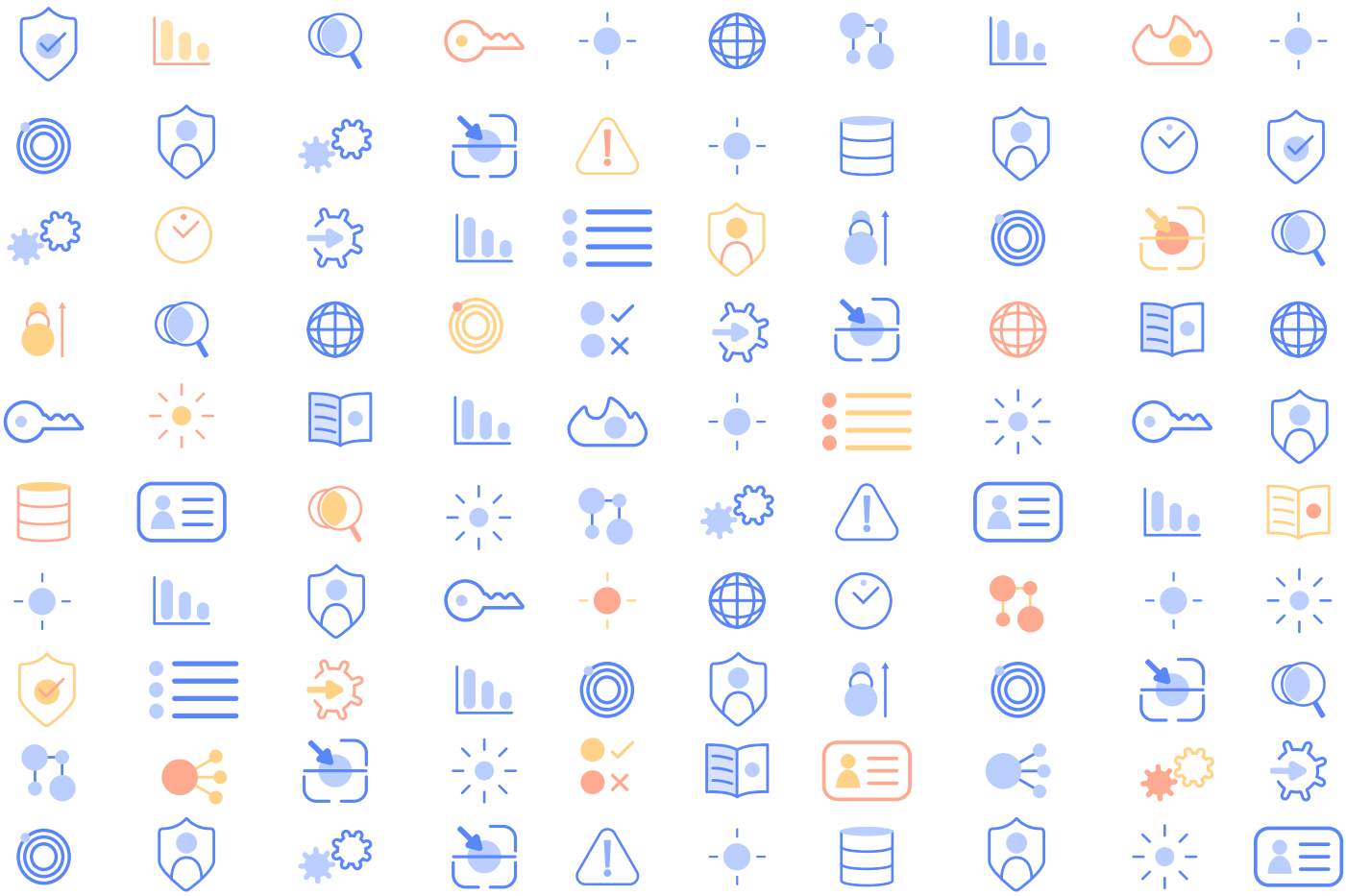
IONIX

ASM CHECKLIST

LOOKING FOR AN ATTACK SURFACE MANAGEMENT (ASM) TOOL?

Comparing multiple solutions?
Use this checklist to help you determine the most important features of an ASM product, how to separate the common features from features that truly stand out, and how to find the best fit for your organization.



DISCOVERY AND ATTRIBUTION

How does your solution operationalize global discovery and scanning? Do you use multiple scan perspectives? If so how many? What types of scanners are employed in your solution?

Look for a solution that is comprised of thousands of probes, aimed at listening in on public registrars as well as crawling all web assets and digital dependencies (both of their own assets and those tied to 3rd party partners - digital supply chain).
Make sure any tool you use take all possible asset and connection candidates into account – and then employs progressive validation techniques (rule-based heuristics, machine learning, expert review) to prune the graph, systematically eliminating assets that aren't yours.

What is the scope of your discovery? IP ranges, Domain Names, third parties, etc? How do you ensure you are capturing the maximum % of the customers real attack surface?

Best practice is to discover and inventory both FQDNs (Fully Qualified Domain Names) and IP address blocks (specifically identifying active IP addresses). Make sure to cover your FQDNs that are used in SaaS platforms, hosted services, and your subsidiaries. Ensure that the solutions you are comparing go beyond discovery and inventory of your organizational assets (managed by your IT/SecOps), but also inventory of dependencies of those assets which can be owned by the organization's vendors and contractors or by other 3rd party entities.

How does your solution assign or attribute assets to my organization? How do you deal with false positives? Do you have any capabilities that reduce the likelihood of them? Can you describe those capabilities in detail?

Sophisticated ASM tools rely on Machine Learning algorithms to avoid false positives by evaluating multiple factors in the attribution of an asset to a company. This iterative process starts off by listing 'asset candidates'. For each asset candidate the algorithm should search for and produce significant evidence of the probability that it is associated with the relevant client. This "discovery evidence" should be easy to understand for any platform user.

Can you detect 3rd party digital supply chain relationships from your scans? For instance, if scanning a website can you detect 3rd party embedded services and links to referral sites etc. and then relate those relationships in terms of risk in your product? What about website information, tags in meta data, third party data feeds etc.?

Look for a provider that has the ability to crawl, discover and assess all types of digital connections and dependencies between a client asset and its potential supply chain, whether 3rd, 4th, nth degree assets. Those risky dependencies include potentially dangerous script inclusions, dangling connections, relying on insecure cloud assets, etc.

RISK ASSESSMENT AND PRIORITIZATION

How does the solution assess overall attack surface risk?	Risk scoring is key to understanding your risk. Make sure your ASM tool is benchmarking against at least 10 indices. You should also be able to see risk score broken down by subsidiary. Ensure your ASM provider enables comparisons to other organizations (in parallel to prioritizing individual security issues and actions that the security teams should take) to ensure risk scores are accurate.
What type of exposures can be identified?	An ASM tool will start by identifying CVEs, misconfigurations, security posture issues and other attack vectors – this is the basics for ASM. More advanced tools also identify exposure using a digital supply chain analysis, evaluate technologies and services offered by the asset, communication response from open ports, expired and soon-to-expire digital certificates, CVEs and CVEs for which there is a known exploit, risks of data exposure due to misconfiguration or exposed configuration and/or log files, hijackable assets, vulnerable components, end-of-life software, compromised endpoint devices (for employees and users), and more.
How do you incorporate vulnerability data into your scans?	An ASM solution should match asset types and identified technologies with the known CVE/CVSS repositories, however advanced solutions use risk scoring mechanisms and check for asset exploitability as well. Check that solutions you evaluate at a minimum use the CISA's Known Exploited Vulnerabilities Catalog (CISA KEV) and as well as EPSS and NIST catalogs for vulnerability and exploitablity data.
How in depth "deep" is the scanning you do? Do you conduct active testing?	Depth of scanning should include vulnerability scanning with various levels of intrusiveness in order to assert if a potential vulnerability is actually exploitable. Also, ask about the approach to mitigation against various types of potentially exploitable risks such as dangling IPs, misconfigured sub domains, etc.
What factors do you take into account for prioritization?	Make sure not to only look at CVSS scores, but to also look at misconfigurations and exploitability, threat intelligence and asset importance. Immediately exploitable vulnerabilities (e.g. dangling DNS records, exposed storage, exploitable OWASP risks, weak/no password) should be prioritized for instant remediation.
How do you handle Zero-days and Zero-day response?	Make sure your ASM can identify all assets relevant to the Zero-day exposure across their entire attack surface inventory, filtered based on technology and versions (where possible). Then make sure you can leverage published exploits and techniques to validate exploitability with a clear view of the precise attack surface and actionable remediation steps for IT teams.

SECURITY OPERATIONS

How big are your largest clients in terms of assets scanned?

An ASM solution should be able to handle monitoring tens of thousands of FQDNs (and even reach hundreds of thousands when including subsidiaries...) and millions of IPs.

How is the asset discovery data processed and analyzed?

The discovery process should not require any input from the organization. Discovery data should include fetching information from the global IP registration systems, scanning of the Internet, global PKI logs (e.g., CTL), global WHOIS and DNS, as well as active discovery of the infrastructures connected to organizational assets (digital supply-chain). Machine Learning (ML) algorithms decide whether an asset (IP, IP range, domain, subdomain, etc.) belongs to the organization or not. Organizational assets and their digital supply-chain should be further analyzed by various assessment modules (Web, Cloud, DNS, Network, PKI, Mail, etc.). Input from the user (either via an application or the API, or by integrations) should be optional.

How does your solution manage subsidiaries? Complex organizational structures? Can it automatically attribute assets to the right subsidiary?

Make sure the platform automatically attributes each asset to the relevant subsidiary or business owner – across on-premises, cloud infrastructure, managed services, and 3rd party platforms. Each subsidiary should have its own risk score, and make sure you can control role-based access to the specific subsidiaries.

How does the solution work with WAF deployments? Can you customize your scanner so that the WAF knows that you are scanning the assets? User agent, IP whitelisting, etc.?

Look for a solution that integrates with Cloud-based WAF (e.g., Cloudflare/Akamai) to audit some configurations and use the information to extend the discovery.

How are all the key threats and other attack surface exposures made accessible to key stakeholders?

Make sure you can prioritize with organizational context and threat intelligence - it should be easy for security and also IT teams to identify and act on critical exposures.
Ensure that your ASM solution maps key insights and exposures across the attack surface layers and details specific remediation instructions in a way that helps your teams visualize what's urgent to fix.

REMEDIATION AND MITIGATION

How can you help us avoid noisy alerting on every small issue the platform finds?

It's critical for your ASM solution to cluster multiple issues together into clear recommendation actions. These recommendations should automatically be attributed to the right subsidiary or functional owner leveraging integrated workflows with SIEM, SOAR and ticketing systems to further streamline your security operations.
In addition, look for a solution that will prioritize exploitable assets, as opposed to every misconfiguration or vulnerability.

Can the solution help us simplify understanding of our security posture?

Executive reports and risk scoring elements help CISOs to understand their security posture and track progress over time.

Does the solution include actionable remediation recommendations?

Make sure workflows align remediation tasks with the way that security operations work inside your org – also test that insights are actionable - meaning simple language insights that provide even non-security personnel with the instructions they need to mitigate and remediate.

Do you have some type of grading/scoring that determines a baseline including given a specific supplier/ subsidiary? If so, what is the basis of this grading?

Choose a solution that provides an attack surface risk score for the organization as a whole, as well as for each subsidiary. Make sure you are able to understand how the risk score is determined and how to break down the elements of your risk score in order to remediate effectively.

INTEGRATIONS

Do you integrate with 3rd party ticketing, SOAR or SIEM products? What type of use cases do you support? What are the most common?

Look for integrations with a wide number of security information and event management (SIEM) systems, SOAR, security operations center (SOC) software, and ticketing systems – to facilitate rapid remediation of critical issues. The integration transmits remediation recommendations to those platforms and can be used to automate the opening of tickets to the owners of the underlying issues and validating that the issue has been resolved once the ticket it closed.

Do you have an API? Is the API two-way or one-way (retrieve only)?

Look for solutions with complete web-based RESTful API that allows programmatic interaction with the platform, not only to query and retrieve data, but also to add/update/remove users/groups/domains/IP addresses, etc.

How do you alert on changes in the attack surface?

A notification module that can push notifications to relevant recipients for various events is a must - such as new assets discovered, new mitigation and remediation suggestions, etc.

What are some of your most valuable integrations and partners in terms of technology and use cases?

Look for solutions that incorporate Threat Intelligence and Digital Risk Protection Service (DPRS) capabilities to ensure that leakage of sensitive data is immediately mapped back to the relevant asset across your attack surface.

Use this checklist as a starting point, and tailor it to your company in order to identify vendors that can best support your ASM needs.