

EBOOK

Attack Surface Management v.2.0

A BUYER'S GUIDE



Cybersecurity teams have been given a set of tools from vendors that are less than ideal – tools that are complex, not well-integrated, that reveal a limited amount of useful information, and provide little or no guidance on how to prioritize and remediate the multitude of threats they face every day. This is particularly true for many of the attack surface management tools that have been available over the past few years. For example, in a [survey](#) of 440 security practitioners we recently conducted, we found cybersecurity staff members were so dissatisfied that 28 percent of them were considering simply dropping their existing ASM once the subscription expired and not replacing it with an ASM, of any sort.

Fortunately, ASM solutions are becoming more sophisticated each year, and it's now possible to acquire a next-generation ASM solution that can ease the burden security teams face. These tools can coherently and consistently inform them about the information and alerts that matter and clearly define what measures they should take in response.

New ASM buyers will clearly benefit from legacy customers having voiced their demands and frustrations, which has informed the innovations in ASM solutions we see today. What follows is a buyer's guide to help narrow down the ASMs available to you so you find one you're actually happy to use rather than one you can't wait to get rid of.



Collecting and Displaying Relevant Data

An ASM is only as good as the information it accumulates. As a baseline, it should create an inventory of all your external assets. For example, it should track those shadow IT assets you wouldn't otherwise know about but that should be on your radar so that you can fully understand their usage. But that's just the beginning. There are unquantified numbers of external assets that potentially can leave your organization vulnerable – those held by your business partners, vendors you rely upon, software supply chains and other sources.

But let's be clear, these assets aren't just physical objects or in-house applications. You also need to be able to discover assets in all public clouds and assess their risk accordingly. An ASM should be able to identify assets that specifically belong to your organization in those clouds.

Asset discovery shouldn't be a one-and-done operation. You'll want to ensure that you receive continual updates on what assets are newly emerged, which should be done through regular scans. But you also may wish to exclude some assets from groups that should have exclusive access to them, and a good ASM can do that for you, too.

All the information gathered should be displayed on a centralized dashboard that summarizes your organization's security posture. This should not just include assets detected or when a scan was last run but also how risk has evolved and been managed over time. Because effective security management requires understanding context, the dashboard should have a unified interface for asset, risk, and policy information.

Finally, all assets need to be grouped in the most logical way, ideally mapping precisely to your organization structure, from subsidiaries down to individual business units and environments within those units. Identifying ownership of assets is a significant challenge in large enterprises, so ensuring assets can be grouped and have an owner is critical to effective management and improves collaborative efforts to manage risks.



Search and Filter Functions

Of course, a pile of assets by themselves doesn't do you much good. You'll need to use filters – risk, asset, category, and vulnerability severity, as examples – to quickly identify what you need to know across the attack surface. This search function should allow customization and retention of search filters so they can be repeated, as well as used by other team members.



Monitoring, Alerts, Scans, and Reports

Keeping on top of your security posture requires flexible and efficient reporting. The ASM solution should have built-in report templates to get you started, but also the potential to create custom reports and alerts, as well as reports that show your overall risk trend. The platform should be able to schedule automated reports that, once completed, can be shared in raw formats like CSV, downloaded as curated PDFs,

and also sent directly from the platform via email, SMS, or Slack/DataDog. Monitoring for sensitive data exposure is critical, and monitoring and alerts for emergent vulnerabilities should take place in near real-time.

Scanning your attack surface also needs to be a function readily controlled by your security team. This means not only setting scanning schedules but also creating and running custom and ad-hoc scans. Most importantly, you should be able to exclude assets from a scan based on the time of day. You don't want to slow a critical operation while you run a scan. Rather, exclude it from the work hours scan and let it run when the asset is not likely to be in use. You also don't want to scan third-party assets without prior approval, so omitting assets from scans becomes a key function to avoid awkward phone calls or even legal action.

Generating reports isn't just to keep your security team informed. They're also essential for keeping the C-suite and board of directors aware of the company's security posture. Cybersecurity has become top-of-mind for these top-level executives, so you need to be able to quickly generate up-to-date reports that give them the information they need. This is in everyone's best interest, including your department when it comes to budgeting and support.



Remediation Capabilities

Having robust remediation capabilities is where many ASMs fall short. They may help you identify assets, but they often leave it up to you to decide what to do next. An ideal ASM platform should be able to provide supporting evidence of the vulnerability it has identified, remediation guidance, and remediation progress.



APIs and Integrations

Your ASM should be part of a larger set of security tools or business functions. That requires using APIs that provide quick response times – 20 seconds maximum. You'll also want to integrate your ASM with key applications that are part of modern business operations, such as ServiceNow, Tenable, Jira, Armitis, Qualys and others.



Miscellaneous Additional Features

In looking at essential additional features, your ASM solution should be able to discover certificates and identify revoked or expired ones, as well as identify dangling DNS from public name servers and domain spoofing. Administratively you will want to be able to use pre-defined as well as customized role-based access and the ability to tag and associate data specific to a customer, business unit, or subsidiary. Finally, any changes made to the attack surface should be visible through an audit trail, as well as through automatic notifications of those changes.

Consider for a minute the Ford Model T. When introduced in the early 1900s, it revolutionized transportation and ushered in the era of affordable, simple, and reliable automobiles. But imagine trying to drive a Model T on today's superhighways. It would be too risky, and the vehicle couldn't possibly keep up with traffic – not even close, especially with Teslas taking over the road.

This is how it is with some of the legacy cybersecurity tools that security teams rely on to defend their companies from the ever-escalating rate of attacks: Model Ts on a superhighway. Teams need an advanced ASM tool that can help them not only keep pace with threat actors but do so in a reliable, rational manner. They not only need complete visibility of internal and external assets, but also the contextual understanding of how to manage them. And they need their ASM tool to fully integrate with other business tools the company relies upon for daily function.

Team Cymru has been at the vanguard in developing an ASM for modern times. We think you'll find that our tool meets all the requirements we've described – and more. [Reach out today](#) and we'll be happy to talk about how we can help you and your organization.

