ECLYPSES API USE CASE

API Security: Unlock Confidence at the Edge

A Breakdown from Eclypses CIO, Jefferson Dance

What is API Security?

1. An Application Programming Interface (API) allows software applications to interact with each other. It is a fundamental part of modern software patterns, such as microservices architectures.
2. API security is the process of protecting APIs from attacks. Because APIs are very commonly used and enable access to sensitive software functions and data, they are becoming a primary target for attackers.
3. API security is a key component of modern web application security. APIs may have vulnerabilities like broken authentication and authorization, lack of rate limiting, and code injection.

Businesses use APIs to connect services and transfer data at the edge of their data ecosystems and operations. A compromised, exposed, or hacked API can expose personal data, financial information, or other sensitive data. Therefore, security is a critical consideration when designing, developing, and deploying RESTful and other APIs.

APIs are vulnerable to security weaknesses in backend systems. If attackers compromise the API provider, they can potentially compromise all API data and functionality. APIs can also be exploited via malicious requests if the API is not properly coded and protected. Sophisticated attackers can inject malicious code to perform unauthorized operations or compromise the backend.

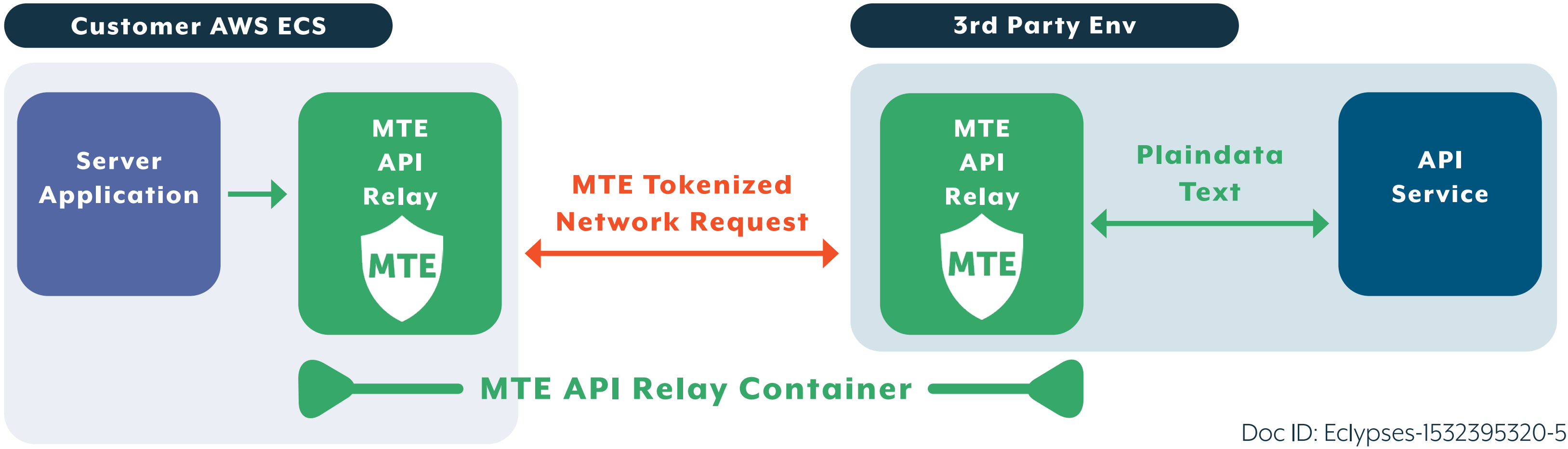
With the popularity of microservices and serverless architectures, every enterprise application depends on APIs for their basic functionality. With the mass adoption of generative AI, APIs are more vital than ever, as they act as a key component to AI operations. Without secure APIs there is no AI. Securing these data end points is critical.

74% of reported data breaches in the past two years were API-related.. 60% reported a data breach in the past two years. Of these, 74% had at least 3 API-related breaches. Alarmingly, 40% had five or more, and 11% faced over seven, stressing the dire need for enhanced API security.

How does Eclypses MTE help organizations secure APIs, secure data, set policy, and improve security while sharing data both internally and with third parties?

Eclypses MTE allows organizations to set Eclypses MTE as a policy across an organization and third parties in APIs for internal sharing and for consumption of data by third parties. No matter where your data flows, your key asset is protected with no third-party reliance or attack vector that can leave you on the hook for reputation and material impacts. Eclypses MTE enables an organization to treat risk across 8 of the 10 OWSAP top API threat vectors and protection, and improve and maintain compliance with DORA for European operations, while simultaneously improving confidentiality, integrity, and availability with a FIPS 140-3 validated and certified data security product.

MTE Relay Server seamlessly integrates with AWS, enhancing security without disrupting your existing setup. It provides end-to-end data protection, ensuring integrity, immutability, and confidentiality across all web transfers. Additionally, it aligns with industry regulations, helping meet compliance requirements and reduce the risk of data breaches, making it a comprehensive solution for bolstering application security and compliance.



Doc ID: Eclypses-1532395320-501
Version No.: 4.0

ECLYPSES API USE CASE

Personal endorsement from

Adam McElroy, *Head of Cyber Security, Bank of Ireland*

“Eclypses delivers an innovative and unique approach to data security, without the implementation burden of complex, heritage crypto solutions.

The simplicity of their deployment model significantly streamlines the change management required in mature, enterprise environments - and has the inherent flexibility to onboard additional users and add new channels and endpoints. The MTE toolkits provide a lightweight approach which can be effectively applied to mobile and other IoT devices, in addition to typical productivity platforms.(SaaS, AI etc.).

Eclypses’ focus on discrete data exchange across the cloud is particularly relevant to secure 3rd party information exchange and the requirements of DORA and other global compliance frameworks, effectively simplifying adoption across the supply chain whilst maintaining ownership & corporate control.

As the industry prepares for potential compromise scenarios from post-quantum crypto exploits, the ability to increase data security from Eclypses is a clear front runner to enhance and embed a pervasive data security model across the business.”

ECLYPSES API USE CASE

API Security

Open Worldwide Application Security Project (OWASP) Top 10 API Vulnerabilities

Eclypses MTE mitigates 80% of the OWASP top 10 API vulnerabilities and data risk:

Risk	Description	Mitigated by MTE
API1:2023 - Broken Object Level Authorization	APIs tend to expose endpoints that handle object identifiers, creating a wide attack surface of Object Level Access Control issues. Object level authorization checks should be considered in every function that accesses a data source using an ID from the user.	Yes
API2:2023 - Broken Authentication	Authentication mechanisms are often implemented incorrectly, allowing attackers to compromise authentication tokens or to exploit implementation flaws to assume other user's identities temporarily or permanently. Compromising a system's ability to identify the client/user, compromises API security overall.	Yes
API3:2023 - Broken Object Property Level Authorization	This category combines API3:2019 Excessive Data Exposure and API6:2019 - Mass Assignment, focusing on the root cause: the lack of or improper authorization validation at the object property level. This leads to information exposure or manipulation by unauthorized parties.	Yes
API4:2023 - Unrestricted Resource Consumption	Satisfying API requests requires resources such as network bandwidth, CPU, memory, and storage. Other resources such as emails/SMS/phone calls or biometrics validation are made available by service providers via API integrations, and paid for per request. Successful attacks can lead to Denial of Service or an increase of operational costs.	Yes
API5:2023 - Broken Function Level Authorization	Complex access control policies with different hierarchies, groups, and roles, and an unclear separation between administrative and regular functions, tend to lead to authorization flaws. By exploiting these issues, attackers can gain access to other users' resources and/or administrative functions.	Yes
API6:2023 - Unrestricted Access to Sensitive Business Flows	APIs vulnerable to this risk expose a business flow - such as buying a ticket, or posting a comment - without compensating for how the functionality could harm the business if used excessively in an automated manner. This doesn't necessarily come from implementation bugs.	Yes
API7:2023 - Server Side Request Forgery	Server-Side Request Forgery (SSRF) flaws can occur when an API is fetching a remote resource without validating the user-supplied URI. This enables an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall or a VPN.	Yes
API8:2023 - Security Misconfiguration	APIs and the systems supporting them typically contain complex configurations, meant to make the APIs more customizable. Software and DevOps engineers can miss these configurations, or don't follow security best practices when it comes to configuration, opening the door for different types of attacks.	No
API9:2023 - Improper Inventory Management	APIs tend to expose more endpoints than traditional web applications, making proper and updated documentation highly important. A proper inventory of hosts and deployed API versions also are important to mitigate issues such as deprecated API versions and exposed debug endpoints.	Yes
API10:2023 - Unsafe Consumption of APIs	Developers tend to trust data received from third-party APIs more than user input, and so tend to adopt weaker security standards. In order to compromise APIs, attackers go after integrated third-party services instead of trying to compromise the target API directly.	No

ECLYPSES API USE CASE

API Security

MTE and the 2023 OWASP API top 10

API1:2023 Broken Object Level Authorization

Object level authorization is an access control mechanism that is usually implemented at the code level to validate that a user can only access the objects that they should have permissions to access.

How Eclypses MTE Helps

If an API request comes from a non-MTE protected source with an altered identification property (even if that identifier is a query parm), that request will be rejected at its source. It will never reach the API.

API2:2023 Broken Authentication

Authentication endpoints and flows are assets that need to be protected. Additionally, "Forgot password / reset password" should be treated the same way as authentication mechanisms.

How Eclypses MTE Helps

In a microservice architecture, if MTE protects the originator and the receiver, then the channel is completely protected. Only "paired" endpoints can communicate. Any other attempt to call an API from a non-paired endpoint will fail.

API3:2023 Broken Object Property Level Authorization

When allowing a user to access an object using an API endpoint, it is important to validate that the user has access to the specific object properties they are trying to access.

How Eclypses MTE Helps

MTE protects the entire http communication into an API from another API. However, if the application does not properly authorize access to a specific data domain, that is an issue in the application design. MTE can assure that the incoming request is secure, but it cannot ensure that the underlying application invokes data domain security.

API6:2023 Unrestricted Access to Sensitive Business Flows

When creating an API Endpoint, it is important to understand which business flow it exposes. Some business flows are more sensitive than others, in the sense that excessive access to them may harm the business.

How Eclypses MTE Helps

MTE ensures that only authorized and paired endpoints can access an API. Any attempt from a rogue endpoint will be rejected because the API will not be able to accept the request.

API7:2023 Server Side Request Forgery

Server-Side Request Forgery (SSRF) flaws occur when an API is fetching a remote resource without validating the user-supplied URL. It enables an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall or a VPN.

How Eclypses MTE Helps

The use of MTE in API-to-API calls ensures that only authorized and authenticated communication channels can work together. Therefore, if a request comes from an external source (or an unintended source) it will be rejected. The MTE Relay protects all aspects of an incoming API request – the route, the query, and the payload.

API8:2023 Security Misconfiguration

Attackers will often attempt to find unpatched flaws, common endpoints, services running with insecure default configurations, or unprotected files and directories to gain unauthorized access or knowledge of the system. Most of this is public knowledge and exploits may be available.

How Eclypses MTE Helps

This is a procedural / infrastructure issue that is not applicable to what MTE can mitigate.

API9:2023 Improper Inventory Management

The sprawled and connected nature of APIs and modern applications brings new challenges. It is important for organizations not only to have a good understanding and visibility of their own APIs and API endpoints, but also how the APIs are storing or sharing data with external third parties.

How Eclypses MTE Helps

Using MTE Relay in an existing, legacy environment ensures that only the proper communication paths will work. Outdated APIs should be placed under the protection of MTE Relay and will require no API changes. Inventorying all existing API's is a daunting task, yet adding the MTE Relay into the mix reduces the chance that data-related exploits into the legacy API are possible.

API10:2023 Unsafe Consumption of APIs

Developers tend to trust data received from third-party APIs more than user input. This is especially true for APIs offered by well-known companies. Because of that, developers tend to adopt weaker security standards, for instance, in regards to input validation and sanitization.

How Eclypses MTE Helps

MTE must be deployed by both the sending application and the receiving API. If the customer does not have access to the receiving API, MTE will not help in this case.

API Security: Unlock Confidence at the Edge

Eclypses MTE and API Security

When an organization sets Eclypses MTE as a policy, they unlock significant benefits and business outcomes:

1. **Immediate and Effective** – Eclypses MTE is efficient and optimized. Treat in days what previously took months or even years. Improve data security at your edge where you acquire and exchange data immediately! Saving time, capital, and the need for added resources.
2. **Improving Compliance** – improve your security posture and compliance in an easy to implement cost effective manner. A focused solution right at the asset that matters the most: THE DATA!
3. **De-Risk your Data** – multiple penetration tests, FIPS 140-3 validation and certification. Eclypses MTE allows your data to move securely wherever it needs to go. Without the ability to access your API's, access credentials, or confidential data, your business can operate smoothly, without the risk or worry of having to wonder if your data can be breached and the financial headaches that come with it.
4. **Improved Operations** –Eclypses MTE seamlessly integrates with all modern enterprise security operations and logging platforms. No longer does a security incident have to become a breach; Eclypses MTE secures the data even if there is an exploitable operating system or application-level vulnerability.
5. **Data Integrity** – Eclypses MTE allows organizations to ensure that all data generated or consumed by the API is verified and secure. Our unique data verification process does not allow data to be processed that is not validated. In any model, you get the cleanest, purest, data from your applications. Eclypses MTE will drop any packets foreign to it, allowing your data sets to be usable faster, with guaranteed integrity.