censys

# The 2022 State of Risk & Remediation Report

## How the Internet Responded to Celebrity Vulnerabilities

# Introduction.

Imagine you've been blindsided by a cybersecurity attack that resulted in confidential data loss, monetary loss and reputation damage. The cause: Internet-facing assets that exploded over the last several years through merger & acquisitions, and numerous divisions spinning up new cloud initiatives. If only you would have had an easy way to discover exposed assets you did not know about, monitor your asset vulnerabilities, bolster your defenses and head off the attack before it occurred.

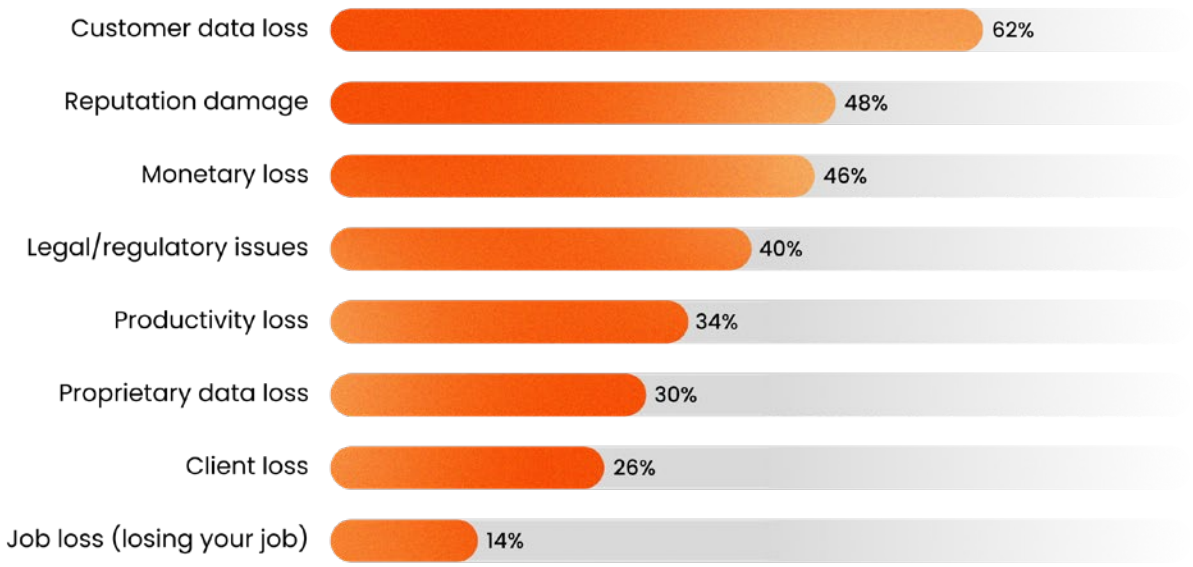
For many cybersecurity professionals this is not an imaginary scenario. Read on to learn how Attack Surface Management (ASM), an emerging cybersecurity solution category, can help you detect, defend and stop threats before they occur.

# Table of Contents

# Cyberattack Worst-case Scenarios.

The top three worst-case scenarios cybersecurity professionals are concerned about are customer data loss, reputation damage and monetary loss. Companies can be extorted via ransomware. When private information is stolen through a data breach, it can be a public relations nightmare.

Please rank the below list of potential outcomes for your organization of a cyberattack based on the degree of damage to your organization




*Source: Paradoxes, Inc Attack Surface Management Study, August 2022 (n50)*

**[If cybersecurity risks are not mitigated] It would impact productivity, and the success of our company. Ultimately, it could result in catastrophic business destruction.**

- CISO, HEALTH CARE

Of the security professionals we surveyed, 62 percent listed customer data loss as one of the top three most damaging potential outcomes of a cyberattack. Reputation damage, monetary loss, and legal/regulatory issues also factored prominently.

The current cost of cyber-crime, an estimated $6 trillion in 2021, is expected to escalate to $10.5 trillion by 2025.[1]

A recent risk report found financial institutions took an average of 233 days (approximately eight months) to detect and address data breaches affecting their systems in 2020.[2] When companies wait days, weeks, or even months to realize an asset is at risk, the fall-out can be catastrophic for business. The sooner cybersecurity professionals can act, the better.

> **"The first thing that comes to mind when I hear Attack Surface Management is continuous scanning. This is an ongoing way to monitor and manage your environment and all your assets. Continuous evaluation of your environment to make sure you're secure."**
>
> – SVP CYBER OPERATIONS, BANKING

An important capability in determining how effective an ASM solution will be is how frequently scanning occurs. This determines how quickly risks are detected and remediation can occur, even for new assets that have come online without IT's awareness. The more frequently you receive data regarding your assets and potential associated risks, the quicker you can act to protect your organization. When scanning and threat detection occurs less frequently, remediation slows, and vulnerabilities increase.

1. Cybersecurity Ventures in Cybercrime Magazine, Nov 2020
2. Varonis – 2021 Data Risk Report: Financial Services

## Top Cybersecurity Professional Concerns

The reason Chief Information Security Officers (CISOs) and other cybersecurity professionals' roles exist is to protect their organizations' digital infrastructures and data. It is paramount to their roles to ensure the business can run daily operations uninterrupted and sensitive data remains confidential.

> **"Our key cybersecurity focus is to secure our client assets."**
>
> - SVP CYBER OPERATIONS, BANKING

Avoiding a large-scale security event, such as a data breach or ransomware attack, is the primary goal of security professionals. In order to do so, they require visibility into their organization's assets, information on their level of exposure, and the most comprehensive protection against varied threats. This is where Attack Surface Management comes in. The stakes are so high if a breach or attack occurs, that it is critical to CISOs, Security Architects, Software Security Engineers, Information Security Analysts, Penetration Testers, Threat Detection Engineers and other cybersecurity professionals to be constantly learning and implementing the latest technical solutions to aid in their protection efforts and stay one step ahead of threats.

**It sounds cliché, but I am most worried about the unknown. I cannot secure what I don't know about. If I know about it, I can wrap tooling around it or put other protection around it. I can give guidance or consulting to my organization about it. Every month, I find out about new publicly facing assets we have that I didn't know existed.**

- SENIOR ENGINEER, TECHNOLOGY

> **"We want to stay off the front page of the New York Times. Unmitigated risks would result in a significant cost and reputation hit."**
>
> – SVP CYBER OPERATIONS, BANKING

Common cybersecurity threats that are top of mind for security professionals include ransomware, phishing, and malware. Results from Paradoxes, Inc's recent Attack Surface Management Study found 70 percent of cybersecurity professionals cite ransomware attacks as the top cybersecurity threat to their organization. Ransomware vulnerabilities are directly linked to exposed assets. Other top threats include phishing, malware and DDoS attacks.


*Source: Paradoxes, Inc Attack Surface Management Study, August 2022 (n50)*

## Covid Accelerated Cybersecurity Risks

The reason Chief Information Security Officers (CISOs) and other cybersecurity professionals' roles exist is to protect their organizations' digital infrastructures and data. It is paramount to their roles to ensure the business can run daily operations uninterrupted and sensitive data remains confidential.

**The transition from on-prem to hybrid to full cloud means gaining efficiency but losing control in visibility.**

- DAVID SOOHOO, VP OF PRODUCT, ASM, CENSYS

Similarly, the shift to remote work that occurred at the onset of the pandemic has given rise to a more dispersed workforce that is harder to track and monitor from a security standpoint.

> **"Key cybersecurity defense activities are focused on staying on top of hybrid environments and getting complete visibility as to what is going on in all environments. If you cannot monitor something, you cannot understand what is going on."**
>
> -CISO, HEALTH CARE

Security professionals are trying to protect against both internal and external threats. Internal threats can be intentional or unintentional. Even unintentional internal threats can have significant consequences for an organization. As Censys' researchers report, if it's possible, someone will do it. Using deprecated SSH ciphers or exposing sensitive services to the Internet can be easy to do, especially without guard rails in place. Find ways to make the "secure" option an easy default in your organization.

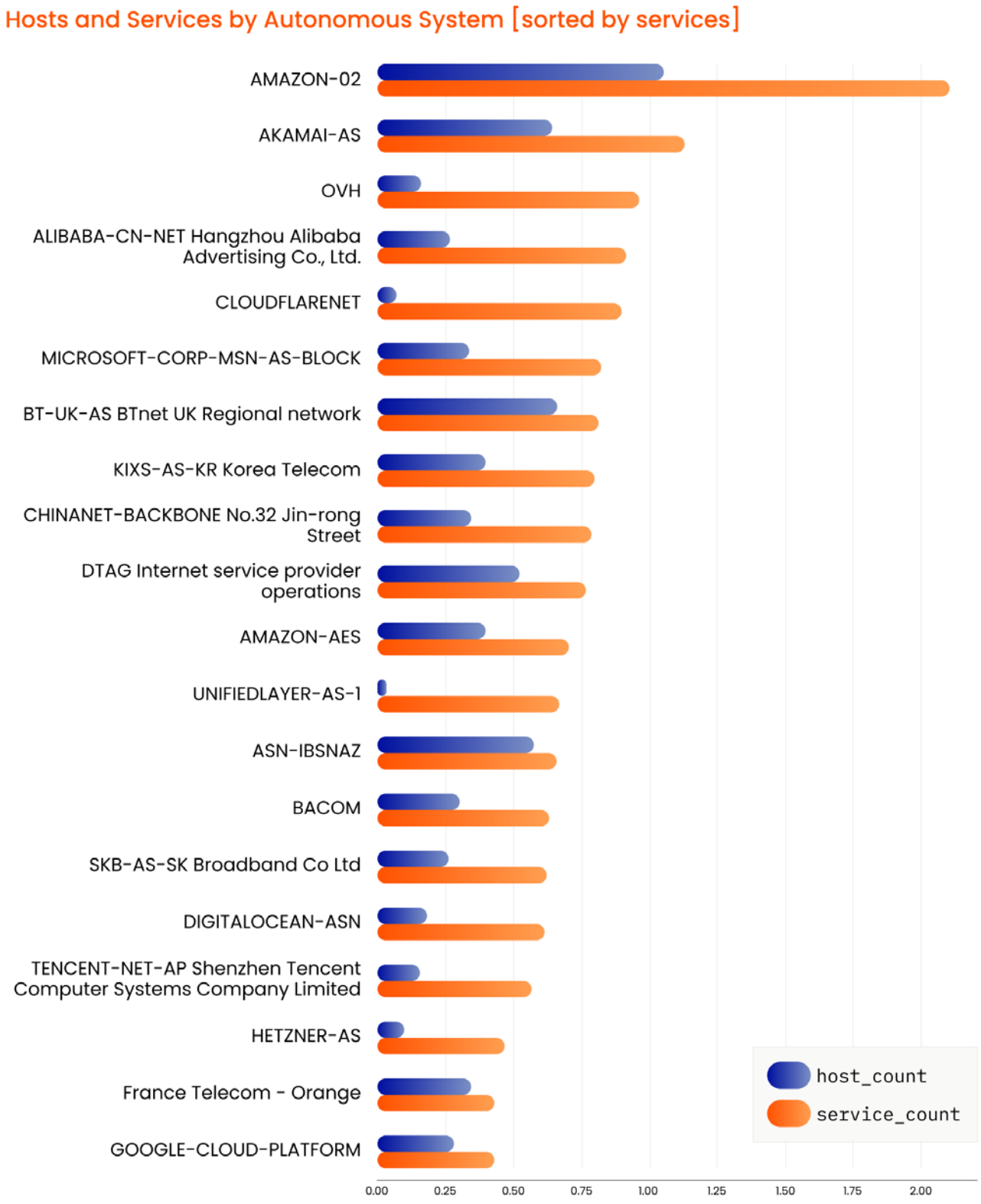
> **"[Mitigating risk] It's a process that evolves over time. We try to mature our capabilities. Threat actors never stop. Our users do things we don't want them to, either intentionally or unintentionally. So, it's a continuous journey. The main objective is layers of defense."**
>
> - CISO, HIGHER EDUCATION

In many instances, business is accelerating faster than the growth of security teams. Digital transformation adds complexity, which in turn increases threats and risk. As the number of publicly facing assets proliferates and keeping track of their details becomes unwieldy, it is more important than ever to have a systematic way to detect, defend, and remediate against threats to your organization.

When examining attack surfaces for a sample of 37 large organizations, Censys discovered they have, on average, 44 different domain registrars and presence in 17 different hosting providers (including cloud, datacenter, and on-premises equipment). Shadow IT is on the rise, likely accelerated by the increase in remote work over the past two years. Organizations must continue enabling their employees, but this can lead to visibility issues when IT and Security teams are left out of the conversation.

# The Cloud: Understanding Where Things Run and Securing Cloud Infrastructures.

Increased migration to the cloud has led to more blind spots for security professionals in terms of knowing and tracking their assets. However, it is useful to know that while the Internet has become increasingly reliant on several large cloud providers - Amazon, Microsoft (Azure), Google, and Oracle make up only 9% of all hosts with services on the Internet. This may initially seem surprising, but the sense that "everything is in the cloud now" is likely primarily driven by the value we assign to services that are in these clouds. If a major cloud experiences an outage, it is not just one business that is also experiencing an outage, but hundreds or thousands across many industries.



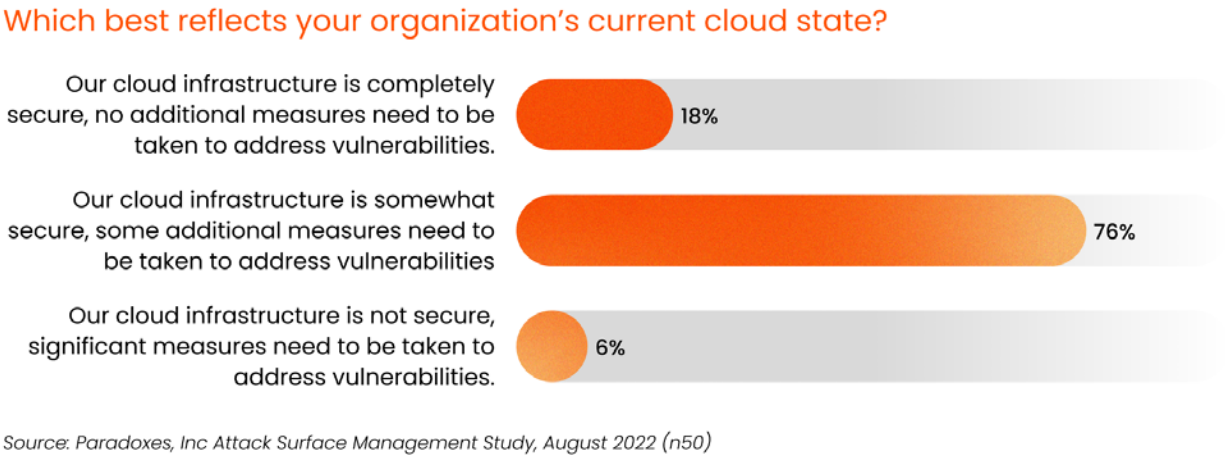

*Censys State of the Internet Report: Hosts and services by Autonomous System, sorted by number of services.*

To better understand where things run in the cloud, take a look at the Censys team's full analysis.

Once security professionals have visibility into their cloud assets, protection measures are needed to ensure cloud infrastructure is secure and vulnerabilities are addressed. An ASM product such as Censys' can provide such threat detection, defense and remediation, in addition to cloud scanning.

Over three-quarters of security professionals surveyed agree with the statement, "Our cloud infrastructure is somewhat secure, some additional measures need to be taken to address vulnerabilities." And 6% admit their cloud infrastructure is not secure and would require significant measures to address vulnerabilities.

> **"[Right now,] We do network access control and some other things around trying to identify assets on network (vulnerability scanning), and public facing things that identify assets across the broader Internet. We are trying to get a good picture and develop inventory. However, it is very ad hoc, immature. We're working on it."**
>
> – CISO, HIGHER EDUCATION



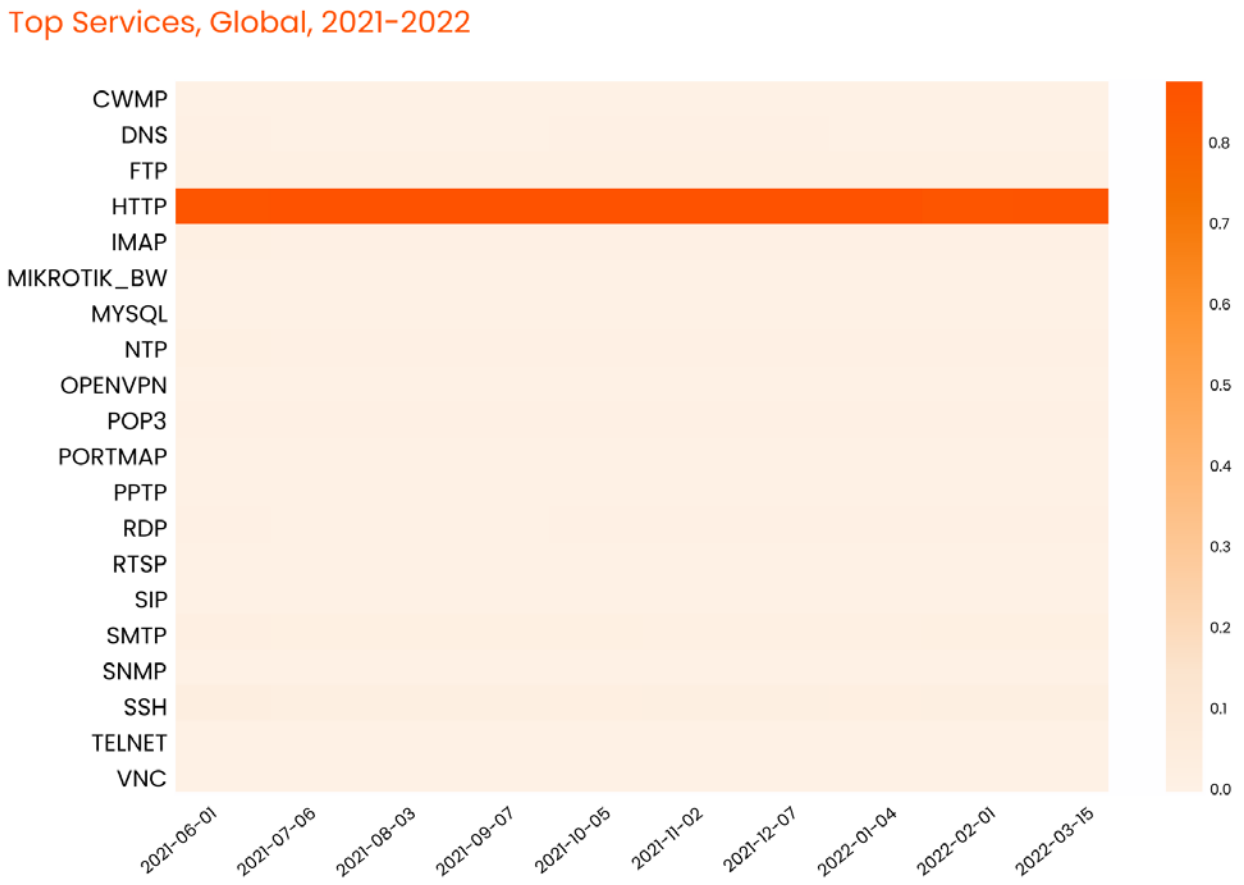

*Source: Paradoxes, Inc Attack Surface Management Study, August 2022 (n50)*

# The Internet: Understanding the Vast Landscape and Internet-wide Trends.

An ASM product scans the Internet and helps locate assets you may have previously been unaware existed or were tied to your organization. The Internet is a huge, constantly shifting landscape that is challenging to pin down, so analyzing historic data helps provide context and understand how vast the space really is.

Recent research by Censys[3] looked at which ports, services and software are most prevalent on the Internet and discovered some insightful findings.

Perhaps not surprisingly, HTTP is overwhelmingly the most common service observed across 222 million hosts on the Internet, making up an average of 81% of Censys-discovered services. In addition to websites and web servers, HTTP includes APIs, caches, proxies, and web-based control panels for Internet-connected devices.




*Censys State of the Internet Report: Breakdown of popular services on the Internet across 222 million hosts.*

**3**. Censys used a single daily snapshot per month from June 2021 to March 2022 – an average of 220,763,081 hosts per snapshot – to analyze Internet-wide trends.

While HTTP is most commonly associated with TCP/UDP ports 80 and 443, we also observe it running across the widest range of ports of any service. Many services have an IANA-assigned default port, though services are often set to run on non-standard ports.

While running services on non-standard ports is not in itself a risk, it can provide a false sense of security, especially if the service owner is relying on security through obscurity to protect their assets. The most commonly observed non-standard ports running HTTP services are 7547 (2%) and 30005 (1%). These percentages may seem low, but 1% and 2% of millions of services still represent a substantial amount of HTTP.

SSH, or Secure Socket Shell, is an encryption protocol that enables secure remote access and file transfer between systems on a network. In contrast to the distribution of HTTP services across many ports, 75% of SSH services observed by Censys run on the IANA-assigned port 22. 25% of SSH services run on a non-standard port.

75% of SSH services observed by Censys use AES or Poly1305 ciphers, which are currently recommended secure cipher options. However, as of March 15, 2022, we observe over 10 million SSH services using 3des-cbc (5% of all observed SSH services), which has been recommended against by NIST since 2017.

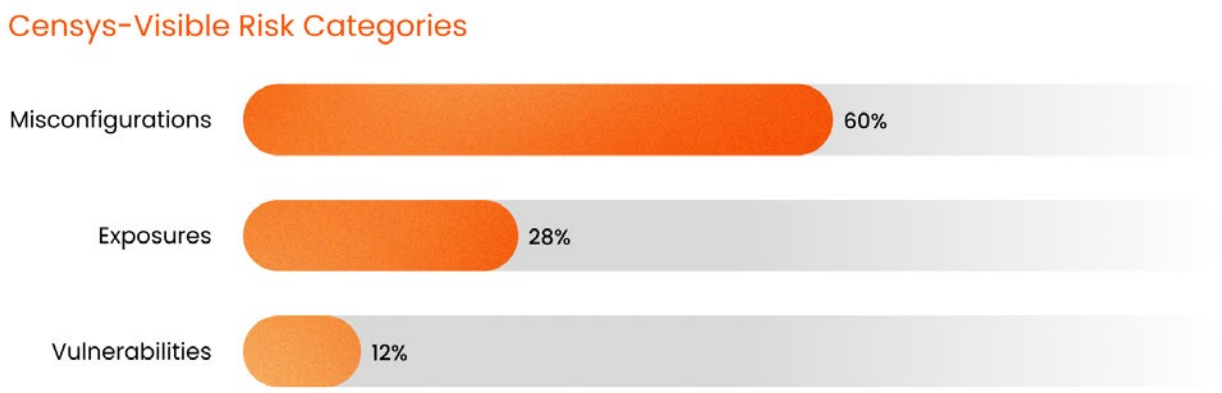
When examining FTP, we see that 84% of FTP services run on IANA-assigned port 21. The next most commonly observed port running FTP is 40029, which runs 3% of all FTP services Censys sees. This was a bit surprising to us, as 40029 doesn't have any IANA-assigned service, and 40029 does not appear in any FTP-related IANA assignments.

For more findings on HTTP, SSH, and FTP, check out the full Censys report.

# The Attack Surface of the Internet.

As devices increasingly move online and digital infrastructure scales, so too does the number of risks that make up the Internet's attack surface. Censys examined the Internet's attack surface in terms of risks and vulnerabilities across the Internet.[4] Risks encompass those settings or conditions (including vulnerabilities) that increase the potential for data breaches, information leaks, or destruction of assets.

Misconfigurations and Exposures represent 88% of the risks and vulnerabilities Censys observes across the Internet. Misconfigurations make up roughly 60% of Censys-visible risks.[5] Exposures of services, devices, and information represent 28% of observed risks.[6] This is relevant because misconfigurations and exposures are often best remedied through good security hygiene. While CVEs and advanced exploits often make headlines, they represent just 12% of risks Censys observes on the Internet.[7]




*Censys State of the Internet Report: Percentages of Censys-visible risk categories*

**4**. We evaluated the presence of various risks and vulnerabilities across samples of 2.2 million hosts from November 30, 2021, and 2 million hosts from roughly half a year later on June 10, 2022, all drawn from UIDS. To perform sample selection for each date, we joined UIDS with ASdb, a dataset that maps public autonomous systems (identified by ASN) to organizations and industry types. We then randomly selected 1% of hosts from each ASdb industry categorization to ensure representation of hosts across a variety of industries. See Censys' full report for details.

**5**. For our purposes, 'misconfiguration' includes risks such as unencrypted services, weak or missing security controls (Content Security Policy, etc.), and self-signed certificates.

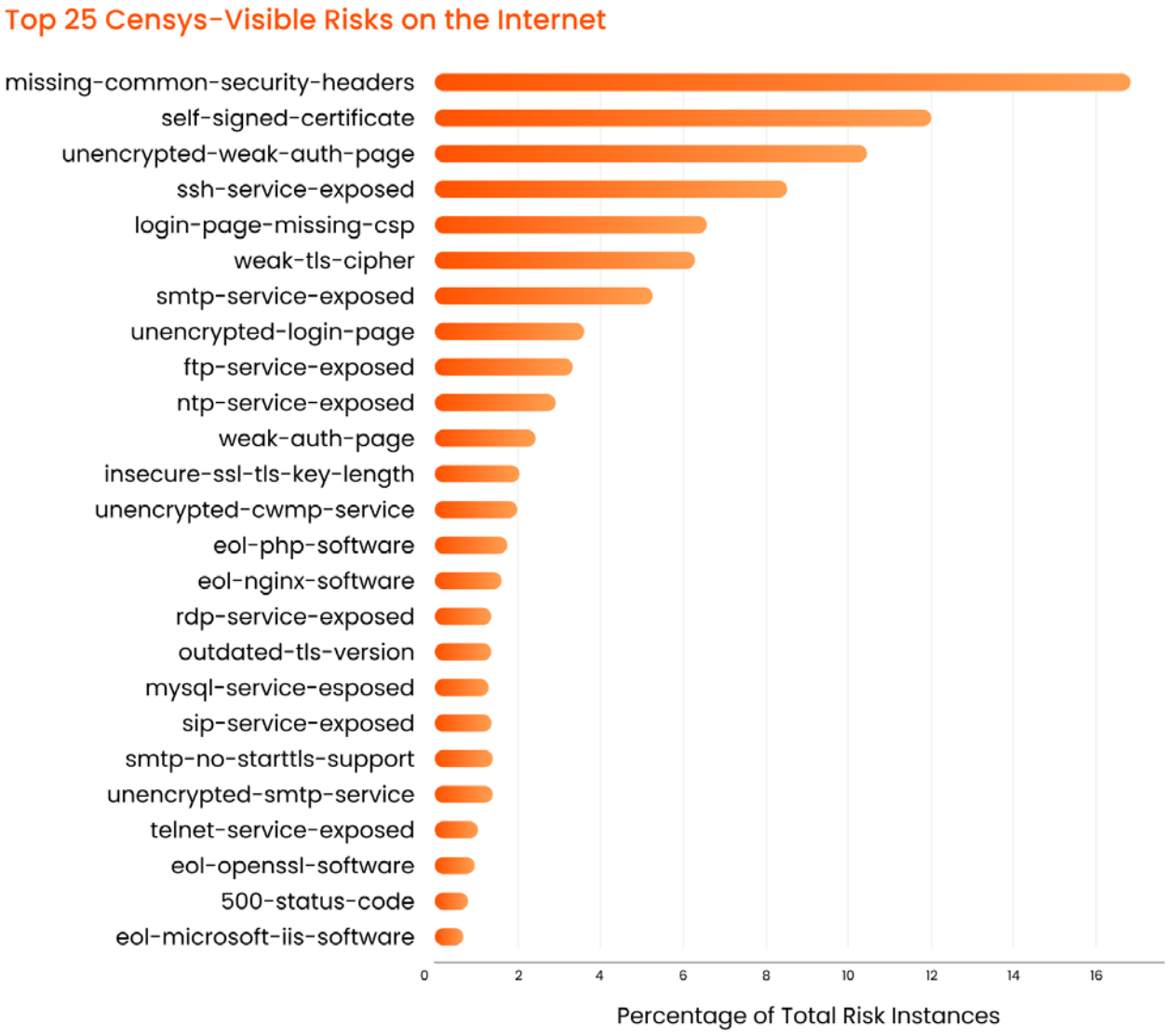
**6**. This includes things like unintentional database exposures, exposed storage, IoT devices, exposed credentials, or API keys.

**7**. Vulnerabilities represent 12% of observed risks in our 2021 and 2022 snapshots. Vulnerabilities include end-of-life or outdated software and CVEs.

# Threat Defense and Remediation Using ASM

While understanding your attack surface and the inventory of your company's Internet-facing assets is paramount, this is just the first step. A good ASM solution will also help you identify where to place defensive measures, understand the criticality of all identified risks, and guide you through the remediation process.

Since not all risks are created equal, let's take a look at how Censys' ASM product categorizes and prioritizes some commonly found risks. As you can see in the chart below, the top 3 risks observed across a random sample of 2 million Internet-facing hosts are missing common security headers, self-signed certificate, and unencrypted weak authentication page, each of which we categorize as Misconfiguration.




*Censys State of the Internet Report: Percentages of Censys-visible risks across 2 million hosts, June 2022.*

Once the risk is identified, the ASM product provides an explanation as to why it is risky and how risky it is, to help security professionals decide how to best proceed with remediation. When examining these top 3 risks, you find that the reason for the risk and its severity vary.

Missing common security headers indicates that we did not detect any common security headers, such as Content Security Policy (CSP), Cross-Origin Resource Sharing (CORS), or Strict Transport Security (STS), on a service. Lack of these headers can make affected services a target for XSS or data injection attacks.

Self-signed certificate indicates that we discovered a certificate that was signed by its own private key instead of a trusted Certificate Authority. Services without identity verification are a target for man-in-the-middle attacks and phishing campaigns.

We categorize both of the above as low-severity risks, meaning that while exploitation of them may not lead a threat actor directly to an organization's crown jewels, they could be weaponized as part of an exploit chain or used to gather additional information about the organization.

Unencrypted weak authentication pages represent just over 10% of the risks we observe in our Internet-wide sample. These authentication or login pages use basic or digest authentication without TLS, making submitted credentials susceptible to interception and hash cracking techniques.

We categorize this as a high severity risk, as it can easily lead to credential theft. Moreover, Verizon's 2022 Data Breach Investigations Report indicates that "Use of stolen creds (Hacking)" is the top distinct Action variety (i.e., tactic) observed across their incidents and breaches dataset (p. 15). While credential theft is by no means a new tactic, it remains effective for threat actors.

For a deep dive into more of the Top 25 Censys-Visible Risks Across all Industries, check out the full report here.

# Differing Remediation for Major Vulnerabilities

The Internet as a whole responds to major vulnerabilities in varying ways. For example, the Log4j vulnerability of December 2021 saw quick, widespread remediation. In contrast, remediation for the GitLab remote code execution vulnerability (CVE-2021-22205) announced in May 2021 didn't catch on until about 6 months later, when it was discovered that a botnet was exploiting the RCE.

There is often extensive coverage about the mechanics of vulnerabilities - how the exploit works and how to detect and defend against it. Less widely understood is how the Internet responds to these vulnerabilities. How long does it take for vulnerable devices to be patched or upgraded? Do devices get patched or simply taken offline?

When researchers at Censys analyzed and compared three major vulnerabilities - Log4j, GitLab, and Confluence - we found three distinct patterns of response:

- **Quick upgrading upon disclosure:** Log4j response was exemplary in speed (but not so much in the chaos and stress it caused for Security teams everywhere).
- **Vulnerability required wide-scale exploitation before remediation:** Gitlab took a botnet to get traction (lots of things fly under the radar until they…don't).
- **Quick upgrading and removing instances from the public-facing Internet:** Response to Confluence was quick but much of the remediation was taking things off the public Internet, rather than upgrading as seen in Log4j or Gitlab.

While most vulnerabilities are nowhere near as severe as the Log4j vulnerability (to every responder's relief), reducing the time between vulnerability disclosure to upgrade for even medium and lower risk vulnerabilities could improve organizations' overall security posture.

The team at Censys has spent extensive time examining the timeline and remediation for major vulnerabilities to better inform the intelligence used in their ASM product.

An in-depth explanation of the Internet's response to the Log4j remote code execution (RCE) vulnerability, the GitLab RCE vulnerability and botnet (CVE-2021-22205), and the Confluence OGNL injection vulnerability (CVE-2021-26084) can be found in Censys' research report.

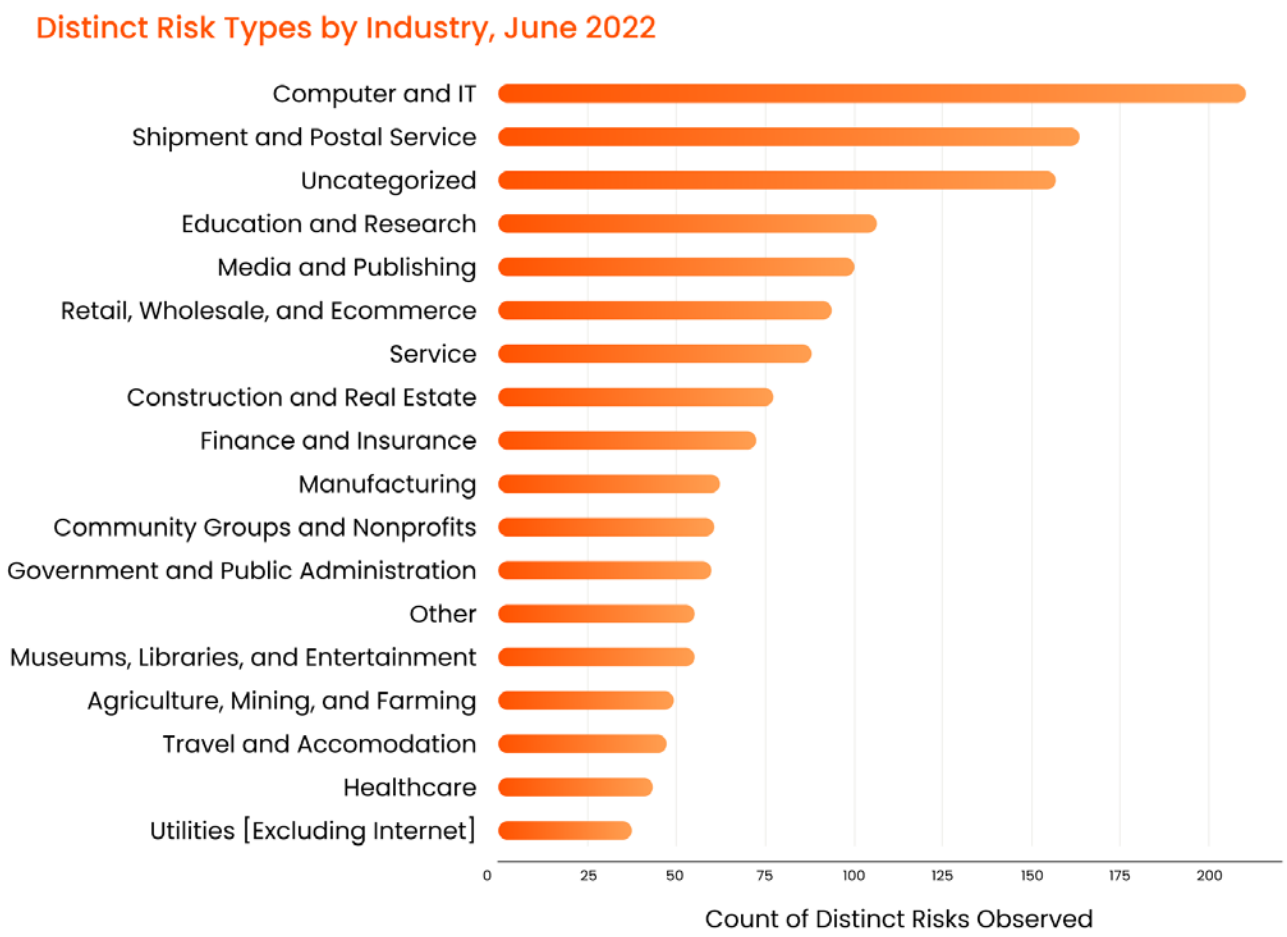
# All Industries Face Cybersecurity Threats, Some More Than Others

All industries can benefit from threat detection, defense, and remediation using ASM. However, certain industries by nature are more susceptible to cyberattacks and have more to lose. These higher risk industries include finance, manufacturing, higher education, health care, and utilities. Organizations that have sensitive or confidential data (personally identifiable information, financial information, product concepts, intellectual property, etc.) are the most appealing to cyber criminals.

- **Finance:** Finance was the most attacked industry in 2020, accounting for 23% of all cyberattacks.[8] Examine the top 25 risks in the Finance & Insurance industries in Censys' research report.
- **Manufacturing:** Manufacturing is an appealing industry for cyber espionage campaigns and intellectual property theft. Manufacturing was the second most-targeted industry in 2020, behind finance.[9]
- **Higher Education:** Universities have databases with extensive amounts of research data and PII (personally identifiable information), both of which are particularly alluring to cyber criminals.
- **Health care:** Due to confidential patient information and large ransom potential, medical records are one of the most profitable things to steal for cyber criminals.[10]
- **Utilities:** According to a recent report, the risk profile of the Utilities industry stands out because so much of it is driven by unencrypted weak authentication pages. While an unencrypted weak authentication page is one of the top three risks observed overall, it represented over half of the observed risks for this industry.[11] Examine the top 25 risks in the Utility industry in Censys' research report.

While certain industries are more susceptible to cyberattacks, a different subset of industries see challenges in the variety of risks present. When we look at industry by distinct risk types (i.e., widest spread of different risk), other industries rise to the top.

8. NTT – 2021 Global Threat Intelligence Report
9. https://www.cloudwards.net/cyber-security-statistics/#Sources
10. NTT – 2021 Global Threat Intelligence Report
11. Censys' State of the Internet Report




*Censys State of the Internet Report Range of risk varieties across hosts from our June 2022 sample, broken down by ASdb industry.*[12]

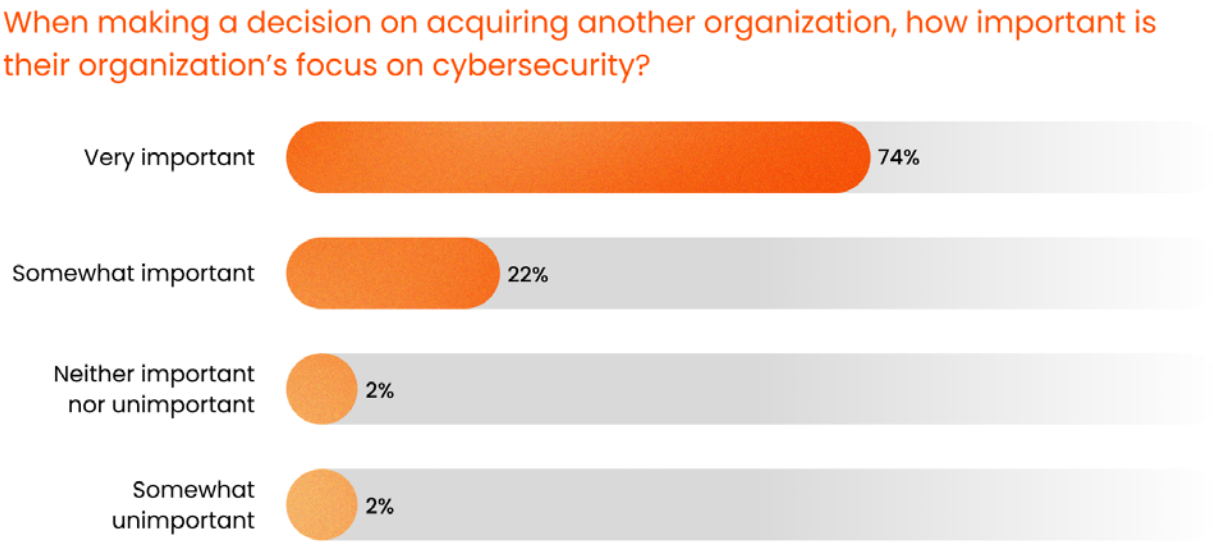
We see that the Computer and Information Technology industry has the highest variety of risks, which isn't particularly surprising given the composition of this industry (ISPs, telecom providers, cloud providers). Freight, Shipment, and Postal Services may seem out of place as the industry with the second-most varied range of risks, but ASdb categorizes two major Amazon ASes as Freight, Shipment, and Postal Services, driving much of the risk variety here.

To learn more about how the amount of distinct risk varies by industry, see Censys' full report.

**12.** At the time of this analysis, Censys had over 300 risk and vulnerability detection fingerprints. The graph above illustrates the spread of distinct risks across hosts in the various ASdb industries, not the amount of risks in each industry.

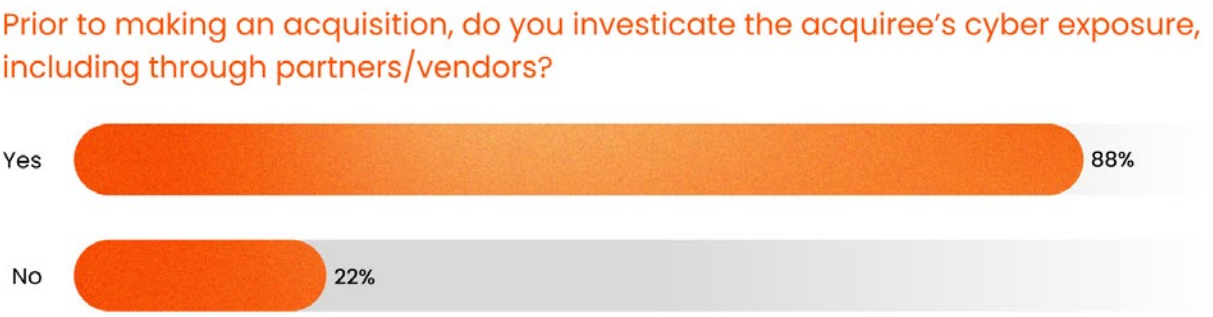
## M&A: A COMMON SCENARIO THAT AN ASM TOOL CAN HELP

Mergers and acquisitions are common transactions that can carry substantial cybersecurity risks. In fact, Gartner predicts that by 2025, 60% of organizations will use cybersecurity risk as a primary determinant in conducting third-party transactions and business engagements.[13]




*Source: Paradoxes, Inc Attack Surface Management Study, August 2022 (n50)*

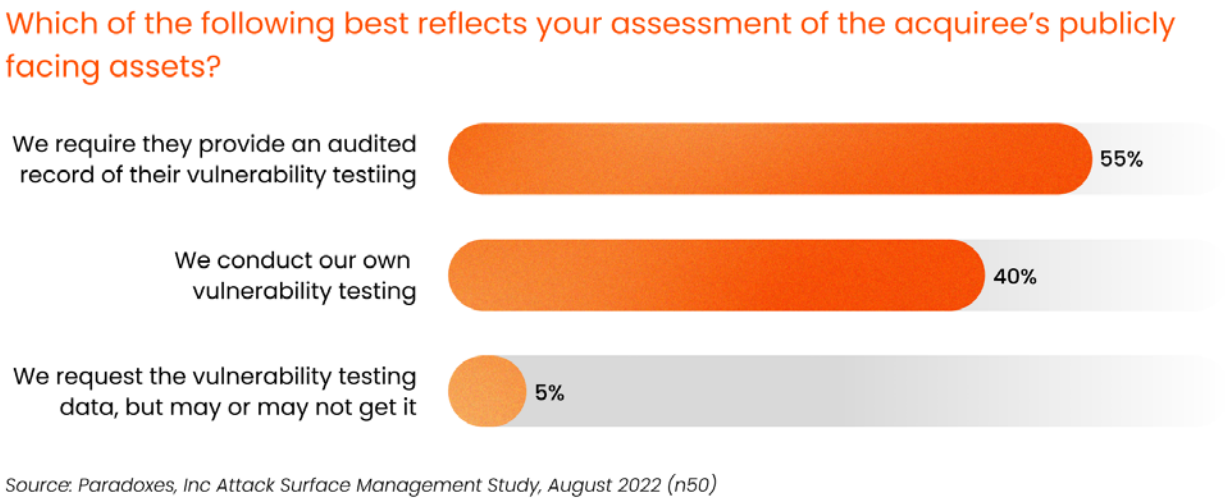
Nearly three-fourths of survey respondents (74%) indicated that when deciding on acquiring another organization, the organization's focus on cybersecurity was "very important."




*Source: Paradoxes, Inc Attack Surface Management Study, August 2022 (n50)*

Meanwhile, a whopping 88% of respondents investigate the acquiree's cyber exposure, including through partners/vendors, of potential targets of acquisition.

13. Gartner - The Top 8 Cybersecurity Predictions for 2021-2022




While most respondents require an acquiree to provide records regarding vulnerability testing prior to acquisition, 40% do the testing themselves.

The challenge for cybersecurity teams is ensuring that risks are detected and disclosed upfront, as opposed to after the acquisition has been finalized, such as during integration. In order to do so, security teams need to make sure they have a comprehensive understanding of a potential acquiree's cyber exposure, which is a scenario where an ASM tool can help. According to Forrester, using ASM tools during M&A due diligence will help the acquiring firm to understand possible risks and create a plan for addressing security and privacy weaknesses earlier in the process, allowing security and risk teams to prepare and allocate resources.[14]

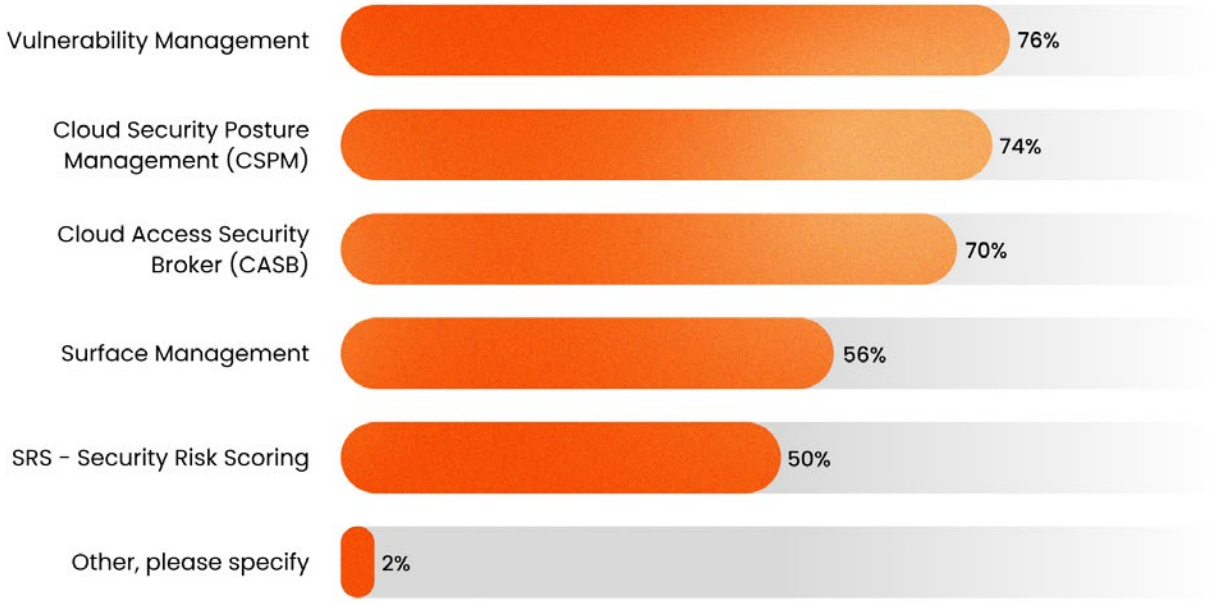
If you've recently inherited infrastructure through a merger or acquisition, or are aiming to be acquired, or just haven't looked at the Internet-facing assets in your organization in a while, there's no time like the present. Now is the time to put on your offensive security hat and do some reconnaissance of your organization's Internet-facing footprint using ASM. If you're concerned there are additional assets you don't know about (spoiler: there probably are), an ASM platform can help identify these assets so you can lock them down and get your sensitive services off the public Internet.[15]

14. Forrester - Find And Cover Your Assets With Attack Surface Management
15. Censys' State of the Internet report

# Where ASM Fits in the Security Stack.

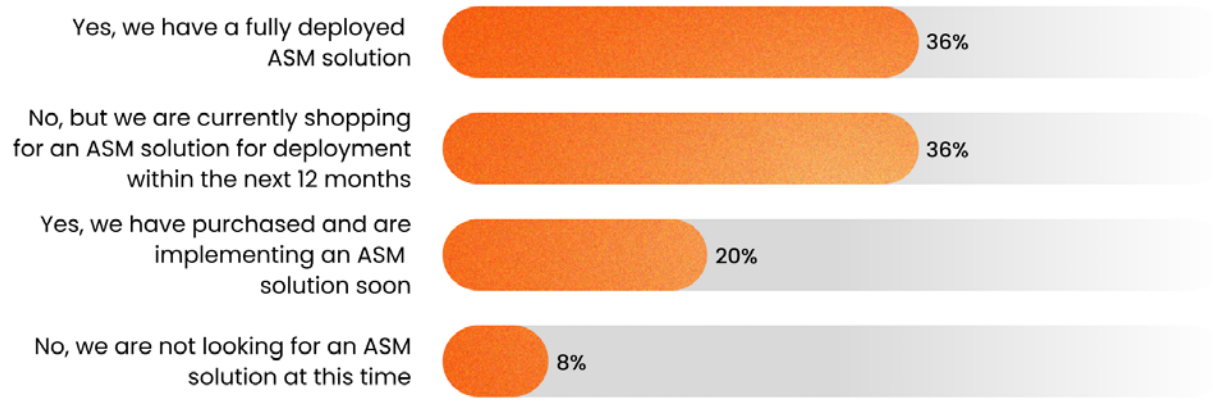
Cybersecurity professionals employ a blend of solutions to protect their organizations. The most common solutions used are Vulnerability Management, Cloud Security Posture Management (CSPM), Cloud Access Security Broker (CASB), and Attack Surface Management.

What tools does your organization employ to combat these internal and external risks? Please select all that apply.




*Source: Paradoxes, Inc Attack Surface Management Study, August 2022 (n50)*

Does your organization currently employ an ASM solution in its security stack?




*Source: Paradoxes, Inc Attack Surface Management Study, August 2022 (n50)*

> "The first thing that comes to mind when I hear Attack Surface Management is a comprehensive solution that analyzes existing vulnerabilities and enables mitigation efforts."
>
> – CISO, HEALTH CARE

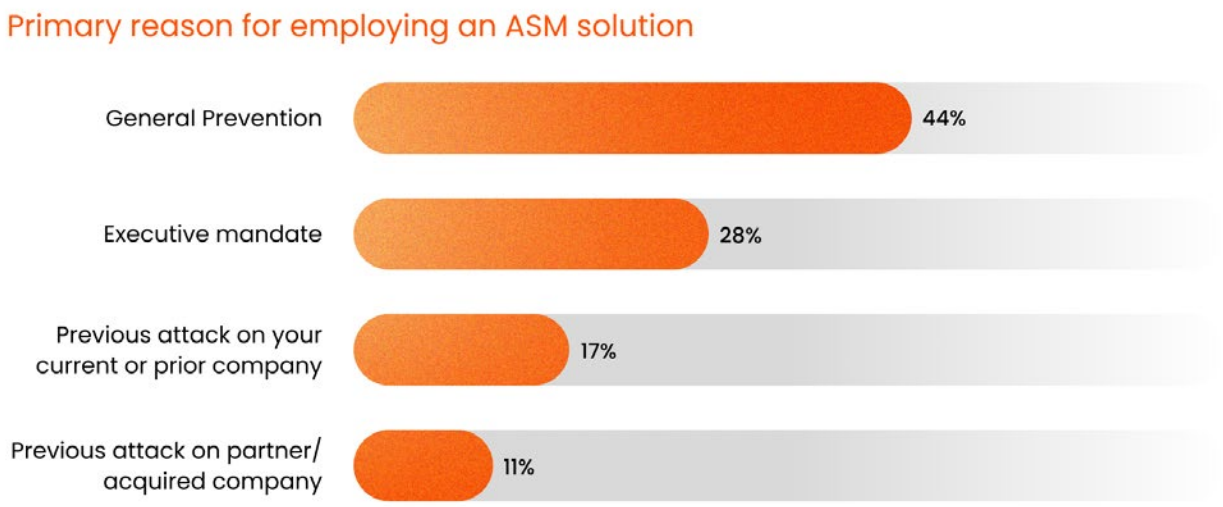
> "The value of ASM is being able to identify the assets that an attacker is likely to discover and exploit."
>
> – DIRECTOR, SECURITY ARCHITECTURE & ASSURANCE

Many teams using ASM also see it as an enabler of their agile processes. Overly burdening development teams with security protocols hinders the speed at which they need to move. ASM provides a layer of protection that does not inhibit developers.

> "An ASM platform is the intersection point with some development teams that are spinning up new resources because [my organization] needs to be agile and we don't want them to go through security roadblocks, but I want to be aware of what they are spinning up."
>
> – SENIOR ENGINEER, TECHNOLOGY

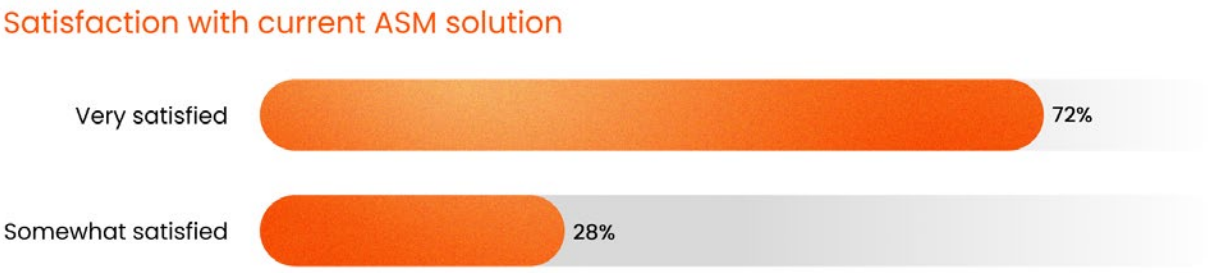
**I see the ASM solution as an initiator of response action. It is also key in the response process to other incidents. For example, when another tool or identifier says there's a security incident, I use my ASM platform as an additional resource for gathering intelligence about the vulnerability.**

– SENIOR ENGINEER, TECHNOLOGY




*Source: Paradoxes, Inc Attack Surface Management Study, August 2022 (n50)*

The main driver for adopting an ASM solution, according to survey respondents, was for general prevention (44%). Executive mandate was the second leading catalyst (28%). Previous attacks on current or prior company (17%) or partner/acquired company (11%) also factored into the mix. For those who do employ an ASM solution, high marks were given for satisfaction (72% report being very satisfied with the product) and value relative to cost (94% in agreement for getting value relative to the cost).




*Source: Paradoxes, Inc Attack Surface Management Study, August 2022 (n50)*


*Source: Paradoxes, Inc Attack Surface Management Study, August 2022 (n50)*

"There is tremendous value in our ASM product. It is definitely something every company needs." - Senior Engineer, Technology

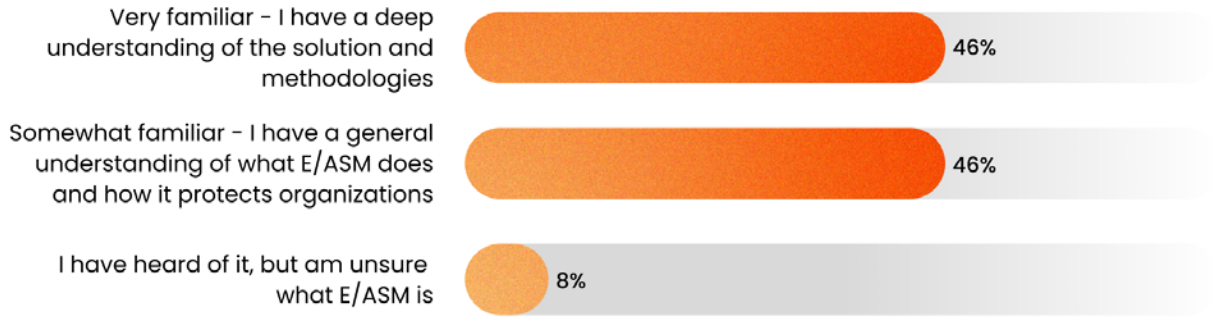
The visibility aspect of ASM is crucial. Being able to scan and identify all devices associated with your organization, particularly those that you were unaware existed, is essential to create the best protection possible for your organization. You cannot protect what you can't see.

> **The risk of not having an ASM product, at a certain company 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 that information to consolidate and make decisions on what is occurring is essential.**
>
> – SENIOR ENGINEER, TECHNOLOGY

Classification of assets helps security professionals keep everything organized they are trying to monitor. A system that breaks down types of assets, where they were found, associated risks and the severity of those risks, and potential remediations makes it easier to understand the entirety of your organization's assets. Once everything is clearly identified and the details understood, then strategies can be put in place to monitor and defend against threats.

Among the current ASM product users that we surveyed, the highest levels of satisfaction were reported for user interface (61% rating 5 out of 5) and remediation recommendations (50% rating 5 out of 5).

How familiar are you with Attack Surface Management (ASM) or External Attack Surface Management (EASM)? By ASM and EASM, we are referring to the process of continuously discovering, identifyinh, inventorying, and assessing the exposures or an entity's IT asset estate.




*Source: Paradoxes, Inc Attack Surface Management Study, August 2022 (n50)*

Survey respondents who did not use an ASM solution provided several explanations as to why – half of respondents (50%) cited their public facing assets were already monitored and/or an ASM solution was not in their security budget, while 25% reported being unaware of ASM in the first place.

# About Censys ASM.

Censys provides a leading Attack Surface Management solution that broadly, deeply and relentlessly searches and proactively monitors your organization's digital footprint, identifies and rates risks and recommends remediation actions. Censys maintains the most comprehensive view of the public Internet by continuously scanning the public IPv4 address space across over 3600 of the most popular ports. This data powers its Internet asset discovery platform, which maps weak points across an organization's infrastructure. These systems provide a valuable lens into the rapidly changing attack surface of the Internet.

> **"[Censys' ASM data] It's valuable. We're moving toward cloud more and more. We need cloud visibility. Related reporting and data analytics are important to me."**
>
> – CISO, PROFESSIONAL SERVICES

> **"We've been able to really mature our understanding of our Internet Presence and have begun to wrap a process around discovery and tracking. Censys ASM has provided us with the flexibility to experiment processing the data it associates with us."**
>
> – DIRECTOR, SECURITY ARCHITECTURE & ASSURANCE

The relevancy of historic data also cannot be understated. Being able to reference prior dates in history to see how your organization looked, risk and protection levels, etc. is incredibly valuable.

> **"Customers are asking more and more about historical information. They want to create a report to see, what did I look like last week compared to this week? Views comparing specific days or to better visualize what has changed in ASM. The application of data is more important than ever."**
>
> – DAVID SOOHOO, VP OF PRODUCT, ASM, CENSYS

Another important element of our ASM solution is its ability to categorize and turn a vast array of information into digestible bites. Security professionals want to see a manageable list of assets with easy-to-understand risk analysis and remediation

tips. For a security team, it is incredibly useful to be able to look at a dashboard that is well-organized, navigate to a risk page, and start investigating individual risks. By triaging high risk items, security teams will immediately make an impact in increasing their organization's protection and lowering overall risk.

> **"Risk data is very valuable. But 800 storage buckets are not helping anybody. We remove the false positives. Our buckets take a giant list of domains and get down to a manageable list."**
>
> – ART STURDEVANT, VP OF TECHNICAL OPS, CENSYS

Censys' ASM solution distills down the data into relevant, actionable pieces which provides tremendous value to security teams. Instead of thousands of risk notifications and alerts with unclear urgency, which is overwhelming and will surely lead to important issues being overlooked, our ASM solution focuses on showing customers what is most important and relevant. By focusing on what is most likely to get compromised and providing context around what the problem is and how to fix it, our ASM solution can equip even the newest member of a security team with the knowledge to immediately make an impact to reduce risk and secure assets. In the end, Censys' ASM solution will help organizations become more organized and faster with understanding their publicly facing assets and exposure, and thus reducing risk.

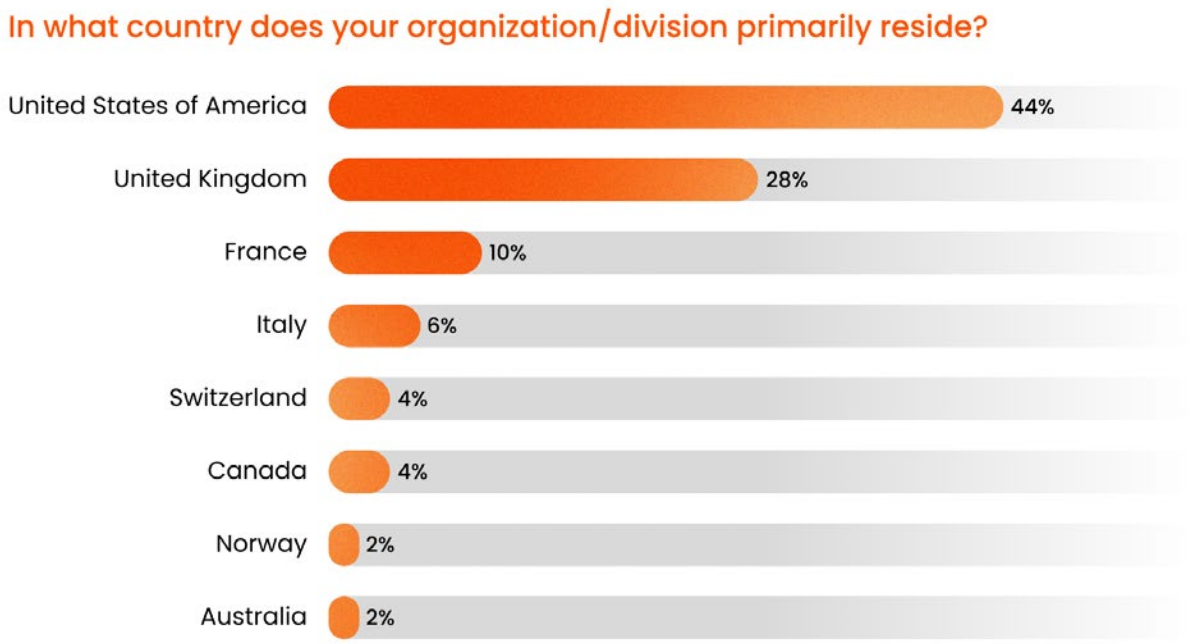
For more information visit www.censys.io.

# About This Report.

Data for the The 2022 State of Risk & Remediation Report was collected in the summer of 2022. Dozens of interviews were conducted with security professions and 50 completed an online survey about their cybersecurity concerns, solutions used and risk mitigation efforts and goals.

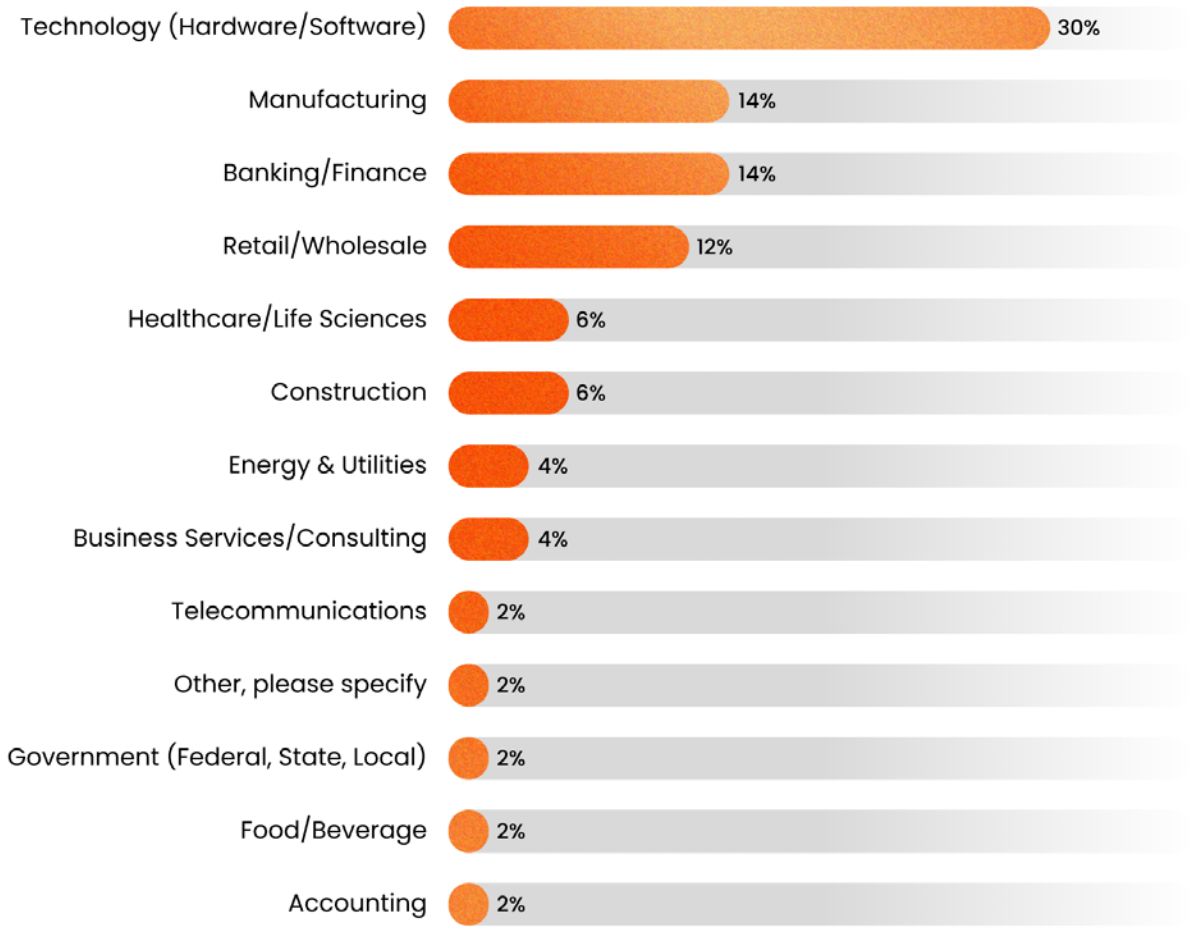
Respondents came from 8 countries, with the largest percentage in the United States (44%), followed by the United Kingdom (28%). The three most common industries for survey participants were technology, banking/finance and manufacturing. Organization size was relatively evenly distributed, with large organizations having more than 5,000 employees representing the largest segment (42%) of the sample. Half of respondents (50%) reported a decade or longer of experience in cybersecurity, followed by 30% of respondents who had 5-10 years of experience.

## PARTICIPANT GEOGRAPHY



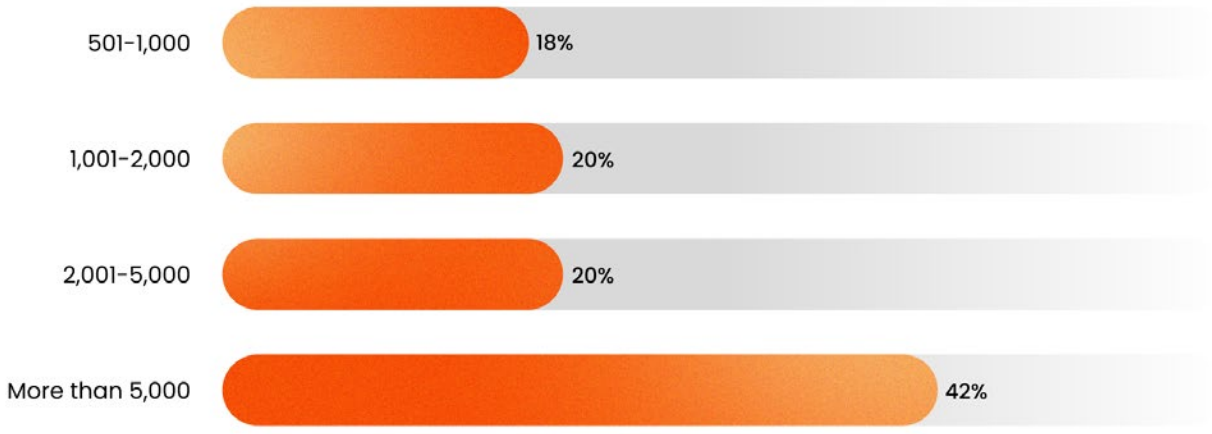
## PARTICIPANT INDUSTRY

What is your company's principal business or industry?




## PARTICIPANT COMPANY SIZE

Approximately how many full-time employees work at your organization across all locations?



## PARTICIPANT EXPERIENCE