# Comparison of AWS Security Services

Yuvraj

| Service | Description | Key Features | Primary Use Case |
|---|---|---|---|
| Amazon Cognito | Provides user identity and authentication management for web and mobile apps. | User sign-up/sign-in, Multi-Factor Authentication (MFA), and social login integration. | User authentication and identity management. |
| Amazon Detective | Helps identify the root cause of potential security issues by analyzing and visualizing AWS account activities. | Security investigation, Visualized security data, Automated analysis. | Security investigation and forensic analysis. |
| Amazon GuardDuty | Threat detection service that continuously monitors for malicious or unauthorized behavior in AWS environments. | Real-time threat detection, AI-driven analysis, CloudTrail, VPC Flow Logs, and DNS Logs integration. | Threat detection and monitoring. |
| Amazon Inspector | Automates security assessments to improve the security and compliance of applications deployed on AWS. | Vulnerability management, Automated security assessments, EC2 and container scanning. | Vulnerability scanning and compliance checks. |
| Amazon Macie | A fully managed data security and privacy service that uses ML to discover and protect sensitive data, such as personally identifiable information (PII). | Sensitive data discovery, Data classification, ML-driven insights, Automated data protection policies. | Protecting sensitive data and ensuring privacy compliance. |
| Amazon Security Lake | Centralized security data lake for storing, analyzing, and acting on security data. | Security event storage, Integration with security analytics tools, Supports multiple data formats. | Centralized security data management and analysis. |
| Amazon Verified Permissions | Provides a managed authorization service that helps build fine-grained access control into applications. | Fine-grained access control, Policy-based permissions management, Integration with AWS services and apps. | Authorization management and access control in applications. |
| AWS Artifact | A repository of compliance reports and agreements that provide evidence of AWS's security and compliance. | Access to security compliance reports, Regulatory compliance, Exportable compliance reports. | Compliance management and audit reporting. |
| AWS Audit Manager | Simplifies auditing by automating evidence collection and helping you continuously audit your AWS usage. | Automated evidence collection, Framework-based audits, Integration with AWS services. | Continuous compliance and audit readiness. |
| AWS Certificate Manager | Manages the creation, deployment, and renewal of SSL/TLS certificates for use with AWS services. | Automated certificate provisioning, Certificate renewal, Public and private certificates. | SSL/TLS certificate management. |
| AWS CloudHSM | Offers hardware security module (HSM) appliances in the AWS Cloud to provide secure key storage and cryptographic operations. | Dedicated HSM appliances, Secure key storage, Cryptographic operations. | Cryptographic operations and key management. |

*Continued on next page*

| Service | Description | Key Features | Primary Use Case |
|---|---|---|---|
| AWS Directory Service | Enables the use of managed Microsoft Active Directory in the AWS Cloud, or integrates with existing on-premises directories. | Active Directory support, Single Sign-On (SSO), LDAP integration. | Identity management and directory services. |
| AWS Firewall Manager | A security management service to centrally configure and manage firewall rules across your accounts and applications. | Centralized firewall management, Integration with AWS WAF and AWS Shield, Policy enforcement. | Firewall management across AWS accounts and resources. |
| AWS Identity and Access Management (IAM) | Enables secure control of access to AWS services and resources for users, groups, and roles. | Granular access control, Role-based access, MFA, and policy management. | Identity and access control for AWS services. |
| AWS Key Management Service (KMS) | Managed service that enables the creation and control of encryption keys used to encrypt data across AWS services and applications. | Key creation and management, Integration with AWS services, Audit and monitoring capabilities. | Data encryption and key management. |
| AWS Network Firewall | Provides scalable and flexible network protection across VPCs. | Stateful and stateless rules, VPC traffic filtering, Centralized management with AWS Firewall Manager. | Network-level security and traffic control. |
| AWS Resource Access Manager (RAM) | Enables sharing of AWS resources across AWS accounts within an organization. | Resource sharing, Centralized access control, Multi-account support. | Cross-account resource sharing within AWS Organizations. |
| AWS Secrets Manager | Helps manage, retrieve, and rotate database credentials, API keys, and other secrets. | Secret rotation, Secure secret storage, Access management. | Managing and storing secrets securely. |
| AWS Security Hub | A security service that provides a comprehensive view of your AWS security posture and helps you automate security checks. | Security alerts, Centralized security management, Integration with GuardDuty, Inspector, Macie, etc. | Centralized security monitoring and management. |
| AWS Shield | Provides DDoS protection to safeguard applications running on AWS. | DDoS attack protection, AWS WAF integration, 24/7 monitoring. | Protection against DDoS attacks. |
| AWS IAM Identity Center | Successor of AWS SSO, enables centralized management of access to AWS accounts and applications. | SSO, Multi-account access control, Centralized identity management. | Centralized access management across multiple AWS accounts. |
| AWS WAF | A web application firewall that helps protect your applications from common web exploits. | Web traffic filtering, Rule-based access control, Integration with CloudFront and Application Load Balancer. | Protecting web applications from attacks. |
| AWS WAF Captcha | A feature of AWS WAF that adds CAPTCHA challenges to web traffic to verify that the access is legitimate. | CAPTCHA-based challenge, Prevents automated bots, Integration with AWS WAF. | Preventing bot-based web traffic attacks. |