perplexity

What security features distinguish each cloud platform for enterprise use

To distinguish the security features of the major cloud platforms—AWS, Azure, and Google Cloud—for enterprise use, consider how each addresses identity, data protection, threat detection, and compliance.

AWS (Amazon Web Services)

- **Identity & Access Management:** AWS Identity and Access Management (IAM) for fine-grained access; supports SSO and MFA; AWS Organizations for multi-account management.
- **Data Encryption:** Default encryption at rest and in transit for S3, EBS, RDS, and more; AWS Key Management Service (KMS) and Hardware Security Module (CloudHSM) for key control.
- **Threat Detection:** Amazon GuardDuty (threat detection), AWS Security Hub (centralized security view), Amazon Inspector (vulnerability scanning), and AWS Macie (data loss prevention).
- **Network Security:** Built-in firewalls, VPC isolation, DDoS mitigation via AWS Shield and WAF, VPC flow logs for network monitoring.
- **Logging & Monitoring:** AWS CloudTrail (API activity logging), CloudWatch (operational logs), Security Lake (centralizes security data for analytics).
- **Compliance:** Hundreds of certifications (PCI, HIPAA, GDPR, FedRAMP, ISO/IEC etc.), automated compliance checks via AWS Config and Audit Manager[1] [2] [3] [4].

Microsoft Azure

- **Identity & Access:** Microsoft Entra ID (formerly Azure AD) with risk-based conditional access, SSO, MFA, and Identity Protection with machine learning for risky sign-in detection[5].
- **Data Protection:** Azure Key Vault (HSM-secured keys/secrets storage), always-on encryption for rest/transit/memory (Azure confidential computing), Transparent Data Encryption for databases[6].
- **Threat Detection & Response:** Azure Security Center and Microsoft Defender for Cloud—threat detection, vulnerability management, and compliance dashboard; built-in DDoS Protection[7] [6].
- **Network Security:** Azure Firewall, application gateway, web application firewall (WAF), private endpoints, and robust network segmentation.

- **Antimalware & Endpoint:** Microsoft Antimalware and integrated external antimalware for VMs.
- **Compliance:** Over 100+ compliance certifications, industry-specific blueprints, and automated policy enforcement[6] [8].

Google Cloud Platform (GCP)

- **Identity & Access:** IAM for detailed role assignment, service accounts, and robust multi-factor authentication (MFA); Zero-Trust security model (BeyondCorp Enterprise).
- **Encryption:** Default encryption at rest and in transit, customer-managed encryption keys, Confidential Computing for encrypting use-state data.
- **Threat Detection & Security Analytics:** Security Command Center (central oversight), anomaly detection, Cloud Audit Logging for tracking activity, Access Transparency logs for auditing Google employee actions.
- **Network Security:** VPC firewalls, DDoS protection with Cloud Armor, Web Risk API for active threat blocking.
- **Endpoint & Operations:** Endpoint Verification, device compliance enforcement, and Security Operations Suite for incident response[9] [10] [11] [12].
- **Compliance:** Comprehensive global certifications, regular third-party audits, and continuous monitoring for regulatory requirements.

Summary Table

Security Domain	AWS	Azure	GCP
Identity Management	IAM, SSO, MFA	Entra ID, risk-based policies, MFA	IAM, service accounts, Zero-Trust
Data Encryption	KMS, CloudHSM, encryption at rest/in-transit	Key Vault, confidential computing, TDE	Default encryption, CMEK, confidential compute
Threat Detection	GuardDuty, Security Hub, CloudTrail	Defender for Cloud, Security Center	Security Command Center, audit logs
Network Security	VPC, AWS WAF, Shield (DDoS)	Firewall, WAF, DDoS Protection	VPC, Firewall, Cloud Armor
Compliance	143+ certifications, automated checks	100+ certifications, blueprint policies	Broad, global compliance, audit logs

Takeaway:

- **AWS** excels in breadth and maturity, with the most extensive service integration and fine-grained controls.
- **Azure** stands out for enterprise identity management and hybrid integration, plus strong confidential computing.
- **GCP** is recognized for security analytics, zero-trust design, and always-on encryption.

All three maintain enterprise-grade multilayer security, but the best fit often depends on existing enterprise tools, compliance, and technical ecosystem[1] [5] [10] [6] [11] [12].

⁂

1. https://aws.amazon.com/products/security/
2. https://www.aquasec.com/cloud-native-academy/cspm/aws-cloud-security/
3. https://www.digitalguardian.com/blog/what-aws-security
4. https://www.upwind.io/glossary/aws-security-explained
5. https://www.sentra.io/blog/azure-security-tools
6. https://learn.microsoft.com/en-us/azure/security/fundamentals/overview
7. https://netcentrix.com/news/security-in-the-cloud-microsoft-azure-security-features/
8. https://learn.microsoft.com/en-us/azure/security/fundamentals/technical-capabilities
9. https://www.geeksforgeeks.org/ethical-hacking/what-is-gcpgoogle-cloud-platform-security/
10. https://www.darktrace.com/cyber-ai-glossary/top-security-best-practices-for-google-cloud-platform-gcp
11. https://www.exabeam.com/explainers/google-security-operations/google-cloud-security-8-key-components-and-critical-best-practices/
12. https://cloudfresh.com/en/blog/10-google-cloud-platform-security-practices/