AWS SECURITY

Secure your cloud transformation

6 security benefits of AWS

The evolving conversation around cloud security

Security will always be top of the agenda in any cloud conversation, but the way we talk about it is changing.

Today, customer concerns have evolved beyond whether or not the cloud is secure: instead, they are asking about the recommended best practices to be secure in the cloud. Customers want to know: What kind of controls are available so I know who is accessing my data and when? How do I access and audit my data so I know I'm in compliance? How can I secure a hybrid cloud environment?

Many customers have already moved critical workloads with confidence knowing that AWS is architected to be the most flexible and secure cloud computing environment available today. These customers have transformed the way they operate so they can focus on their core business—all while making the organization more secure.

The first wave of customers found that security in the cloud was as much a cultural shift as a technological upgrade. They have shared some of the key benefits you should keep in mind when seeking the best way to secure data in the cloud.

As confidence in the public cloud grows, we see that the volume of applications being run on shared infrastructure is also growing. This gives us more and varied use cases that reveal the benefits and best practices for operating securely in the cloud.

51%

51 percent of IT managers said data security is better in the cloud than in their data centers.

58%

58 percent said public cloud was the most secure, flexible, and cost-effective solution for their organizations.[1]

76%

76 percent of companies are rapidly moving their security to the cloud. They're doing away with static, inherently insecure legacy systems in favor of more dynamic, nimble, and integrated cloud and network systems that are secure by design.

[1]SADA systems public cloud survey 2PwC 2021 Global Digital Trust Insights

6 benefits of cloud security

One of the challenges of moving to the cloud is managing multiple stakeholders in an organization with varying levels of enthusiasm for a cloud adoption journey.

Understanding the unique benefits of a secure cloud is the first step toward addressing the concerns of security and compliance professionals within your organization.

A provider who demonstrates these six benefits can help you transform the way you operate, freeing up resources to focus on your core business—all while making your organization more secure.

1. Inherit strong security and compliance controls

2. Scale with enhanced visibility and control

3. Protect your privacy and data

4. Find trusted security partners and solutions

5. Use automation to improve security and save time

6. Continually improve with innovative security features

1.

Inherit strong security and compliance controls

When you're choosing a cloud provider, remember that you'll inherit many of their security controls, strengthening your own compliance and certification programs. If they're the right ones, they can dramatically lower the costs of your security assurance efforts. To ensure you select the right provider, look for third-party validation: internationally recognized security best practices and certifications, as well as industry-specific certifications.

Examples of these controls include internationally recognized security best practices and certifications such as ISO 27001, ISO 27017 for cloud security, ISO 27018 for cloud privacy, ISO 27701 for privacy program management, and SOC 1, SOC 2, and SOC 3. The right provider will also offer services to help you achieve HIPAA or PCI DSS compliance and will have achieved many public sector certifications via FedRAMP and the DoD SRG in the US, C5 in Germany, IRAP in Australia, and MTCS Tier 3 in Singapore. For a full list of certifications and attestations, visit our Compliance Programs page: www.aws.amazon.com/compliance/programs

> ***"The maturity of AWS infrastructure and the level of security audits that AWS performs on its data centers and services gave us peace of mind. We knew that the privacy and security of patient and customer data would be the top priority."***
>
> ***Mark Maalouf, Vice President, Global Digital Health, Teva***

2.

Scale with enhanced visibility and control

The data you store in the cloud isn't out of sight, out of mind. You need to know where it is and who is accessing it at all times. This information should be available in near real time wherever you are, regardless of where in the world your data is stored.

Ensure you have the control you need by looking for key features like fine-grain identity and access controls combined with activity-monitoring services that detect configuration changes and security risks across your ecosystem.

Not only will these controls allow you to reduce risk, but you will also be able to scale your organization more efficiently. Ideally, these cloud-based controls and services will even integrate with your existing solutions to simplify your operations and compliance reporting.

3.

Protect your privacy and data

When you move your data to the cloud, look for a provider who is vigilant about your privacy and offers tools that allow you to easily encrypt your data in transit and at rest to help ensure that only authorized users can access your data.

In addition, when you work with a global cloud infrastructure, you should make sure you can retain complete control over the regions in which your data is physically located. Having control over your data helps you comply with the regional and local data privacy laws and regulations applicable to your organization.

> ***[Using a vendor with a Sydney region] is very important to us from a product performance and a latency perspective. Our customers are in Australia and New Zealand, and data sovereignty was also a concern. We also wanted to use a range of flexible cloud services to optimize the ability of the system to meet customer needs."***
>
> ***Trevor Leybourne, Head of Delivery, Mind Your Own Business***

> ***Our data is hosted in Europe, which is crucial for us from a security perspective. With AWS, we have complete control over where and how data is stored, and who has access to it. This control, along with the extensive encryption, means we feel safe. We know the Trust's data is protected."***
>
> ***Martin Brambley, Director of MSP Sirocco Systems, working with The National Trust UK***

4.

Find trusted security partners and solutions

One of the biggest advantages of working with a leading cloud provider is gaining access to their partners and the cloud security solutions and consulting services that they offer. There are thousands of security technology and consulting services out there, but knowing which ones are right for your particular use case, where to access them, and how to manage those engagements can be hard.

Get started with a partner ›

How can the right cloud security partners help you?

- The right partner will have deep expertise and proven success with your stage in the cloud adoption journey, enabling you to find the right help at the right time. You can also find partners skilled in either hybrid or all-in migrations.
- Use the solutions you already know and trust. Many cloud security partners offer the same tools and services you currently use on-premises, providing a seamless transition to the cloud for your team and your data.
- For highly regulated environments, you can find partners that meet stringent security requirements and have expertise in building, deploying, and managing the types of workloads you wish to migrate to the cloud.
- The right cloud provider will even help you ease billing headaches with “pay as you go” partner pricing and unified billing so you can manage one invoice for all of your cloud spend.

5.

Use automation to improve security and save time

Automating security tasks enables you to be more secure by reducing human configuration errors and giving your team more time to focus on other work that is critical to your business.

You should look for a wide variety of deeply integrated solutions that can be combined to automate tasks in novel ways. This makes it easier for your security team to work closely with developer and operations teams to create and deploy code faster and more securely.

> ***"Migrating to AWS was an important step in creating better delivery velocity for our security applications."***

Jon Barcellona, Cybersecurity Engineering Director, Southwest Airlines

6.

Continually improve with innovative security features

With the right services and tools in the cloud, you can secure your data with greater speed and agility, and your security team can rightly be called an enabler of innovation across the organization.

To achieve this kind of transformation, scale matters. An experienced cloud provider working with millions of customers across the globe should have a team of experienced engineers with deep insights into global trends, giving them remarkable visibility into emerging security challenges. This knowledge, along with customer feedback, should be incorporated back into both their infrastructure and their services. This continual feedback and improvement should enhance core security services like strong identity and access management, detection and monitoring, encryption and key management, network segmentation, and DDoS protection—and everyone benefits.

Next Steps for Cloud Security Success

Security in the cloud is composed of these five areas with some recommended solutions that can help you design and migrate to a cloud architecture with security in mind.

Identity & Access Controls	Identity and access controls are critical to ensuring that only authorized users, groups, or applications can access internal resources. Your provider should give you access to define, enforce, and audit user permissions across services, actions, and resources so that the right people have access to the right resources under the right conditions.	AWS Single Sign-On AWS Identity & Access Management AWS Organizations Amazon Cognito
Detective Controls	Your cloud provider should offer you the visibility you need to spot issues before they impact the business, improve your security posture, and reduce the risk profile of your environment.	AWS Security Hub Amazon GuardDuty AWS CloudTrail Amazon Inspector
Infrastructure Security Clouds	The right infrastructure security controls will enable you to reduce the surface area you need to manage and increase privacy for and control of your overall cloud infrastructure.	AWS Firewall Manager AWS Network Firewall AWS Systems Manager AWS Web Application Firewall (WAF)
Data Protection Controls	You should have access to automatic data encryption and management services, including data management, data security, and encryption key storage.	Amazon Macie AWS Key Management Service AWS Certificate Manager AWS Secrets Manager AWS CloudHSM
Incident Response Controls	Organizations implement mechanisms to respond to and mitigate the potential impact of security incidents to return to a known good state.	Amazon Detective AWS Elastic Disaster Recovery

Learn more in the AWS Well-Architected Security Pillar ›

The paper provides in-depth, best-practice guidance for architecting secure workloads on AWS.