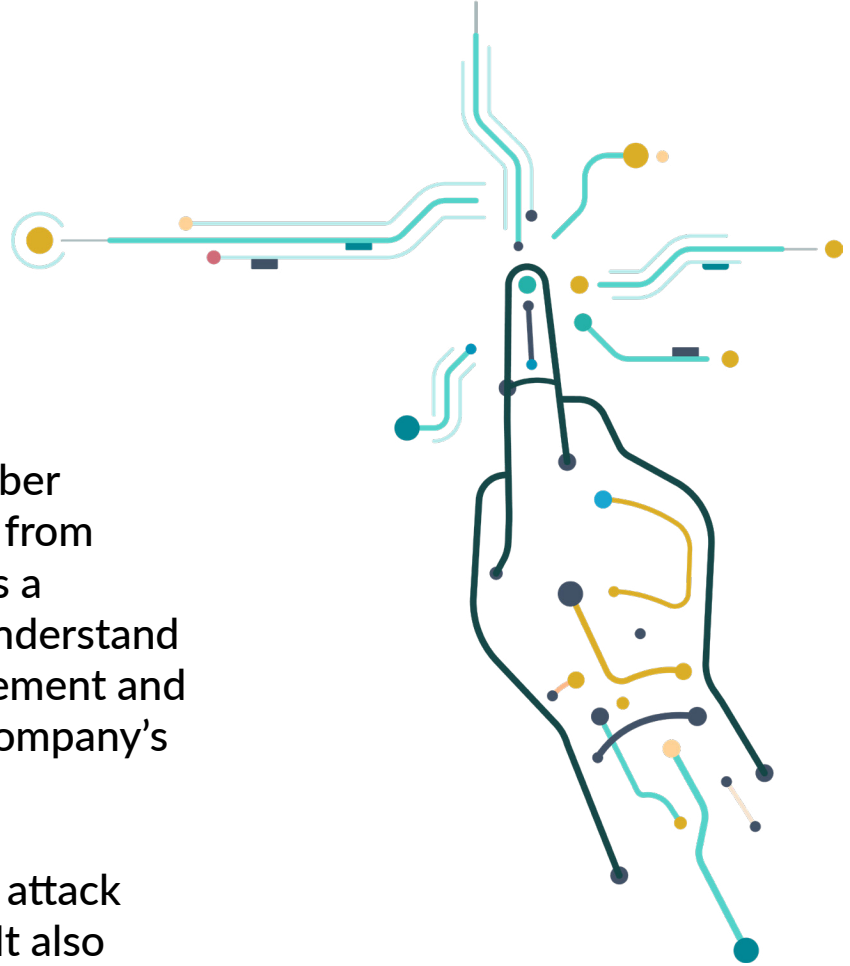
Building An Attack Surface Management Program

A step-by-step guide

stratascale
An SHI Company

In today's interconnected world,



we face increasingly sophisticated cyber threats. Protecting your organization from them has never been more critical. As a cybersecurity leader, it is crucial to understand the concept of attack surface management and its critical role in safeguarding your company's assets, reputation, and bottom line.

This guide explains the "why" behind attack surface management and validation. It also describes "how" to succeed with this type of program in your own organization.

Note: This guide continues a conversation that began in the Stratascale blog, "Your Attack Surface is not just a Buzzword."

Common acronyms mentioned throughout this guide include ASM (attack surface management) and ASV (attack surface validation).

Table of Contents

Beyond your walls:

the importance of attack surface management

As cybersecurity professionals, we spend a lot of time looking internally at our own security environments:

- We have complex tooling and processes to try and detect malicious activity.
- We conduct internal tests to see how fast we can recover when something bad happens, then iterate to improve those processes.
- We constantly evaluate technology, hoping it will make us a harder target or give us better defense.

We get so tied up in what we are doing internally to protect, detect, and respond that we forget our attack surface is not just what we can see inside our own walls. We forget it's also about what's happening outside our walls. An attack surface management (ASM) program will give us that insight into what's going on beyond our walls so we can improve.

You might understand the value of ASM, but still may wonder:

- How do we implement such a program?
- How do we ensure we get the most value out of it?
- What, exactly, makes up a strong attack surface management program?

To be truly effective and deliver the most value, you must also build the people and process around the technology. Just as your security operations center requires multiple domains of skills and technologies, so will your attack surface management and validation program.

An attack surface management and validation program brings the most value when executed continuously–not just one time. In this way, it can positively impact other vulnerability management programs and activities, such as pen-testing, patch management, risk assessments, cyber-insurance vulnerability prioritization, and more.

Step: 1 2 3 4 5 6

Scope & objectives – establishing goals for your program

What do you want to get out of your attack surface management and validation program? It's important to consider the following:

- All the ways the program could be implemented vs. what your business wants to achieve.
- What you'll do with the data and vulnerabilities you discover, as well as how it will impact other areas.
- The business goals for your program need to be clearly defined. What you define initially can change and mature over time.
- Start to define the first few use cases and implementation areas for your attack surface program.
- Consider a long-term strategy linked to achievable, tactical goals for the program.
- It's a bit like building a car. You may have goals for how fast it will go, but that will require a lot of time and thought about the tactics of engine design, suspension, exhaust, etc. Instead of that up-front time getting bogged down in the details, you might instead focus first on the goal of building an engine that can produce 500 HP.)

Program impact on other areas.

Step: 1 2 3 4 5 6

You also need to consider how this program will impact other security programs and business processes, then account for that effort, process, and people. You may want your attack surface management and validation program to influence and strengthen other security programs you already have in place, such as vulnerability management, asset management, internal risk, and other internal defenses.

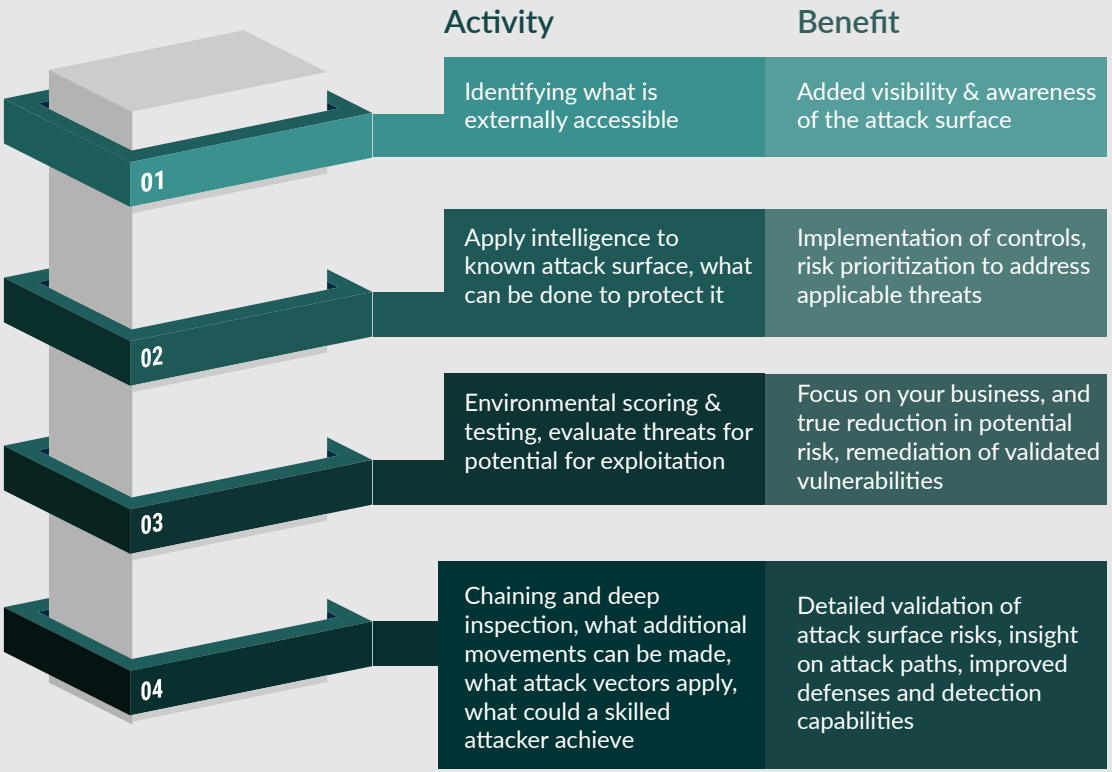
Or, you could be using this new program to improve M&A risk assessments or supply chain risk. There are several ways this program will improve other areas, but it may also create more data and processes. Both types of impacts should be considered.

Building layer by layer.

Think of these programs as being applied in layers. What is it your business needs to achieve, and how quickly? There are costs to consider beyond just technology. You'll also need to consider:

- The program being built.
- How it impacts other parts of your security programs.
- The work it creates.
- The talent required to execute and maintain the program.
- Metrics needed to demonstrate the program's long-term value.

These are all considerations for the business to work out at the start.



Step: 1 2 3 4 5 6

Recommendations for scope alignment

- **Focus on yourself first.** Understand what you're managing and what you're responsible for. Then, expand your focus to the responsibilities of SaaS providers, your vendors, and the rest of your supply chain.

- **See your responsibilities through the lens of shared services.** A shared services model still holds you responsible for several aspects of security. Understand your responsibilities in this model.

- **Consider the priorities of your business.** What you do needs to align with the larger goal of the business. Consider how you will translate the 'security speak' work being done to language & beneifts the stakeholders/leadership will understand. Remember this scope is not just about what you want to get from the program, but will drive the costs, tech, staffing/services model you need. It's not just about technical critera of doing ASM, it's about evaluating the best way to deliver it for your business.

- **To help you define the initial program scope, also consider:**
  - The size of your business, what assets you own, and responsibilities linked.
  - Your prior risk assessment findings, business impact analysis, data criticality assessments, and similar information.
  - Initial costs for technology + people & process build-out, long-term goals, and budget.

Step: 1 2 3 4 5 6

Process - design how to manage and integrate

As stated earlier, these types of attack surface programs require people, processes, and technology. Here is some input on process design.

Think process first.

Spending time on the process part is critical in the earl planning stage of your attack surface program. All too often, it's easy to get caught up in the technology, skills, and training aspects of the program. Don't neglect the impact this new program will have on existing processes, both in security and other business lines. Failing to consider these other process implications can lead to a less successful implementation.

Think in terms of program, not just technology.

As security professionals, we often tell the business to include security at the start. We should adopt this same mantra for process definition in new security programs. Think programmatically, not just in terms of technology.

Here are a few other process considerations:

- Build "hooks" to existing processes. Building everything includes building in the hooks to existing vulnerability management and security operations processes. These types of hooks should be able to make existing processeseven better.
- Design processes needed to run and manage different aspects of the program. It's important to define these types of processes –whether you choose to "buy or build". You still need to define the internal processes to be leveraged(or linked to) by ASM staff.
- Pay special attention to processes that require strong communication and engagement with the attack surface team. To achieve the best results for your business, processes should clearly define which data will be used by the teams as well as how the data will be used. In some cases, you might have service providers run or manage aspects of the program. Your processes should define how you want different providers to work together to deliver different sets of services.

ASM information will typically feed into the following areas of your business:

- Vulnerability management program
- Security operations: Monitoring & detection capabilities
- Threat Intelligence
- Risk Management Programs
- Compliance management, governance programs
- Cybersecurity Insurance
- Third-party/supply chain risk management
- Physical Security
- Security Awareness Training

Step: 1 2 3 4 5 6

People & services – Consider staffing and service models

All the technology in the world won't matter if you don't have skilled people to use it. For the "people" part of your attack surface program, you have various options:

- **Use internal staff.** You can hire and train internal staff. This lets you build an appropriate staffing model to support your defined process and desired goals.
- **Use an external service provider or managed service.** You can also contract this function with a service provider. This occurs most commonly in the form of managed services.
- **Staff augmentation (with contract staff).** There is also a possible option of staff augmentation. Generally, this option tends to be more costly than the other two options. It is also much harder to fulfill long-term, given the highly skilled nature of such positions.
- **Skill levels.** Don't underestimate the skills required. Individuals in these roles need a strong technical background in security technology, networking, applications, cloud, threat intelligence, penetration testing, detection and prevention, security analysis, and more.

Typical program roles. Depending on your program objectives, you'll need teams to cover multiple aspects of the program. Below are some typical roles needed:

Step: 1 2 3 4 5 6

Attack Surface Program Process

Data sources

Program integrations

Service providers

Third parties

ASV program

Validation

Testing

Prioritization

Research

Analysis

Hunting

Step: 1 2 3 4 5 6

Technology – identify which solutions you need

Many products and services are out there to help with your attack surface program. A few issues can complicate ASM technology choices. First, ASM may mean something very different to you than what it means to someone else. ASM products can also vary wildly as there is no industry standard for ASM technology.

You can still navigate these challenges and make good technology choices by looking specifically at your goals. You want to identify the solutions that can meet those goals most efficiently. You will really need to understand not just the data a solution can provide but also the skills and processes needed to translate that data into something you can use.

It's important not to get distracted by a technology that won't necessarily help you achieve your goals. If you do find a solution that offers valuable insights (but you didn't build those types of insights into your original goals), it may make sense to realign your goals accordingly. It's ok to go back, this is cyclical at first, but don't get caught in a never ending cycle

Goals first, then technology. It's critical to use a goal-driven (and objective-focused) lens for your planned technology and solution purchases associated with your attack surface program. This also allows your company to assess its investments based on:

- The business value you expect to gain from this spend.
- How Product X directly contributes to Goal A, etc.
- Staffing linked to objectives and responsibilities. Technology needs to align with staffing, services model capabilities, and skills.

Technology deployment considerations. Another important consideration is where the technology will be ultimately deployed. Such technology and tools may trigger IT policy as "unauthorized". You'll need to understand and solve this issue before you can effectively use some of the technology.

Consider the following details about your technology deployment:

- The type of work you'll be doing with the technology or solution.
- The implications of getting exceptions from IT & Security if you must place ASM technology outside of your typical security.
- Ensuring the SOC/monitoring teams are aware of any exceptions or extra steps needed to access your ASM technology solution.

Dealing with exceptions:

- Incorporate exceptions into specific policies. Exceptions may mean building specific policies for the team to operate safely, even outside the confines of your business.
- Continue to protect these solutions. While such solutions can be decoupled from your company, the information and systems will be valuable to an attacker. So it's essential to protect them.
- Consider using a service provider. A service provider will already be outside your network and will an easier time attracting and retaining talent.

Step: 1 2 3 4 5 6

Pilot – Proof of Value (PoV)

You need the right people, process, and technology (or services) in place to some minimal standard before you can begin the Proof of Value (POV) or pilot. This may involve:

1. Running the tech stack and having the team gather intelligence on either a small subset of data or a larger data set.
2. Testing the team's skills and monitoring the level of effort at various stages of the process.
3. Testing some of the findings.
4. Producing reporting around the risks and remediation.
5. Checking to be sure you're sending risk reporting, remediation to the right processes internally.
6. Ensuring you've set action items and/or timelines.
7. Following up to see the impact.

Using validation to sift through your mountains of data.

As with anything new, when you first start, you need to get over that initial barrage of data and information. This is where validation becomes critical. Everything you find will **not** be something you need to address immediately. One key is knowing what's a priority and what is not. To help prioritize this mountain of data, the people or services you use need the right skills in validation, threat validation, threat hunting, etc.

Your POV goals need to align with your goals defined in Step 1. Once you reach your desired level, you can see where you are and then move into a run state. At each step, you can look at how to integrate it into the processes you want.

Identify externally exposed systems to include, but not limited to domains, IPs, web forms/logins, repos, cloud buckets etc...

Identify "low hanging fruit" to gain traction with the program to include insecure ports/service (FTP,SSH,RDP), out-of-date software/systems, misconfigured sites/repos/buckets, or insecure web applications.

Resolve the "low hanging fruit" and work towards more complex attack paths by chaining the external data together and using some of the internal knowledge as well. (Examples of such internal knowledge could be understanding which systems have SQL, Drupal, WordPress that are not behind WAFs or LBs, etc.).

Develop detections, automation, and playbooks for each action to be taken.

Advancing: use red team findings for improved protections, workbooks, automation, etc. Eventually move program tactics to the internal environment and improve hooks into asset management, rogue device detection, insider threat and other areas.

Step: 1 2 3 4 5 6

Run – the importance of continuous validation

At this stage, your team should have a level of familiarity and comfort. Armed with the right talent, you'll soon evolve.

> *Managing your attack surface needs to be about constant vigilance, not a single event. You need to be aware of the threat actor's view continually, so you can prepare, defend and react to risk before it becomes an incident.*

William Klusovsky, CISSP, CISM, CDPSE

Director Cybersecurity Market Strategy for Stratascale

As your attack surface is continuously validated and tested, you should quickly catch any vulnerabilities that are easy to find. Meanwhile, the attack surface team can start looking for more tangential ways to expand the known attack surface and improve vulnerability and risk management, expanding your defense in depth.

Some of the ways you can do this:

- Introduce additional levels or technologies you may have evaluated at the start.
- Expand to include other vendors, third parties, or a broader scope that you excluded initially.

Work closely with your attack surface team at this stage. They can tell you places where they would like to see added value.

Publicizing your early (and ongoing) wins. As you go, be sure to share relevant findings, remediation, and metrics with the right parties. This includes senior-level management who will be interested in seeing the value and risk reduction you've achieved so far with the program, as well as the output of the team and technology.

Being able to quantify findings goes a long way to demonstrate the value of any solution to those outside of security and IT.

Using validation to realize greater value. You'll notice the use of the term validation in conjunction with management. With a partner like Stratascale, we believe that validation is a critical component often overlooked by many. Validation requires highly skilled people.

By validating the actual risk of data and its vulnerabilities, you can realize more value. Validation is not just about adding more CVEs to a risk register.Validation means you know:

- Which risks pose an actual, executable threat.
- Which things are just noise.
- Data found is actually relevant to your business.

At Stratascale, we provide our services beyond just management. We also have the talent required to test what we find and then bring you actionable items based on those findings.

It's not just about finding risks, either. It's also about quantifying them, helping to remediate them, and then applying that knowledge to reduce the risk to your business long term.

Click here to visit our website to learn more about how we can help you build your Attack Surface Management Program.