WHY USE NGINX FOR API SECURITY?

Advanced Protection
Go beyond basic protection from the OWASP API Security Top 10 with advanced security that detects over 7,500 attack signatures

Security as Code
Enable a shift-left strategy with declarative API security policies that integrate directly into your CI/CD pipelines

Actionable Insights
Mitigate attacks before they result in damage with real-time threat intelligence to identify unique attack signatures

Automate, Monitor, and Secure API Operations at Scale with F5 NGINX

APIs are a top target for malicious attacks. Over the past year, nine out of ten enterprises reported experiencing an API security incident.1

Managing and securing APIs continues to be a challenge, in part due to their open design. APIs are built to share a company’s most valuable data and services, making them appealing targets for bad actors. API breaches often expose personally identifiable information (PII) and other sensitive business data. This can result in lasting reputational damage for companies targeted by malicious attacks.

The rise in API attacks is a direct result of continuous API sprawl. Enterprises increasingly operate modern applications across globally distributed hybrid architectures and multi-cloud environments. For the platform and security teams responsible for managing and securing IT infrastructure, the rapid growth in API attacks creates a unique set of challenges:

• Lack of visibility – APIs are difficult to monitor for vulnerabilities without a consistent view across architectures and environments.

• Inconsistent security controls – Security policies and capabilities are inconsistent across cloud providers and on-premises data centers.

• Continuous code releases – Complex software supply chains and CI/CD pipelines introduce new vulnerabilities faster than they can be fixed.

With F5 NGINX you can apply consistent security policies and gain visibility into APIs deployed across distributed teams and environments. NGINX’s API Connectivity Stack includes NGINX Management Suite API Connectivity Manager, NGINX Plus as API gateway, and NGINX App Protect WAF for advanced security and attack mitigation.

1. Continuous API Sprawl: Challenges and Opportunities in an API-Driven Economy (F5, 2021)
Benefits of API Security for Modern Applications

NGINX helps your organization implement defense-in-depth and Zero Trust API security strategies to ensure comprehensive protection for your APIs and microservices.

Access Control
Implement identity-based security strategies with fine-grained API access control policies:

- **Authentication** – Integrate with identity providers and manage access to your APIs and platform using API Keys or OpenID Connect (OIDC)
- **Authorization** – Apply fine-grained controls to manage who can access specific resources using OAuth 2.0 or JSON Web Tokens (JWTs)
- **Access Control Lists** – Apply positive security using whitelists based on IP address, client IDs, JWT claims, or blacklist-specific IP ranges

Real-Time Monitoring
Monitor and analyze API traffic for actionable insights into the security posture of your APIs:

- **Centralized Visibility** – Analyze threats, view protection insights, and monitor security policies across your entire NGINX App Protect WAF fleet
- **Export Logs and Metrics** – Share metrics and logs with your preferred observability tools including Datadog, Grafana, Prometheus, and more

Data Encryption
Encrypt API traffic in transit and block attempts to exfiltrate sensitive data:

- **Data Guard** – Prevent the exfiltration of sensitive data by detecting and masking credit card numbers and social security numbers in API responses
- **Mutual TLS** – Ensure that API requests come from legitimate, authenticated users to prevent common attacks
- **End-to-End Encryption** – Encrypt “east-west” communication within a data center or cloud to protect sensitive data

Runtime Protection
Detect and remediate attacks as they happen with real-time protection for your APIs:

- **API Abuse Protection** – Go beyond basic protection from the OWASP API Security Top 10 with advanced security that detects over 7,500 attack signatures and threat campaigns
- **Modern Protocols** – Defend REST, gRPC, GraphQL, and WebSocket APIs from even the most sophisticated attacks
- **API Schema Validation** – Import OpenAPI Specifications to create and enforce a positive security model for your APIs

To discover how NGINX can help you, visit nginx.com/api-security

©2023 F5, Inc. All rights reserved. F5 and the F5 logo, NGINX and the NGINX logo, NGINX App Protect WAF, NGINX Management Suite API Connectivity Manager, API Connectivity Stack, and NGINX Plus are trademarks of F5, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, expressed or implied, claimed by F5.