tAM

Feature list

the API Middleware

The API Middleware provides a direct plug and play box for securing API communications. It Logs, Secures, and even redacts information during transmission

AI-Based Classification
tAM leverages AI-driven algorithms to classify APIs in real-time. And make a recognizable patterns for each API category making it easy to detect anomalies in traffic or queries from the endpoints.

Unique

Parameter Tracking
tAM continuously tracks API parameters for both requests and responses, ensuring every key-value pair transmitted is logged, validated, and monitored. This allows organizations to gain insights into data flow and enforce strict policies on parameter behavior, such as rejecting unauthorized or malicious inputs. Parameter tracking also aids in detecting anomalies like SQL injection attempts or unusual data patterns.

Unique

Response Alteration
With tAM, API responses can be dynamically altered based on customizable policies. Sensitive data fields (e.g., SSNs, credit card numbers) can be redacted, masked, or replaced with placeholder values to prevent unauthorized exposure. These transformations are performed seamlessly, ensuring data protection while maintaining the usability of the API.

Only we can do

Data Leak Prevention (DLP)
tAM acts as a robust DLP solution for APIs, scanning all data exchanges to identify and block unauthorized data exfiltration attempts. Policies based on regular expressions and keyword lists ensure that sensitive data is never exposed, even in edge cases or zero-day vulnerabilities. This functionality protects intellectual property, PII, and other critical assets during API communications.

Only we can do

Feature list

the API Middleware

Advanced Query-Based Analytics
tAM provides a powerful analytics module, allowing users to query API logs and events with granular precision. Administrators can track API usage trends, detect unusual patterns, and gain insights into API performance. The analytics engine supports advanced filters, such as searching logs by user, endpoint, response times, or even specific parameter values.

Only we can do

End-to-End Logging
Every API interaction is logged end-to-end, capturing request and response headers, payloads, timestamps, and metadata. Logs are stored securely and are indexed for fast retrieval, enabling comprehensive auditing and troubleshooting. This feature ensures complete traceability, helping organizations detect security incidents or compliance violations quickly.

Unique

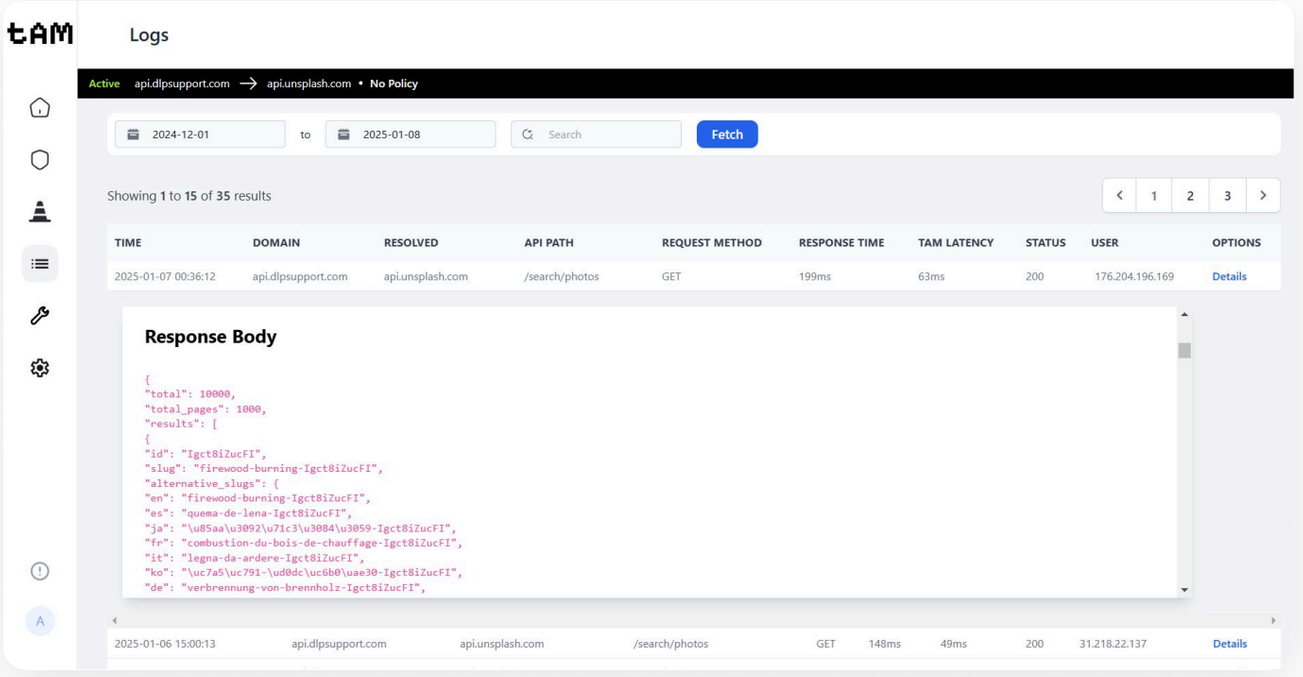
Blacklisting & Whitelisting
tAM enables administrators to define blacklists and whitelists for Methods & URLs. Whitelisting ensures only authorized APIs are accessed, while blacklisting blocks malicious actors or unwanted traffic in real-time. This dual mechanism enhances security by preventing misuse while maintaining operational flexibility.

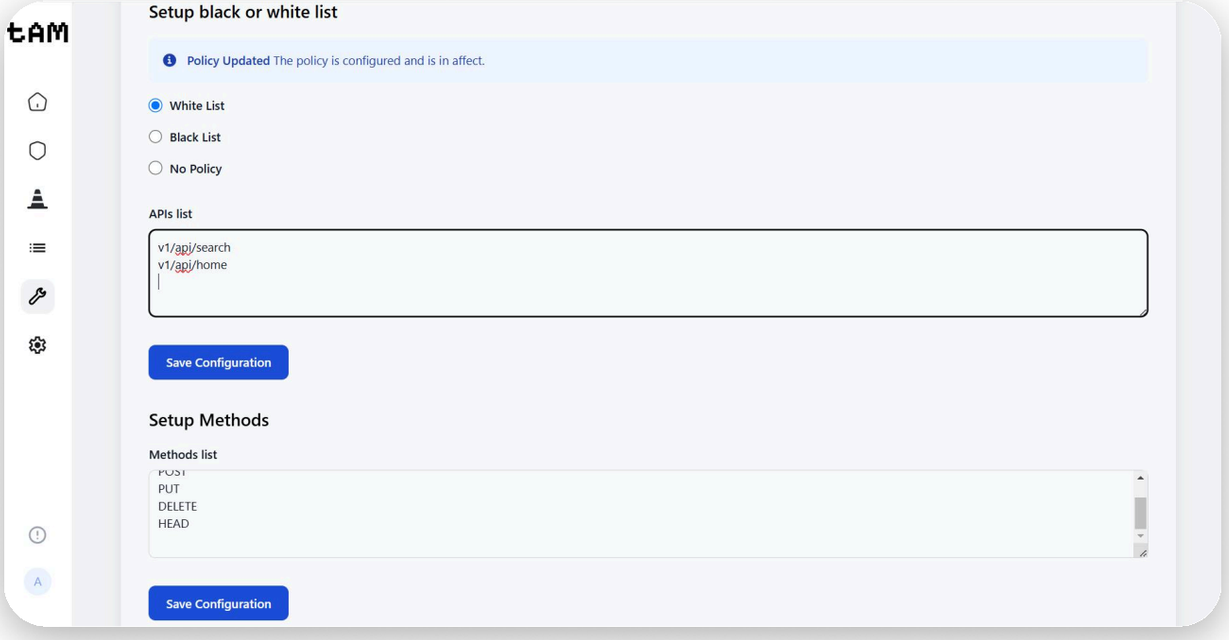
Rate Limiting
Out of the box Administrators can set custom thresholds for API calls, such as the number of requests per second or per user, to prevent abuse (e.g., denial-of-service attacks). Dynamic rate limiting adjusts limits based on traffic patterns, ensuring optimal performance during peak loads.

Alerts - Downloads & Integrations (SIEMs)
tAM offers real-time alerts for critical events, such as unusual volumes, transmission of sensitive information, or policy violations. These alerts can be integrated with Security Information and Event Management (SIEM) platforms for centralized monitoring. Customizable alert thresholds and notification channels ensure administrators are promptly informed of potential threats.

Feature list

the API Middleware





Feature list

the API Middleware