Radware API Security Service

Background

APIs are the backbone of digital transformation, powering modern applications and enabling seamless connectivity across cloud, mobile and third-party platforms. As organizations accelerate innovation, the attack surface expands, making these less-protected and less-monitored APIs prime targets for sophisticated cyberthreats and compliance risks. Despite this urgency, more than 94% of organizations still lack proper API documentation and complete visibility into their APIs.

The democratization of generative AI tools has given attackers a significant edge over organizations. They use AI to map out application API infrastructures and business logic, then launch sophisticated business logic attacks that fly under the radar by abusing legitimate API workflows.

Many API posture management and testing tools rely on static analysis or disconnected telemetry from code scans, software bills of materials (SBOMs) or logs. This results in delayed and incomplete insights into real-world API behavior. Runtime protection solutions also have their limits, providing threat detection and blocking, but no visibility into configuration risks, sensitive data exposure or systemic posture weaknesses. This disconnect leaves organizations with blind spots across the API lifecycle and creates operational silos between development, security and operations teams

Radware's Solution

Radware's API Security solution is purpose-built to tackle today's API security challenges by delivering automated API discovery, runtime posture management, contextual testing and runtime protection—all within a single pane of glass. It bridges the gaps and eliminates silos between the teams responsible for documenting and managing APIs and those tasked with securing them, ensuring seamless collaboration and comprehensive coverage.

By analyzing live production traffic, our solution provides deep visibility into how APIs are configured, exposed, and used without requiring developer instrumentation or pipeline integration. This unified runtime approach empowers your organization to strengthen API security, streamline operations and safeguard your business while maintaining regulatory compliance.

5 Key Challenges in API Security

1. **Visibility & Control:** Many organizations lack full documentation and monitoring of all of their APIs—including third-party and shadow APIs—creating security blind spots.
2. **Expanding Attack Surface:** Attackers often bypass traditional security controls, targeting APIs through embedded attacks, business logic abuse, bots and HTTP DDoS.
3. **Operational Complexity:** Managing multiple-point solutions and keeping pace with rapid API development increases cost and complexity, especially in regulated industries like financial services and healthcare.
4. **Compliance & Risk:** Regulatory mandates (e.g., PCI DSS 4, NIS2, DORA) require robust API protection, including business logic attack (BLA) mitigation and supply chain security.
5. **Data Sensitivity and Overexposure:** Data risks often go unnoticed until it's too late. These could include limited visibility into APIs connected to misconfigured databases that expose sensitive data in traffic, weak authentication headers or inconsistent policy enforcement.

Inside Radware's End-to-End API Security Solution

Empower your organization to innovate safely and confidently. Radware's API Security solution delivers comprehensive API discovery and management, complete runtime protection, contextual testing, and runtime posture management. It helps you stay ahead of threats, compliance requirements and operational complexity.

Radware API Security Service

API Discovery and Management

Gain a comprehensive view of your API catalog and enable your teams to quickly identify trends, anomalies, and application issues. Key capabilities include:

- Complete, Continuous and Automated API Discovery – Covers all endpoints and parameters, including third-party, outdated, shadow and deprecated APIs.
- API Catalog Metrics and Lifecycle Management – Manages catalog configurations as per comprehensive key API performance indicators.
- Business Logic Sequence Explorer – Maps the application's business workflow and dependencies between API calls.
- Performance, Usage and Security Metrics – Unifies API telemetry for holistic visibility and identification of potential performance and security issues.

Complete Runtime API Protection

Against Embedded Attacks:

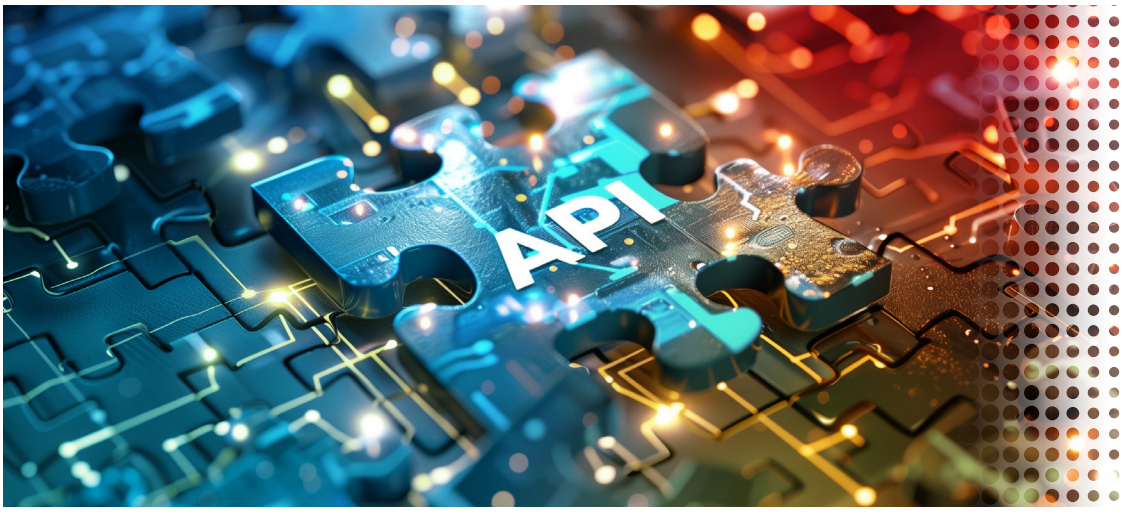
From client certificate authentication and token authorization control to real-time mitigation of embedded API attacks, Radware ensures robust protection.

Against Business Logic Attacks:

Radware provides AI-driven, continuous auto-mapping and analysis of application workflows and auto-generation of business-logic security rules that continuously and automatically adapt to accommodate any changes to the application's business logic. This one-of-a-kind technology ensures real-time detection, alerting and mitigation of sophisticated business logic attacks.

Against HTTP DDoS Attacks:

When it comes to protecting API endpoints against HTTP floods, traditional methods like rate limiting and geo-blocking are ineffective. Radware's industry-leading DDoS protection fills this gap with a unique AI-driven, behavioral-based approach that distinguishes between legitimate and malicious traffic. It automatically generates granular signatures in real-time to effectively and accurately block any type of HTTP DDoS attack on your API-based applications.



Runtime API Posture Management

Radware's Runtime Security Posture gives you a real-time, high-fidelity view of your API security risks based on the only source of truth that matters: your production traffic.

Why it matters: Most security tools focus on pre-deployment scans or code-level issues. But what happens after your APIs are in production?

Radware inspects the behavior of your applications in the wild.
It highlights:

- **Where sensitive data is leaking** (PII in URLs, tokens in headers)
- **Where security policies are broken or missing** (CORS, HSTS, cookie settings)
- **Where authentication and authorization controls are weak or misconfigured**

All insights are based on actual runtime behavior, not theoretical risk.

Radware Runtime Security Posture Management provides coverage of operational, configuration and policy-layer risks, which are only detectable from live HTTP traffic and are invisible to traditional code scanners or log-based ASPM tools. Radware runtime posture management delivers high-fidelity, context-aware insights into your API ecosystem, empowering security teams to detect, prioritize and remediate risks with unmatched precision.

Radware's Runtime Security Posture includes:

Continuous Risk Assessment: Leverages behavioral analysis of runtime traffic to evaluate API exposure and detect anomalies as they emerge, ensuring your security posture evolves with your application

Vulnerability & Misconfiguration Detection: Identifies insecure endpoints, outdated versions, missing authentication and policy inconsistencies that could be exploited by attackers

Live Traffic Monitoring: Observes real user interactions in production environments to uncover hidden risks and logic flaws that traditional testing and pre-production scans often miss

Dynamic Prioritization & Remediation: Uses attacker intent and threat severity to automatically prioritize issues, enabling faster, more effective response and reducing alert fatigue

Posture Drift Detection: Tracks changes in API behavior and configurations over time to detect deviations from baseline security posture. This helps prevent accidental exposures or regressions

Compliance Readiness: Provides audit-ready visibility and reporting aligned with regulatory frameworks like PCI DSS 4.0, NIS2 and DORA

By integrating posture management directly into runtime environments, Radware ensures that your API security is proactive, adaptive and always aligned with real-world threats—not just theoretical risks. This allows your organization to:

- Prioritize what matters most with aggregated risk scores
- Spot systemic issues across applications with risk category analytics
- Expose your riskiest endpoints and monitor sensitive data leakage
- Label and filter risks to match your remediation workflows
- Act fast with contextual risk drill-downs and remediation guidance

Figure 1:

Radware API Analytics Dashboard

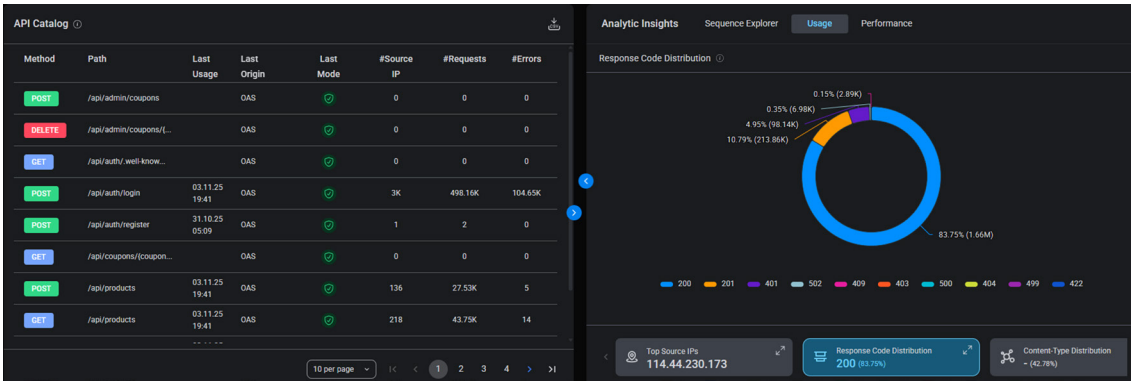
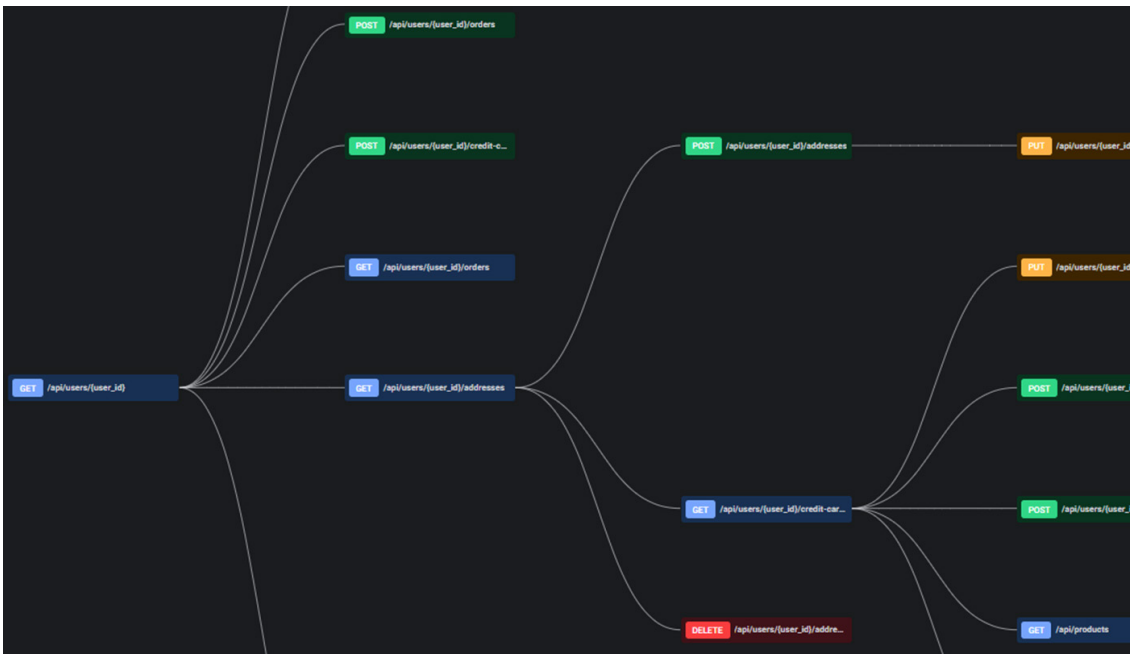


Figure 2:

View from Radware Business Logic Explorer



API Testing

Radware's contextual API testing adapts to your applications' business logic and covers the full OWASP Top 10 API risks. Focus on the risks that matter using effective, contextual and fully automated API security testing that developers will use.

- Spot critical business logic vulnerabilities that are often missed by other tools.
- Empower developers to find and fix API issues early.
- Integrate API security tools into CI/CD pipelines. (Supports seamless integration with 25+ tools.)
- Improve collaboration between AppSec and Dev teams.
- Ensure faster releases with fewer vulnerabilities.
- Reduce cost of remediation and production incidents.

Reducing API Security TCO & Operational Overhead

End-to-End Automation

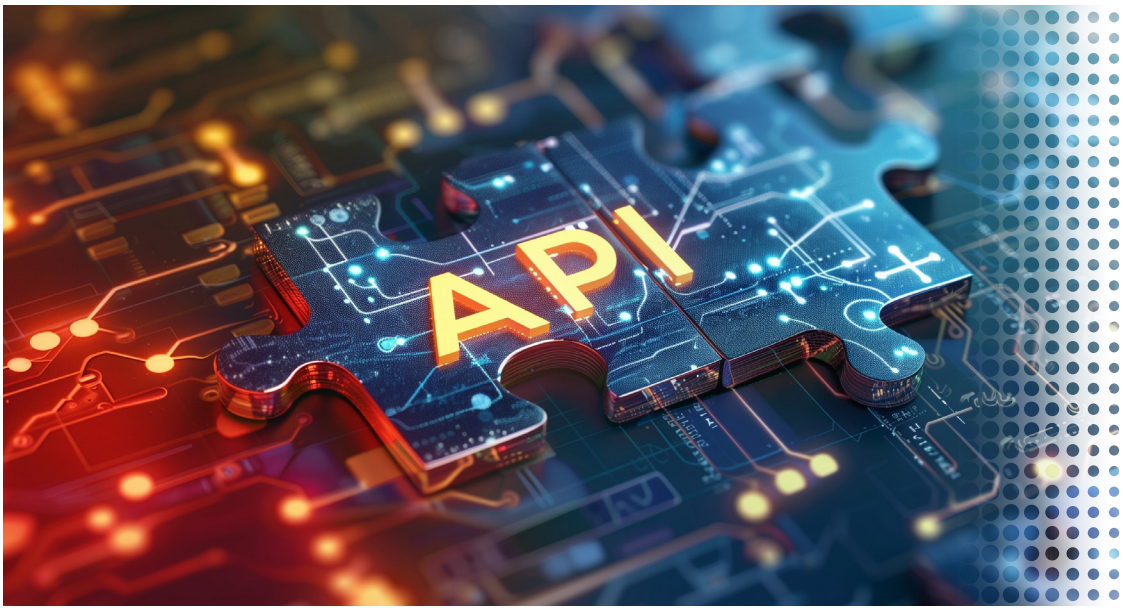
Radware's AI-based automations streamline operations and reduce total cost of ownership though authentication and discovery, risk assessment, policy generation and runtime protection.

Unified Protection

Radware combines WAF, bot management, API security and DDoS protection in a single portal for multi-layered defense and seamless cross correlation.

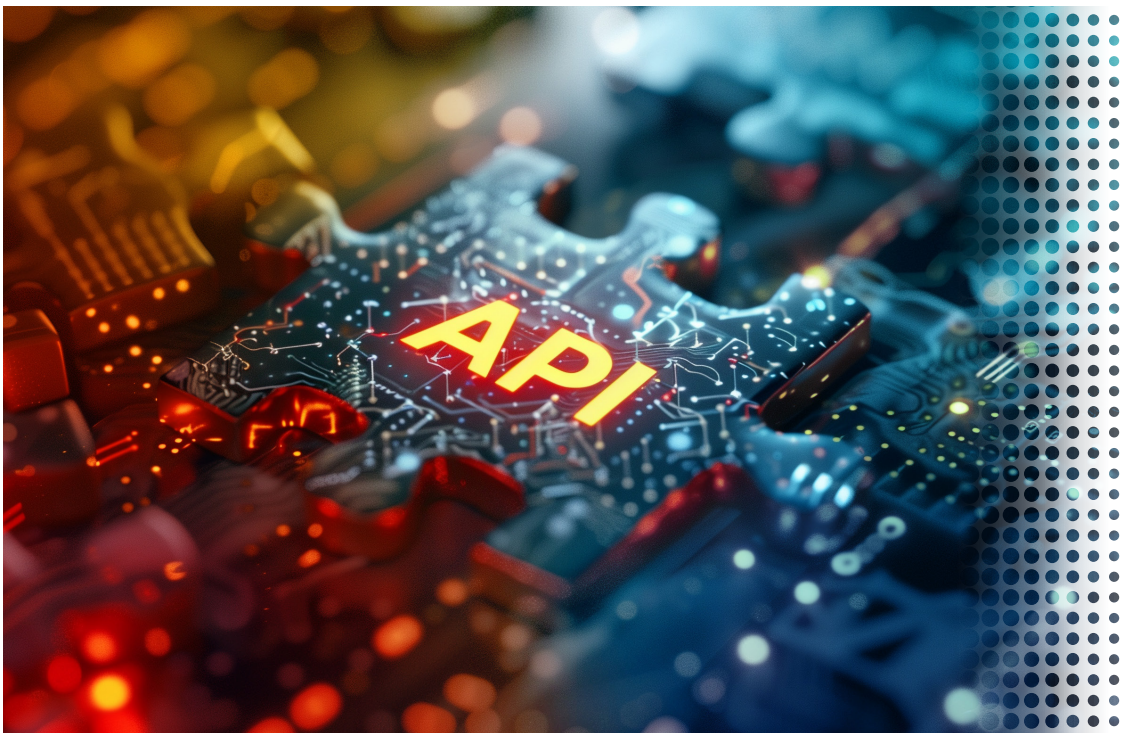
Managed Services

Radware provides the best SLA in the industry with managed services and 24/7 ERT support for under-attack scenarios and incident handling.



Why Radware API Security?

- **Full Lifecycle API Security:** From discovery and analytics to posture management, testing, and runtime protection, Radware helps eliminate silos between development and security teams by providing runtime visibility and a single source of truth to all.
- **Continuous Discovery Across Environments:** Ensure complete visibility into your API catalog, including third-party, outdated, shadow and deprecated APIs.
- **Runtime Posture Management:** Prioritize and manage risk according to real-time, high-fidelity view of your API runtime behavior, not theoretical security posture.
- **Business Logic Attack Mitigation:** Fully automate your runtime protection—no manual policy configuration required.
- **Contextual API Testing:** Find and fix business logic API issues early, integrate into CI/CD pipelines, improve collaboration between AppSec and Dev teams, and enable faster releases with fewer vulnerabilities.
- **Compliance Support:** Ensure full coverage of OWASP API Top 10 risks and alignment with major regulatory standards.
- **Single Portal Experience:** Simplify management and reporting, reducing operational overhead.
- **Cloud-Native Compatibility:** Choose security that seamlessly integrates with modern application environments and coexists with existing security tools.
- **Lowest False Positive Rate:** Ensure accurate detection with minimal disruption through adaptive automation and business logic mapping.



Use Cases

API Discovery & Security

Full visibility and control over all APIs, including shadow APIs, third-party APIs and API workflows **(business logic)**.

API Runtime Protection

Automatic application protection in real-time against all types of API attack vectors, including sophisticated HTTP DDoS and bot attacks.

Runtime Business Logic Protection

Continuous and automated protection against sophisticated API business logic attacks, such as authorization bypass, access to sensitive business flows, and manipulation of content, inventory and pricing.

Runtime Risk Management

Proactive identification and remediation of vulnerabilities and misconfigurations.

API Testing

Contextual API testing that covers the full OWASP top 10 API risks including business logic.

Compliance

Full coverage of the OWASP Top 10 API Security Risks. Meets regulatory requirements with automated reporting and continuous monitoring, including PCI DSS 4, DORA, NIS2, HIPPA, etc.

Multi-cloud protection

Singel pane of glass to control, manage and secure APIs across all your environments.

Trusted by Leading Enterprises

Radware's API Security solution is trusted by Fortune 500 companies across financial services, healthcare, e-commerce, transportation and government sectors. It is recognized by leading analysts for its advanced API security capabilities.

Ready to Secure Your APIs?

Contact us for a demo, free trial or business logic mapping session to see how Radware can help you protect your business in real time.

Contact Radware

RWI6308 | 02.26.2026