

SERVICE DESCRIPTION

Edgescan's API discovery service is performed against an organisations external infrastructure. Using multilayer probing technology API Discovery produces a confidence interval to demonstrate the level of confidence Edgescan has that an API was discovered.

Users are alerted in real time once a new API is discovered.

API Discovery is part of Edgescan's award winning external monitoring service offering. With fast network host discovery and asynchronous port scanning to help you identify and monitor assets and network changes. It supports service and OS detection and can generate alerts based on any notable change to the exposed attack surface.

FEATURES

Edgescan Network Vulnerability Management, External Monitoring & API Discovery are all independently offered services.

- API Discovery: Every 24 hours
- External Monitoring: Every 2-4 hours
- Vulnerability management: As often as you require.

Multi-layered checks are applied on all live IP's and across entire CIDR IP ranges.

Discovery of unknown API's is complex. The Edgescan team have developed an innovative approach to discovering API's which offers visibility of known and shadow APIs that are exposed in many enterprises.

API discovery works by applying "proprietary probing techniques" to each exposed endpoint. These production safe probes that are sent produce specific responses, and the results are then analysed by the edgescan correlation engine, supported by a team of vulnerability and discovery experts.

API Discovery provides a read-only data-stream which will be available via:

- The Edgescan [web platform](#).
- The Edgescan API on the [hosts](#) endpoint.

BENEFITS

- Lightweight tests which provide continuous discovery and on demand alerting.
- Identification of known and unknown API's.
- Confidence level for immediate risk triage.
- Runs in the background and provides full coverage across entire global estates.
- Production safe.
- No configuration needed.

| Address | Label | API Detected | OS |
|--------------|-------|--------------|-----------|
| 54.171.25.72 | none | ✓ | Linux 3.X |
| 54.171.25.70 | none | ✗ | Linux 3.X |

| Address | Label | API Detected | OS | Hostnames |
|--------------|-------|--------------|-----------|-----------------|
| 54.171.25.72 | none | ✓ | Linux 3.X | ec2-54-171-25-7 |

| Port | Pathname | API Type | Confidence level |
|------|----------|----------|------------------|
| 80 | /api | REST | 60% |

API DISCOVERY TESTS

- Common API routes
- API descriptor files (Swagger/WADL)
- SOAP protocol detection
- JSON/XML response analysis
- API endpoints Metadata
- API routes in HTTP attributes
- Cookie based API indicators
- Known API format requests
- HTTP status type checks
- TLS Certificate checks
- API format Requests (SOAP/JSON etc)
- Standard and Non-Standard API indicators
- Manifest file detection
- Hostname checks
- Cert common name checks



IRL: +353 (0) 1 6815330
UK: +44 (0) 203 769 0963
US: +1 646 630 8832

Sales and general enquiries:
sales@edgescan.com

View our latest

**2020 VULNERABILITY
STATISTICS REPORT**

at edgescan.com