NuSummit Cybersecurity

cybersecurity.nusummit.com

SOLUTION BRIEF

# NuSummit Cybersecurity's API Security

API SECURITY

# Securing APIs for Resilience and Compliance

APIs power modern digital interactions but are also prime targets for cyber threats. Organizations risk data breaches, compliance failures, and operational disruptions without proper security measures. We provide a comprehensive API security framework to protect sensitive data, ensure compliance, and mitigate evolving threats.

# Who Needs API Security?

API security is essential for **any organization that relies on digital interactions, data exchange, and interconnected systems.** Protecting APIs is crucial to safeguarding sensitive data, preventing breaches, and ensuring regulatory compliance, whether you operate in finance, healthcare, technology, or retail.

### Financial Services and Banking

Secure payment gateways, trading platforms, and customer transactions.

### Healthcare and Life Sciences

Protect patient data, comply with HIPAA, and secure medical API integrations.

### E-Commerce and Retail

Safeguard online transactions, prevent fraud, and protect customer data.

### Telecommunications

Ensure secure API access to customer data, messaging services, and cloud networks.

### Technology and SaaS Companies

Secure API integrations, cloud applications, and third-party services.

### Government and Public Sector

Protect citizen data, digital services, and government infrastructure.

Any business that **exposes, consumes, or integrates APIs** needs a **robust security strategy** to protect against **unauthorized access, data leaks, and cyberattacks.**

NuSummit Cybersecurity Cybersecurity provides tailored API security solutions to help organizations across industries stay **resilient, compliant, and secure.**

# Key Challenges in API Security

APIs introduce both convenience and risk. Many organizations struggle with visibility, access control, compliance, and monitoring, leaving gaps for potential security breaches. The most common challenges include:

### Unknown API Inventory

Untracked APIs create security blind spots.

### Vulnerable Legacy APIs

Outdated APIs expose systems to attacks.

### Weak Access Controls

Poor authentication leads to unauthorized access.

### Compliance Risks

GDPR, HIPAA, and other regulations require strict API security.

### Lack of Monitoring

Without real-time tracking, threats go undetected.

# Our API Security Approach

We take a proactive, multi-layered approach to securing APIs, addressing vulnerabilities from development to deployment. Our strategy ensures that APIs are protected against cyber threats, monitored in real-time, and compliant with global security standards.

## Threat Modeling and Secure Development

**STRIDE and DREAD Analysis:** Identify threats early and mitigate design risks.

**API Vulnerability Testing**: Detect and fix OWASP API security risks.

**Secure SDLC Integration:** Embed security into the entire development lifecycle.

## API Access Control and Protection

**OAuth and OIDC Integration**: Enforce strong authentication and authorization.

**Secure Development:** Integrate secure coding practices and automated vulnerability scans into the CI/CD pipeline.

**Continuous Inventory Management**: Maintain visibility and control over all APIs.

## API Penetration Testing and Threat Prevention

**Dynamic and Manual Penetration Testing**: Simulate attacks to showcase impact of identified vulnerabilities

**Business Logic Cases:** Uncover tough to find business logic security issues

**Real-Time Threat Monitoring:** Detect and respond to security anomalies instantly.

# Benefits

Organizations can enhance trust, operational resilience, and compliance readiness by implementing robust API security measures. We help businesses achieve the following:

### Strengthened API Security Posture

Proactive threat mitigation across API ecosystems.

### Improved Compliance and Governance

Meet regulatory requirements efficiently.

### Enhanced Risk Management

Minimize data exposure and operational disruptions.

### Operational Efficiency

Automated testing and monitoring for scalable API security.

# Real Stories, Real Solutions

### North American Trading and Financial Corporation

**Challenge**

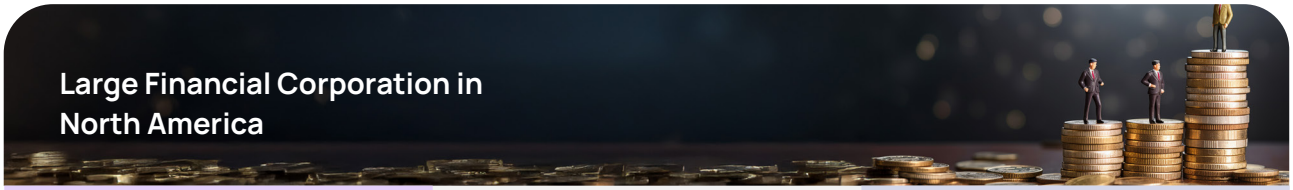
A security flaw in their API exposed user data—names, addresses, and more.

**Solution**

Conducted API penetration testing. Identified and fixed vulnerabilities.

**Outcome**

Secured the API, preventing future breaches and protecting user trust.



### Large Financial Corporation in North America

**Challenge**

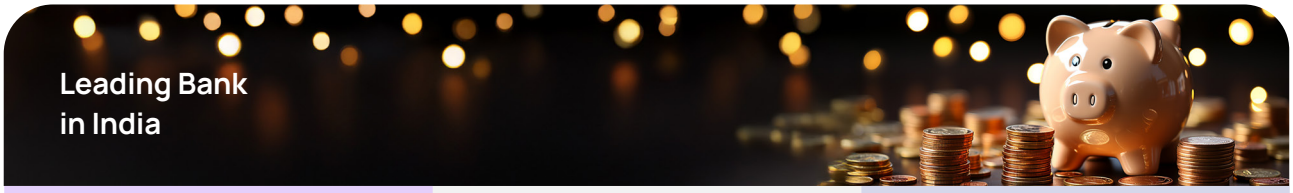
Needed to scale API security testing across hundreds of tests per week.

**Solution**

Implemented automated testing.

**Outcome**

Achieved scalable, efficient API security testing without compromising quality.



### Leading Bank in India

**Challenge**

Required secure integration with a payment gateway handling millions of transactions daily.

**Solution**

Conducted threat modeling and API security testing.

**Outcome**

Ensured secure integration, regulatory compliance, and smooth operations.

**Fintech Company**

### Challenge

Discovered 10 times more APIs than expected without visibility into sensitive data flows.

### Solution

Implemented continuous API discovery and penetration testing.

### Outcome

Identified and mitigated vulnerabilities, including account takeover risks, and secured sensitive data.

# Why NuSummit Cybersecurity?

With deep expertise in **API security, compliance, and threat management,** we are a trusted partner for enterprises looking to **safeguard their API ecosystems.** Here's why businesses choose us:

### Weak Access Controls

Extensive experience securing APIs for global enterprises.

### Comprehensive Security Framework

Covers API development, testing, monitoring, and compliance.

### Scalable and Automated Solutions

Minimize manual efforts and accelerate remediation.

**Secure your APIs today. Contact us for a consultation!**

# About NuSummit Cybersecurity

**NuSummit Cybersecurity** helps build and transform cybersecurity postures to enable businesses to mitigate risks. We are a pure-play cybersecurity services company with deep expertise in Identity and Access Management, Risk Advisory, Security Verification, Managed Detection and Response, and Security Engineering services.

Our unique products and services help businesses build and transform security postures while mitigating risks. Our focus is to strengthen security resilience by minimizing the occurrence of attacks, threats, and risks so that you can drive change, innovate, and accelerate growth.

For more information, visit us at **cybersecurity.nusummit.com** or write to us at **cybersales@nusummit.com**

**Dallas I Jersey City I Cupertino I Ottawa I Riyadh I Dubai Mumbai I New Delhi I Bangalore**



**Follow us at:**