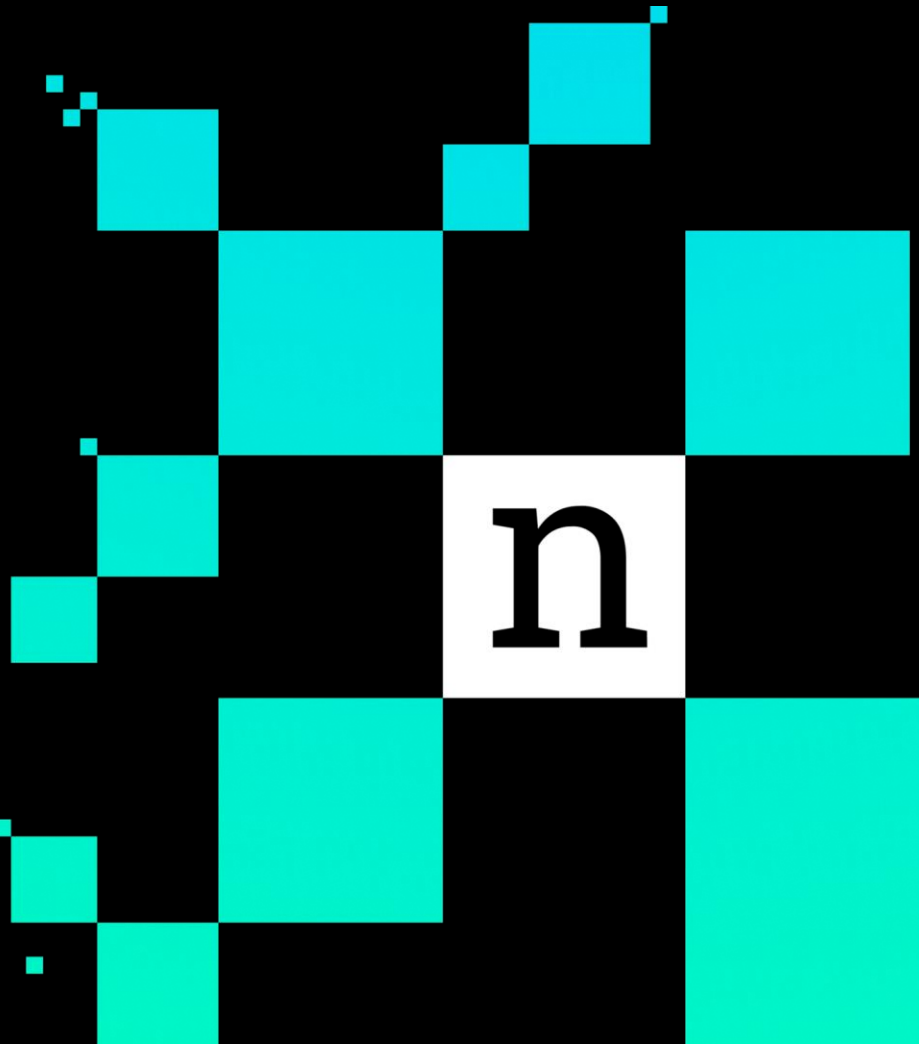
noname

APIs are Eating the World …

June 2023



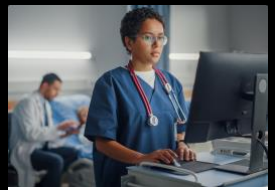
Karl Mattson, CISO

APIs Power the Modern World

Mission Critical Operations, Digital Transformation, and Information Availability - All Rely On APIs

Controlling a nuclear reactor

Transferring millions of dollars



Access to personal information

Existing Approaches Aren't Working

Current technologies, and tactics can't address the API explosion & risk

Limited Effectiveness

- ✓ Web Application Firewalls
- ✓ API Gateways
- ✓ SAST/DAST

Expensive and Infrequent

- ✓ Bug Bounties
- ✓ Red Teams

Manual and Incomplete

- ✓ API Inventories
- ✓ API Documentation

Gartner

"By 2025, less than 50% of enterprise APIs will be managed, as explosive growth in APIs surpasses the capabilities of API management tools"

25,592 APIs

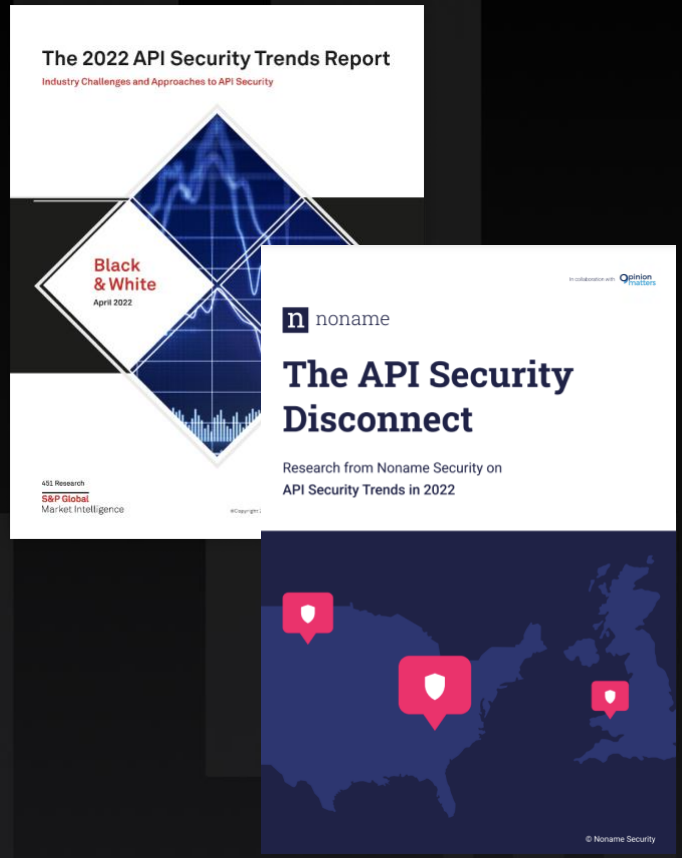
The Avg # of APIs in companies with over 10k employees was over 25,000 APIs

81% incident rate

81% of CISOs reported an API security incident in the last 12 months

35% projects delayed

Survey respondents who said projects were specifically delayed due to API security concerns



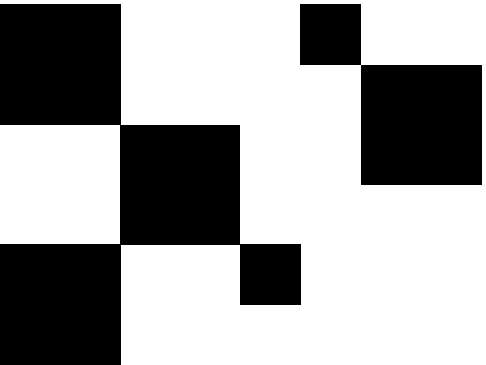
Two thirds of cloud incidents in the data sample related to misconfigured API keys that allowed improper access.

Source: 2021 IBM Security X-Force Cloud Threat Landscape Report.

What to do about it …

A New Competency

We must position our teams to possess routinely sophisticated competencies to secure APIs. Competencies are inclusive of people, process and technology capabilities.



Evaluate Capabilities

Set Courses of Action

Common Criteria

API Security Top 20 Controls

API Security Top 20 – Old Techniques Applied to New Problems

Plan

- API1: Roles and Responsibilities (Governance)
- API2: Policies, Standards and Specifications
- API3: Security Metrics
- API4: Lifecycle Management

Develop

- API5: Developer Training
- API6: Developer Environment (IDE, Repos)
- API7: Documentation
- API8: Defect Tracking and Resolution

Test

- API9: Source Code Testing (SAST, DAST)
- API10: Penetration Testing
- API11: Compliance Review
- API12: Change and Release Management

Operate

- API13: Inventory APIs
- API14: Inventory Sensitive Data
- API15: Vulnerability Management
- API16: Configuration Management

Protect

- API17: Log/Traffic Collection
- API18: Threat Detection
- API19: Sensitive Data Movement
- API20: Blocking and Remediation

API Top 20 Security Controls – Relevant Maturity Ratings

Level	General Description
Initial	Security controls for APIs are absent or are applied by individuals ad hoc.
Baseline	Security controls applied to APIs are not distinguished from those applied for all applications generically (e.g. SDLC policies and standards, application testing, WAF utilization, software asset management)
Intermediate	Security controls applied to APIs are defined and applied specifically to APIs (e.g. API specifications and standards, consistent API management (gateway) utilization, API asset and sensitive data inventories)
Advanced	Security controls for APIs capitalize on automation and intelligent (ML, context-aware) analysis to identify API risks (pre-production and runtime) without significant manual intervention (e.g. CI/CD testing, behavioral detections)
Optimal	Security controls for APIs are automated, enforced, integrated into enterprise workflows and continuously calibrated with risk-informed insights (e.g. real-time metrics, automated compliance checks, threat blocking/orchestration)

API Top 20 Security Controls – Assess Maturity

API Top 20 Controls		Initial	Baseline	Intermediate	Advanced	Optimal
Protect	API19: Sensitive Data Movement	**Control Objective:** Sensitive data requested and received via API is monitored and analyzed to detect for unauthorized or anomalous movement; Security alerts trigger workflows and notifications for timely investigation and response; Control effectiveness is demonstrated through continuous, reliable testing.				

API Security Security Controls Assessment

Diagnosing Current State and Determining Action Plans for Future State

noname

Thank You

For more information visit

nonamescurity.com