AWS Services to SOC 2 Principles - Mapping Table

AWS Service	SOC 2 Principle	Control Purpose
IAM	Logical Access	Manage user permissions and enforce security policie
S3	Data Confidentiality	Control bucket access and enable encryption
CloudTrail	Audit & Monitoring	Log API activity across the environment
Security Groups	Network Restrictions	Restrict inbound/outbound access to instances
KMS	Encryption Key Management	Manage and rotate encryption keys securely
GuardDuty	Threat Detection	Detect malicious or unauthorized behavior
CloudWatch	Monitoring & Alerting	Track performance and trigger alerts
AWS Config	Configuration Management	Audit configuration changes over time
VPC Flow Logs	Traffic Monitoring	Capture IP traffic details for network interfaces
EC2	Data Protection	Encrypt instance volumes and manage access
Security Hub	Vulnerability Management	Aggregate and review security findings
Backup	Data Retention	Ensure regular backups and snapshot policies