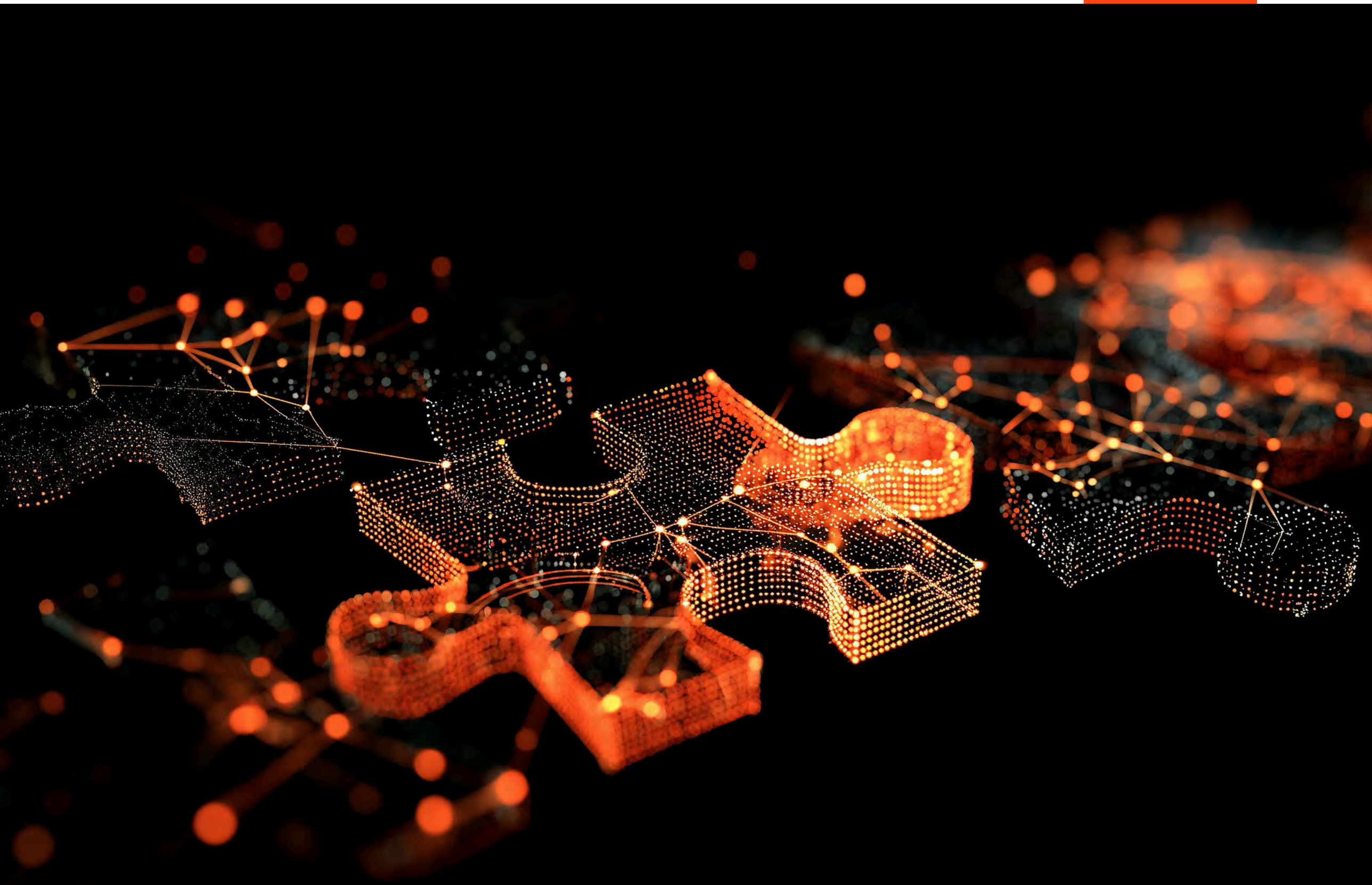
ORYXLABS

API360

COMPREHENSIVE API SECURITY

PRODUCT BROCHURE



INTRODUCTION

Breaking news alerts consistently reveal a troubling pattern: millions of customer records exposed from trusted enterprises are subsequently sold for as little as $2.13[1]. This alarming trend reflects how APIs, the critical infrastructure connecting our digital ecosystem, have emerged as the preferred attack vector for cybercriminals seeking maximum impact.

The severity of this threat landscape is evident through recent devastating API security incidents. Dell experienced a catastrophic breach affecting 49 million[2] customer records when attackers exploited their partner portal API, sending over 5,000 requests per minute[3] for nearly three weeks while remaining undetected. Twilio's Authy service, a two-factor authentication platform designed to enhance security, suffered a breach exposing 33.4 million phone numbers[2] through an unprotected API endpoint lacking proper authentication controls[4]. These cases exemplify a broader epidemic, with 99% of organizations[5] reporting API-related security incidents within the past year, while attack volumes have surged by 3,000%[6] as threat actors increasingly recognize APIs as vulnerable foundation points.

The integration of artificial intelligence technologies with expanding API ecosystems creates unprecedented risk multiplication. Research indicates that 98.9% of AI-related security vulnerabilities[2] originate from API implementation flaws, meaning every AI integration, IoT device, and mobile application potentially introduces new attack surfaces.

99%

Organizations with API security incidents

3,000%

API attack volume increase

98.9%

AI vulnerabilities linked to APIs

73%

Organizations with multiple breaches

95%

Authenticated session attacks

40%

BOLA attack prevalence

THREE CRITICAL TRENDS ARE RESHAPING THE API SECURITY LANDSCAPE

- The **exponential growth of AI-driven applications** creating novel attack vectors that bypass traditional security infrastructures, evidenced by 439 AI-related CVEs in 2024 - a 1,025% increase over 2023, with 98.9% directly tied to APIs[2].
- The evolution of sophisticated **bot attacks targeting API endpoints** at rates 85% higher[6] than traditional web attacks, with automated threats accounting for the majority of API security incidents across enterprises.
- The proliferation of shadow and zombie APIs operating beyond security governance frameworks, with 90% of organizations[5] **lacking proper API inventory management**[7].

[1] Equixly - "Top 5 API Security Incidents of 2023." January 4, 2024
[2] Wallarm - "Annual 2025 API ThreatStats™ Report." 2025.
[3] Salt Security - "It's 2024 and the API Breaches Keep Coming." October 14, 2024
[4] Barracuda - "Shadows, zombies, and Twilio's wide-open API." July 8, 2024
[5] Salt Security - "Salt Labs 2025 Q1 State of API Security Report." 2025.
[6] Cybelangel - "API Security Risks in 2025: What We've Learned So Far." August 3, 2025
[7] Indusface - "API Discovery: What is it and Why is it important?" June 29, 2025

OUR SOLUTION

API360 transforms reactive API protection into proactive digital defense, enabling organizations to achieve comprehensive visibility across their entire API landscape while establishing continuous threat detection capabilities that prevent security incidents before they impact business operations.

API INVENTORY MANAGEMENT

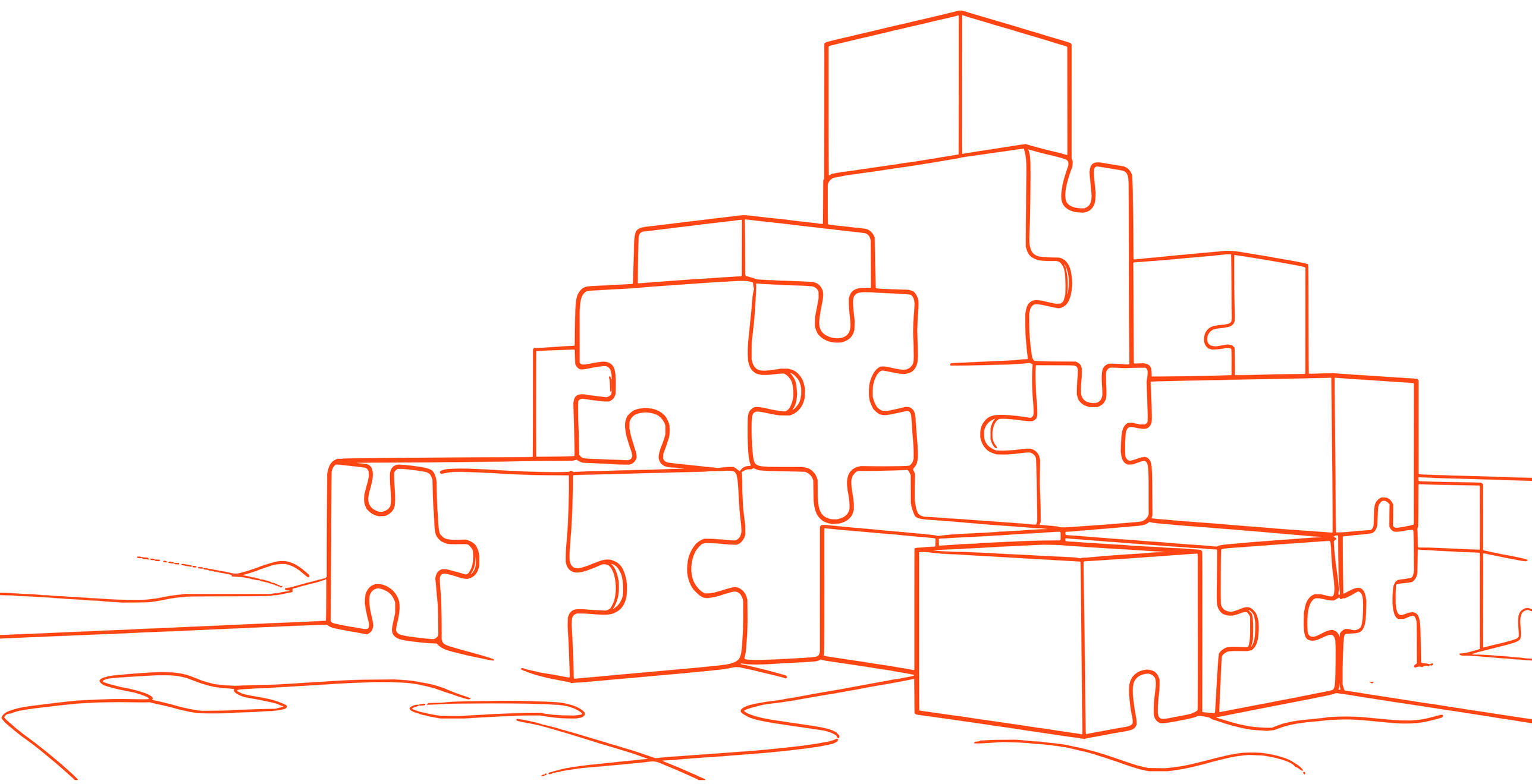
API360 addresses the critical challenge where 90% of organizations lack proper API inventory management by providing complete visibility into all APIs across your infrastructure. This comprehensive approach eliminates the dangerous blind spots created by shadow, orphan, and zombie APIs that operate outside security oversight, ensuring every endpoint is identified, catalogued, and continuously monitored.

Organizations gain immediate transparency into their entire API ecosystem, establishing a foundational security posture that transforms unknown risks into managed assets. The result is reduced attack surface, improved compliance readiness, and strategic control over API proliferation without disrupting existing operations or requiring infrastructure changes.

API SECURITY AND PROTECTION

API360 transforms organizational security posture by shifting from reactive incident response to proactive threat prevention across the entire API lifecycle. This strategic approach addresses the reality that 99% of organizations experience API security incidents by providing continuous protection against both known OWASP Top 10 vulnerabilities and emerging zero-day threats.

Organizations achieve measurable risk reduction through intelligent prioritization that focuses resources on vulnerabilities with actual business impact rather than technical noise. This comprehensive protection model delivers automated threat containment, regulatory compliance through data sovereignty, and operational continuity under attack.



FEATURES

API360 delivers end-to-end protection through integrated capabilities designed to address the complete API threat landscape. From instant discovery to automated response, each feature provides complete visibility, proactive threat detection, and risk mitigation.

- **Agentless API Inventory Management**
  Identifies all API endpoints including undocumented endpoints by passively analyzing mirrored network traffic.
- **Passive Vulnerability Scanning**
  Detects OWASP Top 10 and business logic vulnerabilities through non-intrusive traffic analysis.
- **Attack and Vulnerability Analytics**
  Combines real-time telemetry with passive vulnerability data to deliver deep insights into both ongoing attacks and exploitable weaknesses.
- **Real-Time Behavioral Analytics**
  Establishes baseline API usage patterns and flags anomalous behavior such as bot activity, credential stuffing and injection attempts.
- **Webhook-Driven Automated Mitigation**
  Executes instant defense actions - blocking, rate limiting and throttling.
- **Complete Data Sovereignty**
  Provides full on-premises deployment option for total control over sensitive API data ensuring regulatory compliance.

BENEFITS

Measurable operation efficiency gains, complete data control, and uninterrupted business continuity are key business benefits of API360. These benefits directly address escalating API security losses while transforming security from a cost center into a competitive advantage.

- **Enhanced Operational Efficiency**
  The platform transforms productivity by eliminating manual security processes, giving development teams back precious hours previously spent on manual vulnerability assessments. Automated discovery provides instant API visibility without infrastructure changes and minimal overhead.
- **Business Continuity and Competitive Advantage**
  The platform prevents costly API-related downtime through real-time threat detection and automated response, maintaining business operations even under attack. Organizations gain competitive advantage through enhanced digital trust and faster partner integrations.
- **Sensitive Data Stays with You**
  Our fully on-premises deployment ensures complete data sovereignty, giving organizations total control over sensitive API data without relying on third-party cloud providers. Organizations maintain physical ownership of all security data, ensuring compliance with data residency requirements.
- **Future-Proof Security Investment and Scalability**
  Our solution provides a strategic security foundation that adapts to emerging threats, with advanced intelligence continuously evolving to detect new API attack patterns. Organizations benefit from a platform that becomes more effective over time, providing increasing value.

ORYXLABS

WHO WE ARE

ORYXLABS was founded in Abu Dhabi in 2020 with a passion for cybersecurity-focused engineering.

A proudly diverse staff hailing from 22 different countries with backgrounds ranging from national defense to world-renowned top software engineering organizations joined together to develop best-in-class security solutions.

We leverage research and innovation to provide solutions in four key areas:

- Cyber Security Assessment
- Monitoring
- Prevention
- Improvement

When combined, ORYXLABS solutions provide a holistic approach to situational awareness and attack mitigation.

WEBSITE

Scan to view

VIDEO

Scan to view

OUR MISSION

Our mission is to equip cybersecurity teams with first-in-class intelligence and technical solutions that continuously assess, monitor, and improve environments to mitigate ongoing or future attacks.

WHY US

As an agile and innovative company focused on cybersecurity, we pride ourselves on crafting highly tailored solutions to meet our clients' exact needs, not "one size fits all" products like our competitors in the domain.

With our combined experience in deep learning, AI, vulnerability research and big data, and partnerships with world-renowned subject matter experts, you can rest assured our solutions are built and run on information that is timely and accurate.

COMPANY AWARDS

2025

Most Innovative CyberSecurity Company

CyberSecurity Excellence Awards

2024

Most Innovative CyberSecurity Company

CyberSecurity Excellence Awards

2023

Most Innovative CyberSecurity Company

CyberSecurity Excellence Awards

2022

Top CyberSecurity Solutions Provider Middle East

Enterprise Security

ORYXLABS

21st Floor, Aldar HQ
Al Raha Beach
P.O. Box: 33289
Abu Dhabi, UAE

oryxlabs.ae