Zero Key Management for AWS Cloud

Eliminate Risk Classes | Accelerate Cloud Security | Unlock Compliance at Scale with Eclypses MTE

Preface: A New Era of Cloud Security on AWS

As enterprises accelerate their migration to AWS, the pressure to secure sensitive data—without slowing innovation—is greater than ever. While AWS offers robust encryption and key management services, these tools still rely on a vulnerable architecture: encryption keys.

Keys must be stored, rotated, and protected—creating entire classes of risk: key theft, misuse, insider threats, session hijacking, and more.

Eclypses MicroToken Exchange (MTE) eliminates these risk classes entirely by replacing data with non-reversible, one-time-use microtokens—removing the need for keys altogether.

This document details how MTE helps organizations eliminate key-driven vulnerabilities across AWS services—delivering HyperSecure, HyperEfficient, and HyperScalable solutions across cloud, web, mobile, and AI ecosystems.

The AWS Key Management Problem: Risk by Design

Even with AWS-native tools like KMS and Secrets Manager, traditional encryption introduces systemic risk:

- **Encryption Key Exposure** – If keys are accessed or leaked, so is your data.
- **Insider Threats** – Admins and root accounts often retain access to key material.
- **Session Hijacking & Replay** – Encrypted traffic and tokens can be intercepted and reused.
- **Operational Drag** – Key rotation, audits, and storage slow performance and inflate cost.
- **Compliance Overhead** – Key audits and access logs are mandatory under HIPAA, PCI, GDPR, and FedRAMP.

The MTE Solution:

Eliminate Risk Classes with Zero Key Management

Eclypses MTE removes entire categories of cloud risk by eliminating the need for keys altogether. Instead of encrypting data, MTE replaces it with single-use, non-deterministic microtokens that have zero value outside the authorized session.

- **No Keys to Steal, Rotate, or Misuse**
- **No Data to Exfiltrate** – Microtokens are meaningless if intercepted
- **Resilient Even on Compromised Devices**
- **Works Across AWS Lambda, EC2, EKS, S3, and Amplify**
- **Eliminates Risk Classes** – ATO, replay, credential theft, insider misuse, session hijacking

Zero Key Management for AWS Cloud

Eliminate Risk Classes | Accelerate Cloud Security | Unlock Compliance at Scale with Eclypses MTE

Risk Elimination Matrix – Traditional vs. MTE on AWS

Risk Class	With AWS Traditional Encryption	With MTE on AWS
Key Theft / Exposure	X Keys must be protected	No keys used or stored
Credential Replay	X Session tokens can be reused	Microtokens are one-time use only
Insider Threat / Privileged Access	X Admin access to key material	Tokens expire instantly—no access
API Replay Attacks	X APIs protected by static keys	No reusable data or tokens
Session Hijacking	X Risk via MITM or reverse proxy	Tokenized streams can't be reused
Data Exfiltration (in transit)	X Encrypted but recoverable	Tokenized—no usable data
Mobile/Web Reverse Engineering	X API keys often exposed in client	No static keys stored on device

AWS Services Overview: Traditional vs. MTE

AWS Service	With Traditional Security	With MTE Zero Key Security
AWS KMS / Secrets Manager	X Requires secure key rotation & IAM	No keys to store, audit, or manage
Amazon API Gateway	X API keys & tokens exposed in headers	Microtokenized payloads eliminate static tokens
EKS & ECS Microservices	X Secrets injection & encrypted volumes needed	Stateless tokenization—no secrets or policies required
S3 Buckets / Data Lakes	X Bucket encryption dependent on KMS & IAM	Tokenize data pre-storage—no valuable data inside S3
AWS Amplify (Web & Mobile)	X Requires encrypted tokens and secure storage	No credential reuse—MTE removes static app secrets
SageMaker / AI Pipelines	X Risk of training/ inference data leaks	Tokenized inputs/outputs protect data & IP in motion

Zero Key Management for AWS Cloud

Eliminate Risk Classes | Accelerate Cloud Security | Unlock Compliance at Scale with Eclypses MTE

AWS Use Cases: Risk Classes Eliminated

Tokenized API Communications

→ Eliminate API key theft, payload replay, and credential misuse

Secure Kubernetes on EKS

→ Remove dependency on secrets, vaults, and encrypted sidecars

S3 File Protection

→ Store tokenized versions of sensitive data—nothing to exfiltrate

AI/ML Pipeline Security on SageMaker

→ Prevent training data exposure and model inference leakage

Zero-Trust Web & Mobile Apps via AWS Amplify

→ Stop reverse engineering, hijacking, and static key injection

Business & Compliance Benefits

1. →**Eliminates Entire Classes of Cloud Risk**
2. →**Reduces TCO** – No HSMs, no vaults, no rotation logic
3. →**Enhances Performance** – No encryption overhead
4. →**Simplifies Compliance** – No encryption key audit trails (HIPAA, PCI DSS, FIPS 140-3, GDPR)
5. →**Protects Web & Mobile by Default** – App-layer security with no secrets on device
6. →**AWS-Native Compatibility** – Works across all AWS compute, API, and data services