



# API Security

Nov 3, 2025



Certified & Accredited by



As Featured In



Available On



*\*Confidential - Limited Distribution Under NDA*

## API Security

What problem do we solve?

Traffic Visibility  
(External/Internal)

Sensitive Information in  
Headers

Presence of Sensitive  
Data such as PII, PHI

Traffic  
Segmentation

North-South and  
East-West traffic -  
Security posture

Secure/Insecure  
Traffic Exposure

Shadow APIs

Zombie APIs

Orphan APIs

DORA Compliance

GDPR Compliance

HIPAA Compliance

PCI-DSS Compliance

OWASP Compliance

# Business Impacts

## 2x Attacks from 2023

Over 50% of all recorded cybersecurity exploits in 2024 were API-related.

## Annual Global Losses

\$35–87 billion, with large organizations bearing the majority of high-impact costs.

## API Security Market

API security market is projected to grow to \$6.3B by 2030 (CAGR ~25%).

## Industry Insight - Gartner

API-related breaches have compromised over 1.6 billion records, highlighting the critical need for robust API security measures.

## Dell API Incident in 2024

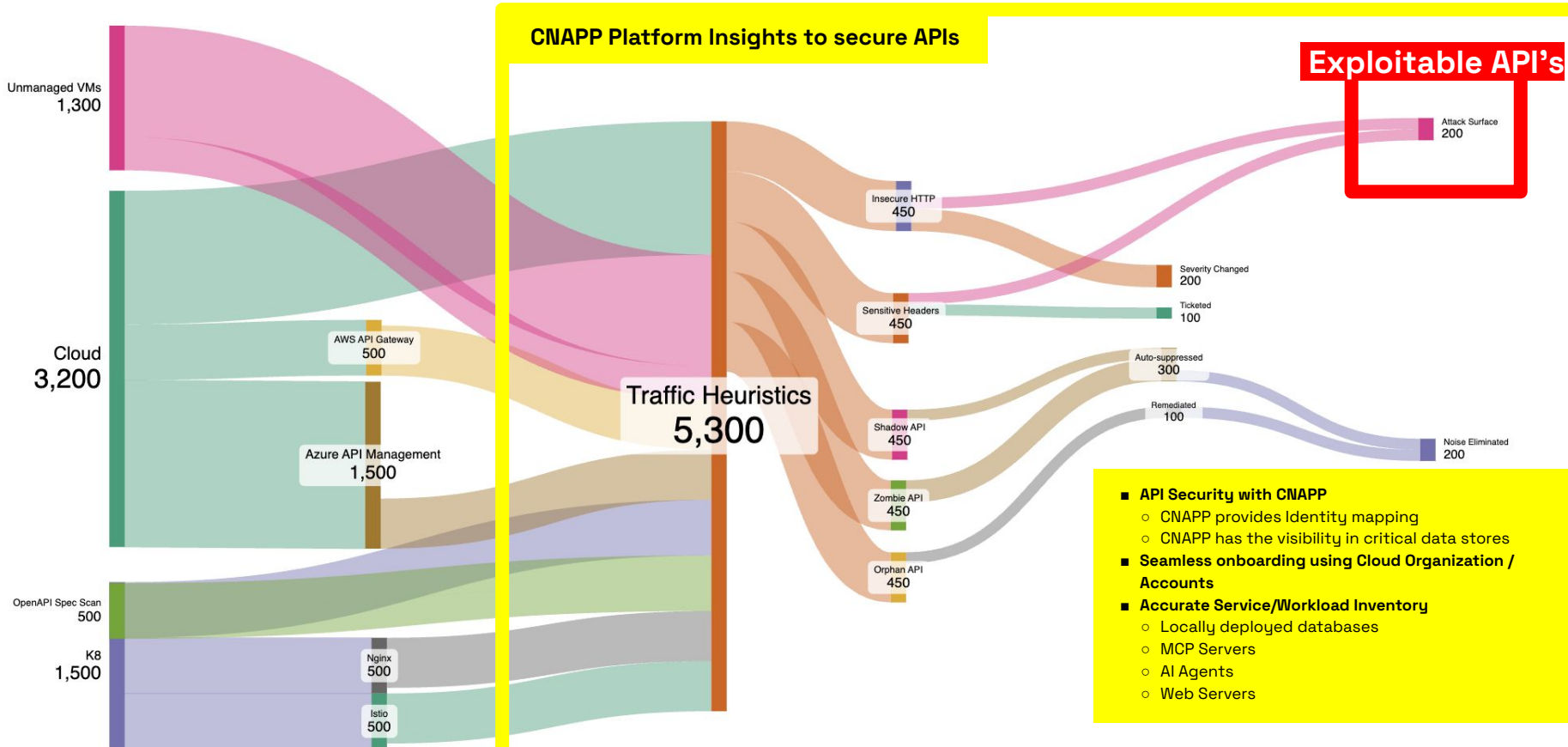
A weak registration API exposed data for an estimated 49 million users.

# AccuKnox API Security Components



Component	Focus Area	Key Functions
<b>API Discovery</b>	Visibility & Inventory	Identify shadow, zombie, and exposed APIs
<b>Runtime Monitoring</b>	Behavioral Security	Detect anomalies in traffic and API usage
<b>Access Policy Control</b>	Identity & Authorization	🚩 Enforce RBAC and policy-as-code for API access
<b>Threat Detection</b>	Attack Prevention	🚩 Block injection, scraping, and broken object-level authorisation
<b>Compliance Reporting</b>	Audit Readiness	🚩 Align with SOC 2, PCI-DSS, and HIPAA standards

# AccuKnox Differentiator - Noise vs Value Flow



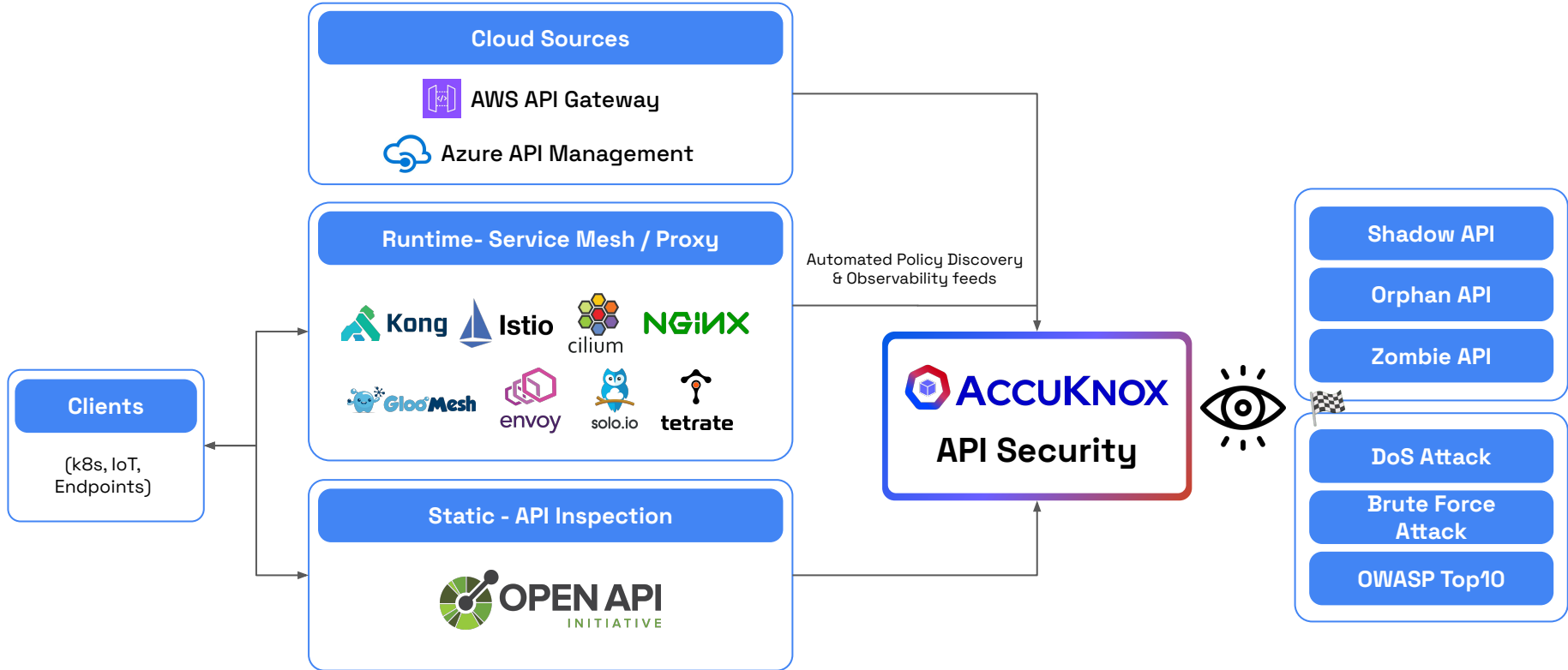
# How are we different/better

Component	AccuKnox	Vendor A	Vendor B
API Discovery & Cataloging	✓	✓	✓
Runtime Monitoring	✓	✓	✓
Access Policy Control	✓	⚠	⚠
Shadow, Orphan, Zombie APIs	✓	✓	✓
On-prem, Air-gapped Installation	✓	✗	✗
Multi Vector Visibility {Process, File, Network, API }	✓	✗	✗

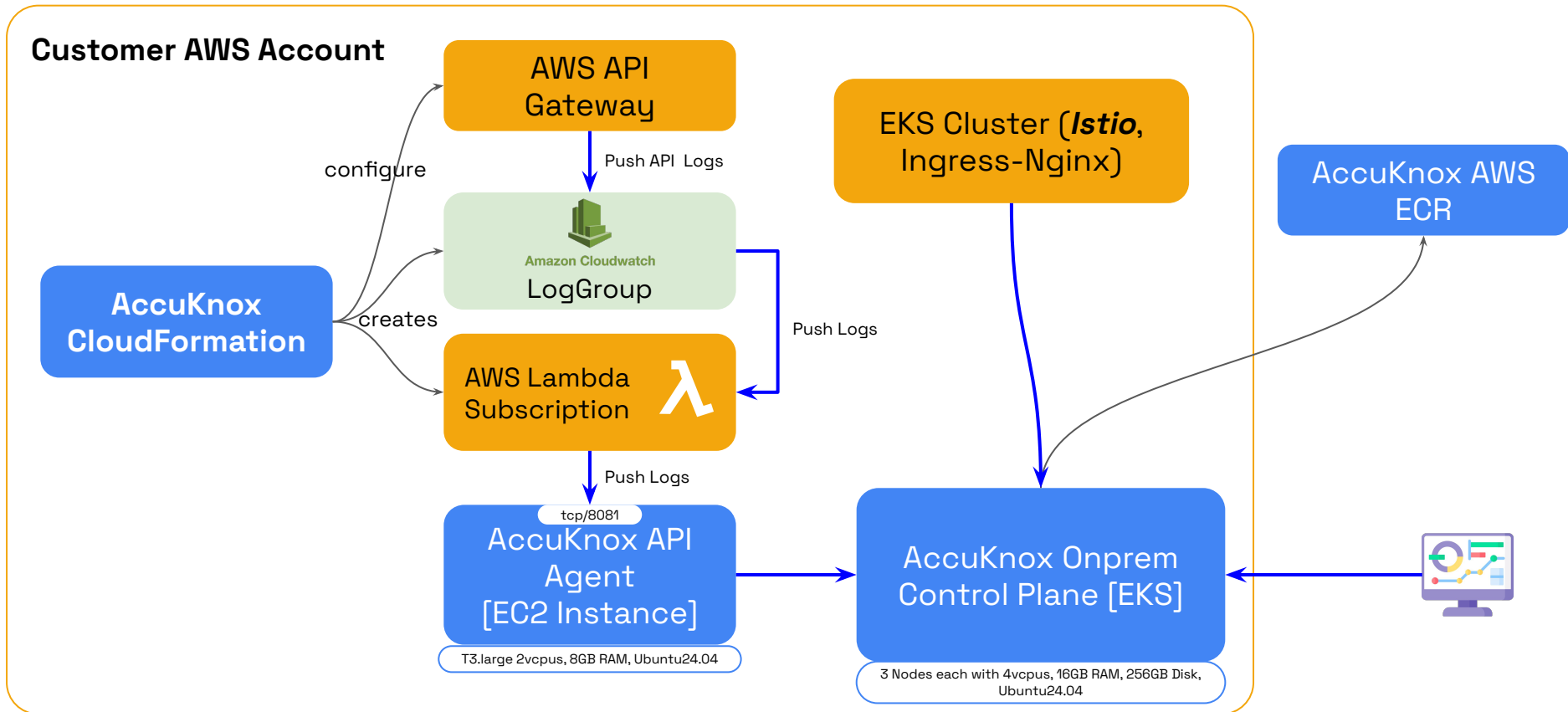
# Use-Cases, Approach mapping

Use-Case	AccuKnox Approach
<b>API Inventory</b> <ul style="list-style-type: none"><li>Discovery and cataloging</li><li>Identify shadow/zombie APIs</li><li>Identify internal/external accesses</li></ul>	✓ Discovery Engine uses the abstraction provided by underlying platform (such as k8s) to discover the service to service communication and identify the API accesses attempted.
<b>Traffic Capture/Inspection</b> <ul style="list-style-type: none"><li>For empirical analysis</li><li>Compliance requirement</li></ul>	✓ Traffic metadata is maintained in the Accuknox data pipeline for empirical analysis.
<b>Shadow, Orphan APIs, Zombie APIs</b>	APIs not part of the spec. APIs in the spec never seen in use.
<b>Deployment modes</b>	Collectors {K8s and non-K8s, API Connectors}
<b>Supported API Connectors</b>	Nginx, Nginx Ingress Controller, Istio, AWS API Gateway, Azure APIM
<b>OWASP Web &amp; API Attacks Protection</b>	Traffic signatures can be used to identify API attacks.
<b>Auto Upgrade to secure connections</b>	Manage service identities and upgrade to secure connections for APIs.
<b>Brute force authn attempts</b>	Identify brute force authentication attempts
<b>Sensitive Data Exposure Identification</b>	<ul style="list-style-type: none"><li>Detect for sensitive data patterns in API responses.</li><li>Customizable sensitive data expression</li></ul>
<b>API Static scanning</b>	Scan the swagger or openapi specs
<b>Rate Limiting &amp; Throttling</b>	Ensure that the valid users don't overuse their permissions
<b>API Spec Generation from Traffic</b>	Automatically get OpenAPI spec from the observed / collected traffic

# AccuKnox API Security Architecture

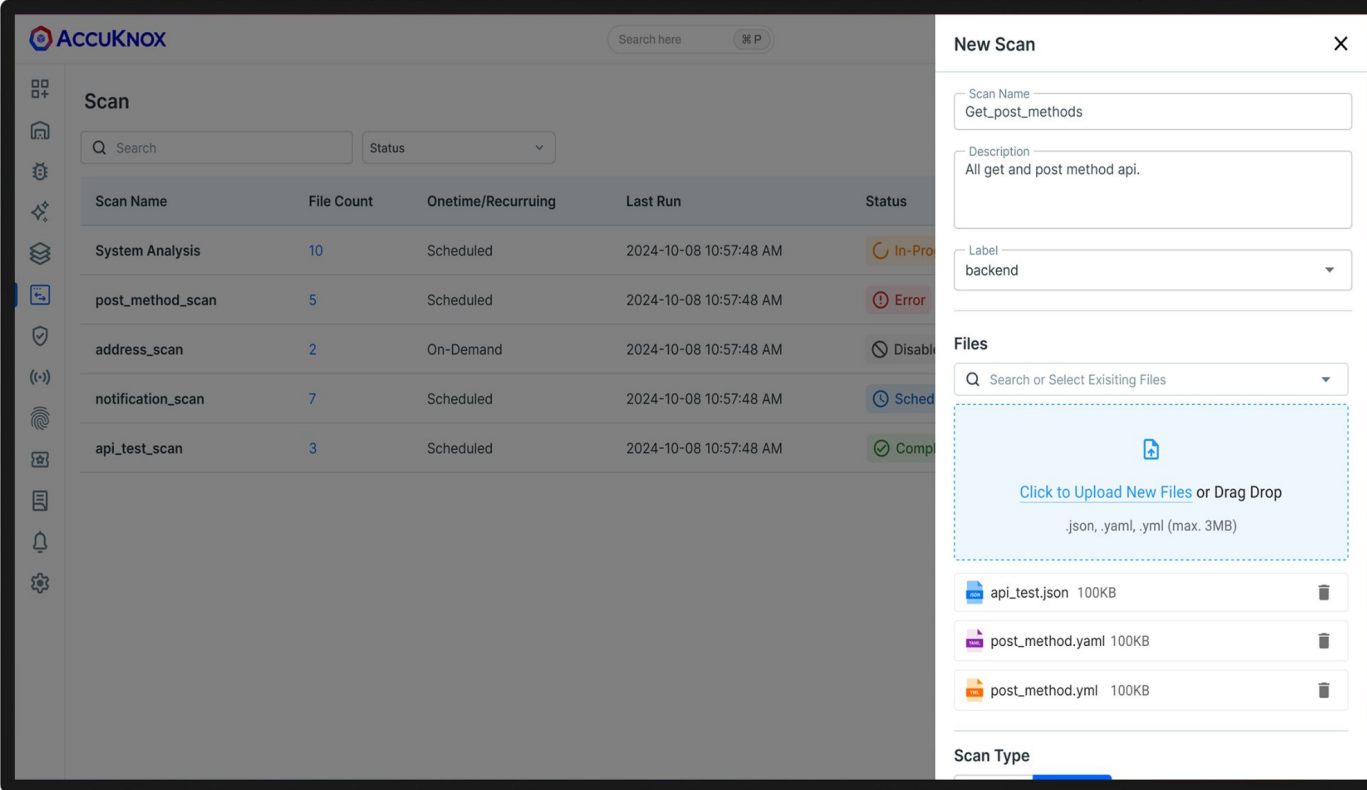


# AWS API Gateway Deployment



# UI/UX Journey

# API Scan Configuration



**Scan**

Search here [P]

Q Search Status

Scan Name	File Count	Onetime/Recurring	Last Run	Status
System Analysis	10	Scheduled	2024-10-08 10:57:48 AM	In-Pro
post_method_scan	5	Scheduled	2024-10-08 10:57:48 AM	Error
address_scan	2	On-Demand	2024-10-08 10:57:48 AM	Disabl
notification_scan	7	Scheduled	2024-10-08 10:57:48 AM	Sched
api_test_scan	3	Scheduled	2024-10-08 10:57:48 AM	Comp

**New Scan**

Scan Name  
Get\_post\_methods

Description  
All get and post method api.

Label  
backend

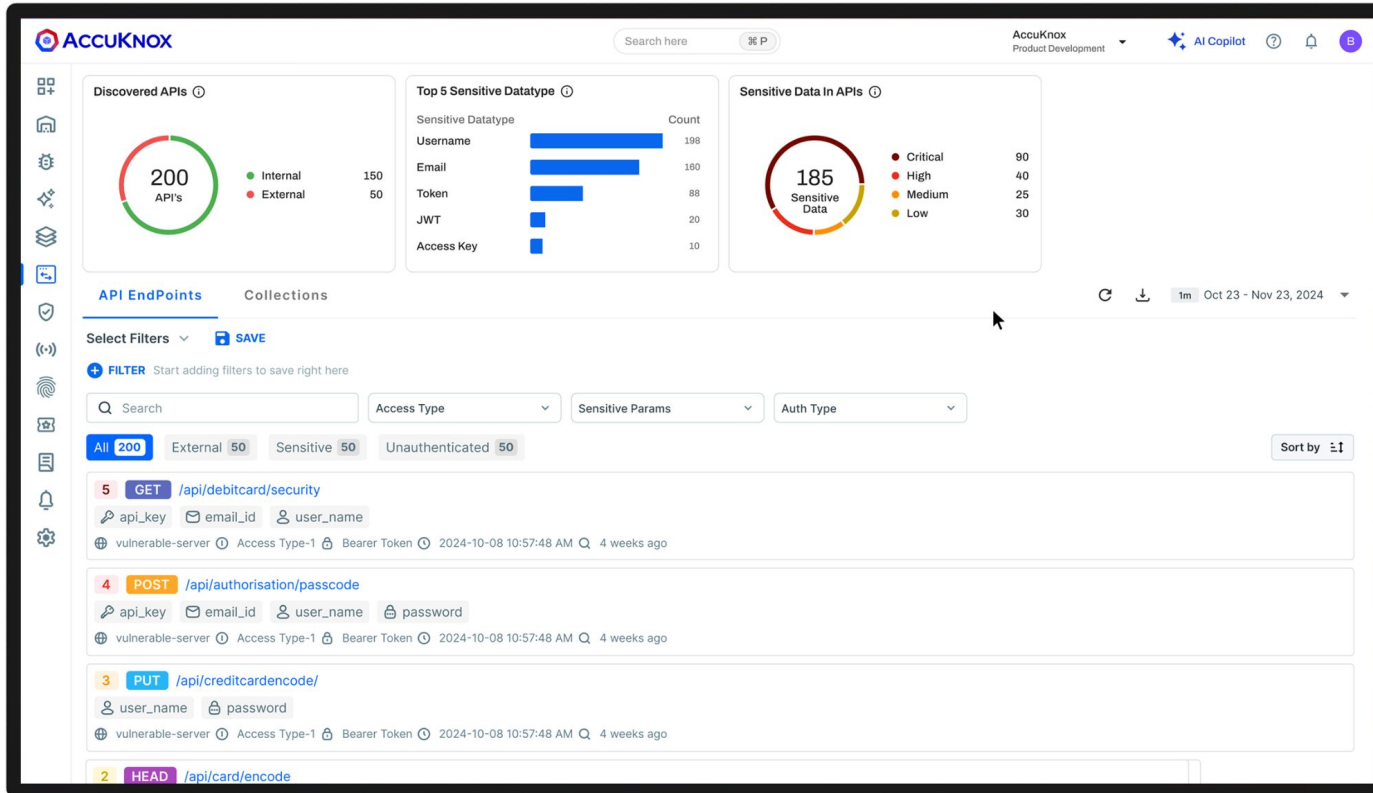
**Files**

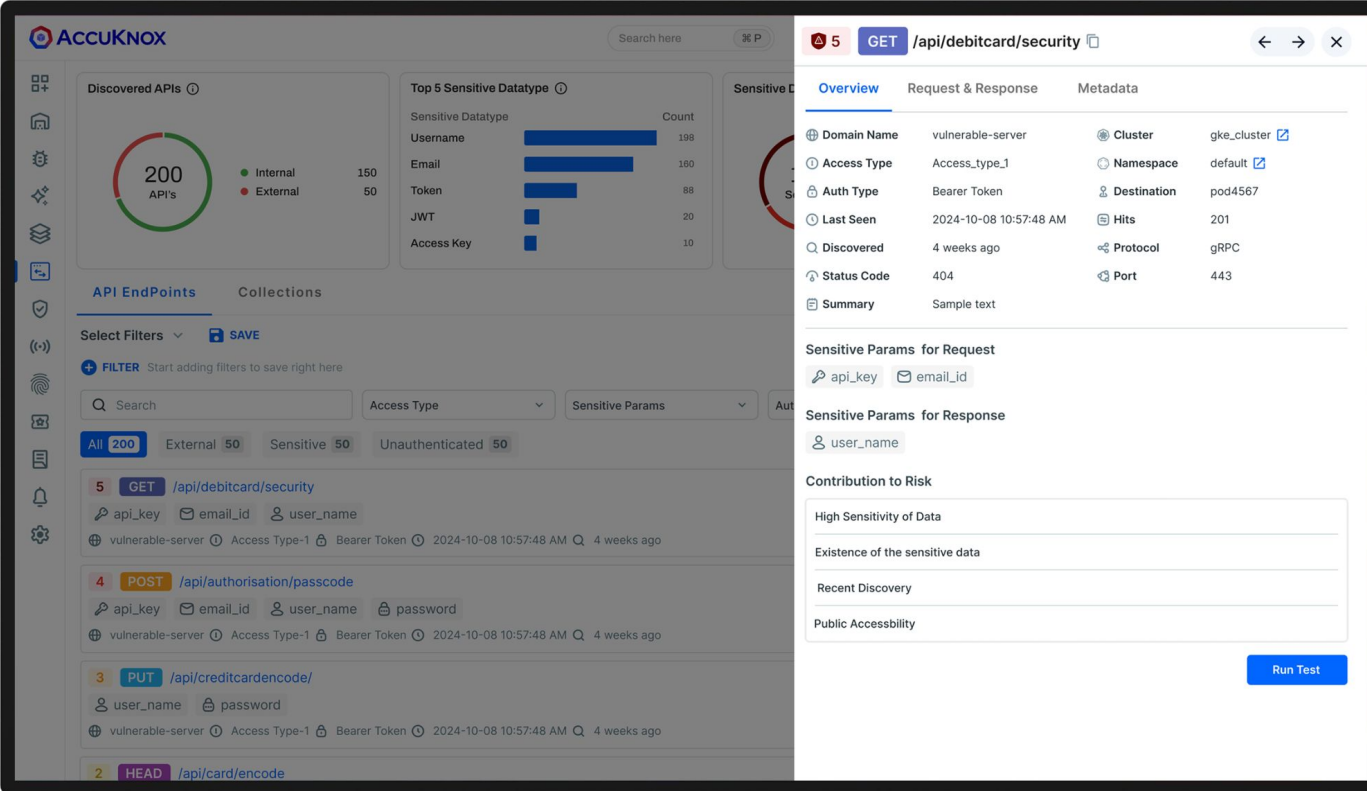
Q Search or Select Existing Files

Click to Upload New Files or Drag Drop  
.json, .yaml, .yml (max. 3MB)

- api\_test.json 100KB
- post\_method.yaml 100KB
- post\_method.yml 100KB

**Scan Type**





The screenshot displays the AccuKnox API Inventory interface. The main dashboard shows 200 discovered APIs, with 150 internal and 50 external. A table lists the top 5 sensitive datatypes: Username (198), Email (160), Token (88), JWT (20), and Access Key (10). The API list includes endpoints like `/api/debitcard/security`, `/api/authorisation/passcode`, `/api/creditcardencode/`, and `/api/card/encode`.

The detailed view for the `GET /api/debitcard/security` endpoint shows the following metadata:

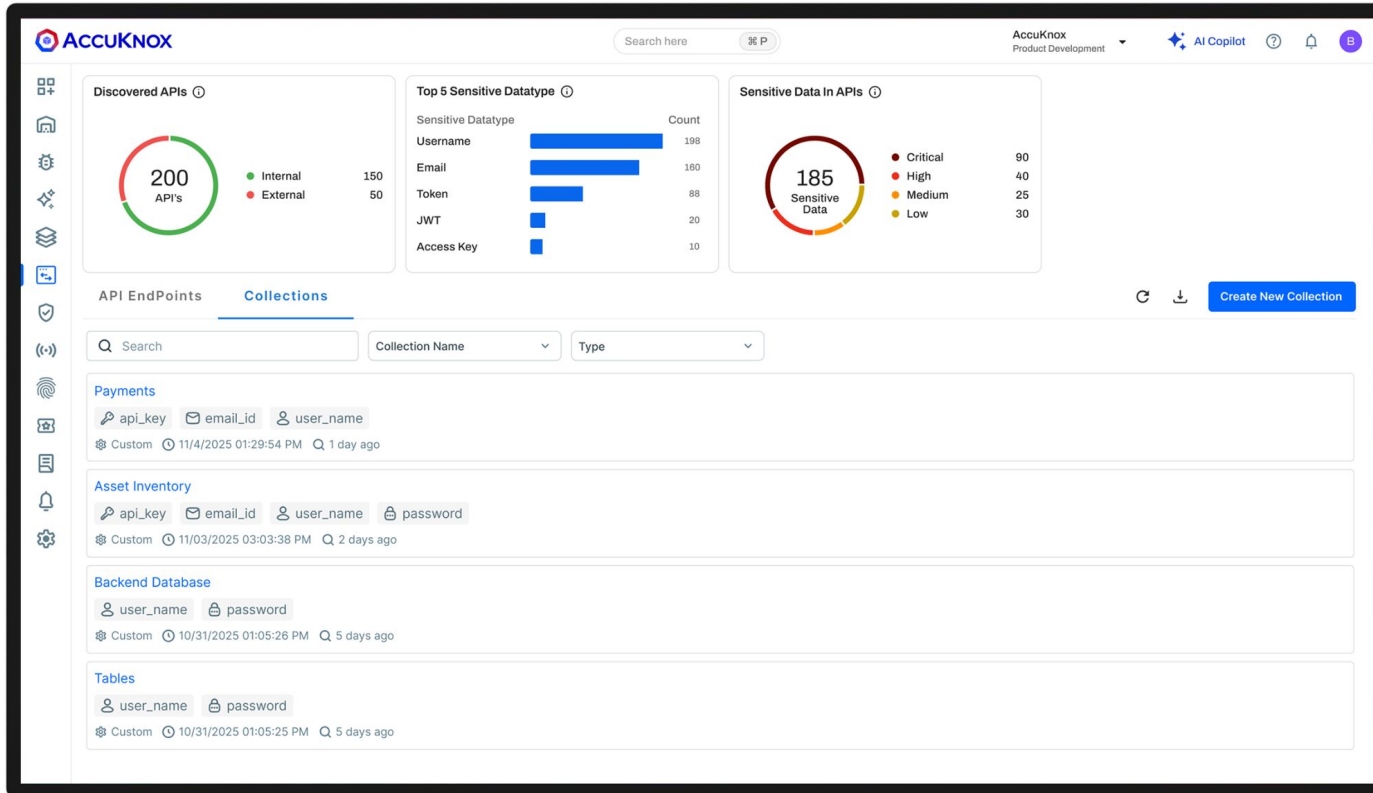
Property	Value	Property	Value
Domain Name	vulnerable-server	Cluster	gke_cluster
Access Type	Access_type_1	Namespace	default
Auth Type	Bearer Token	Destination	pod4567
Last Seen	2024-10-08 10:57:48 AM	Hits	201
Discovered	4 weeks ago	Protocol	gRPC
Status Code	404	Port	443
Summary	Sample text		

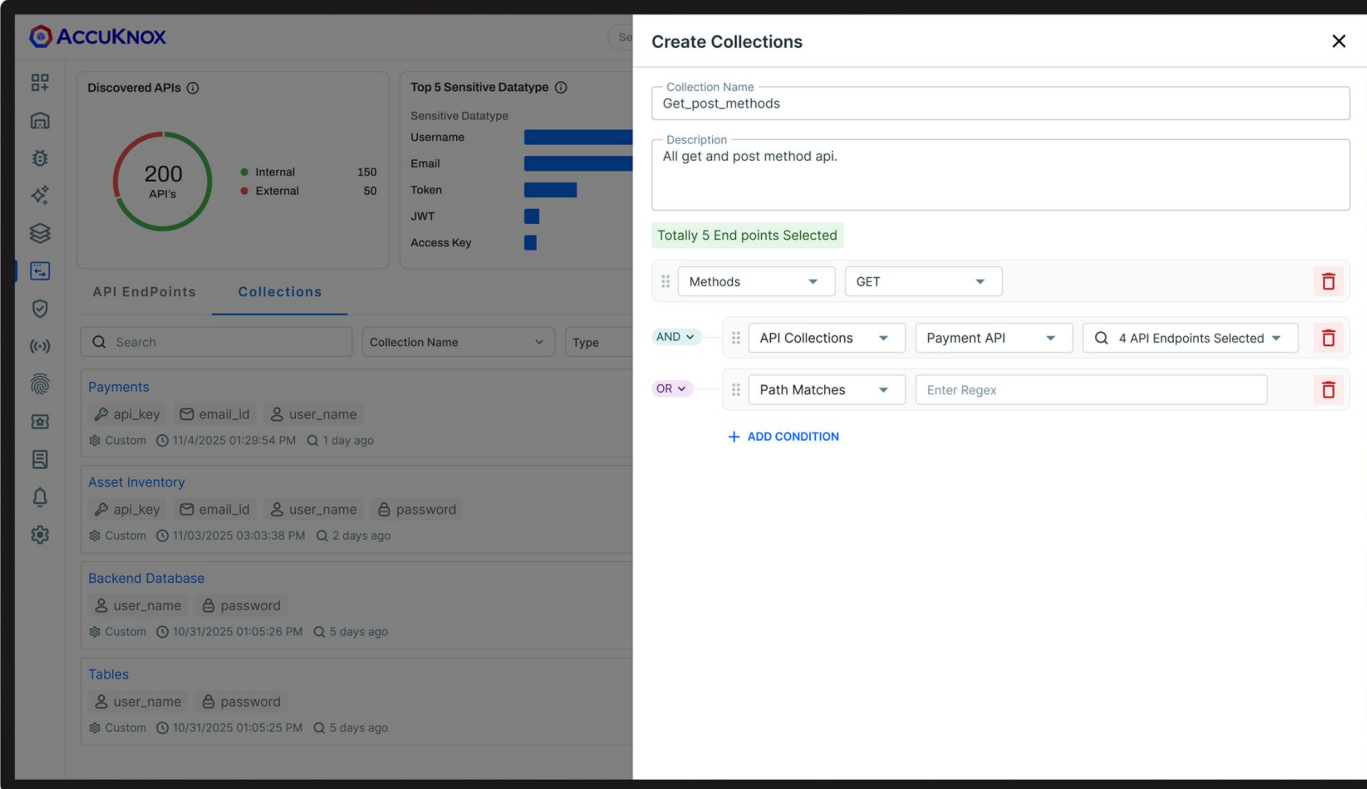
Sensitive Params for Request: `api_key`, `email_id`

Sensitive Params for Response: `user_name`

Contribution to Risk: High Sensitivity of Data, Existence of the sensitive data, Recent Discovery, Public Accessibility

[Run Test](#)





**Discovered APIs** 200 API's

- Internal: 150
- External: 50

**Top 5 Sensitive Datatype**

- Username
- Email
- Token
- JWT
- Access Key

**Payments**

- api\_key, email\_id, user\_name
- Custom | 11/4/2025 01:29:54 PM | 1 day ago

**Asset Inventory**

- api\_key, email\_id, user\_name, password
- Custom | 11/03/2025 03:03:38 PM | 2 days ago

**Backend Database**

- user\_name, password
- Custom | 10/31/2025 01:05:26 PM | 5 days ago

**Tables**

- user\_name, password
- Custom | 10/31/2025 01:05:25 PM | 5 days ago

### Create Collections

Collection Name: Get\_post\_methods

Description: All get and post method api.

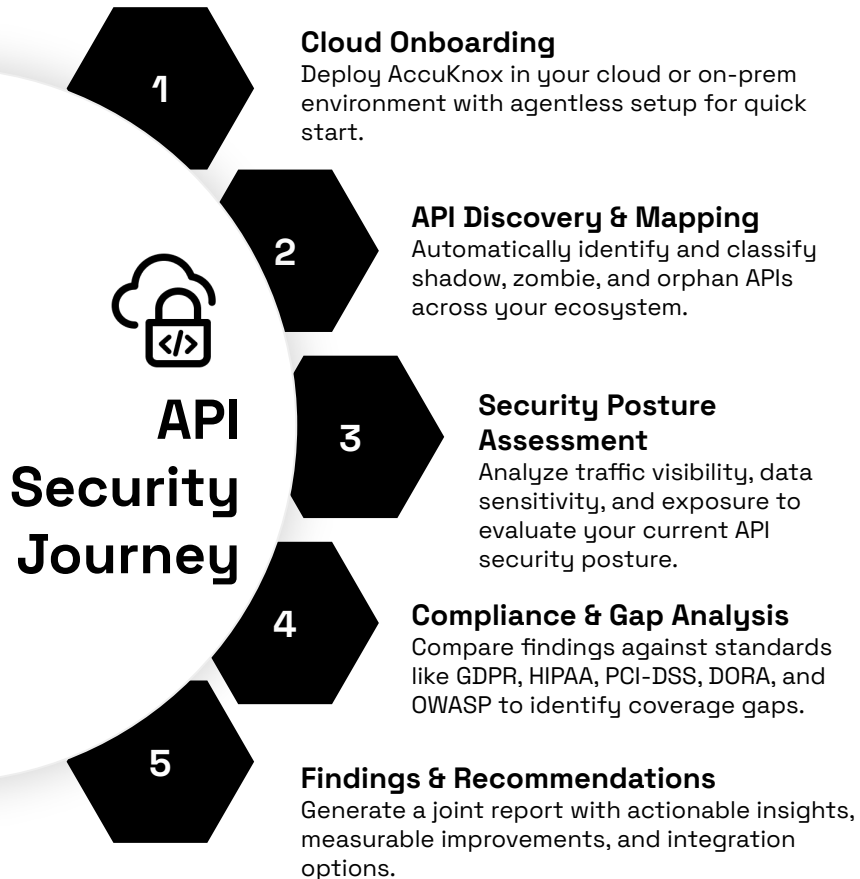
Totally 5 End points Selected

- Methods: GET
- AND: API Collections, Payment API (4 API Endpoints Selected)
- OR: Path Matches (Enter Regex)

+ ADD CONDITION

# Security Report







# SEE US IN ACTION

support@accuknox.com

Certified by



www.accuknox.com

*\*Confidential - Limited Distribution Under NDA*