eSureITy

API SECURITY ASSESSMENTS

APIs are quietly driving breach impact and regulatory risk. Most programs still test them like web apps—and leave the real failure paths wide open.

API Security Assessments That Stop Breaches Before They Start

APIs connect everything—from cloud apps to customer data. They also represent one of today's most exploited attack surfaces.

eSureITy's API Security Assessment identifies vulnerabilities across your connected ecosystem so you can eliminate real-world attack paths before they become incidents, fines, or outages.

APIs connect everything—from cloud apps to customer data. They are also one of today's most targeted attack surfaces.

eSureITy's API Security Assessment identifies vulnerabilities across your connected ecosystem so you can eliminate real-world attack paths before they become incidents, fines, or outages.

Modern business applications rely on a sprawling web of APIs—third-party integrations, legacy services, and open-source components never designed for today's threat environment.

When an exposed API is discovered, the question is rarely "Was there a breach?"

It becomes:

- How long were APIs exposing regulated data before anyone noticed.
- Whether weak authentication, overprivileged tokens, or unvalidated input count as "reasonable controls."
- If gaps against HIPAA, PCI DSS, or NIST 800-53 create legal, regulatory, or contractual exposure.

Weak API controls don't just create security incidents. They create blind spots in investigations, executive reporting, and board-level risk decisions.

Where API Programs Fail in the Real World

APIs now move more sensitive data than web browsers—and attackers know it. A single exposed endpoint can bypass your perimeter and land directly on customer records, payment data, or intellectual property.

Attackers exploit exactly what most teams overlook:

Broken Authentication & Authorization

- Insecure tokens, misconfigured scopes, and session flaws that allow data access without consent.

Logic Flaws in Microservices

- Workflow bypasses that leak customer data, pricing, or transaction details.

Open-Source Component Risk

- Unpatched libraries reused across hundreds of APIs, multiplying every CVE.

AI-Powered Exploitation

- Automated tools testing millions of endpoints for known injection and deserialization weaknesses.

Contact Us

info@eSureITy.com

www.eSureITy.com

APIs are no longer a narrow "appsec" concern. They directly shape operational resilience, regulatory posture, and customer trust.

When these weaknesses go unchecked, they don't just expose data.

They expose your organization to liability, reputational damage, and business disruption that plays out in boardrooms, not just in SOCs.

Deliverables That Strengthen Compliance and Coverage

API Risk Report (PDF + Dashboard)

- OWASP API Top 10 exposure summary
- Detailed vulnerability list with business impact scoring
- Evidence-focused documentation for technical, risk, and executive review

Remediation & Governance Plan

- Prioritized corrective actions mapped to frameworks (NIST 800-53, CIS, PCI, HIPAA)
- Integration with Jira, ServiceNow, or equivalent for tracking and ownership
- Targeted policy updates for authentication, access control, and data validation

Retest & Verification

- Confirmation that critical and high findings are fixed, not just assigned
- Optional quarterly assurance and continuous assessment integrations

The resulting evidence set also helps organizations demonstrate that API security controls meet cyber insurance coverage requirements as those programs increasingly call for documented testing of high-risk services.

This makes API security a repeatable governance control, not a one-time event.

Measurable Results

Clients typically achieve:

- Up to 70% fewer exploitable endpoints after the first remediation sprint
- 100% fix verification on critical and high findings through structured retesting
- Zero critical OWASP API Top 10 gaps within 90 days of follow-up audit

These improvements are delivered in a format executives can understand, track, and use to drive ongoing risk reduction.

Attack-Led API Security Testing

eSureITy combines automated scanning, fuzzing, and human-driven penetration testing focused on how attackers actually abuse APIs—not just how checklists describe them.

Every assessment is:

- Mapped to OWASP API Top 10, NIST 800-53, and CIS Benchmarks
- Structured to satisfy engineering, security, risk, and compliance stakeholders
- Documented to demonstrate duty of care and control effectiveness

This turns API testing from a narrow technical task into a measurable risk-control instrument.

How the Assessment Works

1. Discovery & Mapping
Inventory of documented and shadow APIs, including endpoints, dependencies, and authentication flows across cloud, mobile, web, and third-party integrations.

2. Authentication & Authorization Testing
Validation of OAuth/OIDC tokens, API keys, scopes, and session management controls; targeted testing for broken auth, BOLA/BOPLA, and cross-tenant access.

3. Data Validation & Injection Testing
Fuzzing inputs, JSON bodies, and headers for injection, deserialization, and abuse of business parameters.

4. Error & Exception Handling Review
Identification of verbose error responses that leak stack traces, internal object references, and configuration details.

5. Logging & Monitoring Audit
Verification that API gateways and services record, alert, and retain critical events in ways that support incident reconstruction and root-cause analysis.

6. Encryption & Certificate Validation
Evaluation of TLS configurations, certificate pinning, and payload encryption for downgrade, replay, and MiTM resistance.

7. Business Logic Exploitation Simulation
Real-world attack paths to test privilege escalation, cross-tenant exposure, transaction abuse, and policy circumvention.

Every finding is risk-ranked with CVSS, assigned a business impact score, and mapped to mitigating OWASP and NIST controls to support clear, defensible decision-making.

Why Choose eSureITy

- Standards-Based, Threat-Led – Methodology mapped to OWASP, NIST 800-53, and CIS standards, executed against live attacker techniques.
- Cross-Industry Expertise – Experience securing APIs across healthcare, finance, manufacturing, and SaaS providers.
- End-to-End Support – From discovery through mitigation and validation, with artifacts tailored for technical, risk, and executive stakeholders.
- Risk and Compliance Alignment – Reporting built for security, risk, and audit teams that need defensible, framework-mapped evidence.
- Certified API Testers – CISSP, CEH, OSCP, AWS, and Kubernetes-certified engineers focused on complex, distributed API ecosystems.