Gain the flexibility and control you need to build on the cloud with confidence

AWS puts security at the heart of everything to help you fully realize the promise of the cloud. Custom-built for the cloud, AWS infrastructure meets the most stringent security requirements in the world and provides 24x7 monitoring to ensure the confidentiality, integrity, and availability of your data.

AWS builds high-level security into the datacenter and network architecture, while giving you a choice on how you want to secure the services running on top of it. The nature of this shared model provides the flexibility and control you need to build on the cloud with confidence.

Free up your resources to focus on growing and innovating faster by building with AWS cloud security.

Secure Device as a Service with Becrypt and AWS

The Device as a Service model allows you to safely de-couple End User Device Management from core business activities, enabling valued resources to focus on higher-value tasks.

Becrypt's Secure DaaS platform, developed in collaboration with UK Government, has been designed for organisations that face elevated cyber threats. The combination of AWS and Becrypt security controls allows the adoption of a Zero Trust Architecture as part of cloud migration. Device identity and health measurements combine with existing user access control, to ensure the scale, flexibility and cost benefits of cloud are delivered with increased organisational cyber resilience.

AWS security transforms the way you do business

Inherit the Most Comprehensive Security and Compliance Controls

AWS supports more security standards and compliance certifications than any other offering, including PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171.
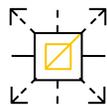
Scale Securely with Superior Visibility and Control

Fine-grain identity and access controls combined with continuous monitoring ensures that the right resources have the right access to right data at all times even as you grow.

Build with the Highest Standards for Privacy and Data Security

We provide tools that allow you to easily encrypt your data in transit and at rest using keys managed by AWS Key Management System (KMS) or CloudHSM (FIPS 140-2 Level 3 validated HSMs).

Automate and Reduce Risk with Deeply Integrated Services

Reduce configuration errors and free up IT to focus on business-critical tasks by using AWS deeply integrated solutions, like machine learning, to automate security tasks in novel ways.
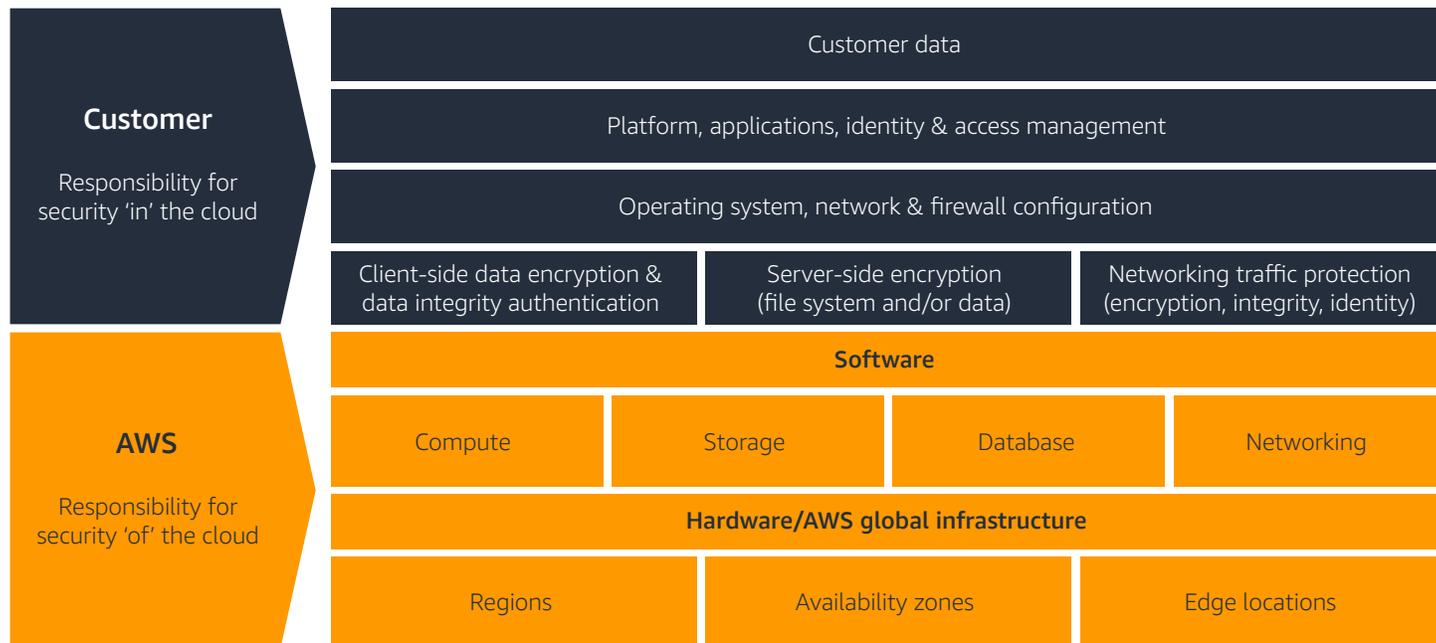
De-couple endpoint management from core business

Reduce IT infrastructure costs and significantly increase cyber resilience with an AWS-hosted Device as a Service, automating device identity and health measurements to support migration to a Zero Trust Architecture.

The Shared Responsibility Model maps your end-to-end security

The Shared Responsibility Model (SRM) makes it easy to understand your role in protecting your unique AWS environment. Choose from the many cloud-ready software solutions to meet the highest standards of data security in the cloud.

Customer

Responsibility for security 'in' the cloud

| Customer data |
| Platform, applications, identity & access management |
| Operating system, network & firewall configuration |

| Client-side data encryption & data integrity authentication | Server-side encryption (file system and/or data) | Networking traffic protection (encryption, integrity, identity) |

AWS

Responsibility for security 'of' the cloud

Software			
Compute	Storage	Database	Networking
Hardware/AWS global infrastructure			
Regions	Availability zones	Edge locations	

Partner Call to Action

We help organisations safely migrate to cloud services. Our Secure DaaS platform 'Paradox Edge' allows for either fully outsourced endpoint management, or simply reducing inhouse endpoint support costs, while increasing cyber resilience through a Zero Trust model with device health and identity management.

We offer a managed cloud security monitoring platform, and consultancy services.

AWS Resources

https://www.becrypt.com/uk/services/paradox-edge/

Additional information

https://aws.amazon.com/compliance/shared-responsibility-model/