

The Attack Surface Management Buyer's Guide

Essential Criteria for Choosing an ASM Solution



Table of Contents

Executive Summary	1
Expanding Horizons, Emerging Threats: The Evolving Attack Surface	3
> Why Attack Surfaces Are Growing	
> Shifts in the Broader Ecosystem	
ASM: A Must for the Modern Security Organization	6
> Key ASM Use Cases	
How Does ASM Compare to Other Tools in the Tech Stack?	9
> ASM vs. Vulnerability Management	
> ASM vs. Cloud Security Posture Management	
> ASM vs. Third-Party Risk Management	
How to Find a Superior ASM Solution	11
> Asset Discovery	
> Inventory and Exploration	
> Data Depth and Accuracy	
> Reporting	
> Risks and Compliance	
> Integrations	
> Operationalization	
How to Build a Business Case for ASM	17
> 5 Reasons to Invest in ASM	
See More with Censys ASM	19
> Identify, Prioritize, and Remediate Threats with Industry-Leading ASM	



Executive Summary



Organizations across industries find themselves in a race to protect their assets against a growing set of cyber threats. Digital infrastructures have expanded exponentially, not just in scale, but in diversity. From cloud services and remote work solutions, to Internet of Things (IoT) devices and beyond, the digital footprint of a modern organization extends far beyond the traditional boundaries of IT systems. This expansion has given rise to what we refer to as the “attack surface” – the sum total of all possible points where an unauthorized user can try to enter or extract data from an environment.

As the attack surface expands, it often becomes more dynamic, adapting to the contours of technological innovation and organizational change. This fluidity presents a formidable challenge to cybersecurity teams: the larger and more diverse the attack surface, the more opportunities there are for adversaries to exploit vulnerabilities. Traditional security measures, designed for a bygone era of less complex IT ecosystems, are often inadequate to address the nuances of this evolving landscape.

Enter Attack Surface Management (ASM), which focuses on providing comprehensive visibility and control over the entirety of an organization’s attack surface.

ASM is a proactive approach to cybersecurity that empowers security teams to comprehensively discover internet-facing assets and remediate associated security risks. Unlike other security solutions, which focus on managing known accounts and assets, **ASM also focuses on actively finding potentially unknown assets and risks tied to an organization’s attack surface.**



ASM solutions help identify vulnerabilities and prevent data breaches by:

1. Automatically discovering internet assets (e.g., hosts, services, websites, storage buckets) across all networks and cloud providers on the attack surface
2. Providing a comprehensive inventory of internet assets and investigative tools to understand organizational dependencies and immediately respond to new threats
3. Continually checking assets for security weaknesses and misconfigurations and providing a prioritized set of risks to address
4. Identifying violations of both organizational policies and external compliance programs (e.g., PCI DSS and NERC CIP)
5. Enabling teams to evaluate the dependencies and security risks of subsidiaries and acquisitions.

ASM is a critical part of the modern security tech stack.

As attack surfaces continue to expand with the rise of third-party and open source infrastructure, multi-cloud strategies, and SaaS tool sprawl, ASM has become an essential means of ensuring these dynamic assets are protected. Consider that [70% of organizations surveyed by Enterprise Strategy Group](#) said they experienced **at least one cyberattack that started through the exploit of an unknown or unmanaged internet-facing asset**, including software, cloud-based workloads, user accounts, and IoT devices. Organizations who underestimate the value of ASM do so at the risk of compromising their security.

What You'll Learn in This Guide

The Attack Surface Management Buyer's Guide is for leaders who recognize the critical importance of adapting their tech stack to meet the needs of a changing cybersecurity landscape. Whether you're a CISO, an IT manager, or a business executive, this guide will equip you with the knowledge you need to understand your organization's attack surface, the challenges it presents, and the criteria for choosing an ASM solution that aligns with your security posture and business objectives.

Let's get started.

Expanding Horizons, Emerging Threats: The Evolving Attack Surface



We'll begin with a basic understanding of the attack surface: what is it, and how is it changing?

An attack surface represents all of the digital endpoints that an attacker could breach to gain access to an organization's network.

When we talk about the endpoints that make up these attack surfaces, we're usually talking about the things like servers, network infrastructure, user devices, internet services, websites, and storage buckets. In general, we're referring to assets that are external-facing and typically visible on the public internet.

Not only does the attack surface represent a potential point of entry for adversaries, it also represents a security perimeter that is increasingly challenging for security teams to manage. That's because attack surfaces are growing and becoming more complex. [The 2023 State of Cyber Assets Report](#) finds that on average, organizations' attack surfaces are growing at 130%+ a year.

There are several reasons for this expansion.

Why Attack Surfaces Are Growing

Cloud Adoption:

The cloud is ubiquitous: 94% of enterprises now use some form of cloud services according to [a report from Colorlib](#). Whereas server infrastructure was once protected behind a network perimeter or firewall, organizations now have hundreds to thousands of cloud accounts, each of which can have internet-facing points of ingress. [The 2023 State of Cyber Assets Report](#) finds that in 2023, "Security practitioners were responsible for an average of 334 unique Cloud Service Provider (CSP) accounts across all organizational sizes, or an average of 225 and 559 unique accounts at large and mid-sized organizations, respectively." For many enterprises, this means the majority of their internet-facing risks are now cloud-based.

Elastic and Serverless Resources:

Cloud has enabled not only quickly scaling server infrastructure (IaaS), but has also introduced new classes of computing infrastructure (PaaS) like serverless compute (e.g., AWS Lambda) and storage (e.g., AWS S3) and ephemeral assets (e.g., containers). These serverless, ephemeral cloud types make it easier to spin up more assets, faster – posing an even greater challenge for security teams tasked with tracking and managing asset inventory.

Shadow IT:

The cloud's low barrier to entry enables development teams to be more efficient, but it simultaneously allows non-IT employees to launch unauthorized infrastructure unbeknownst to security teams. Censys finds that enterprises typically have 30–80% more assets publicly exposed than expected due to Shadow IT. In many cases, assets are hosted by unsanctioned low-cost providers like Digital Ocean and OVH, and are completely unknown to IT teams.

Increased M&A:

Fortune 500 companies are evolving their products by acquiring startups or other small companies with cutting edge capabilities. Unfortunately, many startups or smaller companies have less mature security programs and can introduce risks during the acquisition process. These technological and societal shifts have resulted in a significant increase in both the types and number of internet-facing assets that companies need to track and secure.

Shifts in the Broader Ecosystem

It's not just the explosive growth in the number and types of internet-facing assets that has elevated the importance of ASM. Several major ecosystem shifts also necessitate a dedicated ASM program:

1. Cloud Services Are Riddled with Configuration Pitfalls

Cloud services appear deceptively simple to configure, but a single error can easily expose entire datasets on the public internet. As a result, organizations are now frequently breached simply through publicly exposed storage buckets (e.g., Amazon S3) and databases (e.g., Elasticsearch and MongoDB). According to research conducted in [2023 by Qualys TotalCloud Security Insights](#), cloud resource misconfiguration is the foremost concern for ensuring the security of cloud environments. [Censys' own research](#) has identified nearly 2 million database exposures and more than 1.9 million RDP exposures across a dozen cloud providers that we investigated.

2. **Attacker Efficiency**

It should come as no surprise that the volume of cyber attacks is increasing year-over-year. Comb through headlines on any given day and you'll likely see reporting related to a cyber attack. Reporting from the Harvard Business Review shares that from 2022 to 2023, there was a [20% increase in data breaches](#) in the U.S., and [twice as many data breach victims globally](#).

Attackers are also leveraging the power of AI to increase the speed and sophistication at which they launch attacks. AI can be used for advanced phishing and social engineering attacks, as well as creating malware that's harder to detect, among other objectives. In 2024, [Microsoft and OpenAI reported evidence](#) of nation states using AI to launch cyber attacks.

3. **Increased Compliance Fines**

Companies have faced record-setting compliance fines over recent data breaches. The U.S. Treasury Department ordered Capital One to pay an [\\$80 million civil penalty](#) for its failure to properly secure data in the cloud after attacks stole the personal data of over 100 million customers. The U.S. Treasury Office of the Comptroller of the Currency (OCC) stated that, "The OCC took these actions based on the bank's failure to establish effective risk assessment processes prior to migrating significant information technology operations to the public cloud environment and the bank's failure to correct the deficiencies in a timely manner."

Confronting a Changing Landscape with ASM

The increase in public-facing services, attacker agility, data breaches, and compliance fines associated with a public-facing misconfiguration or vulnerability are just some of the key factors that illustrate why organizations need a formalized strategy for understanding and managing their attack surface on a continuous basis. ASM solutions are built to meet that need. Let's take a closer look at what ASM solutions offer and how organizations can benefit.

"I've seen the consequences of not knowing your assets. I can't defend what I don't know about, right? The benefit of knowing your assets is of course preventing a very, very serious issue from occurring."

- Director, cyber command center, technology insurance | The Total Economic Impact™ of Censys
External Attack Surface Management Report

ASM: A Must for the Modern Security Organization



Attack Surface Management (ASM) is a category of security solutions that comprehensively discover and inventory internet assets and risks. [ASM solutions like Censys](#) are typically cloud-based SaaS products that continually find public-facing assets across all providers, networks, and accounts. ASM solutions employ proprietary algorithms fed by internet data sources (e.g., passive DNS, WHOIS, Internet-wide scans) to automatically identify assets that belong to an organization and, in turn, analyze those assets for security risks and compliance violations.

ASM has been widely recognized as a critical part of the modern security tech stack.

Analyst firms like Forrester and Gartner now regularly report on the ASM landscape and advise on best practices. In their 2022 EASM Landscape Report, Forrester explains that “External attack surface management (EASM) helps security and risk pros better assess third parties and M&A targets, uncover and reduce cloud sprawl, and bring IT and security into agreement about risk prioritization.” In [Forrester’s Security Survey, 2023](#), 72% of security decision-makers said that their organization had adopted EASM or is currently doing so.

The U.S. Federal government is also now pushing for agencies and corporations across sectors to bolster their security efforts through more proactive asset discovery and monitoring. In a [2022 binding operational directive](#),¹ CISA stated that “continuous and comprehensive asset visibility is a basic precondition for any organization to effectively manage cybersecurity risk.” In 2023, CISA went on to release [BOD 23-02](#) with the objective of mitigating the risks associated with remotely accessible management interfaces that might allow configuration or control of federal agency networks from the public internet. The Federal government’s efforts to improve their overall security posture and those of their adjacent systems through stronger asset discovery and management underscores the value of, and need for, solutions like ASM.

¹ CISA, Oct. 2022

Key ASM Use Cases

What specifically makes ASM such an essential addition to the security tech stack? ASM solutions improve security posture and unlock efficiencies by providing:

- Continuous Asset Discovery
- Comprehensive Asset Inventory
- Exposure and Risk Management
- Security Framework and Compliance
- M&A and Subsidiary Risk Analysis

Let's talk in more detail about why each of these use cases are so important.

Continuous Asset Discovery

The foundation of ASM lies in the comprehensive discovery of internet-facing assets and risks. To find potentially unknown assets, ASM platforms continuously crawl internet data sources like Certificate Transparency logs, passive DNS sinks, and internet scans to comprehensively uncover assets that an organization owns.

Competitive ASM solutions uncover traditional assets like internet services, hosts, websites, and certificates as well as modern cloud assets like storage buckets. While some platforms provide additional integrations, an ASM platform should immediately find assets that belong to your organization, and it should continually find new assets as soon as they appear on the public internet.

Comprehensive Internet Inventory

ASM platforms provide a comprehensive inventory of your internet assets regardless of the network, cloud provider, or account they're hosted in. Your ASM inventory should contain assets in both traditional data centers and cloud environments, as well as both conventional assets like hosts and modern assets like storage buckets. In addition to providing a simple inventory, a competitive ASM solution will let you:

- Explore your attack surface (e.g., enumerate networks and clouds you depend on)
- Quickly respond to new threats (e.g., find all publicly exposed Microsoft exchange servers)
- Investigate potentially unknown or risky assets (e.g., When did MySQL first appear online and what network artifacts indicate that it belongs to my organization?)

Exposure and Risk Management

ASM platforms continuously check assets for security problems (e.g., publicly exposed databases, end-of-life software, and vulnerable misconfigurations) and service misconfigurations. A competitive solution should be able to help you detect new, potentially unknown assets as well as assets that fall outside of organizational policies so that you can address exposures and vulnerabilities before they result in compliance violations or data breaches.

Because ASM solutions check all internet-facing assets, your platform should provide you with a prioritized list of your most severe internet-facing exposures and risks across the entire organization. An ASM solution should also make it possible to understand risks by severity level and with ample context about why a risk has been flagged.

Security Framework & Compliance

Noncompliance can have devastating results for organizations – putting them at risk for vulnerabilities, cyberattacks, security breaches, and regulatory fines. While staying compliant can be time-consuming and frustrating for organizations, ASM provides the full visibility into exposed assets that organizations need to determine if they're in compliance. An ASM solution should be able to track every asset so that teams can apply the right security policies and secure all exposures. Access to historical data and detailed security reports as required for audits also offer a means of centralizing and simplifying risk management and compliance needs.

M&A and Subsidiary Risk Analysis

Security teams can be excluded from M&A diligence processes until after an acquisition is announced. Similarly, many security teams are responsible for the security of their subsidiaries, but have little operational control over their assets. Inherited risk can prohibit growth strategy and expose your organization.

An ASM solution allows teams to monitor the security of all the assets associated with subsidiaries and acquisitions. A competitive solution should let teams explore an acquisition's attack surface without vendor involvement. This real-time visibility enables security teams to discover unknown and unmanaged assets with high confidence, allowing them to prioritize remediation efforts or walk away from a high risk deal.

How Does ASM Compare to Other Tools in the Tech Stack?



Many existing security products claim to protect internet assets and monitor the attack surface. Why is a dedicated ASM platform necessary? It comes down to the superior visibility that ASM offers.

ASM vs. Vulnerability Management

In theory, a good Vulnerability Management (VM) tool will identify all known software vulnerabilities in an organization's assets. However, VM tools often struggle with today's increasingly dynamic IT networks. The introduction of virtualization and the cloud have pushed vulnerability management solutions to their limits.

This means there are several key problems with relying on a VM solution alone.

1. VM tools are slow. They were built for slowly changing, internal networks to be run on a periodic basis, such as a weekly, monthly, or quarterly schedule. Some VM tools can be tailored to operate at a faster cadence, but this typically requires trade offs — the heavy burden of all that scanning and vulnerability testing can impact network and host performance.
2. VM tools provide an incomplete view of risks. Over the past decade, VM vendors have increasingly become reliant on the CVE database for vulnerabilities. According to [cvedetails](#), over 100,000 vulnerabilities have been added to the CVE database since 2010, compared to just 40,000 in the prior decade. In 2023, there were 29,000 CVEs added to the database, the highest number of any year record. All those vulnerabilities, though important, generate too much noisy data in VM scans, making it difficult to identify critical issues that must be addressed first.
3. VM tools offer an incomplete view of asset inventory. These tools only scan IP address ranges and host names that are configured for them by practitioners. Their discovery capabilities are limited to enumerating live hosts in these known network address ranges.
4. Fourth, VM tools operate with a traditional definition of assets focused primarily on servers, workstations and other computing equipment. This leaves gaps for security teams dealing with non-traditional assets, such as certificates, domains, cloud resources, and buckets — all of which need to be continuously monitored for security risks and policy violations.

However, VM tools can still provide immense value when complemented with an ASM solution — priorities become clearer, and security teams benefit from the added visibility provided by enhanced discovery and additional asset types that VM tools don't cover.

ASM vs. Cloud Security Posture Management

Many organizations have turned to new cloud management tools including CSPM platforms. CSPM aims to prevent many of the cloud misconfigurations that ASM tools identify. Cloud tools operate by extracting configuration data through service provider APIs. This means that they can extract significant details about accounts, but the method limits their coverage to *known* cloud accounts on popular providers like AWS and GCP. In contrast, ASM solutions identify assets regardless of their cloud provider or account, and also identify security risks in traditional data centers. This is critical as the assets with the worst security postures tend to be hosted in unmanaged accounts or by non-standard providers.

ASM, however, evaluates both known and unknown assets tied to third-party organizations, including those in the cloud. Leading ASM solutions like Censys also eliminate gaps in visibility by providing organizations with a near real-time understanding of the risks that are present *today*. Censys refreshes all 3B+ services in its dataset on a daily basis.

ASM vs. Third-Party Risk Management Solutions

Third-Party Risk Management (TPRM) tools help organizations understand potential risks from external partners. TPRM solutions are built to offer visibility into potential vendor risk, but they do so to a limited extent. A TPRM solution will assess a third-party's *known* assets, but will not provide any visibility into unknown cloud assets and risks. Additionally, TPRM risk dashboards are not updated on a continuous basis; most are refreshed every two weeks, leaving adversaries time to take advantage of risks unknown to organizations in between assessments.

“The risk of not having an ASM product, at a company of a certain size, is that it becomes untenable to know everything about what your company is deploying and exposing to the internet. Having tools that give you the information to consolidate and make decisions on what is occurring is essential.”

– Senior Engineering, Technology Firm; *The Censys 2022 State of Risk and Remediation Report*

How to Find a Superior ASM Solution







We've discussed the importance of adopting an ASM solution, now let's talk about the importance of choosing one that will meet your needs. There are a number of ASM vendors on the market. However, as with any tech, not all are created equal, which is why organizations ready to invest in ASM need to find a solution that's truly best-in-class, built on a foundation of superior data with the capabilities to meet all required use cases.

The following criteria covers the critical features and functionality that any competitive ASM solution should provide to its customers.

Essential Questions to Ask When Evaluating ASM Vendors


Asset Discovery

-  **Continuous Asset Discovery:** ASM solutions should be continuously discovering internet-facing assets with minimal user input.
 - > What types of internet assets can the platform identify? At a minimum, an ASM platform should find internet hosts, services, websites, and certificates.
 - > What data sources does the platform analyze to find unknown assets?
 - > How often does the platform uncover new assets?
 - > Does the platform correctly identify your assets including assets you didn't already know about? Remember to not only consider the true positive cases, but also false positives and false negatives.
-  **Cloud Asset Discovery:** ASM solutions should uncover modern cloud assets like storage buckets.
 - > What types of modern cloud assets can the platform identify? At a minimum, platforms should discover vulnerable cloud storage buckets.
-  **Discovery Explanation:** ASM solutions should explain how and why they attribute specific assets to your attack surface.
 - > Does the ASM platform explain how it linked assets to your organization?
 - > Does the platform provide proof (e.g., specific DNS lookups) to back up attributions?
 - > Are there device type labels clearly identify host type (i.e. IoT, Database, VPN, etc.)?
 - > Do you have the ability to rescan endpoints to validate changes (i.e. a port has now closed)?


 **Asset Inclusion and Exclusion:** ASM solutions should allow you to easily include/exclude assets from your attack surface.

- Does the ASM solution allow you to easily add new assets without contacting the vendor?
- Does the ASM solution allow you to remove/exclude assets from your attack surface independently?


Inventory and Exploration

 **Service and Configuration Enumeration:** ASM solutions should find and inventory running services and their configuration details.

- What ports and protocols does the ASM solution scan?
- How often does it find new services and refresh existing data?
- Does the platform expose service and configuration data that can be used in an investigation?

 **Network Context:** ASM solutions should provide additional context about hosts like geolocation, origin AS, and network owner to enable investigations.


- What additional asset metadata does each ASM platform provide?
- Are you able to intuitively understand where you have assets hosted?

 **IoT and Software Labeling:** ASM solutions should label known software and devices in order to aid in responding to new threats.


- Does the platform appropriately identify software and devices?
- Is metadata exposed to allow investigations when new threats emerge?

 **Inventory:** ASM solutions should let you explore and search your inventory as well as understand your external dependencies.

- Does the platform allow you to understand the assets that compose your attack surface and where they're located?
- Can you easily answer questions about your assets?


 **Asset History:** ASM solutions should provide you a history of each asset to aid in investigation.

- Are you able to look up the history of a host or service to understand when it came online?
- What is the platform's data retention policy?

 **Tagging:** ASM solutions should let you tag assets to help you tag business units, asset importance, and other context.

- Does the platform allow you to easily tag and untag assets?
- Are tags available in all aspects of the platform?

Data Depth and Accuracy


 **Internet Intelligence:** What kind of data will the ASM solution rely on to discover and monitor assets on your attack surface? Data should be comprehensive, accurate, and up-to-date.

- Is data fed from a multi-perspective scanning engine from Tier-1 ISPs across continents?
- Are comprehensive scans of the top 100+ ports conducted daily?
- Is extensive scanning conducted on IPv4, IPv6, and name-based hosts?
- Are all 65K+ ports, both standard and non-standard, covered?
- Does automatic protocol detection provide intelligence protocol awareness regardless of port assignment?
- Are vulnerable cloud storage buckets detected?
- Is there detailed visibility into open ports and running protocols?

Reporting

 **Metrics:** How will the ASM solution organize information about your attack surface for you?

- Is raw attack surface telemetry aggregated in an easy-to-understand dashboard that includes trends and a view of your attack surface at-a-glance?
- Are out-of-the-box metrics that align to security program themes provided? For example:
 - ☐ Attack surface size
 - ☐ Total active risks
 - ☐ Average length of exposure of risks
- Can you drill down into a metric's supporting segments to gain further context that can help explain and defend why a metric changed?

 **Reports:** Can reports on attack surface activity be generated quickly for executive review and compliance needs?

- Can you review reports on hosts and ports to determine total attack surface?
- Can you view dashboards that identify trends in risks and hosts count?
- Do you have access to historical trend analysis to demonstrate progress and justify a program?
- Is it easy to export reports for streamlined reporting?

Risks and Compliance

- ⚠ **Risks:** ASM solutions should identify and help you prioritize risks on your attack surface.
 - What risks does the solution identify? Are found risks accurate?
 - Are hosts with critical risks and CVE priority identified by category or severity?
 - Is precise context about discovered risks provided, along with recommendations for remediation?
 - Does the platform let you customize what risks are checked?
 - Does the platform let you prioritize different risks based on your own organization's policies?
 - How does the platform fingerprint and prioritize critical and zero-day vulnerabilities?
- ✓ **Compliance:** ASM solutions should enable proactive monitoring and easy reporting for regulatory compliance.
 - What compliance programs does your ASM solution support?
 - Does the solution track logbook changes?

Integrations

- 🔗 **Integrations Marketplace:** ASM solutions should easily integrate with other security tools in your tech stack so that you can more efficiently eliminate security gaps and potential vulnerabilities.
 - **Rapid Integrations:**

Does the ASM solution offer rapid integration deployment to streamline your security setup?

 - ☐ Can you select and deploy a tool from an ASM solution's integrations marketplace within 15 minutes?
 - **Access to a Diverse Ecosystem:**

Does the ASM solution integrate with a broad range of supported platforms and tools, both security and non-security? These platforms and tools should at minimum include:

 - ☐ SIEM: Will the ASM solution integrate with your SIEM solution?
 - ☐ Will you get notified when new risks and assets appear, and when known assets change?
 - ☐ What workflows are supported by the SIEM integration?
 - ☐ Does the ASM solution integrate with your SIEM provider?
 - ☐ VM: ASM solutions should integrate with VM providers to import newly found assets for more in-depth checks.
 - ☐ What workflows are supported by the VM integration?
 - ☐ Does the solution integrate with your VM platform?

➤ **Ticketing:**

Can you easily assign tickets to IT teams to address?

- ☐ What ticketing solutions does the ASM product integrate with?
- ☐ Can new tickets be created and checked directly from the ASM platform?

➤ **Cloud Asset Discovery:**

Can you automate the discovery of new cloud assets for early detection and accurate asset inventory?

- ☐ Can you achieve full visibility into your cloud assets without the need to host and maintain your own infrastructure for cloud connectors?
- ☐ Can you access valuable metadata about your cloud assets, including identifiers about product, region, resource IDs, and asset source?
- ☐ Can you include or exclude specific cloud accounts, regions, and products for a custom attack surface view?

➤ **Alerting:**

Can you enhance risk detection with real-time and daily digest risk alerting?

➤ **Data Sharing:**

Can you ensure the seamless flow of internet intelligence to all of your security systems?

➤ **Workflow Efficiency:**

Does the solution offer a robust API and SDK framework to simplify the process of connecting with existing workflows into other systems or applications?


Operationalization

🛡️ **Security Controls:** Your ASM solution can contain sensitive infrastructure data and should support your existing authentication mechanisms.

- Does the ASM solution support your authentication provider?
- Is Role-Based Access Control (RBAC) for different users and workspaces supported?
- Can you create distinct workspaces to support simplified management of subsidiaries, mergers, and acquisitions?

⚡ **API:** ASM solutions should provide a full-featured API to allow programmatic access and integration.

- What APIs are available?
- What is possible through the Web UI that's not possible through the API and vice-versa?

 **Implementation:** An ASM solution should not require extensive configurations to deploy.

- Does the ASM solution offer automated and continuous seed discovery to provide a complete and continuously updated view of your attack surface?
- Does the provider offer dedicated support that includes end-to-end deployment and integration guidance?
- Does the provider offer a dedicated support channel?
- Does the provider offer opportunities for continuous education to maximize use of the ASM solution?

How to Build a Business Case for ASM



You may be convinced that ASM is a critical investment for your security team, but other decision-makers in your organization may not be as familiar with ASM's benefits. If you're looking to build a case for stakeholders to purchase an ASM solution, consider the following cost and time-saving comparisons that many organizations use to justify new security spend.

5 Reasons to Invest in ASM

Reason #1: Monitoring the Attack Surface Is Critical To Preventing Costly Data Breaches

The average global cost of a breach is [\\$4.35 million dollars](#) and in the United States, that average more than doubles to \$9.44 million, the highest average cost of any country. As threat actors and hacker groups become more sophisticated and expand their reach, the global cost of cybercrime is [expected to rise from 8.44 trillion in 2022 to 23.84 trillion in 2027](#). ASM solutions reveal public exposures and potential mistakes before attackers or auditors can identify them. Censys ASM uncovers 65% more attack surface than leading competitors.

TIP: Scheduling a trial or POC with several ASM vendors to determine if they uncover unknown assets can be one powerful way to communicate ASM's critical role in mitigating risk to stakeholders.

Reason #2: Manually Finding Assets Is Difficult and Expensive

Uncovering unknown assets requires crawling global datasets, including passive DNS sinks, certificate transparency logs, and internet scan results, which are expensive to acquire and/or maintain. While open source tools can allow for one-off scans of the internet, operators need to continuously scan thousands of ports to find potentially hidden services. Vendor-provided ASM solutions are much less expensive to operationalize than the costs of individual data sources, not to mention the development time required to find your organizational assets in those datasets. Consider that at 43% of organizations, manual asset discovery takes [more than 80 hours](#), and is typically conducted weekly, bi-weekly, or on a monthly basis.²

² CSO Online, 2022

Reason #3: ASM Enables IT Citizenship and Prevents Cloud Sprawl

Enterprises waste [one-third of their budgets](#) on under-used or unused cloud resources. Rather than trying to dissuade employees from using cloud-based services or other services that can result in Shadow IT, ASM enables teams to be agile and quickly identify unknown cloud instances while effectively monitoring new ones. With a full picture of what your organization owns, you can take action to eliminate or decommission these unneeded assets, and save significant operational expenses in the process. Uncovering cloud sprawl and Shadow IT also creates opportunities to reinforce proper security protocols to team members across the organization.

Reason #4: ASM Helps You Supercharge Existing Security Investments

Your security organization likely already invests in multiple other security tools like a vulnerability management scanner. The typical security toolstack for an average enterprise is estimated to be around 60 to 80 various solutions, with some enterprises operating up to 140 distinct tools. Such extensive tool sprawl introduces significant inefficiencies into security operations and incident response processes. Integrating an ASM solution with your other security tools offers a streamlined, automated, and integrated security ecosystem, empowering security teams to tackle the complexities of today's cybersecurity landscape with greater efficiency and effectiveness.

Reason #5: ASM Helps You Showcase the ROI of Your Security Efforts

Security leaders know the impact of their work is enormous, but they often struggle to procure the concrete proof organization leadership wants to see. The reporting metrics available in ASM solutions arm security leaders with the insights they need to understand their impact, communicate that impact to stakeholders, and take action to better align with business objectives. For example, Censys ASM demonstrates core metrics like attack surface size, total active risks, and average length of exposure for risks. Security leaders can see how these metrics are calculated, access detailed supporting data, and benefit from flexibility in calculations to support business logic.

By enabling comprehensive discovery, assessment, and remediation of internet-facing assets, ASM empowers organizations to preemptively neutralize threats, ensuring that digital transformation enhances, rather than endangers, security posture. Embracing ASM is essential to safeguarding the future of your organization against the unknown, unseen, and unanticipated threats of tomorrow.

See More with Censys ASM



Identify, Prioritize, and Remediate Threats with Industry-Leading ASM

Censys ASM is the leading Attack Surface Management solution, identifying and prioritizing advanced threats and exposures across your entire external attack surface. We leverage our industry-leading internet scanning data to provide complete, contextual and up-to-date visibility into all of your internet and cloud assets, whether known or unknown.

External Attack Surface Management

Gain complete visibility into asset ownership, relationships and history, with the full context necessary to facilitate investigations and remediations. With daily asset discovery and over 95% attribution accuracy, Censys discovers up to 65% more of an organization's external attack surface than leading competitors.

Exposure and Risk Management

Discover and mitigate risks with our comprehensive dataset, attribution engine, and cloud connectors, embedding best practice monitoring into security operations. Identifying assets with over 80% accuracy, Censys significantly reduces false positives, providing defenders with accurate data to prioritize and remediate the threats that are critical to the business.

Cloud Asset Discovery

Achieve effortless deployment and management of cloud assets with Censys hosted cloud connectors, providing optimized scanning and daily ingestion. This ensures security organizations have access to the most accurate, up-to-date information on cloud inventories.

Subsidiaries, Acquisitions & Mergers

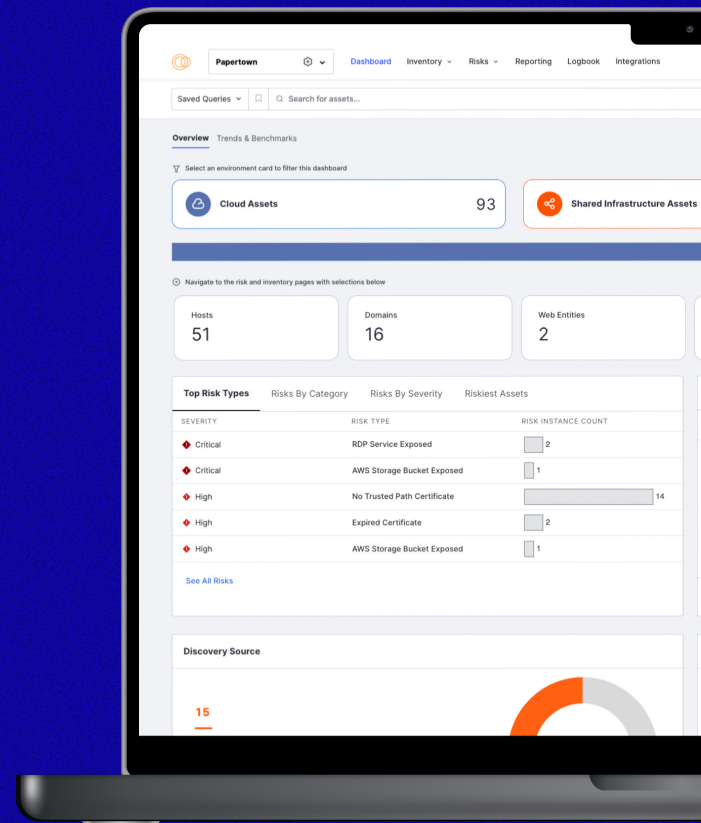
Censys enables security teams to prioritize remediation efforts or walk away from a high-risk deal by discovering unknown and unmanaged assets with high confidence. By effortlessly finding and categorizing asset information and vulnerabilities for new subsidiaries, the need for special asset discovery projects is eliminated, and due diligence time is shortened by 30%.

Forrester Consulting finds that the composite Censys ASM customer achieves an average ROI of 444%.

- The Total Economic Impact of Censys External Attack Surface Management Report



Take the Next Step with Censys



Interested in learning more about how Censys ASM empowers security teams around the world, including over 50% of the Fortune 500?

Reach out to us today at censys.com/request-a-demo/

Censys is the leading Internet Intelligence Platform for Threat Hunting and Attack Surface Management, known for discovering assets six times faster than its closest competitor. Censys offers the most comprehensive, accurate, and up-to-date map of the internet available with daily refreshes of billions of services and the world's largest certificate database empowering our customers to proactively discover, prioritize and remediate threats. Established by the creators of ZMap and trusted by the U.S. Government, along with over 50% of the Fortune 500, Censys' mission is to be the one place to understand everything on the internet.