AWS Zero Trust Architecture

DLT A TECH DATA COMPANY | aws partner network

Bridge Your Current IT Infrastructure to a Zero Trust Future with AWS

About AWS

In 2006, Amazon Web Services (AWS) began offering IT infrastructure services to businesses in the form of web services — now known as cloud computing. A key benefit of cloud computing is replacement of high capital infrastructure expenses with low variable costs that scale with IT needs.

AWS Cloud allows customers to scale and innovate, while maintaining a secure environment and paying only for services used. This enables security at a lower cost than in an on-premises environment. AWS customers inherit all the best practices of AWS policies, architecture, and operational processes while leveraging AWS services to meet their obligations under the shared responsibility model.

Built for Zero Trust since its inception, AWS cloud offerings continue to provide scalable, secure architectures.

How AWS Fits into Zero Trust Architecture

AWS believes that in the Zero Trust security model access to data should rely on multiple criteria, not just network location. Users and systems must prove their identity and trustworthiness and meet fine-grained identity-based authorization rules to access applications, data, and systems. The AWS Zero Trust architecture uses identity to reduce surface area, eliminate unnecessary data pathways, and provide straightforward security.

Because AWS was built from the ground up using the Zero Trust security principles, its myriad of services incorporate security in every component of DLT's Zero Trust architecture:

- **Network Architecture, Monitoring, Access Control**
- **Automated Response**
- **Threat Intelligence**
- **Visibility**
- **Data Protection**
- **Application Security**
- **Identity and Access Management**

DLT 2411 Dulles Corner Park, Suite 800, Herndon, VA 20171 **Main** 800.262.4358 **eFax** 703.709.8450

Coverage	Zero Trust Architecture
Network Architecture, Monitoring, Access Control	• GuardDuty – Intelligent threat detection in the AWS network • Shield – DDoS protection for applications running on AWS • WAF – AWS Web Application Firewall for consistent traffic patterns • Firewall Manager – Centralized firewall and security management • VPC – Network building block of AWS with multiple security layers • Direct Connect – A dedicated fiber-optic connection directly into the AWS network • Site-to-Site VPN – A secure logical connection between on-premises networks and AWS
Automated Response	• Detective – Machine learning-integrated service for root cause analysis and remediation • GuardDuty – Automated remediation in response to identified threats • CloudWatch Anomaly Detection
Threat Intelligence	• Detective – Analysis layer for potential security issues • GuardDuty – Comprehensive intelligence feeds from AWS and third-party tools • CloudWatch Anomaly Detection
Visibility	• Detective – Integrated visualizations for proactive investigations and security findings • Athena – Detailed analysis of security logs with SQL querying • VPC Flow Logs – Monitor all traffic in the VPC
Data Protection	• Macie – Detect and protect sensitive data at scale • Key Management Service – Fully integrated encryption management • Cloud HSM – Dedicated hardware-based encryption on AWS • Certificate Manager – SSL/TLS certificates with hooks into AWS resources for easy in-transit encryption • Secrets Manager – Protect and rotate credentials across the stack
Application Security	• Inspector – Security assessment for AWS-deployed applications • WAF – Protect web applications and APIs against vulnerabilities • Cognito – Application-integrated authentication • Resource Manager – secure resource sharing across accounts during development
Identity and Access Management	• IAM – Least privilege access management across AWS • Single Sign-On (SSO) – Central AWS identity management • Directory Service – Fully managed Active Directory with continuous authorization • Cognito – Federation with enterprise identity integration • Resource Manager – secure resource sharing across accounts during development

About DLT Solutions

DLT Solutions is the premier government solutions aggregator that specializes in understanding the cloud needs of the federal, state, local and education markets. Contact cloud-sales@dlt.com for more information on AWS products and services, and visit www.dlt.com/zerotrust for more information on Zero-Trust architecture.

DLT 2411 Dulles Corner Park, Suite 800, Herndon, VA 20171 **Main** 800.262.4358 **eFax** 703.709.8450