censys whitepaper

Attack Surface Management 101

Your Guide to Total Visibility in Healthcare

Table of Contents

ANALYZE ILLUMINATE PROTECT MONITOR

Attack Surface Management: The Tool to Complete Visibility in Healthcare.

Healthcare data breaches are on the rise, and they have consistently been the most expensive type of breach across all industries since 2011. Healthcare organizations are prime targets for bad actors; for instance, a ransomware attack can hold systems and connected devices hostage until a ransom is paid and bad actors are banking on the desire to reduce disruptions in critical patient care as a strong motivation for payment from healthcare targets. The threat to healthcare systems worldwide is so severe that the United Nations has called it a "global threat that can't be ignored," because in the healthcare sector, the disruption caused by a breach goes beyond financial loss—it can directly affect patient care and human health.

Several solutions, like Vulnerability Management and Cyber Security Posture Management, aim to assist teams with the scoring, planning, and executing threat detection and response actions. These solutions, however, don't offer complete visibility into every single threat. Even the security teams doing everything right by utilizing solutions and third-party services can still experience blind spots resulting from unknown assets.

Censys has found that up to 80% of customers' internet-exposed assets are previously unknown. **In 2024, Censys discovered 14,004 unique IP addresses exposing healthcare devices and data systems connected to potentially sensitive medical information on the public internet.** Leading Attack Surface Management (ASM) tools, like Censys, help defenders automatically identify these unknown or mismanaged assets. 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 healthcare security teams, 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 in Healthcare.

Healthcare digital infrastructures have expanded exponentially, in both scale and diversity. With the rise of third-party infrastructure, multi-cloud strategies, and SaaS tools, the digital footprint of healthcare organizations can extend far beyond the traditional boundaries of IT systems. These expanding attack surfaces create more opportunities for attackers, who are taking advantage. In fact, The Healthcare and Public Health sector is the top target for ransomware attacks, according to the FBI's 2023 Internet Crime Report.

CONNECTED MEDICAL DEVICES

In modern medicine, connected devices are essential and also highly vulnerable. An ongoing concern for healthcare security teams is how to secure the thousands of connected devices that are critical to patient care while also keeping them operational. The sheer number of devices and the need for constant connectivity makes them hard to patch, maintain, and even inventory, but each connected device can serve as an access point that, if breached, could lead to lateral movement across the network and significant data exposure.

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 at Censys

FINANCIAL CONSTRAINTS

By and large, healthcare organizations don't have the same investment priorities as other businesses. Their security budgets are much smaller than other industries, with just 4-7% of a health system's IT budget allocated to cybersecurity, compared to about 15% for other sectors. Healthcare organizations have to be strategic with security investments, since more tools equals more cost. Bad actors know this, and consistently aim for areas with less visibility and protection – areas that would usually be made more secure by higher cost tools.

DIGITAL TRANSFORMATION AND CLOUD MANAGEMENT

Digital transformation in healthcare has been steadily underway for the larger part of a decade, with the COVID pandemic accelerating it for many organizations. Healthcare has evolved to now include telemedicine, electronic health records (EHR), wearable devices, and much more. Plus, many large healthcare organizations have shifted from on-premises storage and management systems to cloud systems. While these advances can create better patient outcomes, it also creates a more complex environment within which IT and security teams need to operate.

TECHNICAL DEBT FROM ACQUISITIONS AND MERGERS

Mergers and acquisition are the nature of modern healthcare networks. Bringing several organizations together, each with their own technology stack, can lead to significant tech debt and security gaps. This makes it easier for bad actors to exploit vulnerabilities through phishing, unpatched software, and even living off the land techniques. Using ASM tools empowers healthcare teams to understand potential risks better and develop a plan for addressing potential security weaknesses.

> **Over the past decade, we've witnessed a surge in the digitalization of healthcare systems to meet evolving patient and infrastructure needs. This has increased the complexity of healthcare security, introducing a wide range of data integration systems and third-party software that can be targeted by ransomware operators.**
>
> - Himaja Motheram, Security Researcher

What is Attack Surface Management?

Attack Surface Management (ASM) addresses the gaps created by the challenges outlined above and provides complete visibility into an organization's attack surface. 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 platform 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. Importantly, ASM platforms discover both known *and unknown* assets, which gives security teams a comprehensive view of all exposed assets that an attacker could target.

> An Attack Surface Management (ASM) solution delivers total visibility into your attack surface with continuous, automated discovery of your organization's internet-based assets.

The ASM Market

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.

ASM Core Capabilities

A leading ASM platform should empower security teams with a number of core capabilities, including:

1. TOTAL ATTACK SURFACE DISCOVERY

An ASM platform allows you to understand and analyze the full extent of your attack surface. Whether assets are known or unknown, you should be able to discover critical exposures and mitigate risks, while embedding best practice monitoring into your security operations. Censys ASM, for example, is proven to discover up to 65% more attack surface than leading competitors.

2. ACCURATE ATTRIBUTION

Get a complete and automated view of your organization's perimeter with an ASM's asset attribution capabilities. Seed data is used to establish high confidence connections to discovered internet assets. The Censys ASM attribution algorithm increases customers' visibility up to 80%.

3. RISK TRIAGE AND PRIORITIZATION

Each asset in the attack surface should be updated daily and measured against an expansive collection of risk fingerprints to determine the severity of security weaknesses that are discovered. Severity should be based on impact, exploitability, and likelihood, so that security teams have a clear understanding of priority.

4. RISK CONTEXT AND REMEDIATION GUIDANCE

An ASM platform should focus on simplifying security decisions with rich and precise risk context to facilitate specific remediation guidance. Details of the type and potential security impacts of each discovered risk should be provided, along with recommended steps for remediation.

5. RAPID RESPONSE

Speed and accuracy are essential to securing organizations from today's evolving threat landscape. Leading ASM platforms like Censys fingerprint and prioritize putting emergency vulnerabilities into our platform as risks, often within 24 hours of the vulnerability disclosure.

6. DASHBOARDS AND INTERACTIVE REPORTING

A leading ASM platform should be able to aggregate raw attack surface telemetry into easy-to-understand dashboards and trends that quickly enable security teams to determine and report on the overall state and security of the organization's attack surface.

7. CLOUD CONNECTORS

Easy-to-use, flexible, and secure hosted cloud connectors with daily asset ingestion and Big 3 Cloud Service Provider support should continuously inventory assets and feed them into an ASM platform.

8. INTEGRATIONS

A leading ASM platform should make it easy to integrate with other security tools. The Censys Integrations Marketplace, for example, allows security teams to onboard any integration, with any vendor, in less than 15 minutes. Rapid and reliable deployment methods deliver a streamlined, automated, and integrated security ecosystem.

Censys provides a good lens into things that we don't know about. Censys was able to quickly discover multiple S3 storage buckets that were publicly accessible on the Internet and contained sensitive data.

- Manager of Cybersecurity, International Real Estate Company

How ASM Integrates with Other Solutions.

As modern threat actors evolve with alarming speed, the demand for an integrated suite of security solutions becomes more critical. Organizations, burdened by disparate and fractured security tools, face the risk of significant coverage gaps and data silos. This underscores the urgency for a unified and comprehensive stack of security tools. ASM platforms should address this urgency by seamlessly integrating into existing security tech stacks.

> **Security and risk management leaders are increasingly dissatisfied with the operational inefficiencies and the lack of integrations of a heterogenous security stack.**
>
> – 2022 Gartner Survey

Key Benefits

Leading ASM platforms that integrate with other tools in the security tech stack should empower security teams to:

STREAMLINE OPERATIONS

Consolidating toolstacks enhances control, visibility, and coordination across various security platforms for more efficient operations.

GAIN A UNIFIED VIEW

Bridging disparate systems eradicates data silos and provides a unified view of security data for integrated risk and exposure management.

AUTOMATE WORKFLOWS

Streamlining tasks like importing cloud assets and integrating Shadow IT into vulnerability systems significantly reduces manual workload.

Common Integrations

Leading ASM platforms should be able to integrate with a variety of other security and non-security solutions. Some of the most useful integrations with ASM platforms include those focused on:

ALERTING

Enhance risk detection with real-time and daily digest risk alert.

CLOUD ASSET INGESTION

Automate discovery of new cloud assets for early detection and accurate asset inventory.

TICKETING

Automate ticket creation for better incident response and improved communication.

SECURITY INFORMATION AND EVENT MANAGEMENT

Send risk and host log events for centralized monitoring, tracking, logging, and reporting.

VULNERABILITY MANAGEMENT

Seamlessly auto-update VM tools with leading internet intelligence.

Check out the Censys Integrations Marketplace to learn more about how seamless ASM integrations can be!

How ASM Compares to Other Security Solutions.

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

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. Cloud Security Posture Management (CSPM) tools were developed 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 require 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
Simulates real-world attackers	Scans the entire internet, cloud services, and other environments
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

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.

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.

TPRM Solutions	ASM
Provides visibility into a third-party's known assets	Evaluates both known and unknown assets tied to third-party organizations
Updates risk dashboards every two weeks, on average	Provides a near real-time understanding of the risks that are present today

Key ASM Use Cases.

To safeguard sensitive patient data and crucial connected devices, healthcare organizations need to proactively monitor and manage assets to help mitigate the potentially devastating impact of a breach. A leading ASM platform will identify and prioritize advanced threats and exposures across your entire external attack surface. Near real-time visibility into all of your internet and cloud assets, whether known or unknown, empowers security teams to aggregate, prioritize, and remediate advanced threats and exposures. Key ASM use cases include:

EXTERNAL ATTACK SURFACE MANAGEMENT

ASM provides complete visibility into asset ownership, relationships, and history, with the full context necessary to facilitate investigations and remediations. For example, with daily asset discovery and over 95% attribution accuracy, the Censys ASM platform discovers up to 65% more of an organization's external attack surface than leading competitors. Censys ASM also continuously monitors for unauthorized services, matching more than 1400 software fingerprints and identifying end-of-life (EOL) software versions.

CLOUD ASSET DISCOVERY

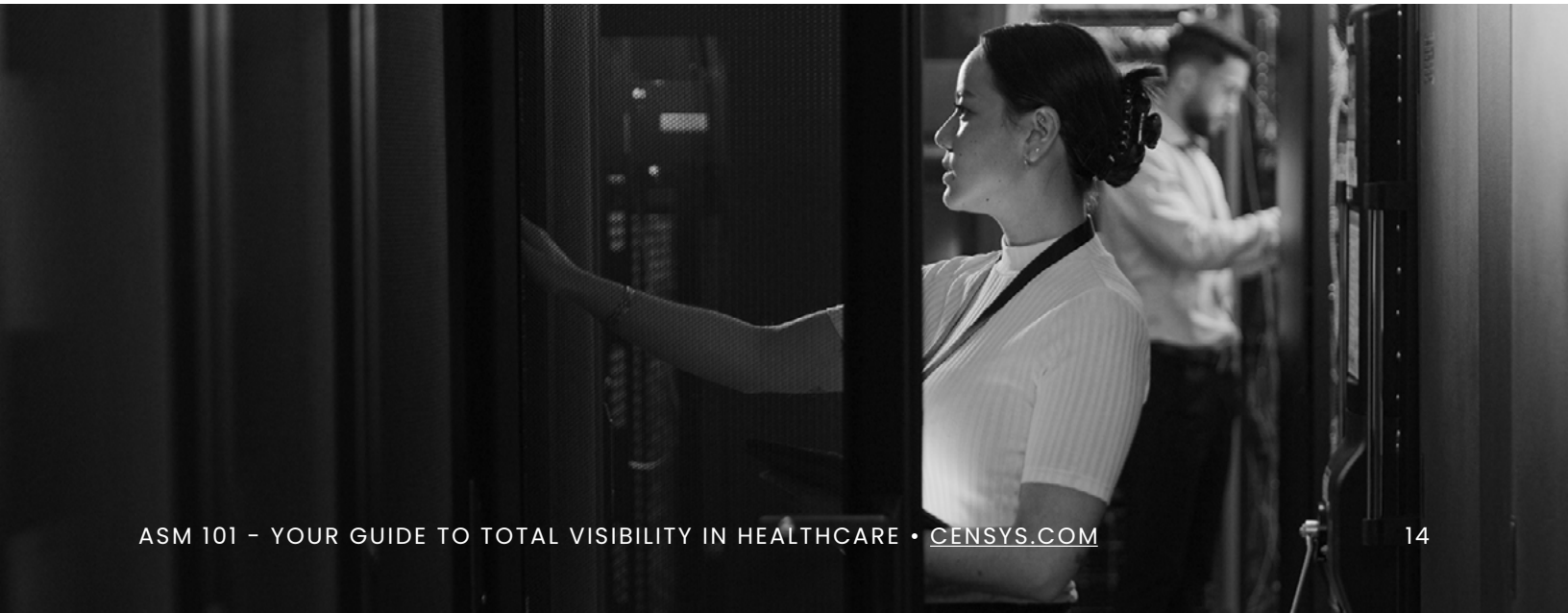
Perhaps the most crucial step toward a comprehensive threat detection and response strategy is the awareness of hardware and software inventories. ASM enumerates unknown assets, uniquely identifies them, and automates the analysis of changes in your organization's IT asset inventory.

EXPOSURE AND RISK MANAGEMENT

ASM empowers healthcare teams to proactively discover and mitigate potentially catastrophic risks with a comprehensive dataset, attribution engine, and cloud connectors, embedding best practice monitoring into security operations. For example, by identifying assets with over 80% accuracy, Censys significantly reduces false positives, providing defenders with the data needed to stay secure in a sophisticated threat landscape. Censys also automates the assessment of each asset against 400+ risk fingerprints, facilitating the determination of severity based on impact, exploitability, and likelihood, offering precise remediation guidance and mitigation steps.

SECURITY FRAMEWORK & COMPLIANCE

As the threat landscape continues to evolve, there are a number of standards and frameworks being created to support healthcare organizations as they approach the critical job of managing exposures, such as NIST and the Biden Executive Order. Additionally, healthcare organizations are obligated to follow strict regulations and laws regarding privacy and patient rights, including HIPAA, the HITECH Act, CCPA, and more. Leading ASM solutions like Censys help ensure organizations are supported with the latest technology and standards required to stay compliant - and stay ahead of the security curve.



Attack Surface Management in Action with Censys.

Censys ASM identifies and prioritizes advanced threats and exposures across your entire external attack surface. We leverage our industry-leading internet scanning data to provide near real-time visibility into all of your internet and cloud assets, whether known or unknown. This information empowers healthcare security teams to aggregate, prioritize, and remediate advanced threats and exposures.

Learn how to find and cover your assets with Censys ASM today.

Request a Demo

censys

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.