APIFORT Platform

AI-Driven API & AI Security Platform

One Platform. Complete API & AI Security.

Core Components

API Security

API Discovery & Classification
Identify and classify APIs automatically through passive traffic analysis.

Runtime Threat Detection
Monitor live API and AI traffic to identify active attacks, abuse attempts, policy violations, and security incidents in real time.

AI-Powered Behavioral Analytics
Apply AI-powered behavioral analysis to identify anomalies, suspicious behaviors, and emerging risks.

Sensitive Data Control
Prevent sensitive information leakage through masking and policy-based protection mechanisms.

Security Analytics & Observability
Provide centralized dashboards, monitoring insights, and attack visibility across environments.

Threat Intelligence Integration
Leverage continuously updated attack intelligence to improve detection accuracy and response effectiveness.

SIEM & SOC Integration
Integrate with existing security operations workflows for alerting, correlation, and incident management.

AI Security

AI Prompt & Content Protection
Inspect AI interactions to block malicious prompts and unauthorized content manipulation attempts.

AI Red Teaming
Continuously test AI systems against realistic attack scenarios to uncover weaknesses and improve resilience.

API Pentest

Automated API Pentesting
Continuously validate API security posture with safe and automated penetration testing.

At a Glance

Secure APIs, AI applications, and critical data flows through a centralized security ecosystem designed for modern digital infrastructures.

The APIFORT Platform combines advanced API security, AI firewall capabilities, and continuous security testing to help organizations gain visibility, reduce attack surfaces, and strengthen cyber resilience across the entire application lifecycle.
Integrated platform components: **API Security, AI Security, API Pentest**

Provides passive API discovery, real-time traffic monitoring, behavioral analysis, and threat detection without affecting production environments

API Security

Secures enterprise AI and LLM interactions against prompt injection, jailbreak attempts, unsafe prompts, and sensitive data exposure.

AI Security

Delivers automated and continuous API security testing to identify vulnerabilities and validate remediation efforts.

API Pentest

KEY BENEFITS

- Faster Detection
- Security Intelligence
- Shadow API Visibility
- Compliance Readiness
- Secure AI Adoption
- Automated Validation
- Full Visibility
- SOC & DevSecOps Collaboration

WHY APIFORT PLATFORM?

- **Single Platform Architecture:** Manage API security, AI protection, and security validation from a unified operational layer.
- **Modern Threat Coverage:** Protect against evolving API attacks and emerging AI-driven threats using adaptive security controls.
- **Continuous Security Lifecycle:** Enable continuous discovery, monitoring, testing, and improvement across digital services.
- **Operational Efficiency:** Reduce tool fragmentation and simplify security operations with centralized management and integrations.
- **Enterprise-Ready Deployment:** Support scalable deployments with low-latency analysis and production-safe monitoring capabilities.