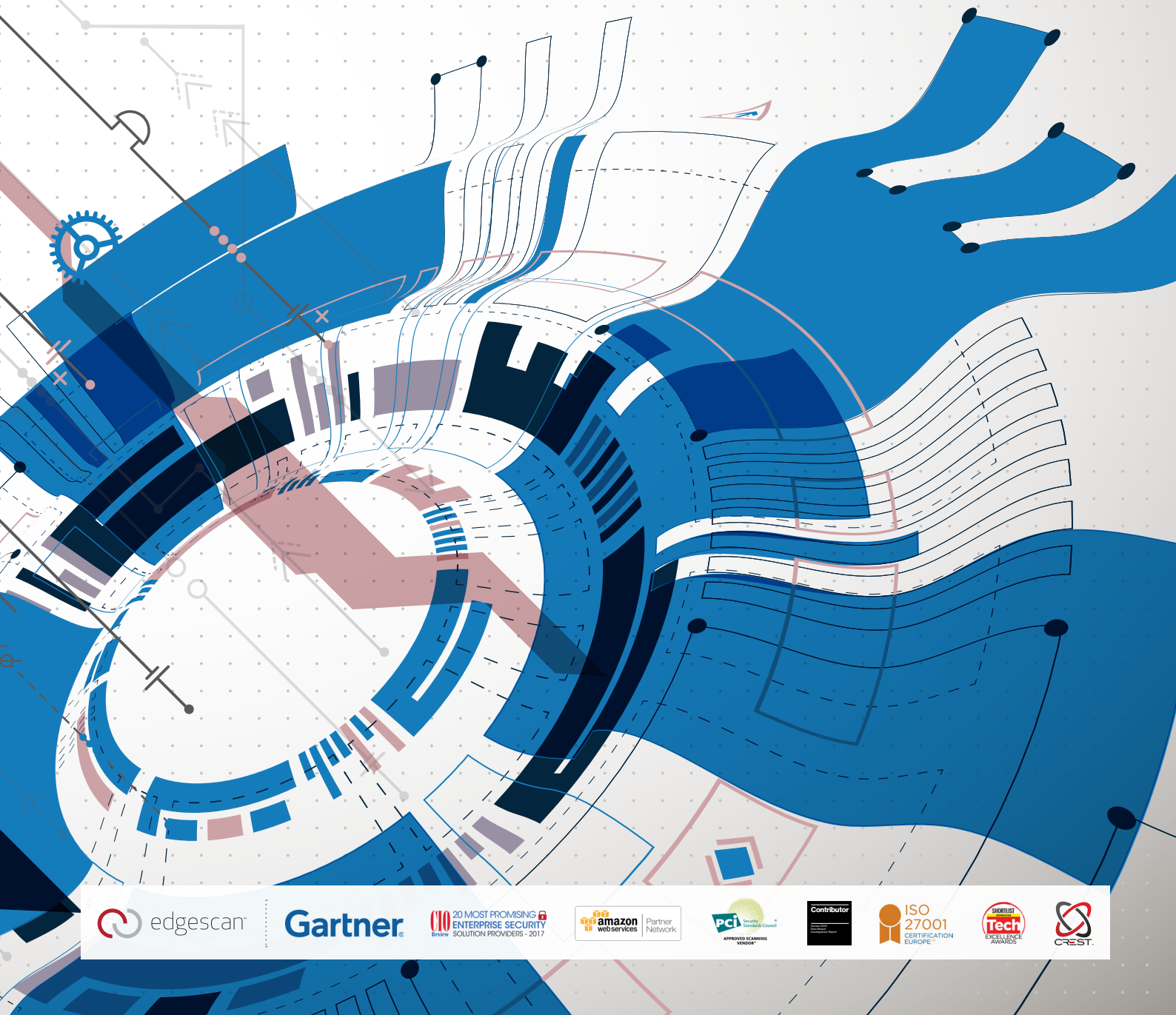
edgescan™

FULLSTACK VULNERABILITY INTELLIGENCE™

API

ASSESSMENTS & SERVICE DEFINITIONS



edgescan | Gartner | CIO Review 20 MOST PROMISING ENTERPRISE SECURITY SOLUTION PROVIDERS - 2017 | amazon web services Partner Network | PCI Security Standards Council APPROVED SCANNING VENDOR | Contributor | ISO 27001 CERTIFICATION EUROPE | SHORTLIST Tech EXCELLENCE AWARDS | CREST

API ASSESSMENT WORKFLOW & PROCESS

STAGE 1

API ATTACK SURFACE RECON

'RECORDING' THE API BEING USED LEGITIMATELY

- Consume WSDL/Swagger/JSON. etc.
- Enumerate the endpoint requests
- Enumerate & understand Access Control:
  - JWT (JSON Web Tokens)
  - API Keys

Recorded Requests: Analysed for parameters which may result in a security issue.

RESTful HTTP Requests: Parameters are examined and marked for assessment.

HTTP Methods: Enumeration (GET, PUT, POST, DELETE).

SOAP and XML security issues: XXE attacks, XML parsing issues, XML encoding, XML Schema assessment and coverage.

Cryptography Checks: weak crypto, poor implementation, data leakage.

Rate Limiting Checks: anti-abuse measures, technical control assessment.

STAGE 2

API ATTACK SURFACE ASSESSMENT & COVERAGE

Input Validation: Assessment of parameters to help ensure Input validation is appropriate.

Output encoding: Assessment of response output for security issues.

Content Type: Assessment of content types such that payloads can only be used as intended.

HTTP Method: Assessment (GET, PUT, POST, DELETE).

Error Handling: Detection of error response codes to help ensure no data leakage.

Security Headers: Check to see if correct content type headers are employed.

- **eg.** *X-Content-Type-Options: nosniff to make sure the browser does not try to detect a different Content-Type than what is actually sent (can lead to XSS). Assessment of CORS (cross origin resource sharing).*

Authorisation Bypass: Assessment of both horizontal & vertical authorisation controls.

Business Logic Flaws: Business contextual assessment of API logic – *"edgescan™ Advanced API license".*

Endpoint / Infrastructure security: "infrastructure security 101" – CVE's, misconfigurations, patching, etc.

HTTPS: Assessment of HTTPS layer employed.

edgescan™ is a sophisticated enterprise-grade vulnerability assessment and management solution that gives the tools you need to control and manage IT security risk.

edgescan™ helps businesses at any size identify and remediate known vulnerabilities in any platform or web application.

edgescan™ is a cloud based SaaS which provides a unique combination of technology and human expertise to assist you with maintaining a strong security posture.

STAGE 3

AUTOMATION & MANUAL VERIFICATION

AUTOMATION FOR SCALE. EXPERT VALIDATION FOR RIGOUR.

- Technical Vulnerabilities are discovered with edgescan™ Automation. Typical examples are Injection attacks (XML, SQLI, RCE, CMDI, XXE etc).
- API assessment coverage manually assessed during onboarding & change.
- Validation on all discovered vulnerabilities – edgescan™ "Delta Analysis".
  - Custom Risk Rating, CVSS, Remediation Advice applied.
- Changes to API's need to be communicated to edgescan™ or a new WSDL/WADL/Swagger needs to be shared when API's are updated.
  - API definitions can be delivered to edgescan™ using a WSDL/ WADL/Swagger or supporting documentation. These are used to map out functions provided by the API ensuring robust coverage.

STAGE 4

VULNERABILITY INTELLIGENCE OUTPUT

VALIDATED VULNERABILITY INTELLIGENCE RESULTS IN THE FOLLOWING:

- **Automated alerting**
  - Slack, jira, ITSM's, GRC, SIEM etc.
- **Reporting & Security Metrics**
  - MTTR, Prioritised Risk measurement, historical data and tracking.
- **Remediation workflow integration**
- **API integration**
- **Remediation support & expertise**
  - 24x7, phone, email, webex support, vulnerability proof of concepts, re-test on demand, developer support etc.
- **Proactive Assessment coverage for continuous visibility**
- **Complete flexibility & managed service approach:**
  - Custom scanning profiles, integration with DevOps via API

SERVICE DEFINITIONS

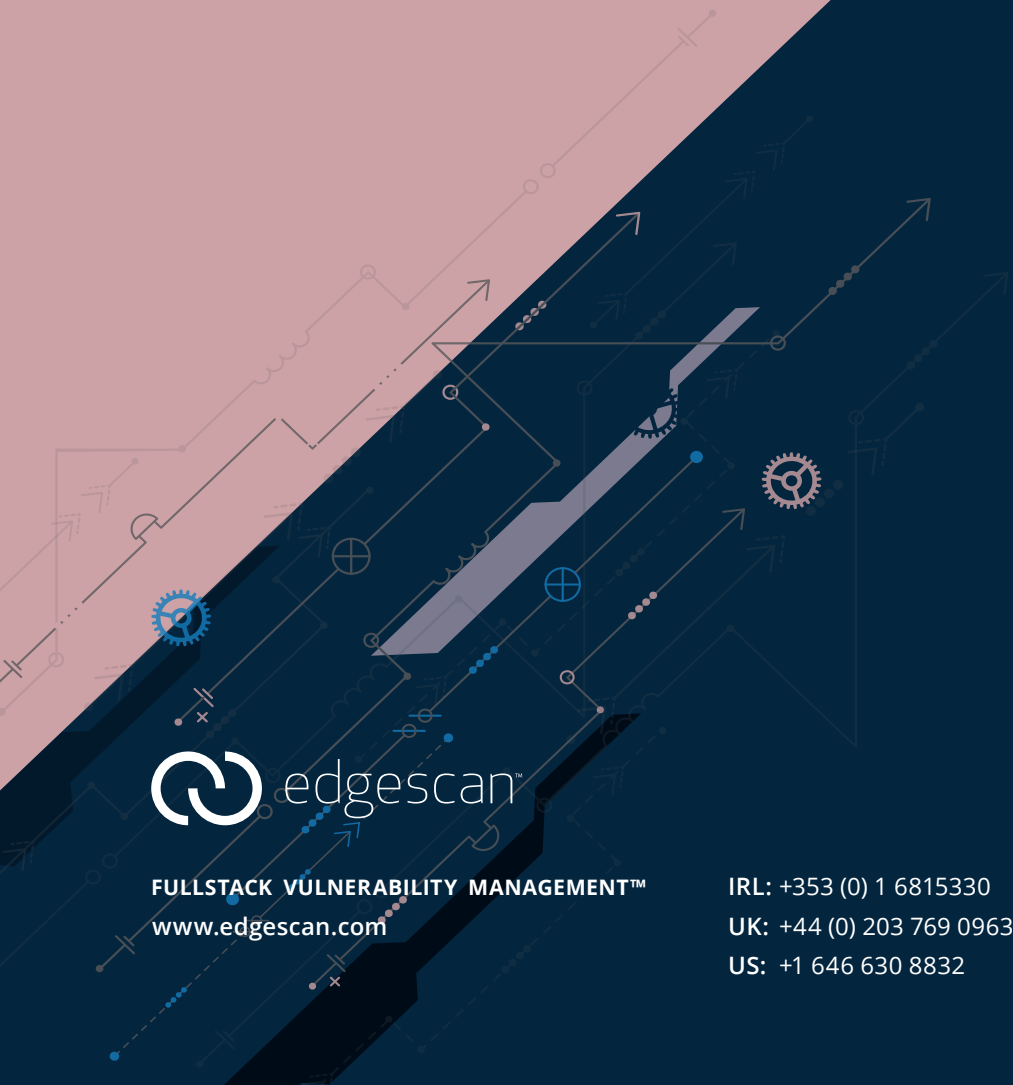
EDGESCAN™ VULNERABILITY MANAGED SERVICE:

edgescan™ is a software-as-a-service platform providing dynamic application security testing (DAST) and host layer vulnerability management coupled with expert validation, alerting, DevSecOps integration and support.

DISCOVERY SERVICES FOR API'S:

API Discovery from edgescan™ is part of the edgescan™ continuous asset profiling service that allows you to understand the API topology within an estate. With edgescan™ cataloguing and categorising correlation technology, it is possible to find the true inventory of APIs and exposures on the internet.

The proprietary discovery process runs at regular intervals across the entire estate, and reports/ alerts the findings back to the end user.



edgescan™

FULLSTACK VULNERABILITY MANAGEMENT™
www.edgescan.com

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

Sales and general enquiries:
sales@edgescan.com

@edgescan