API Security Sizing

F5 Distributed Cloud API Security provides comprehensive protection for your APIs including automatic discovery, schema validation, rate limiting, and behavioral analysis.

API Inventory

API Discovery Requirements

Do you have complete documentation of all your APIs?

- Yes - All APIs are documented with OpenAPI/Swagger specs
- Partial - Some APIs are documented
- No - We need to discover our API landscape

> **Shadow API Discovery**
>
> F5 XC can automatically discover APIs in your traffic, including undocumented "shadow" APIs that may pose security risks.

Known API Count

If you know your API landscape, provide details:

CATEGORY	COUNT
Public APIs (internet-facing)	Enter value
Partner APIs (B2B)	Enter value
Internal APIs	Enter value
Total API Endpoints	Enter value

API Details

For major API services, provide:

API NAME/SERVICE	BASE PATH	PROTOCOL	AUTH METHOD	DOCUMENTATION
Enter value	Enter va	☐ REST ☐ GraphQL ☐ gRPC	☐ API Key ☐ OAuth ☐ JWT ☐ None	☐ OpenAPI ☐ None
Enter value	Enter va	☐ REST ☐ GraphQL ☐ gRPC	☐ API Key ☐ OAuth ☐ JWT ☐ None	☐ OpenAPI ☐ None
Enter value	Enter va	☐ REST ☐ GraphQL ☐ gRPC	☐ API Key ☐ OAuth ☐ JWT ☐ None	☐ OpenAPI ☐ None
Enter value	Enter va	☐ REST ☐ GraphQL ☐ gRPC	☐ API Key ☐ OAuth ☐ JWT ☐ None	☐ OpenAPI ☐ None

API Traffic Volume

Request Volume

METRIC	AVERAGE	PEAK
API Requests per Second	Enter value	Enter value
API Requests per Day	Enter value	Enter value
API Requests per Month	Enter value	Enter value

Base Package

Standard includes up to 500,000 API requests per month for API protection.

API Consumer Distribution

Who consumes your APIs?

CONSUMER TYPE	PERCENTAGE	ESTIMATED DAILY REQUESTS
Web Applications (browsers)	Enter value %	Enter value
Mobile Applications	Enter value %	Enter value
Partner Integrations (B2B)	Enter value %	Enter value
Internal Services (M2M)	Enter value %	Enter value
Third-Party Developers	Enter value %	Enter value
Total	100%	Enter value

API Security Features Required

API Discovery

- **Yes - Critical** - We need to discover all APIs in our traffic
- **Yes - Nice to have** - We have docs but want validation
- **No** - We have complete API documentation

Discovery scope:

- Production traffic only
- All environments (Prod, Stage, Dev)

API Schema Validation

- Yes - Enforce requests match OpenAPI specification

If yes, what actions should be taken on violations?

VIOLATION TYPE	ACTION
Unknown endpoints	☐ Block ☐ Log Only ☐ Allow
Invalid request parameters	☐ Block ☐ Log Only ☐ Allow
Invalid request body	☐ Block ☐ Log Only ☐ Allow
Missing required fields	☐ Block ☐ Log Only ☐ Allow
Wrong data types	☐ Block ☐ Log Only ☐ Allow

API Rate Limiting

- Yes
- No

If yes, provide requirements:

RATE LIMIT TYPE	LIMIT	TIME WINDOW	ACTION
Per API Key	Enter value requests	☐ second ☐ minute ☐ hour	☐ Block ☐ Throttle
Per User/Token	Enter value requests	☐ second ☐ minute ☐ hour	☐ Block ☐ Throttle
Per Endpoint	Enter value requests	☐ second ☐ minute ☐ hour	☐ Block ☐ Throttle
Per IP Address	Enter value requests	☐ second ☐ minute ☐ hour	☐ Block ☐ Throttle
Global (all traffic)	Enter value requests	☐ second ☐ minute ☐ hour	☐ Block ☐ Throttle

Sensitive Data Protection

- Yes
- No

If yes, what data types need detection?

- Credit Card Numbers (PCI-DSS)
- Social Security Numbers
- Email Addresses
- Phone Numbers
- Healthcare Data (HIPAA)
- Custom Patterns:

What action should be taken when sensitive data is detected?

- Block the request/response
- Mask the data in transit
- Log and alert only
- Allow (detection only)

API Authentication and Authorization

Authentication Methods

What authentication methods do your APIs use?

- API Keys (header or query parameter)
- OAuth 2.0 / OpenID Connect
- JWT (JSON Web Tokens)
- Basic Authentication
- Mutual TLS (mTLS)
- Custom authentication
- No authentication (public APIs)

JWT Validation

If using JWT, do you need F5 XC to validate tokens?

- Yes - Validate JWT signatures
- Yes - Validate JWT claims (expiration, audience, etc.)
- No - Application handles JWT validation

JWT issuer (if applicable):

Authorization Requirements

- Yes - Enforce role-based access to API endpoints
- No - Application handles authorization

API Security Threats

OWASP API Security Top 10

Which API-specific threats are you concerned about?

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

Historical API Attacks

Have you experienced any API-specific attacks?

- API scraping / data harvesting
- Credential stuffing on login APIs
- Abuse of business logic
- Inventory/pricing manipulation
- Enumeration attacks
- None / Unknown

Describe any specific concerns:

OpenAPI Specification Import

Existing Specifications

Do you have OpenAPI/Swagger specifications for your APIs?

- Yes - OpenAPI 3.x
- Yes - OpenAPI 2.0 (Swagger)
- Partial - Some APIs only
- No - We need to generate specs

Specification Management

How will you manage API specifications?

- Upload static files to F5 XC
- Automatic sync from API gateway/management platform
- Generate from live traffic discovery
- CI/CD pipeline integration

Number of specification files: _____

Specification Source

Where are your API specifications stored?

- Git repository
- API management platform (Apigee, Kong, etc.)
- Internal documentation system
- AWS API Gateway
- Azure API Management
- Other: _____

Advanced API Security (Advanced Tier)

Behavioral API Security

- Yes - Detect anomalies in API usage patterns

- No - Schema validation is sufficient

> ⚠ **Advanced Tier Required**
>
> Behavioral API security with ML-based anomaly detection requires the Advanced tier.

API Posture Management

- Yes - Score APIs based on security risk
- No

Data Intelligence Tier

What level of data intelligence do you need?

- **Basic** - Standard PII detection
- **Advanced** - Custom patterns + compliance data types
- **Premium** - Full data classification + custom policies

Integration Requirements

Existing API Infrastructure

Do you have existing API management infrastructure?

PLATFORM	IN USE	INTEGRATION NEEDED
AWS API Gateway	☐	☐
Azure API Management	☐	☐
Google Apigee	☐	☐
Kong	☐	☐
MuleSoft	☐	☐
Other: Enter value	☐	☐

CI/CD Integration

- Yes - Scan API specs before deployment
- Yes - Security gates in deployment pipeline
- No

CI/CD platforms in use:

- Jenkins
- GitHub Actions
- GitLab CI
- Azure DevOps
- Other:

Summary: API Security Requirements

REQUIREMENT	VALUE
Number of API Endpoints	Enter value
API Discovery Required	☐ Yes ☐ No
Estimated Monthly API Requests	Enter value
Schema Validation Required	☐ Yes ☐ No
Sensitive Data Protection Required	☐ Yes ☐ No
Tier Required	☐ Standard ☐ Advanced

Additional notes or special requirements: