STATE OF

Attack Surface Management

The Challenges & How Your Organization Stacks Up

TEAM CYMRU®
THE POWER OF PURE SIGNAL™

REPORT

Introduction

The legacy approach to Attack Surface Management falls short of what modern organizations require: contextual awareness. Security teams increasingly suffer from threat intelligence sensory overload while still unable to achieve the visibility they need to protect the organization, its infrastructure, and mission critical digital assets.

Too often, security teams are drowning in a flood of ineffective tools that only provide internal visibility or limited views of owned assets. As a result, they struggle to discover, classify, prioritize, and manage external- assets, which leaves them vulnerable to attack, and defending their organization proactively is a significant challenge.

But how bad is this deluge, and how many security teams threaten to sink due to their current ASM platform being ineffective? We wanted to explore this topic with our own survey and answer questions such as 'is ASM already in the trough of disillusionment? If so, why?' and 'What needs to change for ASM to evolve to truly add value across the organization?'

We conducted this survey to discover the facts and an up-to-date story behind the numbers to highlight the challenges security professionals face with their existing ASM solutions. This report presents our findings and offers senior security leaders and cyber risk stakeholders a factual basis for making the changes necessary to improve their ASM program.

These findings will help you take a critical look at the limitations of your current ASM, as not all ASMs are created equal. Your business demands more as it expands, so you should expect more of your ASM platform as well. See how your ASM measures up to your organizational goals, specifically risk scoring, an important measure to align security with your executive risk management program.

Rabbi Rob Thomas
Chairman, CEO, and Cymru Fellow at Team Cymru

Key Findings

Is ASM 1.0 failing to take off from the launch pad?

- **Shadow IT: 20.0%** *Respondents say their organization implemented ASM to increase their visibility of shadow IT in the enterprise, other surveys have discovered this sometimes in excess of 50%. 23.4% say the identification of rogue or unclassified events is the most valuable capability that ASM has provided their organization.*

- **Cloud Migration: 16.3%** *say that moving more data and assets to the cloud is the primary reason their attack surface is expanding.*

- **Lack of Integration: 14.5%** *cite the main limitation of existing ASM platforms as their lack of integration with automation platforms.*

- **Required Training:** *A plurality of* **21.5%** *indicates that the training needed for analysts to use the platform is their primary challenge with their current ASM platform.*

- **Time to Deploy:** *Of those involved in deploying their current ASM solution,* **23.2%** *said it took 6 to 9 months to get them up and running. For* **18.5%**, *it took over a year.*

- **Security Concerns: 29.7%** *said their top concerns were about the security aspects of data integration and how much access their current ASM platform had across the enterprise.*

- **Cost: 21.1%** *felt they overpaid for their current ASM solution. Of the* **48.5%** *that plan to stop working with their ASM vendor in the next 12 months,* **21.0%** *cite the cost of operation and maintenance as the reason.*

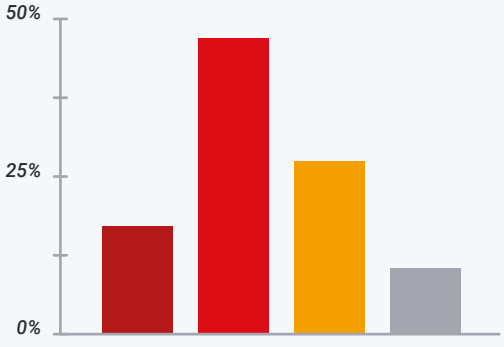
- **Future Plans: 51.0%** *have no plans to stop working with their ASM vendor in the next 12 months. However,* **27.9%** *say they do plan to terminate their current ASM vendor with no intentions of replacing them.*

Table of Contents

Methodology and Participant Demographics

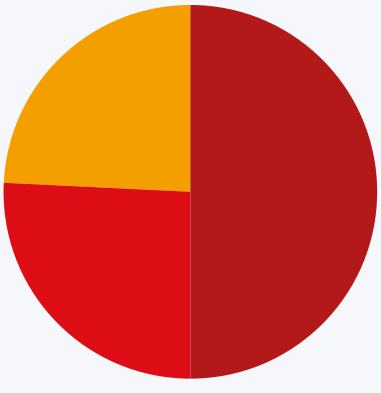
To provide greater context around the findings presented in this report, we offer more details about who we surveyed and the methodology used. Starting on March 14, 2022, we surveyed 440 security practitioners in the US and Europe. The survey was conducted online via Pollfish using organic sampling. Learn more about the Pollfish methodology *here.*

Job Level



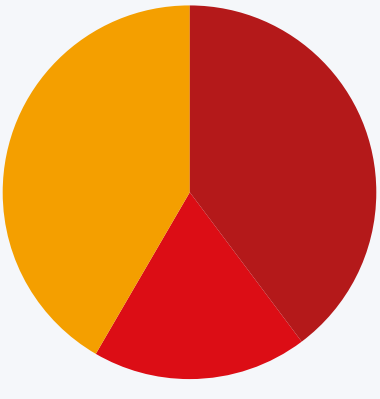
Executive	18.0%
Team Manager	45.0%
Senior Individual Contributor	27.0%
Individual Contributor	11.0%

Region



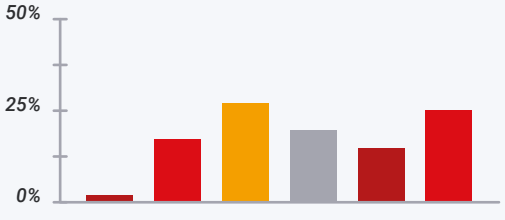
US / Canada	50.0%
EMEA	26.0%
APAC	24.0%

Company Size



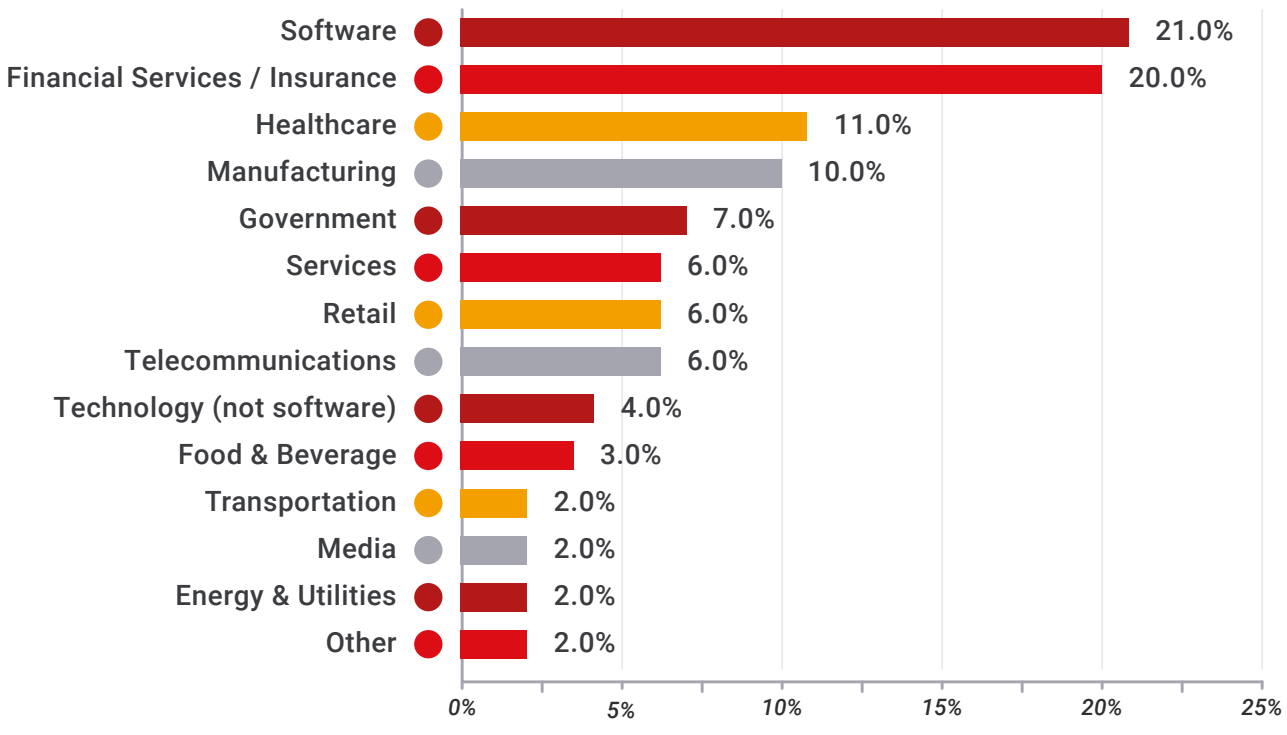
1,000 - 5,000 employees	39.0%
5,000 - 10,000 employees	20.0%
10,000+ employees	40.0%

of Dedicated Security Analysts



None	3.0%
1 - 2	15.0%
3 - 5	26.0%
6 - 9	17.0%
10 - 20	14.0%
More than 20	25.0%

Industry



Gender

Male	54.7%
Female	45.2%

Age

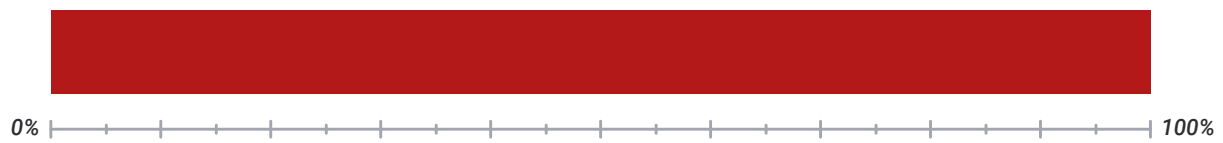
18 - 24	20.6%
25 - 34	27.7%
35 - 44	24.5%
45 - 54	11.1%
> 54	15.9%

Country

Austria	2.5%	Belgium	3.1%	Finland	2.5%
France	2.0%	UK	8.8%	US	62.5%

All respondents work on their company's security team, all currently use an ASM platform, and the plurality (24%) are mid-level professionals. Their sectors vary from finance to IT to military and defense, among others. The team size varies relatively little, from less than 10 to over 30.

What best describes the team you are on at work?

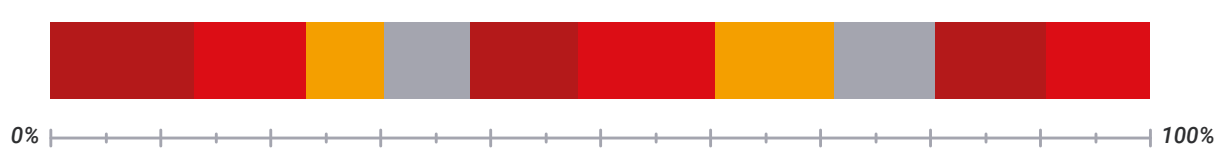


Security team	100.0%

Which of the following is accurate? (As defined by Gartner, Attack Surface Management (ASM) "refers to the processes, technology and professional services deployed to discover external-facing enterprise assets and systems that may present vulnerabilities.)

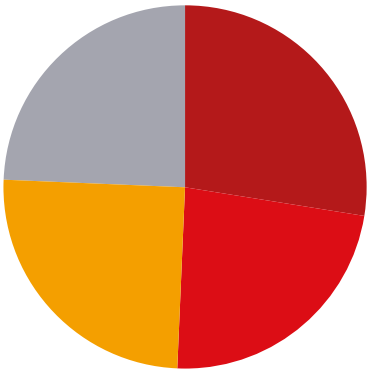
Our team currently uses an Attack Surface Management platform	100.0%

What industry does your company primarily operate in?



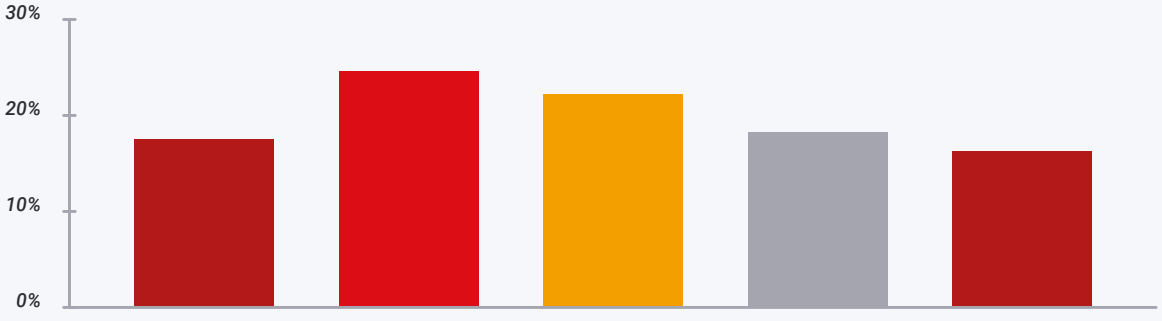
Financial services, insurance, real estate	13.6%
Higher education, K-12 education	10.0%
Non-profit	7.2%
Healthcare, biotech, pharma, medical	7.5%
Marketing, advertising, media	9.5%
IT, technology, software	13.1%
Manufacturing, warehouse, logistics	10.2%
State, local, federal government	8.8%
Military/Defense	10.0%
Other	9.7%

How many people are employed on your security operations team?



Less than 10 people	27.0%
10 - 20 people	23.4%
20 - 30 people	25.0%
30+ people	24.5%

How would you describe your current role?



Early career individual contributor (1-3 years)	17.9%
Mid career individual contributor (4-6 years)	24.3%
Senior individual contributor (7-9 years)	21.8%
Information Security Manager	18.6%
Information Security Executive	17.2%

Now, with context around who our respondents were, let's take a closer look at what we uncovered.

PART #1

Existing Platform

An organization needs a set of robust tools in order to keep it safe — especially when it comes to assessing and protecting the attack surface. But what kind of tools and approaches are modern security teams actually using? In this section, we learn a bit more about respondents' existing ASM platforms, why they purchased their system, what assets they manage, and more. They also give us insights into what's working with their ASM platforms, and where the limitations are.

KEY FINDING #1: The top capabilities are breach and attack simulation, vulnerability scanning, and cloud access security broker.

What cybersecurity capabilities have our respondents and their teams implemented at their organization? Given ten options, our field of 440 respondents selected a combined 1,233 capabilities. That is an average of about three per respondent. The three most commonly used overall are:

BAS tools: 31.1% said they use breach and attack simulation (BAS) software to mimic real-world security threats, helping them prepare incident response plans and discover potential vulnerabilities.

- BAS Limitation: Specifically focuses only on known assets. The use case for ASM 2.0 is to continually discover assets that can then be passed over to the team that takes the lead on BAS, in addition to Vulnerabilities Management.

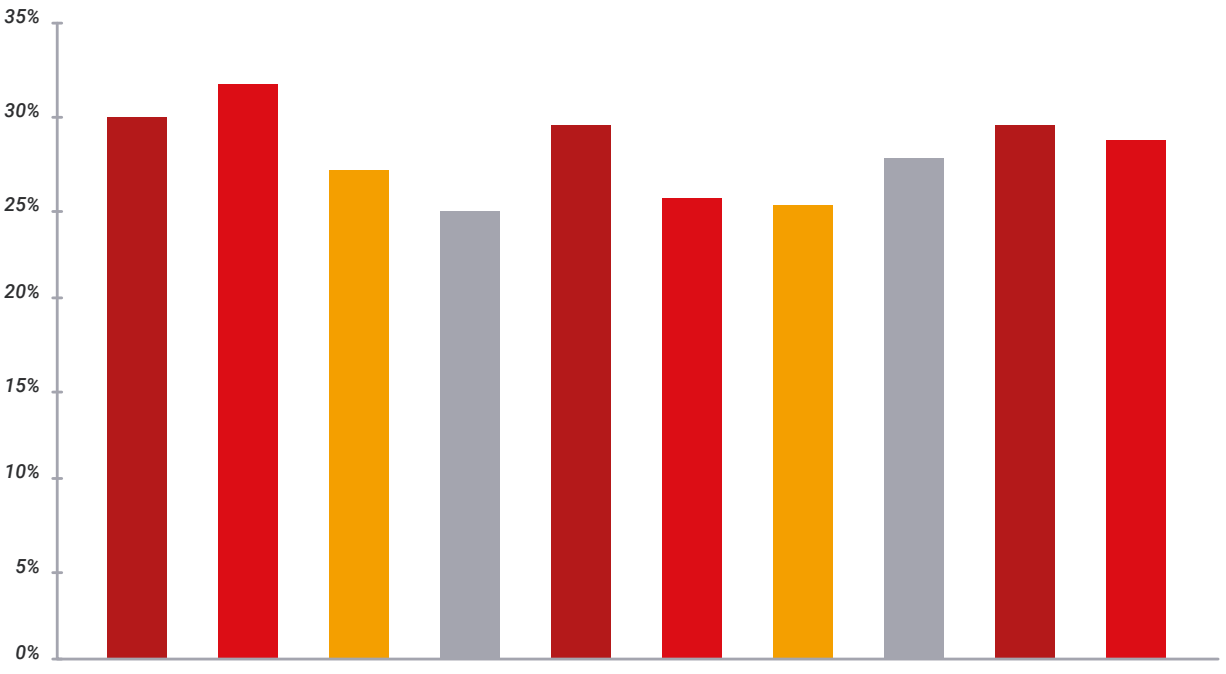
Scanning: 30% of the respondents said they use internal and external vulnerability scanning to detect security vulnerabilities before hackers have a chance to exploit them.

- Scanning Limitation: Similar to BAS, Scanning external assets for vulnerabilities is time consuming and limited in scope to only known assets. Considering we discover between 30% to 500% more assets than organizations are previously aware of, Scanning manually or with a sub-optimal ASM tool doesn't provide a complete picture.

CASB: A cloud access security broker (CASB) is used by 29.3% to manage and enforce data security policies and practices.

- CASB Limitations: Being deployed at the corporate gateway, CASB is only effective at monitoring outbound connections to the Cloud. The use case for ASM is to expand visibility to any Cloud application or service that connects directly, as viewed from the internet. This significantly broadens visibility of Shadow IT beyond border detections.

What cybersecurity capabilities does your team currently have implemented?



Internal and external vulnerability scanning	30.0%
Breach and attack simulation (BAS) tools	31.1%
Enterprise digital forensics	27.0%
Penetration testing	25.0%
Security Information and Event Management (SIEM)	29.0%
Security Orchestration, Automation, and Response (SOAR)	26.8%
24x7x365 Security Operations Center	25.6%
Network traffic decryption and inspection / full packet capture	27.7%
Cloud Access Security Broker (CASB)	29.3%
External Threat Hunting	28.4%

KEY FINDING #2: The biggest reason their organization implemented ASM is to increase the visibility of shadow IT in the enterprise.

IT systems, cloud based services and web based applications deployed without the knowledge of the IT or security group are an ever-present risk for many organizations. While there are plenty of valid and valuable reasons to deploy shadow IT — such as a temporary workaround for shortcomings in central IT

systems or prototypes for future innovation — there are significant dangers because there is likely to be little or no security visibility. This is why the largest segment of respondents (19.8%) said that the main reason their organization implemented an ASM is to increase their visibility into shadow IT.

What was the biggest reason your organization implemented Attack Surface Management?

Difficulty detecting new IT assets outside the enterprise	17.2%
No existing capability to continuously monitor for changes to the attack surface	15.4%
Increased remote workforce due to COVID-19 with more assets outside of the organization	16.8%
Compliance with regulatory and/or audit requirements	15.4%
Increase visibility of shadow IT being used in the enterprise	19.7%
Driven by lines of business such as M&A and Supply Chain Risk Management	15.2%

KEY FINDING #3: Ease of use or user experience is the most important consideration when selecting their ASM vendor.

When security tools are clunky and difficult to operate, the pressures of keeping pace with the demands on a security team will lead to shortcuts, workarounds, or abandonment of the tool. The fact that the largest segments of respondents (17.5%) said their most important consideration was ease of use or ease of user experience indicates that, more than any other single consideration, users must have a tool that doesn't slow them down or make their jobs more difficult.

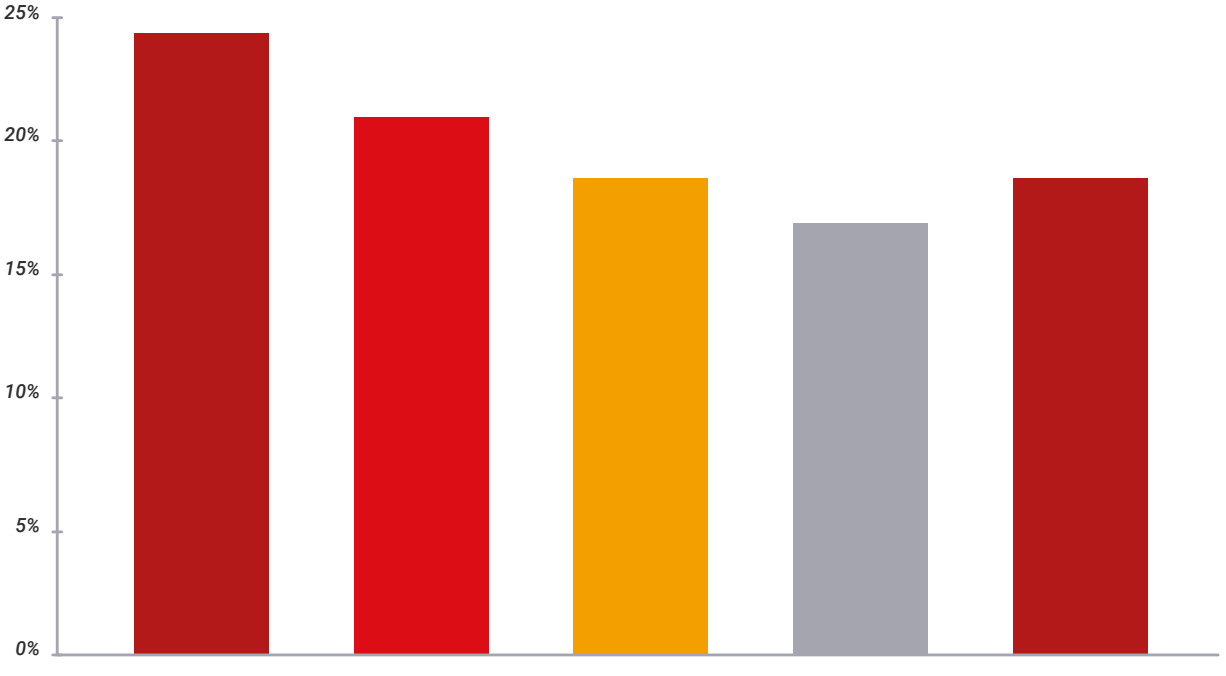
When selecting your Attack Surface Management vendor, what was the most important consideration?

Cost and licensing model (i.e., per asset licensing vs. per user)	13.6%
Ease of implementation	13.1%
Integration with existing security tools/workflows	14.0%
Ease of use / user experience by cybersecurity professionals	17.5%
Functionality and visibility across the enterprise	13.1%
Ability to discover hidden IT assets	16.3%
Reporting and Trending data	12.0%

KEY FINDING #4: Only 25% of respondents define their attack surface as infrastructure and applications that are 100% on-premises in their own data center.

Our survey confirms that most companies — and 75% of our respondents — have at least some applications, software, and infrastructure in the cloud. You could infer that the other 25% are unaware they have external assets, simply because their existing ASM is suboptimal at discovering new ones. ASM is critical for all organizations, regardless of their cloud adoption, but should be an even higher priority for tracking and managing the attack surface for cloud-hosted assets.

How would you define your attack surface?



Infrastructure and applications are 100% on premises in our own data center	24.7%
Majority of infrastructure and applications are hosted on premises, with some software-as-a-service (SaaS) used in the organization	21.5%
A mix of on premise and cloud infrastructure and applications	18.6%
Our organization has a cloud-first policy, but some legacy infrastructure and applications still exist on premise	16.3%
We are 100% in the cloud with the exception of end user devices	18.6%

KEY FINDING #5: 35% have a CIO, CTO, or head of technology, but all technical work is done at the department level.

When asked how responsibilities are laid out in their organization, over one-third (35%) said that while their organization has a CIO, CTO, or head of technology who is responsible for strategy, all technical work is executed at the business unit or departmental level. This explains the need for ASM platforms to craft specific business risk functions to be simple, intuitive and geared towards non-IT operators. The responses to this question are indicative of a growing trend. More than in the past, organizational leaders treat risk holistically, including security risks. Security mitigation and remediation strategies must be risk-based to make a meaningful contribution to the organization's risk profile calculus.

How would you describe IT responsibilities in your organization?

IT is completely centralized and all IT is managed and controlled by our organization's IT department	31.5%
Our organization has a CIO, CTO, or head of technology which is responsible for strategy, but all technical work is done at the business unit or department level	35.0%
IT is responsible for corporate functions (governance, policy, security), but technical resources are embedded within business units	33.4%

KEY FINDING #6: Their ASMs manage servers, code repositories, infrastructure, and desktops.

When it comes to what type of assets they manage with their ASM (and when asked to choose all that applied), our respondents are managing servers (33.6%), code repositories like GitHub (32.1%), infrastructure like routers, switches, and firewalls (30.7%), and desktops (30.7%). Each asset class presents another layer of complexity for attack surface management. ASM solutions must be able to handle everything from open or closed source third-party supply chain and partner vulnerabilities to on-premise hardware and software assets.

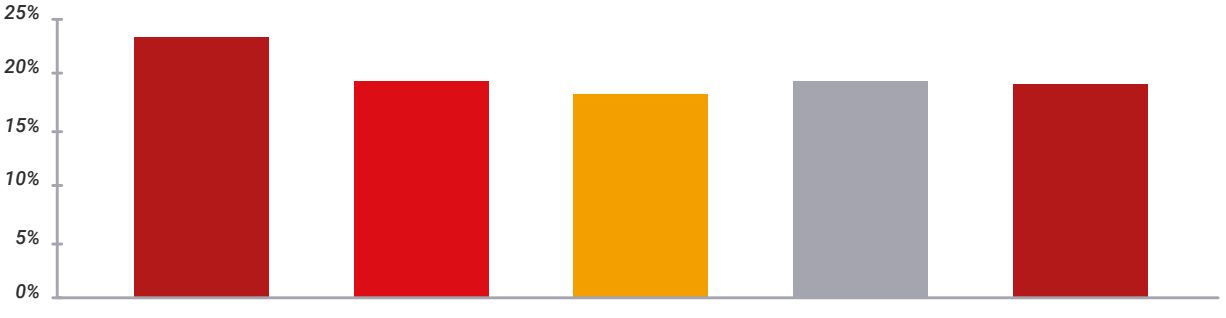
What types of assets do you currently manage with Attack Surface Management?

Servers	33.6%
Desktops	30.6%
Mobile devices	27.9%
Infrastructure (routers, switches, firewalls, etc.)	30.6%
Cloud assets	27.7%
IoT devices	28.4%
Code repositories (GitHub, etc.)	32.0%
Domains	28.4%

KEY FINDING #7: 23% say the identification of rogue or unclassified assets is the most valuable capability that ASM has provided their organization.

While the last question identifies some of the most common assets organizations use ASM to manage, this finding indicates where fear of the unknown makes itself present as a significant cyber risk, and therefore threat vector. The ability to look beyond these known quantities and identify rogue or unclassified assets is the most valuable ASM capability (23.4%). It is these assets that fall outside of enforced policies and procedures that threat actors often leverage during a breach.

What has been the most valuable capability the Attack Surface Management tool has provided your organization?



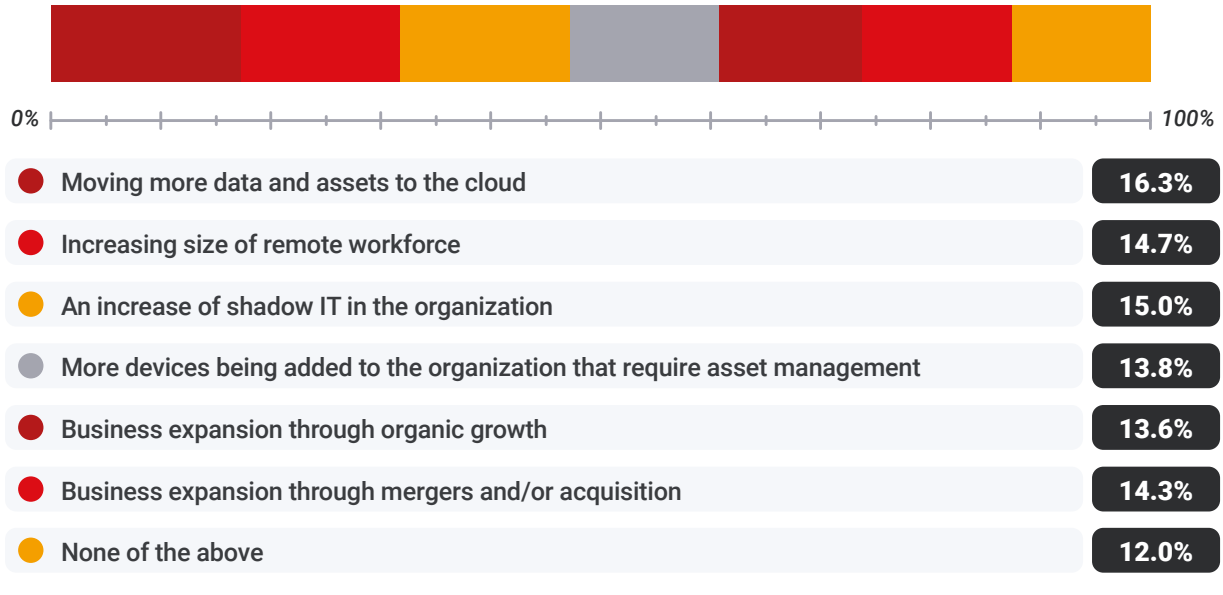
Identification of rogue or unclassified assets	23.4%
Single view of vulnerability and risk posture information	19.7%
Up-to-date asset inventory with ability to categorize assets by risk	17.9%
Monitoring of third party assets such as domain names, data repositories, IP addresses, etc.	19.7%
Coupling vulnerability information with threat intelligence	19.0%

KEY FINDING #8: Moving more data and assets to the cloud is the number one reason their attack surface expands.

It's no question that attack surfaces are expanding, and in turn, this is driving not just a need for ASM, but ASM that can move at the same pace of that dynamic and changing landscape. According to our respondents, the top reasons for that expansion include moving more data and assets to the cloud (16.4%), an increase of shadow IT in the organization (15%), and the increasing size of their remote workforce (14.8%).

The traditional approach of addressing individual security threats breaks down in the face of evolving technologies like mobile, cloud, IoT, and their associated threat vectors. As cloud adoption increases, many organizations still rely on outdated methods of network defense. Cloud security demands a strategy that considers internal and external network infrastructures with an attack surface that's dynamically changing and diverse.

What is the #1 reason for your attack surface expanding?



KEY FINDING #9: The main limitation of existing ASM platforms is the lack of integration with automation platforms.

Even though our respondents have ASM approaches in place, they are finding limitations to those approaches. Top drawbacks include a lack of integration with automation platforms (14.6%), limitations in the customization of risk profile and/or asset criticality (14.3%), and a lack of visibility into certain technologies, like cloud, IoT, and others (13.4%).

Automation is crucial for freeing up security teams to focus on essential tasks. ASM solutions that provide only a limited ability to automate mundane tasks miss the mark for one of the most critical reasons organizations need better security tools: to help them keep pace with emerging threats and a tsunami of vulnerabilities.

What is the #1 limitation of your existing platform?

Lack of visibility with certain technologies (e.g., OT, IoT, Cloud, etc.)	13.4%
Inability to gain a real time or dynamic view of IT Assets	13.1%
Data analytics and visualization of attack surface risk posture	10.4%
Amount of technical expertise required to implement/maintain	11.1%
Customization of risk profiles and/or asset criticality	14.3%
Lack of integration with automation platforms	14.5%
Reports and dashboards that are not executive friendly	10.4%
None of the above	12.5%

KEY FINDING #10: 21% of security teams have used their current ASM platform for 3-4 years.

Security technologies change rapidly to keep up with new threats and address advancements in security, IT, and risk management processes and workflows. Our survey indicates that 66.8% of organizations currently use an ASM solution that is more than three or four years old; some use solutions with more than five-year-old technology. In many cases, this technology is overdue for replacement to a more contemporary platform that offers more cohesive digital risk management, in addition to improved integration.

How long has your security team been using your current Attack Surface Management platform?

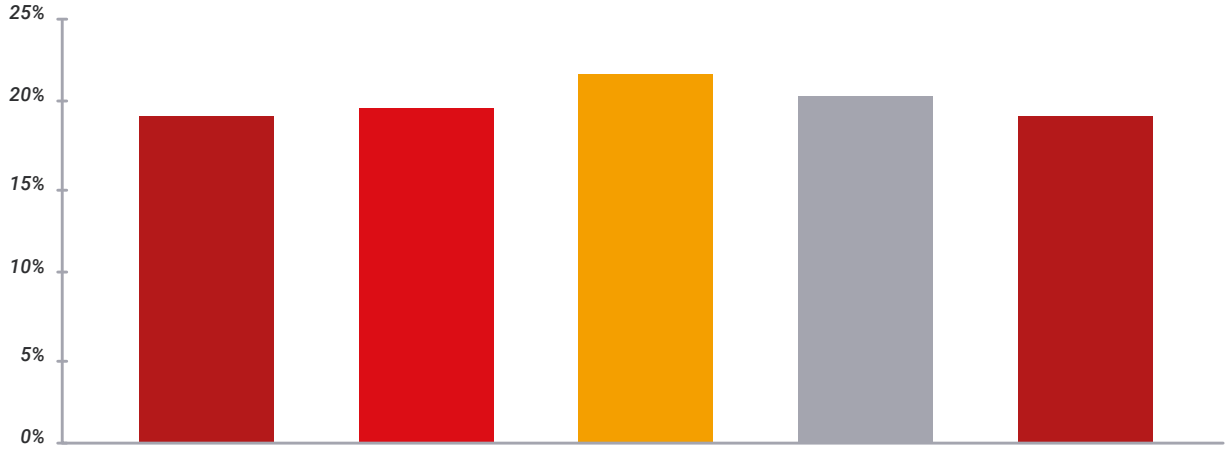
Less than 1 year	16.8%
1 - 2 years	16.3%
3-4 years	20.6%
4-5 years	14.3%
5+ years	18.4%
I don't know	13.4%

KEY FINDING #11: Their top challenge is the amount of training required for analysts to use the platform.

In addition to the limitations of their ASM, we were keen to explore what the day-to-day challenges respondents faced with their platform? Their top challenge is the amount of training required for analysts to use the platform (21.6%), followed by the level of effort required to create alerts, reports, and dashboards (20.5%), and the lack of resources to realize its full potential (19.8%).

When security solutions require an excessive amount of time to get analysts up-to-speed before they can effectively do their jobs, they act as a drag on an already struggling security team staffing problem. Modern ASM solutions typically overcome these challenges associated with legacy platforms by combining an intuitive interface and the flexibility to work within established processes and workflows, or enable easy creation of new ones more likely being the case.

When it comes to interacting with your Attack Surface Management platform day to day, what is the #1 challenge you face with your platform?



Difficulty in interpreting information and creating actionable intelligence	19.0%
Lack of resources to realize its full potential	19.7%
Amount of training required for analysts to use the platform	21.5%
Level of effort required to create alerts, reports, and dashboards	20.4%
Amount of development time necessary for APIs, data feeds, and other integrations	19.0%

Having examined how our respondents use, like, and struggle with their existing ASM solutions, we now turn our attention to the deployment process for these platforms. How long it takes to deploy a solution and the frustration level accompanying the implementation are important considerations for organizations hoping to be successful with their ASM approach.

PART#2

Deployment & Implementation

In our last section, we uncovered the baseline for why respondents chose to implement an ASM in their organization and what they hoped to uncover by doing so, as well as what successes, limitations, and challenges they're finding with their current ASM. This section will take a step back and examine our respondents' experiences with deploying and implementing their current solution. Understanding past experiences can provide an informative guide for organizations looking to implement an ASM, including what to be aware of and questions to ask during the purchase decision process.

KEY FINDING #12: Over half were involved in deploying their ASM platform.

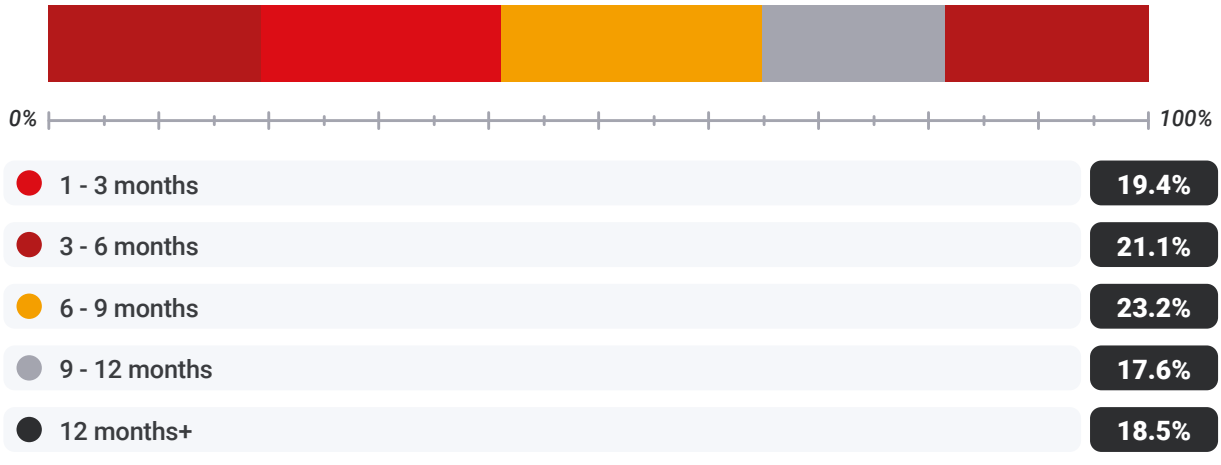
Of those we surveyed, 52.7% were involved in the deployment of their current ASM platform.

Were you involved in the deployment of your current Attack Surface Management platform?

KEY FINDING #13: It most commonly took 6-9 months to deploy their ASM.

For the largest segment of respondents (23.3%), deploying their ASM took six to nine months. 19.4% of our respondents said it took as little time as one to three months, while 18.5% said it took over a year to get their new system up and running. The time it takes to deploy and implement a new security solution is noteworthy because it represents the amount of time the organization needed to integrate their ASM, their tolerance to a lack of full coverage of assets and vulnerabilities, and the improved processes it needs.

How long would you estimate your Attack Surface Management deployment and implementation took to complete?



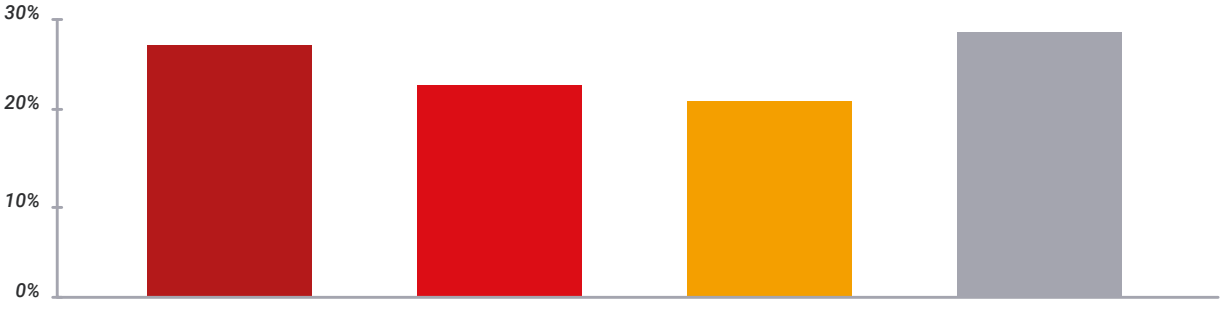
KEY FINDING #14: The top challenge during deploying was security concerns over data integration and the ASM's level of access across the enterprise.

The biggest challenge respondents faced while deploying their ASM was the security concerns that arose over data integration and the level of access their ASM has across their enterprise (29.7%).

Integrating protected data with a new platform or giving an untested solution broad

access across the enterprise will keep a CISO up at night. However, the CISO should find some consolation in the knowledge that sleep will come much easier as the new ASM platform identifies, maps, and manages risks.

What challenges did your team encounter while deploying your Attack Surface Management platform?



Heavy reliance on outside consultants / professional services for implementation	27.5%
Implementation was more difficult than advertised by the vendor	21.9%
Difficulty with accessing data and visibility of assets	20.6%
Security concerns over data integration and level of access the Attack Surface Management platform has across the enterprise	29.7%

Deploying and implementing a new platform certainly comes with a high level of anxiety — and a vendor that tells you ASM is 'plug and play' may warrant a skeptical second look. Vendor selection process should include those with a demonstrable track record of successful, relatively painless implementations, and one that offers to get you up-and-running smoothly. Specifically, features that enable the configuration of ASMs more aggressive features such as proactive vulnerability scanning should be included in your list of RFP questions.

PART#3

Capabilities

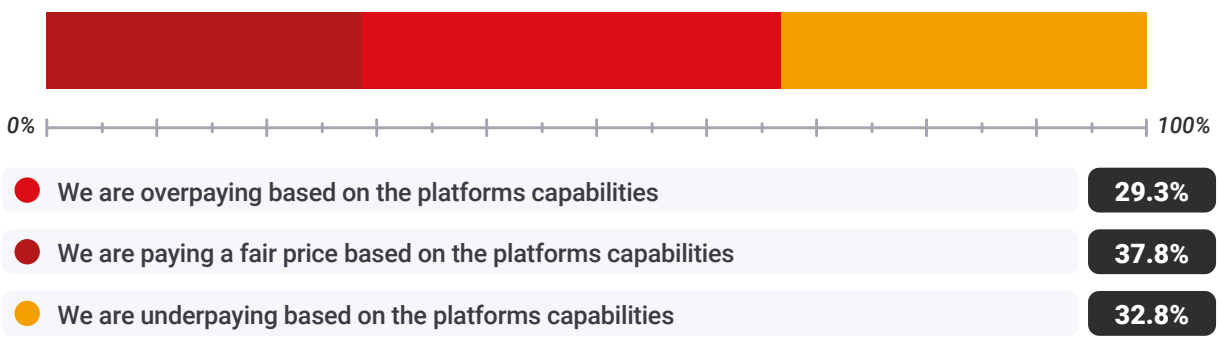
There is a wide variety of specific capabilities that ASM solutions can provide.But do our respondents find that those capabilities are actually doing the job to keep their organization safe? In this section, we'll look at the more common outcomes of using ASM and see how our respondents feel about each, as well as the value they feel they're getting for their current platform.

KEY FINDING #15: 29% said they overpaid for their ASM, 32% said they underpaid, and 37% said the price they paid was fair.

When it comes to the value they feel they're getting for their ASM platform, our respondents are evenly distributed around feeling that they overpaid (29.3%), underpaid (32.8%), and paid fairly (37.8%).

The even distribution in responses likely indicates that most ASM solutions are competitively priced, yet we can't ignore that nearly 30% felt they overpaid, this is significant. This uniformity is good news for an organization looking to kick the tires on a new platform because it shows they can focus more on capabilities than cost.

When thinking about the cost of the current Attack Surface Management platform, which of the following is most accurate?



KEY FINDING #16: 50.9% of respondents say they are not satisfied with the identification of previously unknown IT systems and applications in the environment capabilities of their current ASM platform.

Are you satisfied with the identification of previously unknown IT systems and applications in the environment (e.g., shadow IT) capabilities of your current Attack Surface Management platform?

KEY FINDING #17: 54.3% say they are satisfied with their ability to inventory and classify IT assets capabilities of their current ASM platform.

Are you satisfied with the ability to inventory and classify IT assets capabilities of your current Attack Surface Management platform?

KEY FINDING #18: 54.5% of respondents say they are satisfied with the continuous monitoring of external assets capabilities of their current ASM platform.

Are you satisfied with the continuous monitoring of external assets capabilities of your current Attack Surface Management platform?

KEY FINDING #19: 52.1% say they are satisfied with the dynamic risk and reputation scoring capabilities of their current ASM platform.

Are you satisfied with the dynamic risk and reputation scoring capabilities of your current Attack Surface Management platform?

KEY FINDING #20: 54.1% say they are satisfied with the dynamic monitoring and alerting to changes in IT asset state capabilities of their ASM platform.

Are you satisfied with the dynamic monitoring and alerting to changes of IT asset state capabilities of your current Attack Surface Management platform?

KEY FINDING #21: 50.2% are satisfied with the integration of vulnerability management and prioritization capabilities of their current ASM platform.

Are you satisfied with the integration of vulnerability management & prioritization capabilities of your current Attack Surface Management platform?

KEY FINDING #22: 51.4% are satisfied with the integration of cyber threat intelligence to overall risk determinations capabilities of their current ASM platform.

Are you satisfied with the integration of cyber threat intelligence to overall risk determinations capabilities of your current Attack Surface Management platform?

KEY FINDING #23: 50.9% are not satisfied with the integrations of security risk rating and financial-related metrics capabilities of their current ASM platform.

Are you satisfied with the integration of security risk rating and financial related metrics capabilities of your current Attack Surface Management platform?

KEY FINDING #24: 50.9% are satisfied with the integration with SIEM/SOAR platforms capabilities of their current ASM platform.

Are you satisfied with the integration with SIEM/SOAR platforms capabilities of your current Attack Surface Management platform?

The noticeable trend for the responses in this section is that around half of the respondents were not satisfied with the capability for most questions. This split roughly down the middle indicates no solution currently on the market stands head and shoulders above the crowd. The legacy choices are all so-so; some users are satisfied, and some are not.

Compare those answers to other innovative technologies. Users of new solutions that truly move the needle for how they work widely celebrate them as more than just satisfactory. Organizations should expect that type of response for a new ASM too.

PART#4

Future Plans

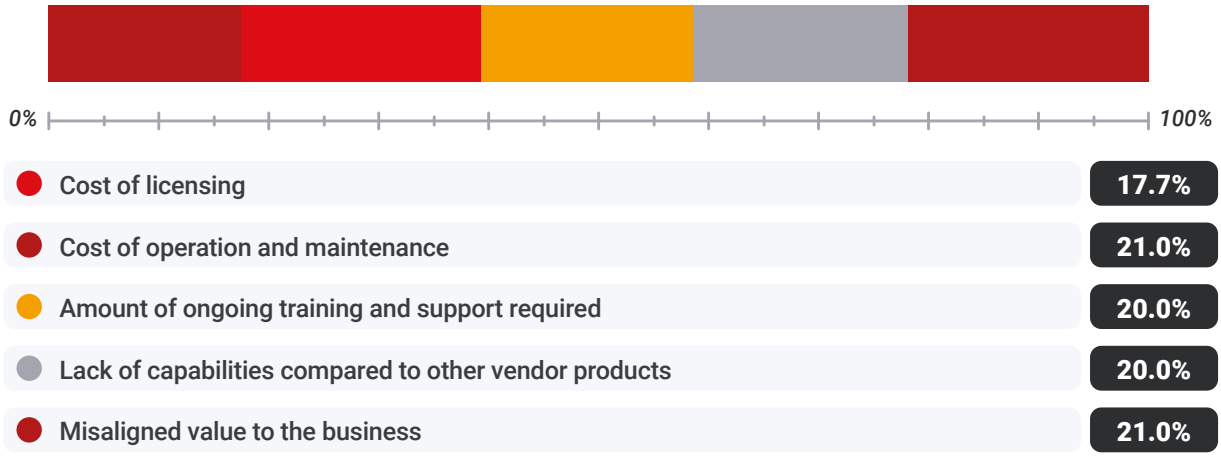
Finally, what, if any, future plans do our respondents have regarding their ASM solution? Considering that many are unsatisfied with how effective their current ASM's capabilities are, our survey reveals their level of frustration and intent to abandon their current provider and, if this is the case, why?

KEY FINDING #25: 51% have no plans to stop working with their ASM vendor in the next 12 months.

Many legacy ASM platforms provide little automation and integration with other crucial security tools. They are labor-intensive and therefore expensive systems to operate and maintain. Of the 48.7% that do plan to end the relationship with their current ASM vendor, a plurality of 21% cites the cost of operation and maintenance as the reason.

Are you planning to end your relationship with this Attack Surface Management vendor in the next 12 months?

If yes, why?



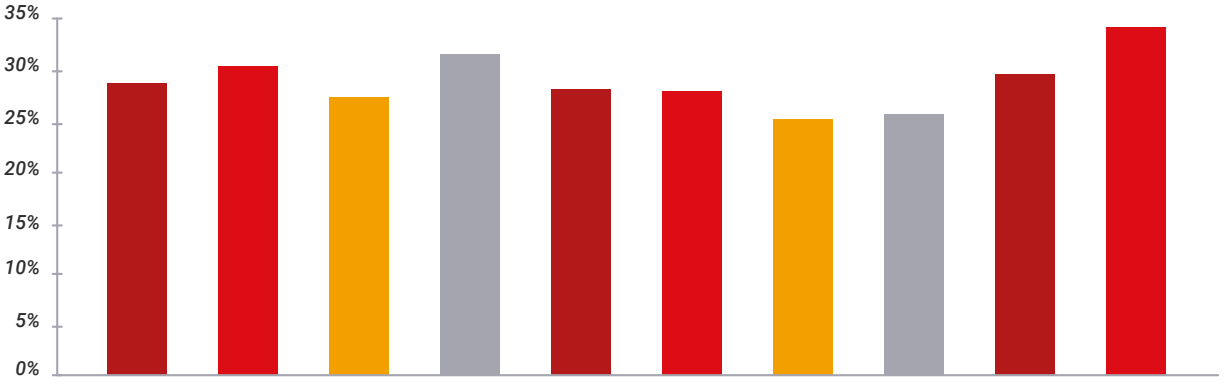
KEY FINDING #26: The most important features and capabilities are integration with SIEM/SOAR platforms, dynamic risk and reputation scoring, and the ability to inventory and classify IT assets.

If our respondents were to evaluate a new ASM platform, they have a few features and capabilities that must be included. Choosing all that they wanted, they primarily

require their ASM platforms to integrate with SIEM/SOAR platforms (34.1%). Then, they want dynamic risk and reputation scoring (30.5%), and the ability to inventory and classify IT assets (30.2%).

In the previous question, we found that users who are unable to automate and integrate are moving away from their current vendor. This next question is about which capabilities are most important. The way the respondents answered supports the premise that integration with other tools, making risk-based security decisions, and confidence in their asset mapping and classification are must-have capabilities.

If you were evaluating a new Attack Surface Management vendor, what features and capabilities would be most important to you?



Identification of previously unknown IT systems and applications in the environment (e.g., shadow IT)	28.1%
Ability to inventory and classify IT assets	30.2%
Continuous monitoring and identification of external assets	27.7%
Dynamic risk and reputation scoring	30.4%
Dynamic monitoring and alerting to changes of IT asset state	28.1%
Integration of vulnerability management & prioritization	27.9%
Integration of and cyber threat intelligence to overall risk determinations	26.1%
Monitoring of malicious assets and incidents	26.5%
Integration of Security Risk Rating and Financial related metrics	28.6%
Integration with SIEM/SOAR platforms	34.0%

CONCLUSION

We believe this survey clearly indicates that it is time for companies to revaluate their ASM. ASM has been a fundamental tool to discover hidden assets and inventory management for many years. Still, when faced with the growing risk of breach from external vulnerabilities, this is no longer enough.

It is also clear that buyers need to demand more as they move away from their legacy ASM. This means a much more detailed RFI and in turn a more robust RFP process with business risk and strategic vulnerability related questions. Capabilities like continuous discovery, automated classification, enabling risk-based security decision making, and more are available and quickly becoming imperative. This should be included right from initial sales engagement and explored during the evaluation process.

Digital business risk for the organization as a whole drives business decisions and must also drive security threat and vulnerability mitigation and remediation strategies.

Don't let your attack surface outpace your ASM solution. Learn how to integrate robust threat intelligence, automation, and risk-based vulnerability remediation to stay ahead of modern threats.

Need Any Assistance?

We are here to help. Get in touch to discuss or learn more – we'll be happy to explain.

LET'S CONNECT

TEAM CYMRU®

THE POWER OF PURE SIGNAL™