

# Edgescan Cloudhook™

Illuminate and eliminate cloud risk.  
Automate manual task pain away.

## Gain full visibility across your public cloud with Edgescan's native cloud integration – Cloudhook.

The Cloudhook integration feeds location data (IPs and hostnames) into the Edgescan platform and leverages both the External Attack Surface Management (EASM) and vulnerability management components to illuminate and eliminate risk. As your Cloud endpoints change Edgescan keeps pace with your evolving environment.



Knowing your global footprint and having complete visibility over all your IT assets is the cornerstone of a robust security posture. Organizations simply cannot secure what they cannot see. The modern cloud attack surface is ephemeral and in constant flux in order to support business critical infrastructure. The Edgescan platform keeps pace, ensures complete visibility and eliminates blind-spots so all IT assets are included in security monitoring and testing to build a resilient business posture.

Security tools that dynamically inventory and monitor your assets as your global attack surface expands into the cloud are no longer a “nice to have.” They are a requirement for robust security program. This is where the Edgescan Platform excels.

## How the EASM Solution Works

Edgescan's EASM solution provides complete visibility across the cloud and identifies security blind spots and maps all assets. It continuously evaluates information in real-time as new assets are deployed, decommissioned or as a system changes and leverages both vulnerability data and business context to prioritize risk.

## How the Vulnerability Management Solution Works

Get full-stack vulnerability management (VM) that includes application security testing, API security and network/device testing across your entire attack surface. VM dynamically assesses JavaScript frameworks, Angular, AJAX, React, HTML5 and single-page applications for vulnerabilities. Everything is validated eliminating false positives and improving efficiency.

**Complete cloud risk visibility. Automate away laborious tasks.**

**Reduce manual processes** by automating cloud syncing tasks.

**Gain complete visibility into your public cloud** and take steps to prevent exposures.

**View and monitor cloud assets** and their security posture in one unified platform.

**Automate the testing on dynamically allocated addresses** and never worry whether a new service is being included.

## Eliminate manual tasks. Give time back to SecOps and Dev teams.

Keeping pace with modern security problems is key to ensuring vital gaps are plugged in the traditional inventory & asset management workflows. Removing the dependence on a human to keep pace with the cloud infrastructure changes allows organizations to be more agile with their asset management and security resilience initiatives.

- Sync IP & hostnames from your cloud environment
- Auto-enroll addresses for EASM (External Attack Surface Management), vulnerability management or penetration as a service (PTaaS)
- Offload old locations (do we even own those pesky dynamically allocated IPs!)
- Auto-licensing allocation rule, allows you to automate the type of license that gets applied to an asset. This allows EASM, Vulnerability Scanning or penetration testing to be planned from provisioning -> results.

### Integration Workflow

