Censys

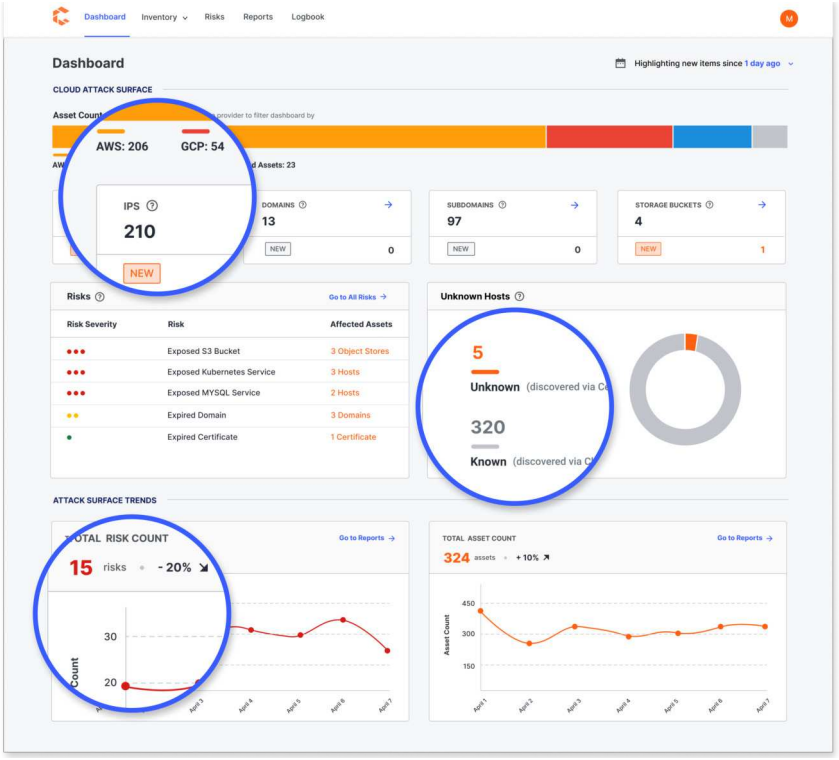
Censys Cloud Security

Best Attack Surface Management for the Cloud

Censys Attack Surface Management Platform continually discovers unknown cloud assets and risks ranging from unknown cloud providers to unmanaged cloud storage buckets, so you can eliminate security blindspots and resolve risks in real time.

Key Use Cases

- Discovering unknown cloud providers, accounts, and assets
- Providing a converged internet inventory across all cloud providers and accounts
- Identifying cloud risks and misconfigurations (e.g., public storage buckets)
- Ensuring organizational compliance across both known and unknown cloud accounts and providers



What Makes Censys the Best ASM for the Cloud

Beyond traditional assets, Censys discovers modern cloud specific assets

Censys offers discovery of cloud assets including storage buckets. Through integrating with your cloud account, Censys automatically analyzes your cloud configuration and finds accounts and assets you own.

Censys provides a cloud inventory that incorporates your unmanaged cloud accounts and hybrid cloud assets

Censys offers visibility across Azure, AWS, GCP, lesser known providers and on prem assets that enables you to import assets into your asset inventory, check for security problems, and contextualize what we've found online.

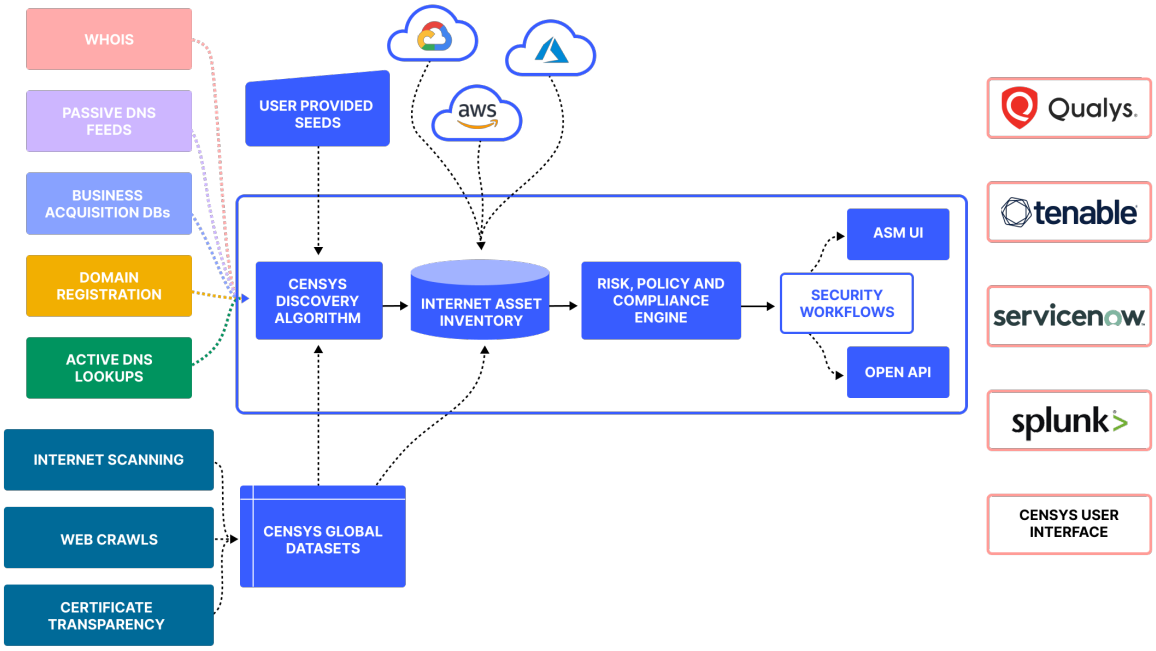
Easy deployment of cloud integrations

Integrations that provide greater visibility and discovery capabilities in AWS, Azure, and GCP are automatically deployed using Terraform or AWS Cloud Formation with no management required.

Your Suite of Security Tools Can't Protect Assets They Don't See

Security tools that rely on cloud APIs (e.g., CSPM, CASB, and CWPP platforms) only find security weaknesses in the cloud accounts that you know about and have configured for monitoring. Unfortunately, known cloud accounts tend to contain IT-managed assets rather than your riskiest assets.

How does the Censys ASM Platform Work?



Censys connects to your existing cloud accounts and continually analyzes your cloud configurations to understand how your organization functions. In turn, our discovery algorithms use these organizational and infrastructure insights to mine our industry-leading Internet scan and crawl data as well as external datasets (e.g., passive DNS feeds) to find cloud assets that you don't yet monitor.

Benefits of Integrating Censys with your Security Stack:

Censys uncovers blindspots in your cloud monitoring

Censys aguments your CSPM through finding accounts and assets that your CSPM tools don't monitor in AWS, Azure, GCP, and other lesser known providers not connected to your CSPM in order to eliminate potentially risky blindspots.

Censys fills gaps in your asset management program

Censys can keep up with the pace of your development and ops teams and feeds potentially unknown cloud assets into your existing asset management tools like Axonius.

Censys feeds your SIEM or ticketing system

Censys can automatically create tickets or security events when new assets or security risks are found in order to help you remediate risks, save time, and promote internal orchestration.