these fall into similar categories including access to their expert network of other members, a seat on the International Standardization Council, discounts on training, and access to exclusive events and webinars

**Assurance**

The CSA has developed one of the most renowned cloud security certification programs: the Security, Trust & Assurance Registry (STAR).

STAR is a provider assurance program providing transparency through self-assessment, third-party auditing, and continuous monitoring against standards. The program comprises of three levels, demonstrating the holder adheres to best practices whilst validating the security of their cloud offerings.

**Education**

To support continual improvement of cloud security in the industry, the CSA offers a range of education services. You can pursue a range of cloud security certifications developed by the CSA, access their knowledge center, and take part in their regularly scheduled educational webinars and events.

**Research**

The CSA continues to support the industry developing and innovating cloud-security best practice through its ongoing research. This is driven by their working groups which now span 30 domains of cloud security.

Most recent and cutting edge include the emergence of working groups for DevSecOps, the Internet of Things, Artificial Intelligence, and Blockchain. The CSA continually publishes its research – free of charge – ensuring the industry can keep up-to-date and informed of the ever-changing nature of cloud security.

**Community**

The CSA also supports the industry by continuing to maintain and develop the cloud security community. They have created and maintain a wide range of communities which allow minds from across the cloud security industry to connect, share knowledge and innovate.

The CSA blog

These growing communities come in many forms. There CSA chapters you can join to connect with local professionals and CSA summits where the best minds share their expertise with the masses. There is even the [CSA blog](https://cloudsecurityalliance.org/blog/) that hosts a community of followers wanting to keep pace with the CSAs practices.

**What is Kaspersky Security Cloud?**

When talking about cloud security, it’s easy to focus on enterprises and forget about the need for individual consumers.

If you’re accessing [cloud services](https://kinsta.com/blog/g-suite/) for your own personal use – photos, [files](https://kinsta.com/blog/saas-products/#8-dropbox), life admin – you need to think about the security of your data: [Kaspersky Security Cloud](https://www.kaspersky.co.uk/security-cloud), the new adaptive cloud-based security solution from Kaspersky.



Kaspersky Security Cloud

Combining the very best features and applications from Kaspersky Lab’s anti-virus software, it creates responsive protection for users’ devices against digital threats.

The platform was designed for individual users, not businesses.

Kaspersky Security Cloud protects your devices against malware and viruses, adding functionality to adapt how you use each device to provide maximum protection at all times. It offers features including antivirus, anti-ransomware, mobile security, [password management](https://kinsta.com/blog/saas-products/#password-management), VPN, parental controls, and a range of privacy tools.

The platform is available on Windows, macOS, Android, and iOS. The Kaspersky Security Cloud Family plan offers protection for up to 20 devices.

**Core Functionality in Kaspersky Security Cloud**

To help you better understand the Kaspersky Security Cloud offering, we’ve taken a closer look at the core functionality within the platform which is split into four sections:

Struggling with downtime and WordPress issues? Kinsta is the hosting solution designed with performance and security in mind! [Check out our plans](https://kinsta.com/plans/?in-article-cta)

Scan

The critical functionality you want from any security solution, Kaspersky Security Cloud can scan your devices and remove any malware or viruses found. You can choose from a number of scanning options including individual files, quick scan, whole system, and scheduled.

Privacy

You can protect your privacy using built-in functionality to check your online accounts to ensure they are not compromised, block your webcam from being accessed, and block website traffic to prevent your browsing activities being monitored.

You can extend your privacy with additional downloads of Kaspersky Secure Connection and Kaspersky Password Manager. Secure Connection encrypts all data you send and receive while also hiding your location, while Password Manager stores and secures your passwords.

Home Network

Home Network gives you the visibility of all devices that are connected to your home network. Identifying those that are protected by Kaspersky Security Cloud. The functionality allows you to be notified when a new device connects and also block any unknown devices.

HD Health

Useful, yet simple, the HD Health functionality gives you a rating of you Hard Drives disk condition and disk temperature. Giving information on error rates, power cycles, power-on hours, total data read, and total data write.

Kaspersky Security Cloud is a great example of how the adoption of cloud services has created the need for new security solutions.

In the next section, we look at a similar example in the enterprise world with the arrival of Cloud Access Security Brokers.

**What is a Cloud Access Security Broker (CASB)?**

A **Cloud Access Security Broker** (CASB) is software that sits between you, the cloud service consumer, and your cloud service provider(s). A CASB extends your security controls from your on-premises infrastructure into the cloud. Helping to enforce security, compliance, and governance policies for your cloud applications. It typically sits on-premises or hosted in the cloud.

Cloud Access Security Broker Model (Image source: Gartner)

A CASB will help you defend against high-level cloud security risks and support ongoing monitoring and mitigation of high-risk events. It does this by securing the data moving between your on-premise and cloud environment using your organization’s security policies.

A CASB will protect you from cyberattacks with malware prevention and secure your data using end-to-end encryption preventing outside users from deciphering the content.

**How does a CASB work?**

A CASB can be deployed in three separate ways: as a [reverse proxy](https://kinsta.com/knowledgebase/reverse-proxy/), forward proxy, or in an ‘API mode’. Each has its own unique advantages and disadvantages, with many industry experts recommending a multimode deployment.

Let’s take a closer look at the different deployment modes of a CASB:

Reverse Proxy

A reverse proxy sits in front of the cloud service, providing inline security capabilities by sitting in the path of the network traffic. The connection of the reverse proxy broker runs from the internet to your application server, hiding information behind it that is coming from the original source.

Forward Proxy

A forward proxy sits in front of the user, with the CASB proxying traffic to multiple cloud platforms. The connection of the forward proxy runs from you, sat behind your firewall, to the internet. Like the reverse proxy, it also provides inline security capabilities.

API Mode

Unlike the proxy deployments, using the Application Program Interface (API) allows for direct integration of the CASB and a cloud service. This allows you to secure both managed and unmanaged traffic.

Depending on the cloud service providers’ API functionality, you can view activity, content, and take enforcement action.

**The Pillars of Functionality in CASBs**

A CASB delivers functionality which falls under four ‘pillars’, these include:

1. Visibility

When a cloud application sits outside the view of your IT department, you create information that is uncontrolled by your business’ governance, risk, and compliance processes.

A CASB gives you visibility of all cloud applications and their usage. Including vital information on who is using the platform, their department, location, and the devices used.

2. Data Security

Using a cloud platform creates an increased risk of inadvertently sharing data with the wrong people. If you’re using cloud storage, a typical data loss prevention (DLP) tool won’t be able to track or control who is accessing your data.

A CASB helps you to enforce data-centric security within a cloud platform combining encryption, tokenization, access control, and information rights management.

3. Threat Protection

One of the most difficult security threats to protect against is your own staff. Even former employees who’ve been disabled from your organization’s core systems may still be able to access cloud apps containing business-critical information.

CASBs allow you to detect and respond to malicious or negligent insider threats, privileged users, and compromised accounts within your cloud infrastructure.

4. Compliance

When your data moves to the cloud, you’ll need to ensure you maintain data security and privacy to comply with industry and governmental regulations. A CASB will do this for you, identifying and enforcing DLP policies on sensitive data in your cloud deployment. Helping you to maintain compliance with regulations including SOX and HIPAA.

A CASB will also help benchmark your cloud security configuration against core regulatory requirements like PCI DSS, NIST, CJIS, MAS and ISO 27001.

**The Top 5 Cloud Access Security Brokers in 2020**

The mass migration of services to the cloud paired with the need to implement cloud security due to the significant risks of data breach and loss has created an explosion in the CASB market.

As a next-generation technology, CASBs have become an essential element of cloud security strategy. With one in five large enterprises uses a CASB to secure or manage their cloud services, according to [Gartner’s “Magic Quadrant for Cloud Access Brokers” report](https://www.gartner.com/doc/reprints?id=1-1XO56V9F&ct=191022&st=sb):

Gartner 2019 Cloud Access Security Broker (CASB) Magic Quadrant

Gartner has identified five the leaders in the CASB market using their ‘Magic Quadrant’, these include:

McAfee

McAfee entered the CASB market in January 2018, with its high profile its acquisition of Skyhigh Networks. Now known as MVISION Cloud, the platform provides coverage across all four CASB pillars for a broad range of cloud services.

The platform provides a comprehensive DLP engine and offers advanced controls including encryption, and tokenization of structured and unstructured data. The CASB can be deployed for API inspection with reverse-proxy-mode capabilities, and forward proxy.

McAfee has also made an on-premises virtual app available for those that require it.

Microsoft

Microsoft’s CASB offering is called Microsoft Cloud Application Security. The platform supports multiple deployment modes including reverse proxy and API connectors. Microsoft continues to develop the CASB solution with enhanced visibility, analytics, data control, and innovative automation functionality.

Microsoft Cloud Application Security also natively integrates with Microsoft’s growing portfolio of security and identity solutions including Azure Active Directory and Microsoft Defender Advanced Threat Protection.

This allows Microsoft to offer customers a fully integrated solution across their Microsoft platforms with single-click deployments.

Netskope

Unlike many players in the space who are simply acquiring CASB solution providers, Netskope remains an independent company. The provider is renowned for excellence in application discovery and SaaS security assessments.

Netskope supports thousands of cloud services through published APIs and inline decoding of unpublished APIs. The CASB offers DLP and identifies threats in real-time using combined threat intelligence, static and dynamic analysis and machine learning-based anomaly detection.

Symantec

Symantec’s CASB offering is called CloudSOC, enhanced in 2016 with the acquisition and integration of Blue Coat Systems’ Perspecsys and Elastica products.

CloudSOC offers DLP using automated data classification and multimode oversight using native cloud APIs, real-time traffic processing, and input from multiple data feeds. You can automatically identify and nullify threats from inside and outside your organization with advanced user behavior analytics (UBA).

Bitglass

Bitglass Cloud Security is referred to as a next-generation CASB, designed to integrate with any app, device, or network.

The platform runs natively from the cloud and is renowned as the only provider securing corporate data on mobile devices without using agents or profiles. Bitglass rose to prominence by introducing a zero-day approach focussed on trust ratings, trust levels and at rest encryption.

**A Look at the Top 10 Cloud Security Certifications in 2021**

To successfully protect your cloud platform, you’re going to need advanced cloud security skills and knowledge. You’ll also need to learn platform-specific skills so you can configure access, network security and ensure data protection all within your chosen cloud provider.

Thankfully, the cloud training and certification market continues to evolve and offer up a number of solutions. You can now choose from a wide range of **platform-specific and vendor-neutral certifications** to help you develop and prove the skills you need. Whether you’re looking to develop foundation knowledge or tailor your skillset to a specific job role, there is a certification for you.

To help in your search, we’ve compiled a list of the **top 10 cloud security certifications** to achieve in 2021.

Earning just one of these certifications will not only help you better secure your cloud deployment, but it’ll also make you more employable, and advance your salary.

**(ISC)2 – Certified Cloud Security Professional (CCSP)**

The [CCSP](https://www.isc2.org/Certifications/CCSP) is a globally recognized cloud security certification aimed at IT and Information Security leaders.

Earning the CCSP demonstrates you have the advanced technical skills and knowledge to design, manage and secure data, applications, and infrastructure in the cloud. You will do this using the best practices, procedures, and policies developed by cybersecurity experts at (ISC)2. The CCSP is ideal if you’re an Enterprise Architect, Systems Engineer, Security Administrator, Architect, Engineer, or Manager.

Before training and attempting the CCSP exam, you’ll need to meet some [strict experience requirements](https://www.isc2.org/Certifications/CCSP/experience-requirements). You’ll need five years full-time experience working in IT, including three years in cybersecurity and one year in one or more of the six domains of the CCSP CBK. You can substitute the experience requirements you hold the equally advanced [(ISC)² CISSP credential](https://www.isc2.org/Certifications/CISSP) – titled ‘The World’s Premier Cyber Security Certification.

**Cloud Security Alliance – Certificate of Cloud Security Knowledge (CCSK)**

The [CCSK certificate](https://cloudsecurityalliance.org/education/ccsk/) is a widely-recognized entry-level certification in cloud security. It was developed by the Cloud Security Alliance, a member organization helping to ensure secure cloud computing environments by defining and raising awareness of industry best practice.

Earning the CCSK certification will prove you have the foundation skills and knowledge required to secure data in the cloud. You’ll learn how to build a baseline of security best practices mapped to a range of responsibilities from configuring technical security controls to cloud governance.

By becoming CCSK certified, you will also meet some prerequisite experience required if you intend to pursue the more advanced CCSP certification from (ISC)².

**AWS Certified Security – Specialty**

The [AWS Certified Security – Speciality](https://aws.amazon.com/certification/certified-security-specialty/) credential is ideal if looking to develop your career working with the AWS cloud platform.

By achieving the AWS Certified Security, you’ll validate your skills across data classifications, encryption methods, secure Internet protocols, and the AWS mechanisms required to implement them.

Working towards the certification, you can choose from a [diverse learning pathway](https://aws.amazon.com/training/path-security/) to shape your knowledge and skills across security fundamentals, architecting and security engineering on AWS. By the end of the pathway, you’ll have developed the control and confidence to securely run applications in the AWS Cloud.

To start working towards the credential, you should be in a security role and have at least two years of hands-on experience securing AWS workloads.

**Microsoft Certified: Azure Security Engineer Associate**

Recently, Microsoft transformed their certification pathways to be role-based. By earning one of their certifications, you are now proving you have the required skills and knowledge to perform a specific job role.

So, earning the [Azure Security Engineer Associate certification](https://docs.microsoft.com/en-us/learn/certifications/azure-security-engineer) shows you have the skills to be a Security Engineer on the Azure Cloud Platform. This includes the ability to protect data, applications, and networks in a cloud environment. Implementing security controls and threat protection as well as managing identity and access.

There are no prerequisite skills requirements before you attempt the AZ-500: Microsoft Azure Security Technologies exam.

**Google Cloud – Professional Cloud Security Engineer**

Earning [Google’s Professional Cloud Security Engineer credential](https://cloud.google.com/certification/cloud-security-engineer) proves you can design, develop, implement, and manage secure infrastructure on the Google Cloud Platform. You’ll do this using Google security technologies aligned to security best practices and industry requirements.

By pursuing the Professional Cloud Security Engineer certification, you’ll need to learn how to configure access, network security and ensure data protection within the Google Cloud Platform. You’ll also need to develop knowledge to ensure compliance and managed operations.

Like the Azure and AWS certifications, this credential is ideal if you’re looking to develop cloud security skills specific to the Google Cloud Platform. Advancing your career with this leading cloud provider.

**Alibaba ACA Cloud Security Certification**

This [ACA Cloud Security certification](https://edu.alibabacloud.com/certification/aca_cloudsecurity) is the first in a certification pathway from Alibaba. Gaining this certification will prove you have the foundation knowledge to apply cloud security principles in an Alibaba cloud deployment.

You’ll develop fundamental skills with Linux and networking operations. While also learning about hosting, application, network and data security solutions all within the Alibaba Cloud Platform. You’ll cover several key security products from Alibaba including Server Guard, WAF, Anit-DDoS basic, and Pro.

After achieving the associate level certification, you can then pursue the Alibaba ACP Cloud Security certification.

**Alibaba ACP Cloud Security Certification**

The [ACP Cloud Security certification](https://edu.alibabacloud.com/certification/acp_security) is the second certification in the Alibaba cloud security pathway. It is a more advanced certification aimed at architects, developers and O&M professionals working with Alibaba Cloud security products.

Building on the foundation skills and knowledge achieved in the ACA Cloud Security certification, you’ll learn about Alibaba Cloud’s core products in security, monitoring, and management.

Once you have achieved the Professional level certification, you can then pursue the Alibaba ACE Cloud Security certification. Though the expert level certification is still in development and is expected to launch soon.

**Cloud Credential Council – Professional Cloud Security Manager Certification (PCS)**

The [CCC Professional Cloud Security Manager credential](https://www.cloudcredential.org/certifications/cloud/pcs/) is an advanced certification from the Cloud Credential Council. It’s ideally suited if you’re a governance and risk professional, auditor compliance specialist, or a cloud computing specialist.

Working towards the certification you will learn the skills and knowledge to apply best practices in a cloud environment for security and governance. Covering key topics like cloud service management, governance, and strategy. You’ll also learn how to design, deploy, and migrate a cloud service in a secure environment.

Due to the advanced nature of the certification, it is recommended you already hold the [CCC Cloud Technology Associate](https://www.cloudcredential.org/certifications/cloud/cta/) and [CCC Cloud Virtualization Essentials](https://www.exin.com/certifications/ccc-cloud-virtualization-essentials-exam) delivered by EXIN.

**Oracle Cloud Platform Identity and Security Management 2019 Certified Associate**

The title of [Oracle’s cloud security certification](https://education.oracle.com/oracle-cloud-platform-identity-and-security-management-2020-specialist/pexam_1Z0-1070-20) is self-explanatory, you will learn about identity and security management on the Oracle Cloud Platform. Ideal if you’re a security professional looking to demonstrate their expertise in implementing cloud solutions.

Preparing for the certification, you’ll cover core security functionality in the Oracle cloud platform. Building knowledge and skills to implement Oracle Identity Cloud Service, Oracle CASB Cloud Service, services Architecture and Deployment, and Identity Security Operations Center Framework

Passing the 1Z0-1070 exam will certify you as an Oracle Certified Associate (OCA), a globally recognized credential. You will validate your capabilities with the Oracle Cloud Security portfolio, including configuration of the services. Before getting started, you’ll need up-to-date and hands-on experience with Cloud Security implementations in an administrator role.

**SANS SEC524: Cloud Security and Risk Fundamentals**

The [SEC524: Cloud Security and Risk Fundamentals](https://www.sans.org/course/cloud-security-fundamentals) is a course, not a certification. I’ve included it regardless as it teaches vital skills and knowledge not covered by the other certifications listed.

Most importantly, you’ll learn how to evaluate the security of different cloud providers. Covering the [cloud computing delivery models – SaaS, PaaS, and IaaS](https://kinsta.com/blog/types-of-cloud-computing/) – and their unique security requirements. As well as additional security considerations when operating in a public, private, or hybrid cloud scenario.

Finishing the course you’ll come away with a range of key abilities. How to assess cloud contracts, adapt security architecture, tools, and processes for use in cloud environments and perform vulnerability assessments of your cloud setup.

[Cloud security is a complex interaction of technologies, processes, and policies. Get to know the top 10 security recommendations for cloud customers (and best practices) ☁️🚨CLICK TO TWEET](https://twitter.com/intent/tweet?url=https%3A%2F%2Fbit.ly%2F3eVqCxj&via=kinsta&text=Cloud+security+is+a+complex+interaction+of+technologies%2C+processes%2C+and+policies.+Get+to+know+the+top+10+security+recommendations+for+cloud+customers+%28and+best+practices%29+%E2%98%81%EF%B8%8F%F0%9F%9A%A8&hashtags=security%2Chosting)

**Summary**

Moving to the cloud, you need to be ready to implement a comprehensive cloud security strategy from day one. This starts with [identifying the right cloud service provider(s)](https://kinsta.com/why-us/) and then implementing a strategy combining the right tools, processes, policies and best practices.

It is fundamental you understand your shared responsibility and focus on compliance.

In cloud security, your staff — or your cloud provider’s — are among the most critical and often overlooked aspects of defense against cybercriminals.

It’s important to remember that cloud computing is no less secure than deploying your services on-premises. In fact, many cloud providers offer [advanced security hardware and software](https://kinsta.com/blog/google-cloud-hosting/#5-state-of-the-art-security) you would otherwise not have access to.

Choosing the right provider will improve your security stance and reduce your risks, regardless of those introduced by cloud computing.

Save time, costs and maximize site performance with:

* Instant help from WordPress hosting experts, 24/7.
* Cloudflare Enterprise integration.
* Global audience reach with 28 data centers worldwide.
* Optimization with our built-in Application Performance Monitoring.

All of that and much more, in one plan with no long-term contracts, assisted migrations, and a 30-day-money-back-guarantee. [Check out our plans](https://kinsta.com/plans/) or [talk to sales](https://kinsta.com/contact-us/) to find the plan that’s right for you.