https://research.gigaom.com/reprint/gigaom-radar-for-attack-surface-management-22-626-2-cyberpion/?mkt_tok=NzgzLVRLTC01MzkAAAGLOSpHXq3K-r4ehxrfnjDZprs9n4W8OgtZhD2jaKFMQ7TmIrvRnVAr-oKN82iVJpASuQNhiSj9N0x3_Htb0FOhBC4dBPzVL-xvFq1ejzw

This GigaOm Research Reprint Expires: Feb 15, 2024

Gigaom

This GigaOm Research Reprint Expires: Feb 15, 2024

- Tweet
- Share
- Post

Chris Ray Feb 15, 2023 -- Market Radar

GigaOm Radar for Attack Surface Managementv2.01

Table of Contents

1. Summary

The difficulties and challenges presented by rapid digital growth, cloud adoption, and the sprawling public IP space leave organizations unable to accurately identify their rapidly changing attack surface, creating more opportunities for attackers. Compounding this problem is the lack of visibility into the risks resulting from the dynamic nature of the attack surface. Attack surface management (ASM) tools provide value through the continuous discovery of and insight into an organization's attack surface.

The attack surface encompasses all services, application programming interfaces (APIs), applications, IPs, and infrastructure, regardless of the host type (virtual machine or VM, container, or bare metal) or location (on-premises or cloud). ASM tooling builds a proper management process around the attack surface it identifies. This includes automated asset discovery and tracking asset details.

An organization's attack surface is dynamic; it can change daily, if not more often, and tracking these changes in an automated fashion is crucial for an ASM solution. But simply knowing the entirety and composition of the attack surface is not sufficient. Delineating the types of assets in an attack surface as well as the severity of the risks rounds out an ASM solution's value proposition.

ASM is a recent addition to an organization's defensive tool set, and like other new technologies, it's still evolving. As more vendors enter this space, they are compelled to innovate to differentiate from one another, so prospective buyers should keep in mind that the full potential of this space has yet to be realized.

This GigaOm Radar report highlights key ASM vendors and equips IT decision-makers with the information needed to select the best fit for their business and use case requirements. In the corresponding GigaOm report "Key Criteria for Evaluating Attack Surface Management Solutions," we describe in more detail the key features and metrics that are used to evaluate vendors in this market.

HOW TO READ THIS REPORT

This GigaOm report is one of a series of documents that helps IT organizations assess competing solutions in the context of well-defined features and criteria. For a fuller understanding, consider reviewing the following reports:

Key Criteria report: A detailed market sector analysis that assesses the impact that key product features and criteria have on top-line solution characteristics—such as scalability, performance, and TCO—that drive purchase decisions.

GigaOm Radar report: A forward-looking analysis that plots the relative value and progression of vendor solutions along multiple axes based on strategy and execution. The Radar report includes a breakdown of each vendor's offering in the sector.

Solution Profile: An in-depth vendor analysis that builds on the framework developed in the Key Criteria and Radar reports to assess a company's engagement within a technology sector. This analysis includes forward-looking guidance around both strategy and product.

2. Market Categories and Deployment Types

To better understand the market and vendor positioning (**Table 1**), we assess how well ASM solutions are positioned to serve specific market segments and deployment models.

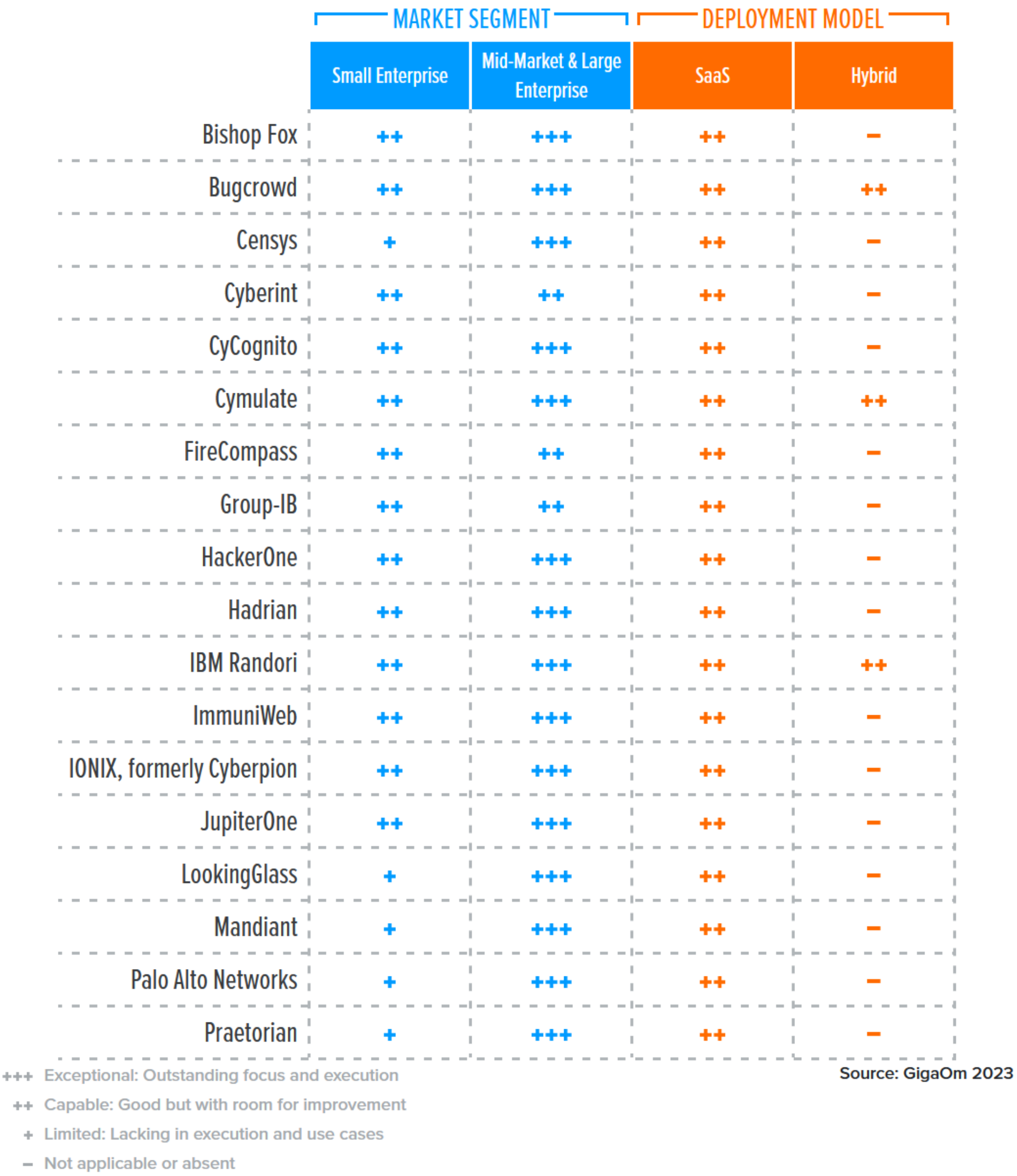
For this report, we recognize the following market segments:

- **Small enterprise:** In this category, we assess solutions on their ability to meet the needs of organizations ranging from small businesses to medium-sized companies. Solutions in this category provide simplified cost structures that make ASM achievable for small security budgets.
- **Mid-market and large enterprise:** Here, offerings are assessed on their ability to support large and business-critical projects. Optimal solutions in this category have a strong focus on flexibility, performance, data services, and features that improve security and data protection. Scalability is another big differentiator, as is the ability to deploy the same service in different environments.

In addition, we recognize two deployment models for solutions in this report:

- **Software as a service (SaaS)** These solutions are available only in the cloud. Often designed, deployed, and managed by the service provider, they are available only from that specific provider. Because the data collected during ASM operations is taken entirely from the attacker's perspective, ASM solutions do not have an on-premises, private cloud, or other required component.
- **Hybrid:** These solutions are still cloud-based like the cloud-only solutions above, but leverage a sensor, collector, or agent as an additional telemetry source or to create a better understanding of the composition of a client's technical environment.

Table 1. Vendor Positioning



	MARKET SEGMENT		DEPLOYMENT MODEL	
	Small Enterprise	Mid-Market & Large Enterprise	SaaS	Hybrid
Bishop Fox	++	+++	++	−
Bugcrowd	++	+++	++	++
Censys	+	+++	++	−
Cyberint	++	++	++	−
CyCognito	++	+++	++	−
Cymulate	++	+++	++	++
FireCompass	++	++	++	−
Group-IB	++	++	++	−
HackerOne	++	+++	++	−
Hadrian	++	+++	++	−
IBM Randori	++	+++	++	++
ImmuniWeb	++	+++	++	−
IONIX, formerly Cyberpion	++	+++	++	−
JupiterOne	++	+++	++	−
LookingGlass	+	+++	++	−
Mandiant	+	+++	++	−
Palo Alto Networks	+	+++	++	−
Praetorian	+	+++	++	−

+++ Exceptional: Outstanding focus and execution
++ Capable: Good but with room for improvement
+ Limited: Lacking in execution and use cases
− Not applicable or absent

Source: GigaOm 2023

3. Key Criteria Comparison

Building on the findings from the GigaOm report, "Key Criteria for Evaluating ASM Solutions," **Table 2** summarizes how each vendor included in this research performs in the areas we consider differentiating and critical in this sector. **Table 3** follows this summary with insight into each product's evaluation metrics—the top-line characteristics that define the impact each will have on the organization.

The objective is to give the reader a snapshot of the technical capabilities of available solutions, define the perimeter of the market landscape, and gauge the potential impact on the business.

Table 2. Key Criteria Comparison

	KEY CRITERIA					
	Flexibility in Asset Discovery	Active Assessment	Converged Protections	Internal ASM	Risk Scoring	Asset Categorization
Bishop Fox	+++	+++	++	–	+++	++
Bugcrowd	+++	+	+++	++	+++	++
Censys	++	–	++	–	+++	++
Cyberint	+++	++	+++	–	+++	++
CyCognito	+++	+++	++	–	+++	+++
Cymulate	++	+	+++	++	+++	++
FireCompass	++	+++	++	–	++	+++
Group-IB	++	++	+++	–	+++	+++
HackerOne	++	+	+++	–	++	++
Hadrian	+++	+++	++	–	+++	+
IBM Randori	++	++	+++	++	+++	+++
ImmuniWeb	+++	–	+++	–	+++	+++
IONIX, formerly Cyberpion	+++	+++	++	+	+++	++
JupiterOne	++	–	+++	++	+	+++
LookingGlass	+++	++	++	++	++	+++
Mandiant	+++	++	++	–	++	+++
Palo Alto Networks	+++	++	++	+++	++	+++
Praetorian	+++	++	+++	–	++	–

+++ Exceptional: Outstanding focus and execution

++ Capable: Good but with room for improvement

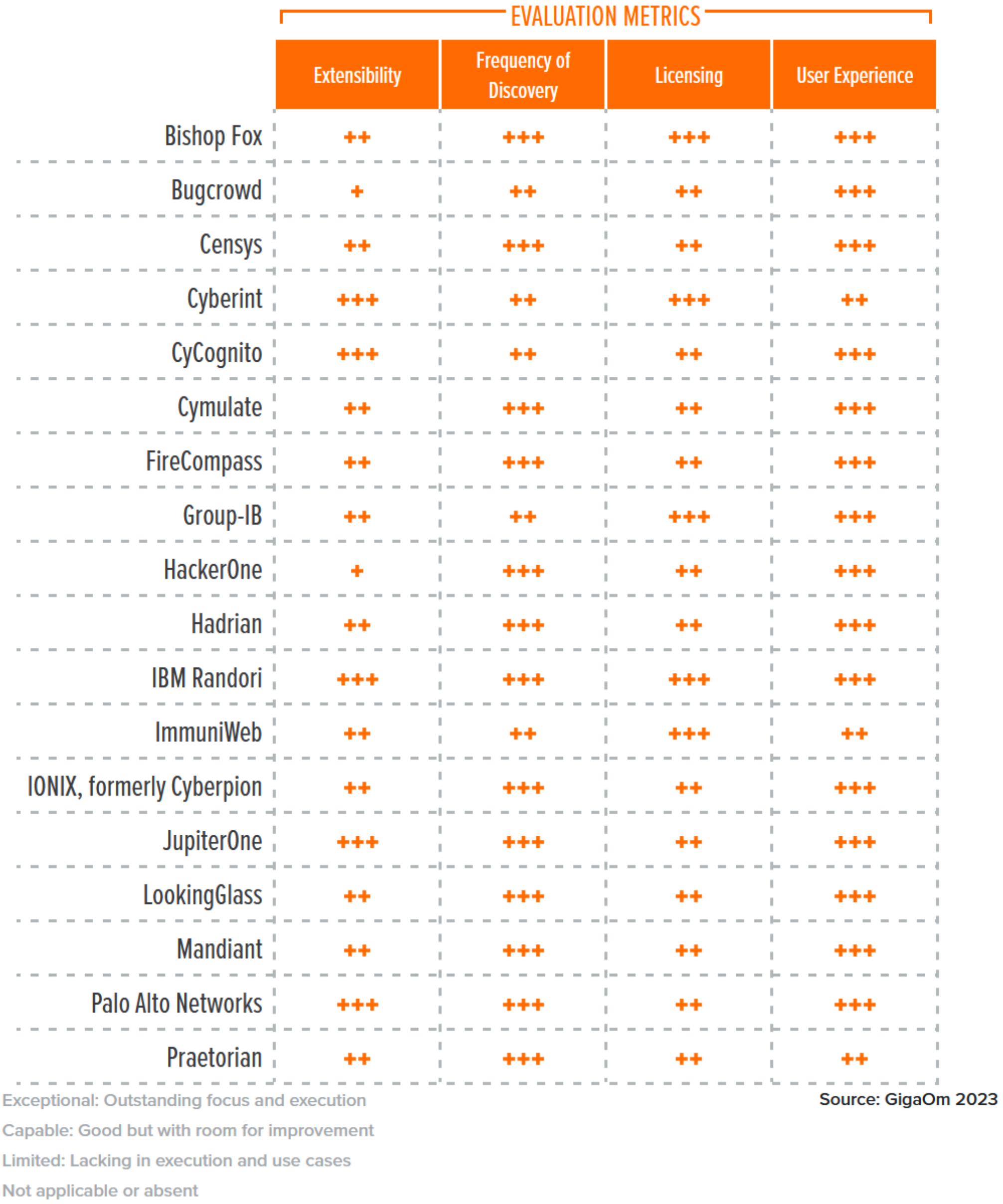
+ Limited: Lacking in execution and use cases

– Not applicable or absent

Source: GigaOm 2023

Table 3. Evaluation Metrics Comparison

Table 3. Evaluation Metrics Comparison



	EVALUATION METRICS			
	Extensibility	Frequency of Discovery	Licensing	User Experience
Bishop Fox	++	+++	+++	+++
Bugcrowd	+	++	++	+++
Censys	++	+++	++	+++
Cyberint	+++	++	+++	++
CyCognito	+++	++	++	+++
Cymulate	++	+++	++	+++
FireCompass	++	+++	++	+++
Group-IB	++	++	+++	+++
HackerOne	+	+++	++	+++
Hadrian	++	+++	++	+++
IBM Randori	+++	+++	+++	+++
ImmuniWeb	++	++	+++	++
IONIX, formerly Cyberpion	++	+++	++	+++
JupiterOne	+++	+++	++	+++
LookingGlass	++	+++	++	+++
Mandiant	++	+++	++	+++
Palo Alto Networks	+++	+++	++	+++
Praetorian	++	+++	++	++

+++ Exceptional: Outstanding focus and execution

++ Capable: Good but with room for improvement

+ Limited: Lacking in execution and use cases

– Not applicable or absent

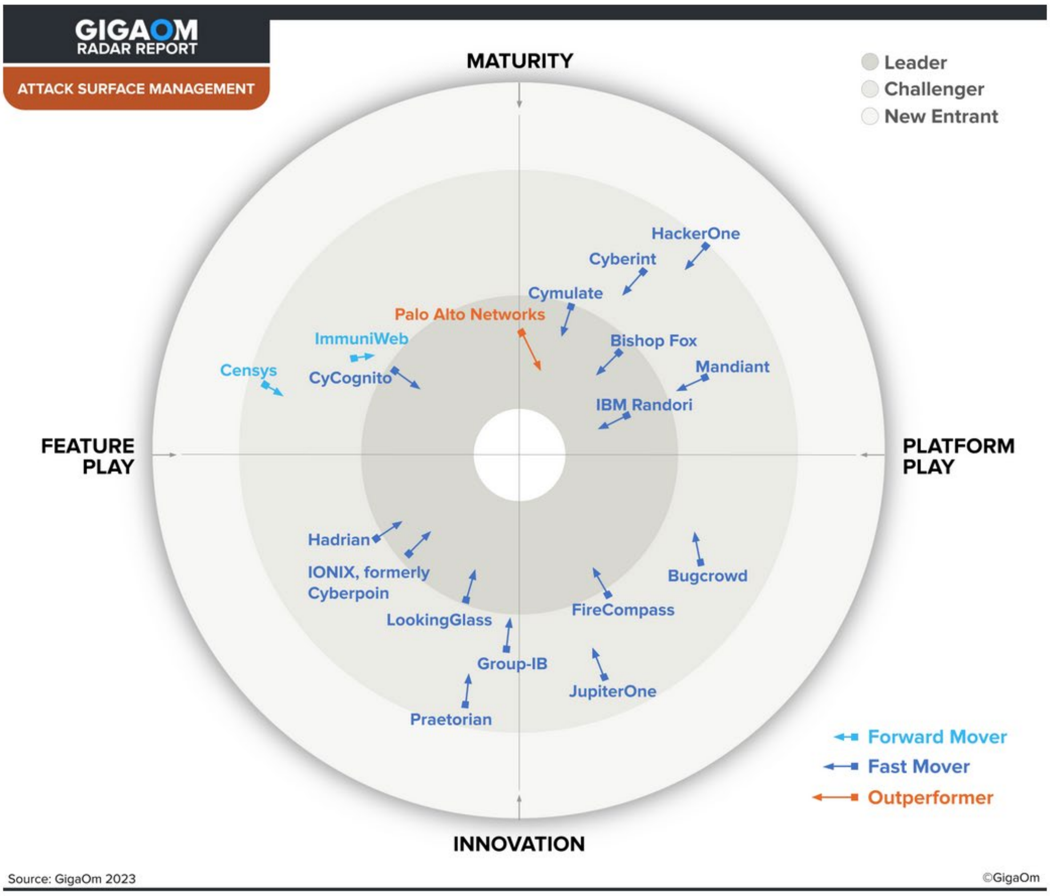
Source: GigaOm 2023

By combining the information provided in the tables above, the reader can develop a clear understanding of the technical solutions available in the market.

4. GigaOm Radar

This report synthesizes the analysis of key criteria and their impact on evaluation metrics to inform the GigaOm Radar graphic in **Figure 1**. The resulting chart is a forward-looking perspective on all the vendors in this report, based on their products' technical capabilities and feature sets.

The GigaOm Radar plots vendor solutions across a series of concentric rings, with those set closer to the center judged to be of higher overall value. The chart characterizes each vendor on two axes—balancing Maturity versus Innovation, and Feature Play versus Platform Play—while providing an arrow that projects each solution's evolution over the coming 12 to 18 months.



Source: GigaOm 2023

©GigaOm

Figure 1. GigaOm Radar for ASM

As you can see in the Radar chart in **Figure 1**, this is a very well-populated space that has experienced tremendous growth in the past 12 months. With vendors ranging from small startups to the largest technology companies entering through acquisitions, this is a diverse field offering numerous opportunities. The explosion of vendor participation is only one defining aspect of this market, though. Tother is the speed and depth of solution development. This space has seen some of the fastest expansion of features, rivaling that of any other security solution market.

Starting in the upper right Maturity/Platform Play quadrant of the Radar, Palo Alto Networks continues to build on an already capable feature set and delivers enhancements on top of its V1 solution. Cymulate offers a modular platform approach to ASM that simplifies adoption, while Bishop Fox continues its platform development and added several new features this year, earning a place in the Leaders ring. IBM's ASM offering, IBM Randori, is new to this report; it can be paired with IBM's strong red team services. Mandiant's ASM solution (by way of a Google acquisition) combines Mandiant's famous threat intelligence with its ASM. Cyberint offers a simplified experience for operators, as well as a digital risk protection (DRP) feature set, coupled with dark web monitoring capabilities, not yet common in the ASM space. HackerOne rounds out this Radar quadrant by layering a human-centric approach to ASM onto its scanner and integration capabilities.

Moving down into the Innovation/Platform Play quadrant, FireCompass's emphasis on adversary emulation and automated testing provides a simple risk verification and prioritization capability. Bugcrowd offers a split approach, one side leveraging humans and the other relying on programmatic discovery capabilities to create a hybrid ASM solution. JupiterOne, built atop graphQL technology, provides valuable context through simplified asset relation and asset vulnerability identification.

Moving to the left into the Innovation/Feature Play quadrant, LookingGlass has completed its acquisition and integration of the AlphaWave ASM solution and now offers a single user interface for its threat intelligence-enhanced ASM solution. IONIX, formerly Cyberpion, delivers a unique perspective on ASM with its extended coverage of external digital supply chain risks, integrations into open source intelligence sources and prioritization based on contextual awareness. Hadrian offers an event-based architecture that aims to unify all related ASM context and information into an intuitive experience for its customers. Group-IB, a long-time player in the threat intelligence market, delivers an ASM tool built to satisfy its own requirements for broad discovery and powerful attribution. Praetorian offers one of the only fully managed ASM solutions in the marketplace, powered by competent discovery and enumeration capabilities.

The Maturity/Feature Play quadrant holds three vendors. Cycognito, which deploys artificial intelligence (AI) technologies like natural language processing (NLP), provides enumeration and attribution capabilities uncommon in this space. ImmuniWeb's solution offers straightforward licensing and rapid results with minimal input, while Censys brings its ASM to market with very broad discovery capabilities and an emphasis on simplicity.

Inside the GigaOm Radar

The GigaOm Radar weighs each vendor's execution, roadmap, and ability to innovate to plot solutions along two axes, each set as opposing pairs. On the Y axis, **Maturity** recognizes solution stability, strength of ecosystem, and a conservative stance, while **Innovation** highlights technical innovation and a more aggressive approach. On the X axis, **Feature Play** connotes a narrow focus on niche or cutting-edge functionality, while **Platform Play** displays a broader platform focus and commitment to a comprehensive feature set.

The closer to center a solution sits, the better its execution and value, with top performers occupying the inner Leaders circle. The centermost circle is almost always empty, reserved for highly mature and consolidated markets that lack space for further innovation.

The GigaOm Radar offers a forward-looking assessment, plotting the current and projected position of each solution over a 12- to 18-month window. Arrows indicate travel based on strategy and pace of innovation, with vendors designated as Forward Movers, Fast Movers, or Outperformers based on their rate of progression.

Note that the Radar excludes vendor market share as a metric. The focus is on forward-looking analysis that emphasizes the value of innovation and differentiation over incumbent market position.

5. Vendor Insights

Bishop Fox

Founded in 2005, US-based Bishop Fox has spent most of its existence providing security services to much of the Fortune 100. In 2018, the company raised $25 million to develop its Cosmos platform, which combines technology, automation, and expert-driven testing to continuously identify and validate perimeter assets and exposures. In 2022, the company raised an additional $129 million in Series B funding.

The Cosmos solution's ability to continuously discover the diverse assets in an organization's attack surface is excellent, and it can inventory and provide attribution for those assets. Moreover, because Cosmos verifies discovery results using a blend of human-driven analyses and automation, the burden of verification is removed from its clients. Whenever asset ownership is in question, the Cosmos team works with the client to verify it. This verification process results in a continuous, accurate view of the attack surface.

Cosmos sets itself apart from the competition through its high-touch white-glove delivery methodology. For instance, while most ASM vendors use humans during the discovery phase of the ASM solution, Cosmos uses them throughout. Beyond discovery, Cosmos combines machine learning (ML) and automation with expert-driven testing to validate initial exploitability and post-exploitation business impact, and leverages an adversarial operations team during remediation planning. This human-in-the-loop process effectively delivers zero false positives (the company claims to never have delivered a false positive to a client). If this human element was considered important previously, it should now be viewed as critical for most organizations that are feeling the pain created by the tight labor market.

Once the risk has been identified and actively assessed, the Cosmos solution provides a step-by-step remediation plan and direct access to adversarial operations via built-in instant messaging that uses a familiar timeline-based presentation.

Asset categorization, by which logical rules are applied to similar assets to create groups, is a new feature that lets clients apply tags to assets. Each tag can have a unique set of associated workflows that determine how the asset is handled during various stages of the Cosmos identification, triage, and validation processes.

The Cosmos solution does not offer internal ASM capabilities, though it does have software development lifecycle (SDLC)-related ASM components slated for release in late 2023.

The Cosmos platform is API-first, meaning everything that can be performed or collected through the graphical user interface (GUI) can be achieved by leveraging the API. The RESTful API, which is public and fully documented, can facilitate integration with third-party solutions. Since the first version of this report, Bishop Fox has worked to expand the client-facing API and associated documentation to build additional extensibility into the solution.

Depending on the asset type, discovery is performed monthly, weekly, or daily. For instance, domains, which typically don't change often, are discovered monthly, while ephemeral assets which change frequently, like open ports or IPs in cloud services, are discovered daily.

The Cosmos platform is priced relative to the size of your attack surface. If the size of the surface isn't known, Bishop Fox performs a brief discovery to provide numbers to use in the sales conversation. While licensing based on asset count can be difficult for clients, the Bishop Fox solution applies a flexible approach so that minor fluctuations in asset counts will not result in increased costs.

Keep in mind that Cosmos is a bundled service (not just ASM). If your organization needs assistance verifying risks and creating remediation plans, this service will provide great value. On the other hand, if these are steps that you would prefer to leave in-house, the Cosmos platform is sold in a tiered model that lets organizations select the capabilities they desire.

Strengths: The Cosmos platform delivers broad, powerful discovery features that underpin all other capabilities. This solution uses a hybrid approach, combining humans with ML in all stages to deliver a unified, comprehensive ASM solution. Extensibility is good and the service is delivered with a white-glove approach that reduces in-house staff workloads.

Challenges: Internal ASM, which is new to the entire sector, is not a capability of this solution.

Bugcrowd

Bugcrowd is known for its crowd-sourced hacker community that delivers a range of red team services through its Bugcrowd Security Knowledge Platform, which includes bug bounty, penetration testing, and ASM. Bugcrowd's solution in this space is, of course, executed with a Bugcrowd twist. It features two ASM modules, one of which—Asset Risk—represents the crowd-sourced approach to ASM, adding a crowd-sourced element to the validation and risk assessment processes. It is powered by the trusted hacker community to perform reconnaissance and risk-based prioritization of security issues. The second module—Asset Inventory—is a software-based solution for continuous asset discovery and management. The combination of Asset Risk's human-led venture with Asset Inventory's software-led solution results in a hybrid approach that is uncommon in this space. This report is based on the capabilities of both modules, which are sold separately.

The asset discovery capabilities of the solution are derived from Bugcrowd's unconventional, yet highly effective, approach to ASM. Discovery is automated using the Asset Inventory module, crawls the internet and identifies assets programmatically while the Asset Risk module integrates human expertise to identify difficult-to-attribute assets.

Active assessment capabilities are part of the larger Bugcrowd Security Knowledge Platform, but they are not directly available from either the Asset Risk or Asset Inventory modules. With that said, if a customer chooses to engage Bugcrowd for bug bounty or pen testing services, assets found within the ASM solution can be sent directly into the bug bounty or pen testing programs.

This solution offers a converged approach to ASM with the broader capabilities of the Bugcrowd Security Knowledge Platform available through simple module purchases. Internal ASM is facilitated by the Asset Risk module which leverages crowd-enabled reconnaissance strategies for internal discovery.

The risk-scoring mechanism in the solution is unique in that it leverages the Bugcrowd AssetGraph, which contains data from over 1200 unique customer engagements. This data is applied to the information derived from the ASM solution to identify and prioritize security risks, delivering effective prioritization of efforts.

Asset categorization is achieved using tags, as is common in this space. Customers can create tags, allowing assets to be sorted and filtered based on matching tags.

The Bugcrowd ASM solution is all-inclusive, with additional features easily integrated from the Bugcrowd Security Knowledge Platform. Its extensibility outside of this ecosystem is limited but asset discovery is performed continuously.

The two modules covered in this report have different licensing modes, mainly reflecting their differing functionality. Asset Risk is licensed on a per engagement basis while Asset Inventory is sold in a tiered model according to the number of assets.

Strengths: Bugcrowd's highly converged, hybrid approach to ASM blends human-expertise from its pool of hackers with a programmatic approach to continuous discovery. This solution also includes features for internal ASM, simple risk-based prioritization of security issues, and a flexible licensing model.

Challenges: This solution's extensibility is limited and active assessment capabilities are unavailable in either of its ASM modules.

Censys

Founded in Michigan, US in 2017, Censys initially launched with service reminiscent of Shodan. It perpetually scanned the internet, identifying assets, services, and secure sockets layer (SSL) connections. Shortly after launch, Censys found the optimum use case for its technology: ASM.

The Censys ASM solution offers a very comprehensive and robust discovery capability (though no active assessment capability). The discovery algorithm that searches the internet is completely automated from beginning to end; unlike many other vendors in this space, it does not integrate a human-in-the-loop during some aspect of the discovery process. Regardless, the output of the Censys discovery process is very thorough and has extremely low false positives.

Censys defines anything that could present or create a risk to an organization as an asset. This includes common objects like servers, load balancers, applications, and services, and some less-common things like login screens and S3 buckets. This definition allows Censys to provide a more granular risk assessment. This granularity plays into its risk scoring method, which leverages default severity rankings (like High or Critical) that can be customized by users if desired. While this is a good feature, some other vendors in this space are able to integrate metadata or contextual information that provides an even clearer picture of the risk, thus allowing for easier prioritization of work.

However, the information given to practitioners when reviewing risks is an important benefit. While some vendors state a risk and assign priority, Censys ventures to provide remediation steps (both primary and secondary) for every risk found on an attack surface. This practical guidance offers a dramatic reduction in time to remediate. Additionally, it highlights the evidence that was used to detect the risk, providing valuable context around risk.

Censys goes to extraordinary lengths to ensure false positivity rates are kept low. For example, before a new feature is added to the ASM solution, Censys performs thorough tests, measuring the feature's impact on the false positive rate. If clients find a false positive, they can remove it from the portal or API, where it's still tracked but not included in reporting or visuals. Asset categorization is made possible through the creation of custom categories that allow assets to be sorted by a number of different vectors including region, environment, and cloud provider.

Strengths: This solution delivers high-quality discovery, easily understood asset attribution, and a very low false-positive rate. Additionally, it provides a good value, is highly extensible with a fully documented API, and offers some out-of-the-box integrations.

Challenges: This solution lacks active assessment capabilities and its risk scoring doesn't integrate context or other data to prioritize risks.

Cyberint

Founded in Israel in 2010, Cyberint offers its ASM flagship service, which is part of the Argos Edge platform. The ASM solution is integrated with other services like DRP and threat intelligence that together deliver a very comprehensive understanding of a customer's entire digital footprint and its associated risk.

Argos Edge can leverage as little as a single piece of organizational data (like the company's primary URL) to start the discovery process. While some vendors use an industry-standard discovery infrastructure like Shodan, Cyberint has developed its own discovery infrastructure, which scans more frequently, offering greater detail about and faster discovery of the often-changing attack surface.

The strong ASM capabilities of Argos Edge are matched by its equally capable digital risk protection features, which enable a unified view into common attack surface assets, like IP addresses, domains, and certificates as well as phishing websites, fraudulent social media, and even information from the dark web. If customers decide to act on fraudulent social media or websites, they are able to leverage Argos Edge's automated takedown functionality, which is a unique feature of the solution.

Additionally, its visibility into various deep and dark web sources allows Argos to detect unique threats to company assets, such as leaked access tokens to certain domains (whether sold on the dark web, or accidentally shared over source code repositories or paste sites), or brute forcing tools configured to attack a certain URL for sale in the dark web. This detection could lead to immediate risk reduction actions such as replacing access tokens.

Active assessments provide the greatest level of certainty when determining the risk presented by an issue. Argos Edge executes both passive and active assessments, which are performed by Argos security professionals to ensure accuracy while minimizing potential harm during the assessment process. Assessment risk is further detailed as common vulnerabilities and exposures (CVEs) associated with detected assets receive a dynamic threat score, based on the industry standard common vulnerability scoring system (CVSS) and on dark web activity which can detect exploits becoming available in real time, for potential attackers.

Internal ASM features are not built into this solution, but it does offer a related capability—the output of the DRP process can identify at-risk internal assets (based on information from dark web sources).

False positives are managed effectively by AI during the discovery phase, which results in a simplified onboarding process for clients. As with any vendor, though, false positives are possible and should be investigated. Asset categorization is another crucial component of ASM solutions, and Argos Edge allows customers to add and create labels for assets that allow them to be categorized by any attribute.

Cyberint deviates from the norm in the way it licenses its product. Rather than basing the cost on either a flat fee per organization or on the number of assets, Cyberint maps the entire asset inventory, yet allows clients the flexibility to exclude specific assets from the licensing. This option could be useful for large organizations in which each team or department is responsible for its own security operations and budget. The ability to determine the scope of the ASM practice is a feature that’s unique to this solution.

Strengths: Argos Edge offers a simplified user experience, DRP capabilities that illuminate otherwise dark portions of the attack surface, human-led active assessments for great accuracy, good asset categorization features, and adjustable licensing.

Challenges: The internal ASM capabilities are not very robust.

CyCognito

Founded in 2017 in California, US, CyCognito has roots in the famed Israeli IDF 8200 (cyber operations) unit. Starting with a seed round of funding in 2018, CyCognito grew rapidly in the ASM space.

Unknown or under-managed internet-facing assets are common vectors that attackers use to gain entry into an organization, and CyCognito approaches the attack surface the same way an attacker approaches an organization. Starting with a piece of seed data about the organization, CyCognito leverages ML and NLP to create a comprehensive understanding of the attack surface. NLP plays a special role in the discovery process, unique to CyCognito, which is how this solution classifies assets accurately at speed and scale.

A significant change from the previous CyCognitio ASM solution is the introduction of the Org Graph, a visual model built using ML Bayesian models. This tool provides clients with a high-confidence understanding of their assets found within the attack surface.

The addition of Exploit Intelligence, a clever feature that merges threat intelligence with bespoke data gathered from the customer’s attack surface, takes prioritization to the next level. With the Exploit Intelligence module, customers are able to get accurate information specific to their environment to enable better decision-making.

CyCognito has focused heavily on automating processes and this continues into the assessment phase of the ASM process. The CyCognito dynamic application security testing

(DAST) service looks at exposed applications, injection vulnerabilities, misconfigurations, and default credentials while the vulnerability scanning engine focuses on identifying missing patches, exposed (sensitive) data, services, and cryptographic issues.

Asset categorization leverages NLP to automatically categorize assets found within the attack surface, and the solution then adds metadata such as platform type, geolocation, and organizational ownership to accurately identify and attribute assets to specific categories. These categories can then be used to influence the visualization of attack surface data as well as to narrow the scope of reporting.

Internal ASM is a new area for this space, and while most vendors have opted not to provide this capability, CyCognito has developed an introductory feature that can integrate with internal vulnerability management solutions so that internal attack surface information can be considered in the broader context with the external attack surface.

CyCognito leverages organizational business mapping capabilities, automated asset classifications, and enumerated vulnerabilities to develop a risk score that includes a confidence level, a potential impact level, and a business importance level. The result is a scorecard for each vulnerability that simplifies and accelerates risk assessment. This level of detail is not common for ASM solutions and so is a stand-out feature.

This solution is packaged into different capability tiers, with successive tiers providing more extensive testing and analysis capabilities aligned with the maturity of an organization's ASM strategy. As is typical in this space, customers often don't know the size or composition of their attack surface. For this reason, CyCognito will run an initial discovery during the sales process to accurately determine the asset count, which is how licensing costs are determined.

Strengths: This solution delivers comprehensive discovery capabilities, thoughtful risk scoring, and prioritization insights powered by practical ML, NLP, and automation capabilities. Enhanced with the Org Graph visualization engine and Exploit Intelligence, the solution demonstrates a commitment to evolving the ASM space.

Challenges: CyCognito's internal ASM capabilities are limited.

Cymulate

Founded in Tel Aviv, Israel in 2016, Cymulate offers a platform-based approach to ASM. This broad portfolio of solutions is derived from the company's goal of providing any organization, regardless of size or maturity, the ability to manage its own security posture. Security posture management is a comprehensive approach that considers information and data from all available sources and then identifies risks and areas for improvement. Cymulate is attractive to businesses of all sizes with modular internal and external ASM and breach and attack simulation (BAS). This solution helps fill gaps left by the skills shortage and employment challenges in today's organizations.

The Cymulate platform consists of several modules, each with a specific set of capabilities designed to achieve one goal. The base module that is the topic of this report is the ASM component, and other modules or capabilities can be easily stacked on top, though these come with an additional cost. Note also that while the base ASM module requires only a URL to start the discovery process, other modules may require an agent to be deployed to a handful of representative servers in the organization to gather the required information.

Asset categorization is achieved through the concept of an environment. Each environment can be created and defined by the customer and can be based on geography, business unit, functionality, or other parameters. This logical grouping can be selected from a drop-down menu to limit the view to only those assets that are in scope for the security activities at hand.

Risk scoring is based on the MITRE ATT&CK Framework, NIST 800-50 Special Publication, CVSS v3, and Microsoft's DREAD Framework. It also provides an attack-based vulnerability management score (ABVM). ABVM takes the attacker's view of the threats identified through the solution and scores them according to the perceived risk based on what would likely happen during a real attack. In this way, the Cymulate's risk scoring provides a better understanding of risks and allows security teams to prioritize efforts accordingly.

While the solution can directly integrate or interact with tools for actively assessing identified vulnerabilities, it doesn't have any active assessment capability.

A truly stand-out feature of this solution is its internal ASM capabilities, which can be enabled through the deployment of a small agent. Using the foothold agent (this term references the initial state after an attacker has breached a victim's perimeter and is starting to pivot internally) installed on a handful of customer machines, Cymulate is able to perform comprehensive yet safe security testing of internal assets. The information thus gained is combined with external ASM data to provide customers with a clearer picture of real risk.

Attack surface assets can be grouped into predefined categories that include domain, IP, port, web application type, known vulnerable code, web services, and email services. This level of sorting is adequate for most customers but may fall short for customers who need custom categorization capabilities for internal processes.

Strengths: This solution brings several powerful features into play, including internal ASM capabilities, ABVM, and easy integration with other Cymulate modules. Combined, these solutions deliver simplified and comprehensive insights into the attack surface.

Challenges: Active assessment capabilities are not built into the solution, and its asset categorization methods are not customizable.

FireCompass

Founded in 2019, FireCompass is a SaaS platform for continuous automated red teaming (CART) and ASM. A core practice of the FireCompass ASM solution is continuous discovery and testing.

Starting with the usual seed information, FireCompass uses its scanning infrastructure to discover an organization's attack surface continuously. It leverages common sources, such as the internet and open source intelligence tools (OSINT) sources from the deep web and dark web, and uses playbooks to identify and remove false positives during its discovery process. The playbooks number in the thousands, and if a particular playbook does not exist, customers can create their own.

Note that FireCompass' CART is very tightly integrated with the ASM solution. If purchased, CART enables true attacker behavior emulation and multiple-stage attack emulation. The results of these emulations are then used by the ASM solution to further enhance the ASM process. Alone, the ASM solution provides both passive and active assessment capabilities, but no internal ASM capabilities.

FireCompass focused on building out its extensive library of playbooks and the CART integration, but its risk scoring capabilities are also notable. For example, CVSS scores are the starting point for analysis (as they should be). The proprietary risk scoring algorithm then integrates additional context from various sources, such as the priority of the asset, the weakness of the vulnerability, and the likelihood of exploitation. The end result is a risk score that is easy to digest and actionable.

FireCompass provides out-of-the-box integrations with other tech stacks, like vulnerability scanners, Amazon Web Services AWS, and Microsoft Azure. For integrations that don't yet have an out-of-the-box solution, the FireCompass API is fully documented to meet those requirements. This documentation demonstrates moderate to advanced levels of extensibility. The solution is sold by asset count, a common licensing model in the ASM space.

Finally, a novel function that's not found with other vendors, but solves a common challenge, is how FireCompass integrates with threat intelligence feeds. Threat intelligence is a critical component of an organization's security program. However, most threat feeds are consumed manually, or it's left up to vendors to figure out how to use integrations best. FireCompass, in contrast, offers the ability to integrate threat feeds into its playbooks, then the playbooks that impact your assets are selected and run automatically. This approach delivers a timely and accurate assessment of organizational risk found in the attack surface by leveraging up-to-date threat intelligence.

Strengths: The FireCompass ASM solution has a powerful discovery capability matched with passive, active, and multiple-stage risk-validation methodologies. Those, together with a common-sense approach to risk scoring, make FireCompass easy to use as it delivers actionable guidance.

Challenges: There are no internal ASM features.

Group-IB

Founded in Moscow, Russia in 2003 and later relocated to Singapore to ensure an adequate level of independence could be maintained, Group-IB is a cybersecurity and digital forensics company that specializes in the prevention and investigation of cybersecurity events. Group-IB's stated mission is to make sure security incidents simply don't happen.

Group-IB's arrival in the ASM space is a result of its threat intelligence business requiring the collecting of data that wasn't commercially available. This drove Group-IB to develop its own search and discovery capabilities as a means of gathering intelligence about the broader internet landscape, and these capabilities evolved into its ASM solution.

This solution's discovery capabilities provide broad discovery outcomes, meeting or exceeding the standard set by competitors. In the near future, domain squatting identification and API endpoint discovery will be integrated as well.

Active discovery starts with passive reconnaissance, as is common in this space, then applies additional vulnerability scanning and active discovery methods to identify the more difficult to find security risks.

Group-IB's extensive experience in threat intelligence, incident response, and managed detection enables it to provide a simple bridge to acquiring a converged ASM solution that can be combined with DRP, bespoke red teaming, pen testing, and even a managed extended detection and response (mXDR) solution. This level of convergence is above standard for the space.

However, although it offers a powerful discovery and assessment feature for the external attack surface, this solution does not offer internal ASM features.

Risk scoring is a critical component when evaluating an ASM solution's suitability for an organization. This solution provides a transparent system for identification of assets, security checks, and supporting evidence. Although customers are not currently able to adjust the risk scoring mechanics, seeing how the risk score is arrived at is nearly as useful.

Asset categorization can be tremendously useful for organizations, both large and small. For small organizations, being able to quickly distinguish production from development can greatly improve the understanding of risks. For larger organizations, being able to accurately assign assets to specific teams or groups based on a tagging system streamlines many workflows. This solution offers both manual and automated tagging of assets with customer-created tags.

This solution provides a very intuitive interface that delivers a simple user experience. Licensing is flexible, and this is one of the few solutions that is channel friendly, meaning value added resellers (VARs) or managed service providers (MSPs) can easily offer this technology in their portfolio of services. There are no operator seat limits or API rate limits, and pricing is accessible and transparent.

Strengths: This solution offers powerful discovery and risk identification, coupled with a simple-to-use operator interface and a clear focus on delivering real risk reduction. This solution is also one of the few that offers channel-friendly licensing and an easily understood risk-scoring mechanism.

Challenges: This solution doesn't offer internal ASM features or API discovery capabilities.

HackerOne

HackerOne is a cybersecurity platform that employs a large pool of white-hat hackers and is known for its bug bounty and PTaaS practices. HackerOne has naturally grown into adjacent spaces such as ASM, with the same goal as its other services have—to help organizations identify and fix vulnerabilities before they can be exploited by malicious actors.

Its ASM solution—HackerOne Assets—is the cornerstone of HackerOne's Attack Resistance Platform. HackerOne Assets combines ASM capabilities with human security expertise for an exceptional understanding of the customer's attack surface.

The licensing model for HackerOne Assets is based on the customer's asset count. To obtain an accurate count, HackerOne performs a preliminary scan during the sales cycle, which also allows the company to provide an accurate proof of value. Additional HackerOne services, such as pentesting, bug bounties, and security services, can be layered on top of Assets.

Discovery is performed by both human experts and an ML-based scanning process. This approach is designed to ensure broad discovery capabilities that can find hidden or difficult to track assets, while also reducing false positives. Because the discovery process focuses on domain names, some assets (like IP addresses or DNS information that other ASM solutions leverage) are not included at the time of publishing. By April 2023, coverage for IP address and DNS asset types will be available in the scanner as well as by white-hat hacker submission. HackerOne Assets can integrate and combine scan and static asset data from any source via its OpenASM initiative for risk ranking and testing. Internal ASM capabilities are not included with this solution.

Active assessment is provided by way of additional HackerOne products like Bounty, Response, or Pentest. On its own, the ASM solution does not have an active assessment capability. However, for existing HackerOne customers who are not yet ASM customers this drawback won't be an issue.

The HackerOne platform is a good example of how ASM and adjacent technologies are being thoughtfully converged to deliver a holistic view of customer attack surfaces. The Assets product, when combined with other components of the HackerOne platform, can create a complete end-to-end solution not easily replicated with other solutions in this space.

Risk scoring is achieved via two avenues. First, risk rankings are the result of combined automated scanning and human expert analysis. Second, risk scores are derived from the automated scanning alone, without the expert analysis. Asset categorization is performed using customer-created tags that can be applied to assets to filter, sort, and group them per organizational needs.

Strengths: The HackerOne Attack Resistance Platform provides converged security solutions that can deliver an attacker's understanding of customer attack surfaces like no other solution.

Challenges: This solution's discovery capability is somewhat limited compared to others in the space, and active assessments are not built in but are available through add-ons.

Hadrian

Founded in 2021 by two long-time members of the red team community, Hadrian.io is a newcomer to ASM. It offers a single product that focuses on making organizations harder to hack using ML and automation to discover, inventory, and monitor assets, and subsequently manage an organization's attack surface.

Hadrian licenses its product based on the number of assets, with tiers that decrease the cost per asset as the customer's attack surface grows. Because many organizations don't actually know the true size of their attack surface, Hadrian performs an initial discovery during the sales process to determine the asset count.

Hadrian approaches the ASM space with a unique take on the problem created by massive data sets inherent in this space. The solution is designed around an event-based architecture, which is powered by automation that takes note whenever a change is detected in the attack surface, resulting in rapid, comprehensive discovery of the attack surface. This also allows Hadrian to continuously monitor the attack surface, unlike some other solutions in this space that perform only periodic scans.

Active assessment capabilities are a strength for this solution. Leveraging its event-driven architecture, active assessment (using probes) is triggered as candidate vulnerabilities are detected. As probe results are returned to the solution, this can build confidence in the identification and classification of the vulnerabilities or trigger additional probes to gather more information.

Hadrian's solution does not offer internal ASM capabilities, although it's expected that this capability will be generally available in early 2023. The internal ASM capability will be driven by a cloud connector for AWS, Azure, and Google Cloud. Asset tagging is currently weak, but the solution will soon have the ability to tag assets based on customer-defined tags, which will allow customers to filter, sort, and group assets.

Risk scoring within the Hadrian solution is a result of the information gathered by probes. Because risk scores are based on the results of tests, the scores do a better job of reflecting real risk compared to legacy fingerprinting methods employed by vulnerability scanners. The company states, "Hadrian's ethical hacker team performs manual testing for newly implemented modules to ensure their quality and minimize the number of false positives delivered to customers."

As noted earlier, ASM must deal with massive amounts of data, which is why organizations find these solutions attractive. The Hadrian solution uses a novel visualization method called the Attack Surface Graph, which assists customers in better understanding their attack surface. The graph is a dynamically updated, interactive visual map that can accelerate a user's understanding of asset relationships, asset attribution, and the overall state of the attack surface.

As a final note, for managed security service providers (MSSPs) that are looking to add ASM to their portfolio of services, Hadrian offers the ability to easily manage multiple clients from a single UI.

Strengths: Hadrian's event-driven architecture, employment of ML, and its human-in-the-loop expertise provide an effective approach to ASM. It delivers rapid, comprehensive discovery of the attack surface with actionable risk scores assigned to every security issue. The Attack Surface Graph also provides a visual representation of the attack surface, which makes it more comprehensible.

Challenges: This solution does not offer internal ASM nor does it currently provide a method for grouping assets.

IBM Randori

Founded in 2018, Randori was a provider of ASM and other cybersecurity initiatives until its recent acquisition by IBM. Initially, Randori built a CART solution, an essential feature of which was its ability to discover and enumerate customers' external assets. These robust and comprehensive discovery capabilities became the ASM solution known as Recon. In 2022, IBM acquired Randori to bolster its offensive security capabilities.

Like other ASM solutions, discovery starts with a single piece of organizational information, like a URL or an email address, which enables the solution to define the external attack surface using a variety of protocols to gather information, which it calls artifacts. These artifacts are then used to match security events like vulnerabilities to customer assets.

The Recon solution has broad and robust passive and active scanning capabilities. For passive scanning, numerous public repositories—including ARIN, Clearbit, Crunchbase, Zetalycis, and WHOIS lookups—are queried to build a profile of an organization. Active assessment then performs interactive information gathering on assets, using techniques like running DirBuster on identified directories, attempting telnet and secure shell (SSH) to common ports, and scraping when detections occur.

Recon's ability to integrate with other security tooling is a strength. It includes native bi-directional integrations with many popular tools as well as an open API customers can use to develop bespoke integrations.

While this report focuses on Recon, it's important to identify the relationship between Recon and its adversary-focused counterpart called Attack. Customers can subscribe to both Recon and Attack, which provides numerous benefits but most notably (for this report) it enables the solution to perform internal ASM in the event an external vulnerability allows the Randori Attack team internal access to the customer environment. Without Attack, the solution has no native internal ASM capability.

A notable feature of Recon is its method of risk scoring. The Randori team has developed a novel approach to measuring and understanding risk scores, which it calls the "target temptation score." This score uses common vulnerability information like CVE data, and also goes a step further and takes into account other factors such as an asset's unique characteristics and value to the business to arrive at a final score meant to help customers prioritize their limited remediation cycles. This capability is ultimately what ASM tools set out to achieve, but often fall short of delivering.

Asset categorization is a largely automated process, leveraging Recon's ability to identify asset characteristics and then sort based on these characteristics. Customers can tag assets automatically by policy or they can do it manually.

Recon is the only ASM solution included in this report that bases its ASM licensing on the number of employees in each organization (not to be confused with the number of operators of the Randori ASM solution). This method of cost calculation might be the most straightforward to date.

Strengths: Recon offers effective discovery capabilities along with good active and passive assessment features. The target temptation score simplifies understanding the information produced by Recon, and asset categorization can be entirely automated or performed manually, which is a nice touch.

Challenges: Without the additional Attack solution, Recon does not offer internal ASM.

ImmuniWeb

Based in Geneva, Switzerland, ImmuniWeb is an application security service provider that offers a suite of services focused on securing an organization's internet-facing components. The SaaS ImmuniWeb Discovery delivers the ASM solution. Discovery is a part of the ImmuniWeb AI Platform, where all work is performed and the operator portal is accessed.

The solution offers effortless setup; all that is needed is your organization's name. The rest is handled by the ImmuniWeb ML algorithm with assistance from the vendor's analysts as needed. The initial setup and discovery are not instantaneous as it does take a few days for your dashboard to become available in your portal.

It's important to understand that the discovery portion of this service is performed in the same manner an attacker would discover your assets. The solution leverages multiple OSINT and data from the dark web to build a comprehensive view of an organization's internet-facing assets. ImmuniWeb's capabilities are broad, extending to finding assets hosted on-premises and across infrastructure as a service (IaaS), platform as a service (PaaS), and SaaS. This includes the ability to discover data in locations like Github, Docker hub, and content versioning systems (CVSs).

The solution combines several external attack surface and digital reputation protections into one converged platform that includes the ASM capabilities along with digital brand protection, cyber threat intelligence (CTI), and dark web monitoring. The digital brand protection capability enables a client's social media platforms to be monitored continuously for fraudulent accounts, while CTI and dark web monitoring provide special sources of threat intelligence that when combined with ASM features create a state of situational awareness that can be difficult to achieve otherwise.

The risk customization workflow is simple and intuitive and enables users to tune risk scores to their existing security controls (like the existence of a web application filter) or their risk appetites. New this year is the solution's automated asset classification capability, which streamlines triage and reduces noise by isolating alerts to only the individuals that need to receive them.

With ImmuniWeb Discovery, organizations get unlimited asset tracking and discovery capability for a flat monthly fee of $2,000. ImmuniWeb clients have unlimited access to its security analysts to assist with findings in the Discovery platform.

Strengths: ImmuniWeb is very easy to set up and customize, and provides a growing feature set and capabilities list. It combines several in-demand features like ML-driven analysis, digital brand protection, cyber threat intelligence, and dark web monitoring to create a simple and effective ASM solution.

Challenges: The solution does not perform active assessment of vulnerabilities, although other SaaS services offered by ImmuniWeb can perform this if needed.

IONIX, formerly Cyberpion

Based in Tel Aviv, Israel, IONIX's ASM solution aims to provide total visibility of and rich contextual information regarding customer attack surfaces and connected digital supply chains. This ASM solution is sold using a three-tiered model, with each tier providing a distinct level of service and a different associated discovery frequency (monthly, weekly, or daily).

This solution's discovery capabilities are both broad and deep due to its integrations with open source intelligence solutions, ML asset attribution (minimizing false positives), and extension across connected digital supply chains. Attack surfaces consist of many different asset types, each requiring a different method to discover and validate them. This solution applies appropriate discovery and validation techniques according to the asset type to achieve a low false positive discovery result while also ensuring a comprehensive view of the attack surface.

Active assessments are applied to all confirmed assets, including organizational assets and external directly connected assets that may involve a third party and even a fourth or fifth level of exposure. This capability stems in part from the emphasis IONIX has placed on understanding and identifying risks produced by customer supply chains. The type of assets that receive active assessments varies, but includes networks, web applications, email servers, DNS, certificates, TLS protocols, mobile, and public cloud assets.

IONIX has identified the adjacencies that exist between ASM and DRP and offers DRP capabilities within its ASM solution by way of an official partnership agreement with a leading DRP solution provider. This converged solution couples ASM data with DRP data, such as that from brand protection and social media monitoring, executive identity protections, and dark web monitoring. The result is a more accurate understanding of the attack surface and the attacker's view of an organization. A partnership with a penetration testing as a service (PTaas) provider is underway.

Internal ASM capabilities are limited to discoverable data provided via links to public cloud providers. This information includes assets the organization has deployed in its cloud, which can be used to identify potential misconfigurations. Additional internal ASM capabilities are on the roadmap.

Risk scoring is delivered through a global organizational risk score that is composed of numerous asset categories (such as network, cloud, DNS, PKI, web, email, and hijacked assets). For each asset category's score, the solution will show the user which items are negatively impacting the score and what actions need to be taken to resolve those issues. In this way, the customer is able to quickly identify the highest-risk issues and prioritize their remediation efforts around them.

Integrated workflows with leading ticketing, security information and event management (SIEM), and security orchestration, automation, and response (SOAR) solutions using clear playbooks with action items, evidence, and impact accelerate remediation. The solution automates mitigation for certain immediately exploitable risks.

Asset categorization is achieved by sorting the various asset types and aligning them with subsidiaries, business units, and the personas that match the customer's management needs. Customers are able to create custom groups based on logic they define, and assets can be automatically sorted based on these definitions.

Strengths: This solution provides an end-to-end ASM solution that discovers broadly, identifies high-priority security issues and risky connections to external assets easily, applies automatic mitigation for specific exploitable risks, and offers converged DRP and soon PTaaS capabilities.

Challenges: The solution's internal ASM capabilities are just starting to appear with additional development expected.

JupiterOne

Founded in 2018, JupiterOne set out to design a solution set that helps organizations manage their cloud-based infrastructure, with the goal of simplifying the process and automating as much as possible. JupiterOne empowers security teams to assess and manage their attack surface through continuous monitoring and correlation of the attack surface and the information obtained from it. This solution is built atop a graph data model, sometimes referred to as a graph database, which enables it to analyze how assets are related to each other. It also displays the connections as an interactive graph that customers can navigate to easily identify security event root causes.

An ASM solution's ability to adapt to the ever-changing attack surface composition is critical for the success of a security program. This solution's ability to discover, track, and identify the varied components of an attack surface is quite strong. Discovery frequency is configurable by the customer, without an additional cost. This frequency can range from 30 minutes to once a week with several stops in between. Discovered assets are cataloged so that when data is ingested in the future, relationships can be identified and recorded.

Validating findings through active (rather than passive) assessment provides a higher level of confidence regarding vulnerability data. While this solution doesn't offer active assessment, it undertakes other measures to build up to the confidence level that customers require. This includes automatic correlation of all assets, identification of vulnerabilities on those assets through passive means, identification of critical assets, collection of evidence for automated compliance assessments, and then updating dashboard and reports accordingly.

The JupiterOne platform is a convergence of several previously separate capabilities, beyond just ASM. This includes cloud security posture management (CSPM) and vulnerability management features, as well as broad coverage of identity-related risks that some ASM solutions are unable to include in scope.

Risk scoring is a weak spot for this solution, though this isn't uncommon in the space. While a risk score isn't calculated and no analysis of risk occurs that can deliver a single number to the customer, risks are identified and triaged and then prioritized based on data gathered from the ASM activities.

Internal ASM occurs via API connections to customer environments. JupiterOne comes with built-in integrations for a growing list of on-premises solutions including Microsoft Active Directory, VMware vSphere, Kubernetes Native, Jira Data Center, GitHub Enterprise, and Jenkins. In addition, through integrations with device management and endpoint security solutions, JupiterOne gains access to on-premises devices to provide visibility across the enterprise.

Asset categorization is a key strength of this solution, with close to 100 out-of-the box asset categories. This delivers rich context that can be combined with other ASM data to answer questions that are typically found only with humans in the loop. For example, discovering who can access sensitive information found inside of storage objects (like an S3 bucket) can be achieved using the simple and intuitive JupiterOne Query Language.

JupiterOne's tiered licensing model offers free, freemium, and enterprise levels. While a few vendors offer either a free or freemium model, no others offer both. This can be a great way for prospective customers to test the waters if they're unsure of what they can get from ASM.

Strengths: This solution delivers a mature ASM feature set converged with other security technologies like CSPM and vulnerability management. The JupiterOne Query Language is simple and intuitive and allows customers to quickly find the answers they need. The reporting and visualization capabilities are quite strong. The free and freemium tiers make getting into ASM easy for almost any organization.

Challenges: This solution doesn't have active assessment capabilities, and its risk scoring capability is limited.

LookingGlass

Founded in 2019 in the US, AlphaWave ASM was acquired by LookingGlass Cyber Solutions during the summer of 2021. LookingGlass is a threat intelligence vendor that produces unique threat intelligence sources. After the acquisition, the solution was rebranded as scoutINSPECT and it boasts a number of new capabilities.

Starting with the usual seed, an organization's name or URL, LookingGlass leverages ML and human analysis to sift through both open sources of intelligence and passive reconnaissance data to map out the attack surface. Of note is the depth to which scoutINSPECT goes to discover web services—generally a layer deeper into the web stacks than other ASM vendors do.

scoutINSPECT also offers a unique capability in the discovery phase. Simple integration with AWS, Azure, and Google Cloud Platform (GCP) enables it to map external assets to internal assets. This feature greatly reduces the manual effort required to identify internet-facing assets with vulnerabilities. LookingGlass concludes that the best information about your attack surface will be found in your existing tooling, such as cloud providers and DevOps solutions.

Once discovery is complete, assets are inventoried and available contextual information is added automatically. At this stage, some vendors offer the ability to assess identified risks actively, leveraging either humans or automation to perform penetration test-like analyses of risks. LookingGlass does not offer this capability but indicates it will be available in the future. scoutINSPECT currently provides a useful feature by which a specific asset and issue can be shared with users outside of the solution via a read-only link. This can be very handy when coordinating remediation efforts with other business units, teams, or other organizations.

Internal ASM features are delivered through cloud integrations with AWS, Azure, and GCP. By integrating these cloud services, externally and internally identified assets (and their associated vulnerabilities) can be easily correlated. The internal ASM capabilities are limited to the data that can be gathered from these cloud providers' APIs, however, because the LookingGlass solution does not offer an agent for deployment to endpoints.

While this solution performs robust discovery activities, its active assessments at this time are more limited, though it has plans to greatly expand the scope of assessments in future releases. Moreover, LookingGlass combined its threat intelligence with the Alphawave ASM to create a converged threat intelligence-ASM solution. Additional solutions could potentially be integrated with the open and documented LookingGlass API, though this bespoke development would be dependent on the customer.

Pricing follows a flat fee model with a few variables, including the frequency of scans, the retention period for data, and the number of integrations. This pricing structure is predictable and suits most organizations because it won't grow as your attack surface grows. Instead, it will increase only as your organization's ability to use more advanced features comes online.

Strengths: scoutINSPECT offers robust discovery capabilities with emphasis on web stacks. Its cloud integrations create a complete picture of the ASM, with simple internal-to-external mappings of assets. The integration of the LookingGlass threat intelligence feed into the ASM solution bolsters an already capable solution with timely threat intelligence.

Challenges: This solution offers minimal active assessment capabilities and limited internal ASM features.

Mandiant

In late 2021, Mandiant acquired Intrigue.io ASM. Mandiant quickly integrated the Intrigue solution into the Mandiant Advantage platform, formally launching Mandiant Attack Surface Management in early 2022. The new solution fully leverages the Mandiant Advantage unified platform experience as well as its industry-leading Threat Intelligence product. In 2022, Mandiant was acquired by Google Cloud but retained the Mandiant brand.

The Mandiant Advantage platform is the company's flagship product, delivering threat intelligence and other cybersecurity services designed to help organizations identify and respond to cyber threats by providing real-time visibility into threat actor targeting, their systems, networks, and now the broader attack surface. Mandiant Attack Surface Management is one of a very few ASMs that offer a free, limited version for organizations to try before they buy.

This ASM solution uses Mandiant Threat Intelligence to enrich assets with intelligence, which is gathered from Mandiant professionals deployed in the field as well as from sources unique to Mandiant. This is the solution's greatest differentiator when compared to competitors.

Like others, this solution starts discovery with a piece of seed data (such as a company name, URL, or email address), and it is then able to discover and enumerate the associated external attack surface assets, like domains, URLs, IPs, and certificates. The solution connects to data sources like Akamai DNS Edge and GitHub and collects passive DNS data; however, it's unable to discover internal attack surfaces. Asset discovery scans occur daily, though this process can be adjusted by the customer, depending on the license that is selected.

Asset categorization is handled in the Mandiant Attack Surface Management module via Collections, which organize the relevant attack surface data into assets, technologies, and security issues. Assets such as domains, IPs, certificates, applications, storage buckets, and VMs, are bundled under the Entities tab. While the Issues tab contains notable security concerns that are identified and sorted by severity, the Technologies tab holds lower-level assets, such as specific application versions, exposed operating systems, and cloud services. These objects live under the Collections parent object, and in this way they can all be easily sorted and grouped together.

Active assessments are performed for significant risk issues, leaving lower severity issues with just passive assessments methods for validation.

The solution presents security events to the user as issues. Issues are associated with a single asset and include a description of the security issue, resources, proof, and remediation guidance. Severity scoring is performed on a per-issue basis, not a per-asset basis. This style of assessment isn't unique to Mandiant, although it's not common either. The advantage to this approach is that all security risks are considered as a whole and not in a vacuum of a single asset, where the lack of contextual information might lead to incorrect assumptions on the actual risk presented.

The ASM solution is sold as a part of the larger Mandiant Advantage platform, but can be purchased as a standalone module. There are several modules in the Mandiant Advantage platform and bundles of popular modules can be purchased together to reduce the overall cost. Additionally, Mandiant offers numerous professional services that range from technical assurance to cyber defense and incident response. More notably, Mandiant has a service called Expertise-on-Demand where customers can engage with a security expert to help accelerate response.

Strengths: Mandiant offers good, broad discovery capabilities applied with high frequency to ensure a thorough understanding of the attack surface. It also provides severity scoring that occurs on a per-issue basis and is driven by the best-in-class Mandiant threat intelligence with asset categorization achieved through the intuitive concept of collections.

Challenges: Active assessments are limited to significant security issues, and there are no internal ASM capabilities.

Palo Alto Networks

Palo Alto Networks' acquisition of Expanse, completed in December 2020, expanded the company's robust lineup of security services and solutions to include ASM. With Expanse's Expander product as its ASM solution, Palo Alto Networks is now placed solidly in the Platform Play half of the Radar chart and market landscape.

Recently, V2 of the Expander solution was launched, bringing a number of enhancements including automated remediation of risks delivered through the new Cortex Xpanse Active Response Module. Additional improvements include new dashboarding and visualization experiences for simplified creation, expanded role-based access controls (RBACs), and an overall emphasis on taking a more active approach to ASM.

Expander offers comprehensive and frequent discovery results, some of the most frequent of all ASM solutions included in this report. At first glance, its approach using both ML and human analysis is like that of most other vendors in this space. However, a key differentiation is found in how it executes the discovery process.

Expander leverages two types of scanning infrastructure: one attributed to Expanse and one that is obfuscated, which allow Expanse to deliver results that stalwarts of the internet scanning industry, like Shodan, are unable to. This is possible for the following reasons. As scans of internet assets are performed, sources are often blocked to stop the scanning. If the scanning infrastructure remains unchanged (thus blocked), then over time, a portion of the internet will become invisible to this scanner, resulting in blind spots for organizations in their ASM. Expander overcomes this problem by employing an obfuscated, ephemeral scanning infrastructure. In addition, Expander performs protocol-level handshakes to determine service types, which is a nice feature that increases the certainty of results as the analysis progresses.

The discovery results are analyzed using policies that are built and maintained by the Palo Alto Networks Expander team. These policies perform passive assessment and sift through the results, looking for indicators that point to possible vulnerabilities, misconfigurations, or compliance issues. Importantly, clients of the Expander ASM solution can’t create custom policies themselves. However, they can request the creation of specific policies by the Expander team, and Expander policies are updated weekly. Active assessments are reserved for engagements with Palo Alto Networks managed service teams, though the vendor anticipates it will be added to Expander within the next 12 months.

The value that most organizations get from any security solution, ASM solutions included, is usually derived from reports and dashboards within the platform. With the launch of V2, the Expander solution’s reporting, dashboards, and visualizations are now a focal point that makes consuming ASM data easier.

The success that many organizations have found using ASM for the external attack surface has driven demand for a similar capability set for the internal attack surface. Expander V2, with its Active Response module, is now able to integrate with IT and security tools to gather data on the internal attack surface to automatically resolve exposures delivering on the management portion of ASM, which is unique to Expander.

Expander’s other features show that the platform’s extensibility is very mature. While some security solutions provide integrations that only deposit or extract data, Expander’s integrations appear to be based on use cases designed to increase its utility. Risk scoring is achieved using a four-level priority scoring system that is based on guidance derived from Palo Alto Networks’ own research team. Customers are able to customize this system to their preference or needs.

Asset categorization is achieved with a tagging system. This might oversimplify the process, however, as categorization activities include automated attribution that occurs during the discovery process. The tagging system is simply the method by which customers can apply language to asset groups that makes sense in their organization.

Buying Expander requires first paying a platform fee and then for a certain number of assets under management. Customers can acquire additional modules based on their needs, such as Palo Alto Networks’ managed services (for example, Internet Asset Enumeration andInternet

Landscape Intelligence) or SaaS modules like Link (for supply chain risk) and Active Response (for automated remediation).

Strengths: The solution includes comprehensive discovery capabilities, active responses that reduce operator burden, numerous integrations with third parties, and very deep integrations with other Palo Alto Networks solutions. The emphasis on active protections in V2 along with improved dashboards and reporting capabilities rounds out a capable solution.

Challenges: The solution doesn't yet have active assessment capabilities built in.

Praetorian

Founded in 2010, Praetorian is a cybersecurity solutions company. Its Chariot solution combines an ASM platform with an offensive security managed service. Leveraging automation, ML, and human expertise, the Praetorian ASM aims to deliver a zero-false-positive solution. While Praetorian is relatively new to the ASM space with just over a year of time in the field, the solution is competitive.

Praetorian offers other solutions that complement Chariot, such as a CART and attack and breach simulation service, as well as a CSPM component. The entire Praetorian solution set is coupled with a robust managed service offering that is designed to be supportive and flexible.

The solution begins with a thorough discovery of the customer's attack surface during which Chariot catalogs and sorts assets and associated vulnerabilities. Assets are discovered using common ASM techniques and through connections to customer cloud environments. In this way, Chariot offers both outside-in and inside-out perspectives for a complete understanding of the attack surface.

The Praetorian solution does not offer internal ASM capabilities, although some basic internal functionality exists with the cloud connection capability. Additionally, this solution does not provide a method to categorize assets currently.

The risk scoring methods employed by the solution take the discovered and enumerated assets, then employ human expertise to fully understand the risk potential of a vulnerability. While evaluating the vulnerability, Praetorian operators often chain together seemingly separate vulnerabilities to identify risks in the same way an adversary would. Having people (Praetorian operators) chain vulnerabilities together is unique to the Praetorian solution, so this is a differentiating feature.

Because of the emphasis placed on delivering a fully managed solution, along with Praetorian's overarching goal to support customers in the ways they need to be supported, the solution's information is often delivered through real-time communication methods like Slack, Teams, Jira, or email. These channels, together with regular meetings at a cadence defined by the customer, deliver a user experience unlike any other in the space.

The licensing for this solution is based on asset count and, as is common, a preliminary discovery can be performed during the sales process to determine the count for the purposes of licensing and cost. This solution is sold in three tiers: fewer than 1,000 assets, 5,000 or more, and 10,000 or more assets. All services are the same across the tiers, regardless of asset count.

Strengths: Praetorian has the most service-oriented delivery of any ASM solution. Its emphasis on practical security improvements made by innovating its technology, together with its human experts, provides turn-key ASM for organizations.

Challenges: The solution doesn't currently offer asset categorization and has only limited internal ASM capabilities.

6. Analyst's Take

When traditional vulnerability management processes were presented as a solution to the ever-expanding digital footprint of the modern organization, nearly all organizations ran into the same problems. Lack of insight into the known attack surface limited the efficacy of vulnerability management. Once assets were discovered, associating assets with owners was a time-consuming process because of the abstracted nature of internet and cloud-based assets. Moreover, legacy vulnerability scanners are not equipped to discover modern cloud misconfigurations that pose the greatest threat to organizations today.

The ASM solutions surveyed in this report resolve these issues. Because ASM vendors recognize that most organizations can't keep up with the rapid changes to their attack surface, robust discovery is a ubiquitous feature of all ASM solutions. From the discovery phase through the risk identification phase, leveraging both active and passive assessment methods and moving onto the reporting and alerting phases, it's clear that this field has matured rapidly to fill the gaps created by legacy vulnerability management.

Looking back at the chart in **Figure 1**, it's clear that this space contains an even mixture of feature and platform players. Some solutions were born of a single purpose and developed rapidly to meet the needs of the market. Some of these solutions evolved into market leaders while others were acquired or merged and are now part of a larger ecosystem of security solutions.

From our initial evaluation in 2022 to now, the evolution of the market is apparent from the abundance of converged solutions. This includes solutions that are delivering ASM capabilities alongside digital reputation protection, data exposure identification, CART, threat intelligence, and CSPM. Additionally, this year's report highlights the explosion of vendors who are now solidly in the ASM category, with a doubling of the number of vendors in this Radar compared to last year's, and a 500% increase in vendors claiming ASM features market-wide.

We anticipate that convergence of both technologies and vendors will continue for the next 18 to 24 months. It's possible that this market will no longer be referred to as ASM, and that the ASM features highlighted in this report will become part of broader security solutions that include enhanced internal capabilities and features that enable proactive as well as automated reactive security management. We'll continue to report on this space as the market evolves.

7. About Chris Ray

Chris Ray

Chris Ray is a veteran of the cyber security domain. He has a collection of experiences ranging from small teams to large financial institutions. Additionally, Chris has worked in healthcare, manufacturing & tech. More recently he has acquired an extensive amount of experience advising and consulting with security vendors, helping them find product-market fit as well as deliver cyber security services.

8. About GigaOm

GigaOm provides technical, operational, and business advice for IT's strategic digital enterprise and business initiatives. Enterprise business leaders, CIOs, and technology organizations partner with GigaOm for practical, actionable, strategic, and visionary advice for modernizing and transforming their business. GigaOm's advice empowers enterprises to successfully compete in an increasingly complicated business atmosphere that requires a solid understanding of constantly changing customer demands.

GigaOm works directly with enterprises both inside and outside of the IT organization to apply proven research and methodologies designed to avoid pitfalls and roadblocks while balancing risk and innovation. Research methodologies include but are not limited to adoption and benchmarking surveys, use cases, interviews, ROI/TCO, market landscapes, strategic trends, and technical benchmarks. Our analysts possess 20+ years of experience advising a spectrum of clients from early adopters to mainstream enterprises.

GigaOm's perspective is that of the unbiased enterprise practitioner. Through this perspective, GigaOm connects with engaged and loyal subscribers on a deep and meaningful level.

9. Copyright

Gigaom

Knowingly Corporation

3905 State Street #7-448
Santa Barbara, CA 93105-5107