API Security Testing

Rapid Analysis.
Immediate Risk Triage.

Application Program Interfaces (APIs) are the foundation for most of the software that runs the Internet today. Whether used in public or private clouds as well as mobile applications, APIs share some, but not all, of the security controls and software concerns as traditional web applications. API security goes beyond these web application controls to include discovery, posture assessment, and vulnerability testing – with the goal of ensuring connections between systems are safe, reliable, and scalable. DevOps teams must effectively collaborate with SecOps teams to achieve this goal.

Edgescan API Security

API Security Testing is a key component of the Edgescan Platform, offering complete visibility and continuous monitoring to expose weaknesses and risk across your entire attack surface, from unknown assets to API endpoints.

The Edgescan API Security Testing solution is easy to deploy and discovers, tests, and verifies APIs running in hosts across multi-cloud environments. Edgescan uses a hybrid approach that provides automated vulnerability intelligence, coupled with validation that leverages cyber analytics and human expertise - eliminating the unwanted noise of false positives. Providing actionable, prioritized information differentiates Edgescan from legacy scanning tools and results in faster remediation.

A three-phase approach to ensure complete API protection:

1. **Discovery** to understand your overall API topology;
2. **Vulnerability scanning** to accurately detect exposures;
3. **Pentesting** by a CREST certified analyst to manually test and validate your organization's critical host APIs.

Rapid Analysis.
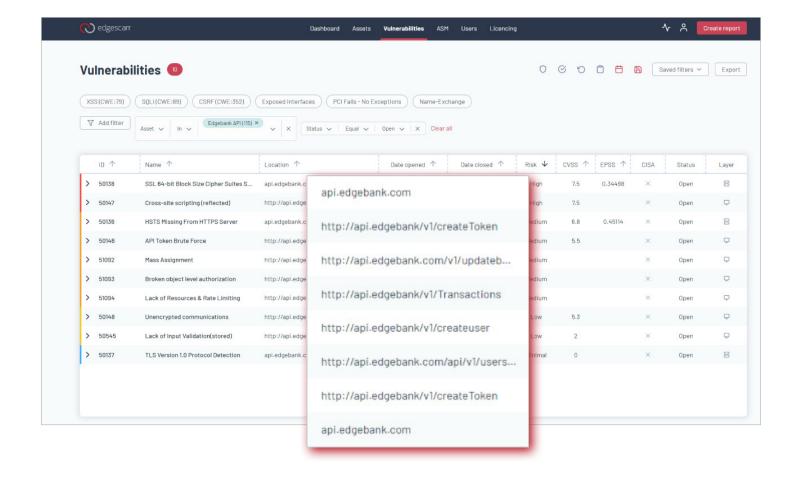### Increased Coverage.

Key features and benefits include:

API Discovery – Identify known and rogue APIs on each host across your IP/CIDR ranges using patented, multi-layer, production safe API probing technology.

Accurately monitor and track changes – Map out entire APIs to ensure a rigorous assessment and detect changes by consuming OpenAPI/Swagger/GraphQL files.

Proactive and continuous API protection – Establish unfettered monitoring and defense against botnets, advanced threats, and DDoS with on demand and real time alerts.

A full suite of API tests – Use Common API routes, API descriptor files (Swagger/WADL), SOAP protocol detection, JSON/SML response analysis, API endpoints metadata, API route in HTTP attributes, Cookie based API indicators, and more.

Complete cloud coverage – Discover hidden and rogue APIs across your cloud providers including AWS, Microsoft Azure, GCP, VMware NSX, and Cisco ACI.

Licensing

Edgescan for API Testing is a subscription-based service and the license includes the following capabilities:

API Discovery: every 24 hours

External monitoring: every 2 to 4 hours

Vulnerability assessments are on demand and unlimited

For more information on how Edgescan can help secure your business, *contact us here*.

**One platform.
Five full-featured solutions.**

EASM   RBVM   AST   API Security
Testing

PTaaS