



# Protecting Cloud Data in the AI age

## A Better Way to Secure Your Data for the Quantum Era

### Where Conventional Controls Stop

Data has been encrypted in motion since the 1980s, shielding sensitive information as it moves between users and systems. Despite modest upgrades to these tools, modern computing power now makes data vulnerable to interception and decryption across any network.

Eclipses' patented Micro Token Exchange (MTE<sup>®</sup>) eliminates today's risks to data in transit, delivering robust, future-proof security, operational simplicity with rapid integration — particularly applicable in containerised architectures, critical and sensitive industries, and for organisations prioritising zero trust strategies.

MTE<sup>®</sup> can be deployed as a gateway for API-scale infrastructures, a secure Kubernetes layer for agile DevOps environments, or as paired Relays to protect data exchange across any network from the application layer. MTE<sup>®</sup> turns application security into a simply configured utility for your AWS estate with zero-key management.

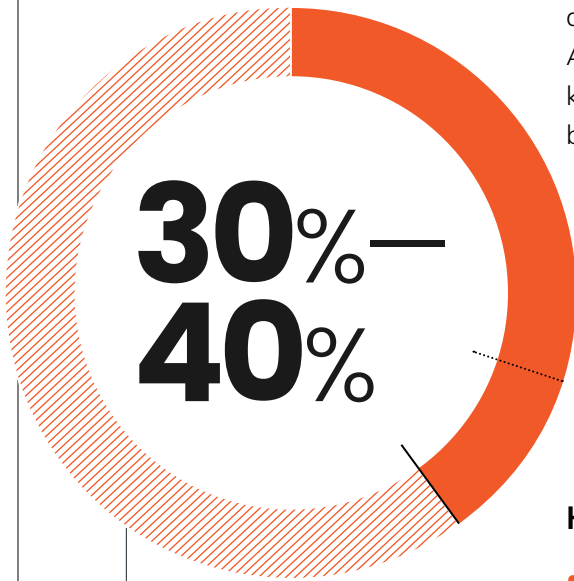
### How Eclipses Works & Strategic Scope

Through its involvement in the AWS Global Startup Program, Eclipses MTE<sup>®</sup> turns data protection in transit into a utility for the AI age.

Eclipses defines the new standard for data protection across hyper-scale infrastructures by embedding continuous, quantum-resistant encryption



When you can't trust the network, you have to be able to trust your data



of AI/API traffic is malicious; wasting compute power & scraping protected information

Source: Eclipses

directly within the data. MTE® protects data in motion between machines, APIs or application users, utilising ephemeral and constantly rotating keys from the quantum-resistant Crystals-Kyber algorithm patented by NIST, and a unique endpoint pairing process — in a combination of post-quantum encryption and tokenisation, without any need for key distribution or lifecycle management.

Only the intended receiver can transform the tokens back into the original data, keeping sensitive information safe from malicious adversaries and rogue bots while it is being transmitted across any network without reliance on network layer security controls across internal or external connections.

### Here's how it works:

- Senders and receivers connect through a secure, private channel — no keys to exchange, no certificates to manage.
- Each message is transformed into a stream of one-time tokens that only the intended receiver can read.
- The receiver seamlessly rebuilds the data and delivers it to the right application — all without touching or changing your existing systems.

## Use Cases

Real-world scenarios where MTE adds value by protecting sensitive data during application processes that traditional security tools do not fully cover.

### 1 API & Payments

**Problem:** Payment fields are exposed during transit. Sensitive details, such as account numbers, can be at risk if attackers intercept the data in transit.

**MTE Solution:** MTE turns every piece of sensitive data into a unique, single-use token. Even if someone intercepts the account numbers, they only get a useless token, not the real payment

### 2 Kubernetes / Service-to-Service

**Problem:** Unknown and untrusted routes often exist between microservices in cloud environments. These paths are vulnerable, and attackers can try to access sensitive information as it moves from one microservice to another.

**MTE Solution:** MTE secures these internal communications by exchanging sensitive messages for secure tokens. The result is very low added latency (less than 3ms) and a significant reduction in possible breach fallout.

### 3 Healthcare & Regulated Data

**Problem:** Protected health information (PHI) and personally identifiable information (PII) are particularly vulnerable when being transferred between services. The law requires more than standard data safeguards.

**MTE Solution:** MTE protects this information by replacing each sensitive field with a token during transit. This ensures that intercepted data is unreadable, reducing legal liability for failure to protect patient data and simplifying audit and compliance obligations.

Even with the innovative PQC-powered tokenisation, it's still essential to use regular security measures (like strong authentication, robust passwords, and network protections) alongside Eclipses MTE, which works **with** other security controls to elevate the overall data protection posture, not to replace them.

## Adoption Path & Buying Motion

Adopting MTE is a straightforward process designed to help put strong data protection in place quickly, without needing to rebuild systems from scratch. Here's how it's done:

### 1 Decide where you need protection

**A** Use MTE Relay Server if you want to protect communication between users and servers (like website logins or payments).

**B** Use MTE API Relay if you've got different services or apps inside your system talking to each other and want those messages protected, too.

### 2 Pick the right mode for your data

**A** Standard MTE is for secrets (like passwords) or IDs. This keeps small, important stuff safe.

**B** FLEN (Fixed-Length Encoding) makes all messages the same size, so hackers can't guess what's inside based on length.

**C** MKE (Managed Key Encryption) is for sending big files or lots of information securely across any network.

### 3 Set up secure places to store token info

Use tools like Redis or ElastiCache. They track the moving parts and keep everything safe.

### 4 Always keep TLS (Transport Layer Security) on

Maintain a robust defence in depth strategy with network layer controls.

### 5 Test MTE out

Start with a small pilot and build on that. Try it on a few test cases to prove the value of deployment across your AWS estate.

### 6 Buy and finish setup

**A** Buy MTE through AWS Marketplace (Amazon's online place for business software).

**B** Accept a Private Offer (a special deal designed just for you).



## Experience the power of Eclipses MTE firsthand.

[Request your AWS Private Offer](#)

**Request your AWS Private Offer**, book a 30-minute architecture fit session, and watch Adam's 10-minute technical walkthrough to see how easy and effective MTE is for securing your data in transit.

