censys whitepaper

Attack Surface Management 101

Your Guide to Total Visibility

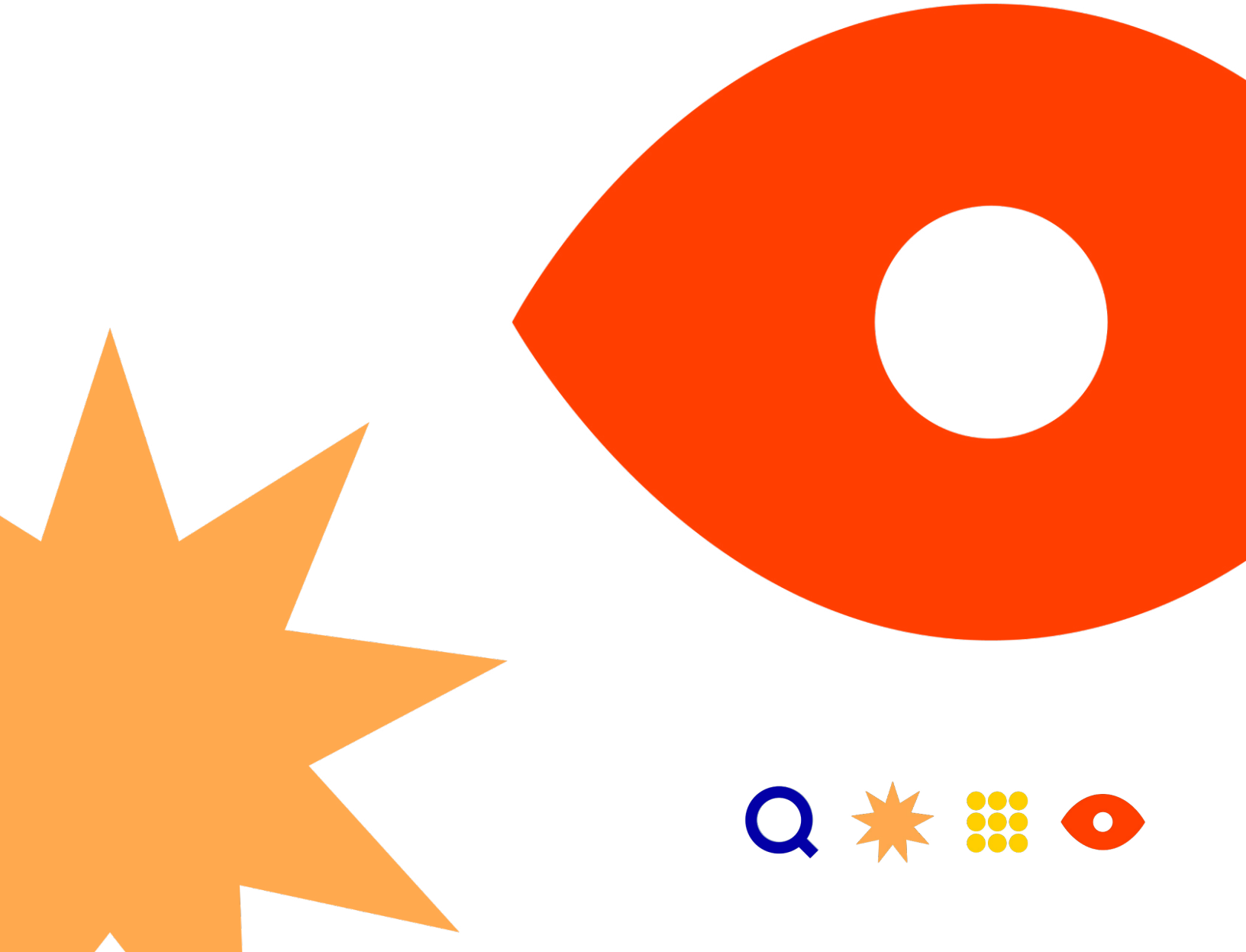


Table of Contents

ANALYZE ILLUMINATE PROTECT MONITOR

Attack Surface Management: The Tool to Complete Security Technology.

Even the most equipped and experienced security operations teams have limitations regarding their resources and skillsets. Information Technology (IT) and Information Security (IS) professionals cannot manage the full extent of every security threat at once, so teams have had to understand the severity of their vulnerability better and plan their security management accordingly. Several solutions have been developed to assist security teams with the scoring, planning, and executing threat detection and response actions. These solutions include Cloud Security Posture Management (CSPM), Vulnerability Management (VM), Cyber Asset Attack Surface Management (CAASM) or Cloud Access Security Broker (CASB), and Security Rating Services (SRS).

These solutions, however, do not offer complete, 360-degree visibility into every single threat. Even the security teams doing everything right by utilizing solutions and third-party services can still experience blind spots. Attack Surface Management (ASM) tools discover an average of 30% more cloud assets and applications than IT teams are aware they have. An ASM solution integrates with other threat detection software to supplement existing data sources, fill gaps in threat awareness, and provide visibility into those otherwise unknown blind spots.

In this whitepaper, we'll dive into the challenges experienced by security teams of all sizes, important trends in the threat landscape, and how ASM integrates into your existing or new security stack to complement your other security products.

The Challenges of Modern Security Risks.

Every organization is different, and as a result, the resources and skill sets available to every security team can vary drastically. Let's explore the distinct pain points and obstacles experienced by security teams at midmarket and enterprise organizations.

Midmarket Organizations

Midmarket companies moving beyond check-the-box-compliance to develop or prioritize their security programs face two key issues: early exposure and shadow IT and cloud services.

EARLY EXPOSURE

Utilizing the Shift Left model, security teams can make great progress by implementing early testing and creating continuous deployment cycles. However, these teams can miss important elements of a strong security posture, even with a sophisticated process in place. Quick-release cycles can result in unchecked sources. Reliance upon third-party software and supply chains can create obstacles to true visibility, risking unidentified exposures.

Attackers are becoming more efficient because they have more opportunities now that almost everything is outside of a firewall. Once an attacker finds an easy way to bypass security protocols, it becomes easier to duplicate that effort with security managing an enormous software supply chain.

Zakir Durumeric,
Co-founder and Chief Scientist, Censys

SHADOW IT AND CLOUD SERVICES

Shadow IT refers to projects managed outside of or without the knowledge of IT and IS teams. While Shadow IT and cloud services were previously limited by physically purchased IT software, today's average company currently uses 1,083 cloud services in total — 108 known services plus 975 unknown services. Due to inadequate threat detection products and legacy management processes, technology and security leaders often have little idea how many cloud services are being used to store sensitive data.

Enterprise Organizations

Enterprise companies with robust security protocols experience a different set of threat detection challenges.

SHADOW IT AND CLOUD SERVICES

Unknown tech and cloud services issues are not only a problem for midmarket organizations but for large ones, as well. According to a report by Forrester, one Fortune 100 prospect felt confident that their company was only using nine different cloud providers. Still, an ASM vendor's initial scan revealed that they had applications and data in 23. The larger and more spread out an organization's technology, the greater the risk of Shadow IT and cloud services outside the internal IT team's scope of awareness. It is also somewhat common for large organizations to have extensive development teams with small security teams; with limited resources, Shadow IT and asset coverage can be nearly impossible.

SPEED DEMANDS

Large organizations equipped with large development teams, as mentioned above, have high expectations to meet when it comes to the speed with which new deployments take place. Strict time constraints coupled with disproportionately small security teams result in developers deploying risky, vulnerable code without giving security professionals the time to test it properly.

LACK OF COMMUNICATION

As remote work increases in popularity, especially for technology professionals, IT and security teams discover that they don't have the proper communication

solutions in place. Teams are experiencing a lack of essential integrations to empower them to work together, support communication, and perform quick and efficient resolutions. Instead, communication breakdowns due to insufficient or nonexistent remote workflows enable threat exposures to be missed and decrease the time to remediation.

CLOUD MANAGEMENT

Along the same lines as the remote work push, many large organizations are also shifting from on-premises storage and management systems to cloud systems. While this direction has its many advantages, it also creates a new, more complex environment within which IT and security teams must operate. Moving from on-premises to the cloud requires extensive coordination, time, and planning, pulling resources away from vulnerability monitoring.

What is Attack Surface Management?

Attack Surface Management (ASM) fills the gaps created by the challenges outlined above and the missing pieces of current threat detection solutions. Your attack surface refers to all of your assets that store your data – from hardware to software – that are accessible from the internet. With this in mind, an ASM complements an existing security stack by providing comprehensive, real-time internet attack surface discovery and scan data to help security teams clearly see their digital risk and exposure.

> An Attack Surface Management (ASM) solution integrates with other threat detection software to supplement existing data sources, fill gaps in threat awareness, and provide visibility into those otherwise unknown blind spots.

The Emerging ASM Market

Recently, the emerging ASM market has taken off rapidly because new security threats require new solutions. As attackers have become more sophisticated in their approach, security teams have been struggling to hit the moving target of perpetually detecting threats throughout the external attack surface. According to a Forrester survey of security decision-makers, 35% of attacks were exploited through software vulnerabilities, 33% through supply chain and third-party breaches, and the remaining 32% through web application exploits.

Companies continue to grow, increasing external infrastructure and further complicating hyper-dimensional attack surfaces. Rapid organizational growth paired with advanced attack methods has revealed blind spots in the existing security stacks of even the most experienced teams and created a need for a supplementary threat detection solution.

Elements of ASM

An ASM comprises six major elements that facilitate ongoing discovery through extensive data sources and risk scoring.

1. ASSET DISCOVERY

An ASM provides a robust, continuous, and complete discovery of assets that belong to your organization on the internet. This solution empowers practitioners to proactively find unknown internet-facing assets like IPs (or hosts), domains, certificates, and storage buckets like S3 or GCP Storage.

2. UNIFIED GLOBAL INVENTORY

Security teams require a single source-of-truth view for all the internet-facing assets regardless of location, type, or previous knowledge. An ASM leverages its visibility of more than 99% of the internet from a proprietary scanning engine and attribution algorithm to find assets that belong to your organization.

We have the infrastructure to support cloud asset discovery — you can do name-based scanning to a term to determine whether this is actually your asset. Censys helps give this differential within the platform, which is really valuable.

Morgan Princing,
Director of Customer Experience, Censys

3. CLOUD GOVERNANCE

To address the challenges of unknown cloud services, an ASM creates an easy-to-understand assessment of shadow IT manifested in unsanctioned cloud environments within your organization. As this problem continues to grow, ASM provides solutions to the systemic issue to better manage cloud infrastructure within your organization.

4. RISK DETECTION AND REMEDIATION

An ASM checks assets daily for thousands of risks and security problems, including but not limited to end-of-life software, data leakage, service exposure, and poor endpoints. In addition, it provides operators with insight on how to mitigate detected problems and tools to verify successful remediation. Finally, a rapid response program immediately helps security professionals fix the most critical software vulnerabilities.

5. POST-ANNOUNCEMENT M&A RISK ASSESSMENT

With an ASM in place, teams have greater flexibility to easily have multiple attack surfaces per new acquisition you are bringing into your security program. These "workspaces" allow for independent assessments of the portfolio of acquisitions and make it easy to understand the new assets you are now responsible for protecting, including the newly inherited security risks. Each workspace comes equipped with unique integrations and API keys.

6. SUBSIDIARY RISK ASSESSMENT

Similar to new acquisition cyber risk, subsidiaries can be challenging for security teams to uplevel to the required security standard at the company. Segmentation of the attack surface per subsidiary is easy to implement and can be up and running fast. With a self-service model of ASM, security teams have complete control of adding new assets to their attack surface and making changes, so they can more easily see and address subsidiary issues.

How ASM Integrates with Other Solutions.

A common misconception among security teams is that ASM will replace your other security software. Rather, ASM seamlessly integrates into your new or existing security stack to complement and supplement each tool's unique contributions to threat detection and response.

> **We help prioritize things that should be looked at — a discovery tool that is complementary to a vulnerability management tool.**
>
> Levi Richardson,
> Senior Customer Success Engineer, Censys

ASM vs. CSPM

One of the most common problems experienced by developers and security professionals is cloud misconfiguration. As developers deploy code to the cloud, security teams need to evaluate the status of misconfigurations within known cloud environments constantly. Organizations developed Cloud Security Posture Management (CSPM) tools to address this challenge by providing continuous monitoring of known cloud services and environments to identify, address, and limit misconfigurations.

While this is an essential step in mitigating cloud misconfigurations in an increasingly complex environment, data sources limit the efficacy of CSPM software. The CSPM can only identify misconfigurations within cloud spaces it knows to scan. On the other hand, an ASM scans the entire internet, cloud services, and other

storage buckets to identify misconfigurations beyond those only known to the organization or the CSPM. The ASM can seamlessly integrate with a CSPM tool to fill in the source gaps and locate all cloud vulnerabilities.

CSPM	ASM
Provides continuous monitoring of known cloud services and environments to identify, address, and limit misconfigurations	Provides continuous monitoring of all cloud services and environments to identify and score the severity of misconfigurations
Scans cloud spaces that it and the organization are aware of	Scans the entire internet, cloud services, and storage buckets

ASM vs. VM

Organizations need to implement a regular cadence of security testing. To facilitate this, Vulnerability Management (VM) simulates the TTPs of real-world attackers, which can provide visibility into existing security effectiveness and offer insights into addressing any pitfalls. VM focuses on the internal, software-based cyber landscape and individual assets that threat actors may target.

While VM homes in on software and code-based vulnerabilities to address a company's internal on-premises and cloud-based cyber health, ASM takes a more holistic approach. ASM takes a step back to examine the security of the entire infrastructure, internal and external, by scanning every corner of the internet, cloud services, and other environments. VM and ASM have the same goal of reducing risks and securing data, yet their differing approaches make them complementary when integrated for one big-picture solution.

VM	ASM
Homes in on software and code-based vulnerabilities to address a company's internal on-premises and cloud-based cyber health	Examines the security of the entire infrastructure, internal and external, to assess all assets and data within the attack surface
Simulates real-world attackers	Scans the entire internet, cloud services, and storage buckets

ASM vs. CAASM/CASB

Despite the extensive technology available, it can be difficult for IT, security, and cloud teams to answer even the most basic questions about their assets. Cloud access security brokers (CASBs) and cyber asset attack surface management (CAASM) provide these answers. Gartner defines CASBs as "security policy enforcement points placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies" to gain visibility of the applications that host assets within the cloud environment. CAASMs are focused on zooming that visibility into assessing the assets themselves.

While CASBs and CAASMs provide essential knowledge of known cloud services, applications, and their assets, they only provide that knowledge within an organization's internal infrastructure. According to a Forrester report, however, organizations see an average of 30% of unknown and external assets through discovery, and some saw several hundred percent more assets. ASM completes the picture by scanning the entire internet and all external sources to identify and assess the vulnerability of assets outside the internal infrastructure.

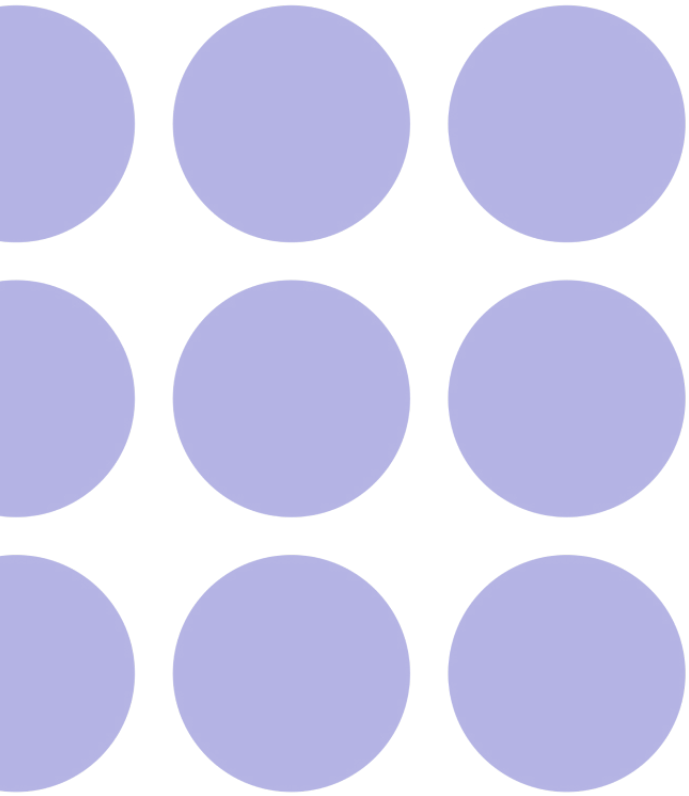
CASB	CAASM	ASM
Secures and provides visibility into internal cloud services and applications that store assets	Secures and provides visibility into internal assets stored within cloud services and applications	Secures and provides visibility into internal and external applications and assets
Assesses internal infrastructure and known sources	Assesses internal infrastructure and known sources	Assesses internal infrastructure, as well as entire internet and external cloud sources

ASM vs. SRS

Third-party security is an essential element of a comprehensive attack surface management strategy. Your infrastructure is only as secure as your supply chain's. Security rating services (SRS)address this risk management by gathering data from public and private sources, analyzing the data, and rating entity security posture using a proprietary scoring methodology.

As third-party risk assessment is the primary function of an SRS, it cannot perform a thorough and complete assessment without access to important discovery data. The ASM complements the SRS by providing additional insights into third-party partners through all internet and cloud sources.

SRS	ASM
Provides third-party security assessment and monitoring	Provides digital asset discovery and vulnerability management
Focuses on risk management	Focuses on threat and exposure management



Attack Surface Management Use Cases.

Regardless of where assets, data, and software live, there is an attack surface to be managed. ASM is not limited to one organization's perimeter or cloud environments. Therefore, it is uniquely relevant to many use cases within your security stack. It offers significant benefits for every IT team and even teams outside IT, including:

- **DevOps and cloud teams:**
  cloud misconfiguration and other cloud monitoring
- **Compliance teams:**
  data regulation for on- and off-premises privacy
- **Security Operations Center (SOC):**
  SOC threat analysis and storage identification
- **Vulnerability management teams:**
  ongoing vulnerability scanning and assessment
- **Business development teams:**
  due diligence for M&As and other business transactions

ASM is not limited to any one organization's perimeter or cloud environments, and, as such, is uniquely positioned for an extensive number of use cases within your security stack.

Asset Discovery and Inventory

Perhaps the most crucial step toward a comprehensive threat detection and response strategy is the awareness of hardware and software inventories. ASM enumerates unknown assets, uniquely identifies them, and automates the analysis of changes in your organization's IT asset inventory.

Cloud Misconfiguration Monitoring

Gartner's research indicates that misconfigurations are responsible for over 90% of all cloud security issues. Hence, as developers deploy new code and store information in the cloud, enterprises need to reduce the risk of privacy failures and data breaches. The best way to ensure this end is by continuously enumerating cloud weaknesses and misconfigurations.

Third-Party Risk Management

According to a Forrester prediction, 60% of security incidents will result from issues with third parties in 2022. In conjunction with your SRS, the ASM will continually discover and assess vulnerabilities of third-party supply chain partners to detect potential breaches, compliance concerns, and risky software.

M&A Due Diligence

While mergers and acquisitions can introduce exciting opportunities, they also typically come with cybersecurity risks. Unfortunately, it is very common for those risks to remain undiscovered until the company integration is well underway. Using ASM tools during the M&A due diligence period empowers firms to understand potential risks better and develop a plan for addressing security weaknesses much earlier in the process.

Compliance Management

As governing agencies continue to develop evolving cybersecurity and data privacy compliance requirements, compliance management needs to be top of mind for security and IT professionals. ASM helps ensure regulated data is not stored in unknown or external cloud providers or other prohibited locations. It can also be automated to monitor and alert teams to expired or missing digital certificates, ensuring sensitive data is always encrypted to compliance standards.

Attack Surface Management in Action with Censys.

Even a sophisticated, complex security stack does not provide complete visibility into vulnerabilities and risks. Censys fills in the gaps to provide organizations with a holistic approach to threat detection and response. To understand how your organization operates, attack surface management with Censys continually analyzes your known assets — either directly provided by you or collected through integrations with your cloud providers and security tools. Request a demo today if you're ready to learn how to find and cover your assets with Censys ASM.

Request a Demo