API Security Survey

Section 1: API Security Priorities & Readiness

Strategic Importance of API Security

1: How important is API security for your organization in the next 12 months? (0 = Not Important, 1= Slightly Important, 2= Somewhat Important, 3=Moderately Important, 4=Very Important, 5= Extremely Important)

* API security for **"Business Impact"**
* API security for **"Digital Transformation Priority"**
* API security for **"Regulatory compliance Requirement"**

Organizational API Security Readiness

2: How mature are your organization's API security capabilities? (0 = Non-existent, 1= Initial, 2= Emerging, 3= Developing, 4= Mature, 5= Best-in-class)

* API security capabilities in terms of **"Technical Expertise"**
* API security capabilities in terms of **"Tool Maturity"**
* API security capabilities in terms of **"Process Maturity"**

Who Manages API Security Risks?

3: Who has primary responsibility for API security in your organization?

* Security Operations
* Development Teams
* Cloud Security Team
* Digital Transformation Team
* Dedicated API Security Team

Security Investment Trends

4: How do you expect your API security investment to change in the next 12 months?

* Decrease
* Minimal change (-10% to +10%)
* Moderate increase (10-25%)
* Significant increase (>25%)

Section 2: API Landscape & Digital Initiatives

API Usage Classification

5: How frequently does your organization use the following type of APIs? (0= Never, 1= Rarely, 2= Occasionally, 3=Regularly, 4=Very often, 5= Always)

Business Purpose APIs:

* Customer-facing public APIs
* Partner integration APIs
* Internal system APIs
* B2B marketplace APIs
* Mobile app backend APIs

 6: How frequently does your organization use the following type of APIs? (0= Never, 1= Rarely, 2= Occasionally, 3=Regularly, 4=Very often, 5= Always)

Technical Architecture:

* REST APIs
* GraphQL APIs
* gRPC/RPC APIs
* Event-driven APIs
* Streaming APIs

API Usage in AI/ML Implémentations

6: How frequently does your organization use the following AI/ML APIsRate usage frequency (0= Never, 1= Rarely, 2= Occasionally, 3=Regularly, 4=Very often, 5= Always)

* Large Language Models (LLMs)
* Computer Vision APIs
* Custom ML models

7: What is the deployment model for each AI/ML API your organization uses? (1= Cloud-hosted only, 2= On-premises only, 3= Hybrid deployment )

* Large Language Models (LLMs)
* Computer Vision APIs
* Custom ML models

Section 3: API Security Concerns & Effectiveness of Protection Strategies

API Security Concerns & Effectiveness of Current Solutions

8: For each of the following API security aspects, please rate how concerning they are for your organization? (0 = No Concern, 1= Minimal Concern, 2= Slightly Concerning, 3= Moderately Concerning, 4=Highly Concerning, 5= Extremely Concerning)

* API Discovery & Mapping
* API Posture Management
* API Access Control
* API Runtime Protection
* API Security Testing

9: For each of the following API security aspects, please how effective your current solutions are in addressing them? (0 = Not Effective, 1= Minimally Effective, 2=Somewhat Effective, 3=Moderately Effective, 4= Highly Effective, 5 = Extremely Effective)

* API Discovery & Mapping
* API Posture Management
* API Access Control
* API Runtime Protection
* API Security Testing

API Discovery Concerns & Effectiveness

10: How concerning are the following API Discovery challenges for your organization? (0 = No Concern, 1= Minimal Concern, 2= Slightly Concerning, 3= Moderately Concerning, 4=Highly Concerning, 5= Extremely Concerning)

* Shadow/ undocumented APIs
* Zombie/ dormant APIs
* API Usage & Visualization
* API Cost / Metering / Billing
* Identifying APIs relevant for compliance (privacy, resilience, etc.)

11: How effective are your current solutions in addressing the following API Discovery challenges within your organization? (0 = Not Effective, 1= Minimally Effective, 2=Somewhat Effective, 3=Moderately Effective, 4= Highly Effective, 5 = Extremely Effective)

* Shadow/ undocumented APIs
* Zombie/ dormant APIs
* API Usage & Visualization
* API Cost / Metering / Billing
* Identifying APIs relevant for compliance (privacy, resilience, etc.)

API Posture Management Concerns & Effectiveness

12: How concerning are the following API Posture Management measures for your organization? (0 = No Concern, 1= Minimal Concern, 2= Slightly Concerning, 3= Moderately Concerning, 4=Highly Concerning, 5= Extremely Concerning)

* Implement API gateways
* Implement API Access and Authentication
* Authentication Discovery and Risk Scoring
* Rate limiting
* Encryption
* API Specification & Compliance
* Integration with API Lifecycle process
* API Risk scoring

13: How effective are your current solutions in implementing the following API Posture Management measures within your organization? (0 = Not Effective, 1= Minimally Effective, 2=Somewhat Effective, 3=Moderately Effective, 4= Highly Effective, 5 = Extremely Effective)

* Implement API gateways
* Implement API Access and Authentication
* Authentication Discovery and Risk Scoring
* Rate limiting
* Encryption
* API Specification & Compliance
* Integration with API Lifecycle process
* API Risk scoring

API Access Control Concerns & Effectiveness

14: How concerning are the following API Access Control challenges for your organization? (0 = No Concern, 1= Minimal Concern, 2= Slightly Concerning, 3= Moderately Concerning, 4=Highly Concerning, 5= Extremely Concerning)

* Complying with standard access control methods such as OAuth/OIDC
* API access control for third-party partner companies
* API access control for App-to-App communications
* API access control for external users

15: How effective are your current solutions in addressing the following API Access Control challenges within your organization? (0 = Not Effective, 1= Minimally Effective, 2=Somewhat Effective, 3=Moderately Effective, 4= Highly Effective, 5 = Extremely Effective)

* Complying with standard access control methods such as OAuth/OIDC
* API access control for third-party partner companies
* API access control for App-to-App communications
* API access control for external users

API Runtime Protection Concerns & Effectiveness

16: How concerning are the following API Runtime Protection challenges for your organization? (0 = No Concern, 1= Minimal Concern, 2= Slightly Concerning, 3= Moderately Concerning, 4=Highly Concerning, 5= Extremely Concerning)

* Data Leakage
* Data Tampering
* Data Policy Violations
* Sensitive Data Detection and Masking
* API Security Attacks
* ML-based Traffic Monitoring
* Automated Policy Generation
* Suspicious Behaviour
* Open API Specification/Swagger enforcement
* Malicious user detection

17: How effective are your current solutions in addressing the following API Runtime Protection challenges within your organization? (0 = Not Effective, 1= Minimally Effective, 2=Somewhat Effective, 3=Moderately Effective, 4= Highly Effective, 5 = Extremely Effective)

* Data Leakage
* Data Tampering
* Data Policy Violations
* Sensitive Data Detection and Masking
* API Security Attacks
* ML-based Traffic Monitoring
* Automated Policy Generation
* Suspicious Behaviour
* Open API Specification/Swagger enforcement
* Malicious user detection

API Security Testing Concerns & Effectiveness

18: How concerning are the following API Security Testing challenges for your organization? (0 = No Concern, 1= Minimal Concern, 2= Slightly Concerning, 3= Moderately Concerning, 4=Highly Concerning, 5= Extremely Concerning)

* Code-based discovery (e.g., static/dynamic code analysis)
* Crawler-based discovery (e.g., scanning APIs)
* Traffic-based discovery (e.g., monitoring API traffic)

19: How effective are your current solutions in identifying vulnerable and/or undocumented/shadow APIs? (0 = Not Effective, 1= Minimally Effective, 2=Somewhat Effective, 3=Moderately Effective, 4= Highly Effective, 5 = Extremely Effective)

* Code-based discovery (e.g., static/dynamic code analysis)
* Crawler-based discovery (e.g., scanning APIs)
* Traffic-based discovery (e.g., monitoring API traffic)

Code-Based Discovery

20: Which stage of the API lifecycle would benefit most from code-based discovery in your organization?

* Development
* Testing
* Deployment
* Operations and Maintenance (O&M)

21: How has code-based discovery improved your organization’s API security?

* Improved visibility into internal APIs
* Faster detection of vulnerabilities
* Reduced risk from shadow or dormant APIs

22: Which stage of the API lifecycle would benefit most from the following discovery method in your organization? (1 = Development, 2 = Testing, 3 = Deployment, 4= Operations and Maintenance (O&M) )

* Crawler-Based Discovery
* Traffic-Based Discovery

23: How has the following discovery method improved your organization’s API security? ( 1= Enhanced identification of exposed APIs, 2 = Better API inventory management, 3 = Reduced risk from shadow or dormant APIs )

* Crawler-Based Discovery
* Traffic-Based Discovery

Regulatory Compliance Concerns & Effectiveness

24: How concerning are the following regulatory compliance challenges for your organization? (0 = No Concern, 1= Minimal Concern, 2= Slightly Concerning, 3= Moderately Concerning, 4=Highly Concerning, 5= Extremely Concerning)

* Data residency requirements
* Cross-border data transfer restrictions
* Privacy law compliance
* Industry-specific regulations
* Unclear or rapidly evolving regulatory landscape

25: How effective are your current solutions in addressing the following regulatory compliance challenges for your organization? (0 = Not Effective, 1= Minimally Effective, 2=Somewhat Effective, 3=Moderately Effective, 4= Highly Effective, 5 = Extremely Effective)

* Data residency requirements
* Cross-border data transfer restrictions
* Privacy law compliance
* Industry-specific regulations
* Unclear or rapidly evolving regulatory landscape

Section 4: OWASP API Security Risks

Top OWASP API Security Risks

26: Select the top 3 OWASP API security risks your organization is most concerned about

* API1:2023 - Broken Object Level Authorization
* API2:2023 - Broken Authentication
* API3:2023 - Broken Object Property Level Authorization
* API4:2023 - Unrestricted Resource Consumption
* API5:2023 - Broken Function Level Authorization
* API6:2023 - Unrestricted Access to Sensitive Business Flows
* API7:2023 - Server-Side Request Forgery
* API8:2023 - Security Misconfiguration
* API9:2023 - Improper Inventory Management
* API10:2023 - Unsafe Consumption of APIs

Readiness & Prevention Strategies

27: How ready is your organization in mitigating these risks? (0 = Not ready,1 - Initial Stage, 2 – Developing,3 – Progressing, 4 - Advanced Preparation,  5 = Fully prepared)

* API1:2023 - Broken Object Level Authorization
* API2:2023 - Broken Authentication
* API3:2023 - Broken Object Property Level Authorization
* API4:2023 - Unrestricted Resource Consumption
* API5:2023 - Broken Function Level Authorization
* API6:2023 - Unrestricted Access to Sensitive Business Flows
* API7:2023 - Server-Side Request Forgery
* API8:2023 - Security Misconfiguration
* API9:2023 - Improper Inventory Management
* API10:2023 - Unsafe Consumption of APIs

Prevention Strategies

28: What security measures does your organization currently have in place to protect APIs? (Check all that apply)

* API Access Control in API Gateway
* AI/ML-driven security solution
* Web Application Firewall
* Identity & Access Management Solution
* Load-Balancer
* Bot Protection
* SIEM (Security Information & Event Management) & Log Management
* DDoS Protection
* Automated API Security Testing Tools