Protecting a Fintech Company from Ransomware with Eclypses MTE (Technical Deep Dive)

Technical Overview of the Ransomware Threat

Attack Scenario

FinTrust, a fintech company, suffers a ransomware attack via a compromised third-party API in its payment processing system. The attack follows these steps:

1. **Initial Breach**:
   - Attackers exploit an API vulnerability to gain unauthorized access.
   - API credentials are compromised, allowing deeper infiltration.
2. **Lateral Movement & Data Exfiltration:**
   - Attackers move laterally, accessing cloud databases containing financial data.
   - Transaction records, user PII, and account details are exfiltrated.
3. **Encryption & Extortion:**
   - Ransomware encrypts customer data, preventing FinTrust from accessing its own financial records.
   - Attackers demand payment in exchange for decryption keys and threaten to leak exfiltrated data.

How Eclypses MTE Prevents Ransomware Damage

Data Tokenization at the Application Layer

Unlike traditional encryption, which stores and transmits raw data that can be decrypted by attackers, Eclypses MTE replaces sensitive data with single-use, non-reversible microtokens before it ever leaves the application.

- **Data is tokenized at the application layer before reaching the network or storage.**
- **Microtokens have no exploitable value, even if exfiltrated.**
- **No stored encryption keys, making decryption attacks ineffective**

Mitigating Credential Theft & API Attacks

Traditional Weakness: Attackers often target API credentials to gain access to backend systems.

MTE Defense:

- Attackers exploit an API vulnerability to gain unauthorized access.
- API credentials are compromised, allowing deeper infiltration.

Stopping Ransomware Encryption Attacks

Traditional Weakness: Ransomware encrypts files, making them inaccessible to the company.

MTE Defense:

- The actual data is never sent or communicated in the channel.
- Encrypting microtokens ensures the data is meaningless because they do not contain readable financial data.
- Utilizing MTE instantly removes access to the data in transit without the need for ransom payments.

Protecting a Fintech Company from Ransomware with Eclypses MTE (Technical Deep Dive)

Deployment & Integration of Eclypses MTE in FinTrust

Application-Level Implementation

- **FinTrust embeds MTE Mobile and MTE Web SDKs** in its fintech applications.
- **Tokenization occurs before data is transmitted to APIs, databases, or external processors.**
- **All sensitive data fields are replaced with microtokens, preventing exposure.**

Backend Security with MTE Relay Server

- **MTE Relay Server (deployed via AWS Marketplace)** integrates with FinTrust's cloud infrastructure.
- **Synchronizes microtokenized requests across all internal services.**
- **No changes to client-side application logic, ensuring seamless deployment.**

Securing API Transactions

- **API calls are verified at the endpoint level** using MTE authentication.
- **Requests lacking valid microtokens are rejected,** preventing unauthorized API usage.
- **Sensitive transaction data (card details, PII) is tokenized before it enters FinTrust's system.**

Technical Response to a Ransomware Attempt

Attack Phase	Traditional Outcome	With Eclypses MTE
API Breach	Credentials are stolen, giving attackers deep system access.	Stolen API keys are useless without valid MTE synchronization.
Data Exfiltration	Customer records are leaked and sold on the dark web.	Exfiltrated microtokens hold no value to attackers.
Ransomware Encryption	Business operations are halted until the ransom is paid.	Encrypted microtokens remain useless; FinTrust restores backups instantly.
Extortion Attempt	Attackers demand ransom, threatening to leak data.	No real financial data was exposed, eliminating leverage.

Protecting a Fintech Company from Ransomware with Eclypses MTE (Technical Deep Dive)

Business & Security Benefits of MTE Deployment

100% Elimination of Exposed Sensitive Data –
Ensures that no actual financial data can be stolen.

Prevention of API Credential Abuse –
Protects API transactions from misuse by attackers.

Seamless PCI DSS & GDPR Compliance –
Eliminates data exposure, reducing compliance burdens.

Rapid Deployment with Minimal Disruption –
MTE integrates without requiring a full system overhaul.

Future-Proof Security –
MTE is quantum-resistant, preventing future cryptographic threats.

Conclusion: A Proactive Approach to Ransomware Defense

By integrating Eclypses MTE, FinTrust eliminates the core vulnerabilities exploited by ransomware attacks. Unlike reactive cybersecurity tools, MTE ensures that even if attackers gain access, they cannot **steal, encrypt, or extort sensitive financial data.**

No Data Exposure | No Ransom Payments | No Business Disruption

Contact us today to deploy Eclypses MTE and future-proof your security strategy.