Censys

Attack Surface Management

What is Attack Surface Management?

Attack Surface Management (ASM) is a security vertical that focuses on the continuous discovery of all Internet-facing assets and their associated risks. Gartner defines External Attack Surface Management (EASM) as:

> *"An emerging product set that supports organizations in identifying risks coming from internet-facing as sets and systems that they may be unaware of"* (Gartner, 2021)

Why is Attack Surface Management a Priority for CISOs in 2021?

Organizational security boundaries have become tremendously complicated. Enterprises frequently have assets spread across hundreds of cloud accounts and dozens of other networks. Organizations also struggle to track down cloud services that employees launch outside the purview of traditional IT and security teams ("Shadow IT").

Not only are the locations of risks increasing, but the types of risks are themselves diversifying. Every cloud provider has unique services, and even seemingly simple services like Amazon S3 are riddled with configuration pitfalls that can lead to a data breach.

What do ASM Platforms provide?

Competitive ASM platforms provide several key features:

- Continuous discovery of unknown Internet assets like services, websites, and storage buckets.
- Comprehensive inventory of all Internet assets regardless of location or account.
- Investigative tools to understand organizational dependencies and respond to new Internet threats.
- Risk engine to identify Internet-facing misconfigurations, risks, and compliance failures.

73%

of cybersecurity incidents in 2020 involved ***external cloud assets***

Capital One was fined

$80 million

in connection with a misconfigured cloud asset in 2019 ***after the exposure of***

100M+

customer data records

50%

of enterprises will ***unknowingly*** and ***mistakenly expose*** IaaS storage services, network segments, applications or APIs on the public internet in 2021.

Censys

Censys Attack Surface Management Platform

Continuous Internet Discovery and Complete Cloud Visibility

Censys continuously discovers your Internet assets and monitors them as part of a comprehensive inventory, identifies egregious security issues, and prevents oversights from becoming data breaches or compliance failures.

Customers use Censys to:

Discover Potentially Unknown Assets

Censys eliminates security blindspots by continually discovering Internet assets and cloud accounts that you don't know about. Censys ASM automatically learns how your organization operates and uses that insight to uncover potentially unknown services, hosts, websites, and storage buckets regardless of their location or provider.

Inventory and Investigate Internet Assets

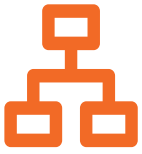
Censys provides a comprehensive inventory of your Internet assets drawn from our Internet Discovery Algorithm and cloud connectors. Our investigative tools help analysts understand every Internet asset's attack surface, ownership, history, and configuration, as well as immediately respond to new Internet threats.

Cloud Governance

Censys continually checks all of your Internet assets for misconfigurations and security weaknesses regardless of provider. We integrate with your existing security platforms like SIEMs, VM providers, and ticketing systems to enable workflows around when new assets and security risks are identified.

Identify and Remediate Risks

Mismanaged cloud services (e.g., S3 Storage Buckets) regularly result in massive data breaches. Censys helps uncover potentially unknown and misconfigured cloud services, projects, and accounts, as well as aids the transition of assets to managed cloud accounts regardless of the cloud provider.



Organizational Compliance

A misconfiguration outside of your primary cloud provider or enterprise network can easily bring your organization out of compliance. Censys checks all of your Internet assets for security weaknesses that could bring your organization out of compliance. In addition to external compliance programs, Censys lets you define your own organizational policies.

Mergers and Acquisitions

Censys enables security teams to immediately begin understanding and remediating security problems stemming from a new acquisition before they pose risk to your organization.