Censys Attack Surface Management

THE PROBLEM
Keeping track of publicly exposed assets can be difficult, especially as companies migrate to the cloud, workforces become more distributed, and companies acquire security debt from mergers or acquisitions.

THE SOLUTION
Censys helps discover, monitor, and remediate risks in your digital landscape. The founders of the Zmap Project created the Censys Attack Surface Management Platform to help organizations understand their external exposures with the most-trusted Internet-wide dataset.

POWERED BY THE BEST DATA IN THE INDUSTRY

HOW OUR ASM PLATFORM WORKS
1. Push discovered assets into a Vulnerability Scanner or Web Application Scanner to conduct a deep scan.
2. Censys automatically discovers connections between Internet entities to enumerate every asset in your attack surface. This process runs on a daily basis.
3. Our risk framework identifies exposures that you may not be aware of and provides remediation recommendations.
4. Our APIs and integrations can push discovered assets or critical exposures into your existing workflows.

PLUG INTO EXISTING WORKFLOWS

ENHANCE WITH OTHER CENSYS PRODUCTS
Cloud Connector
- Push your cloud IPs into Censys to get daily scan updates on exposures in your known cloud environments.

Home Network Risk Identifier
- Push IPs from your VPN logs into the Platform’s vulnerability database to provide network-wide insights.

Censys Global Dataset
- Empower Threat intelligence with the industry’s largest Internet-wide net lists to identify and track threat actors or to tweak SOC playbooks.