Mandiant

ATTACK SURFACE MANAGEMENT

Mandiant Advantage Attack Surface Management (MA-ASM) helps companies understand their digital footprint and focus on the vulnerabilities that attackers are most likely to target. This is achieved in a couple of ways.

- **Asset discovery**: MA-ASM helps organizations by discovering external assets within the IT infrastructure that the company is connected to. These assets are known as **Entities** (https://docs.mandiant.com/home/asm-entities).
  - Customers begin using MA-ASM by choosing a **Scan Workflow** (https://docs.mandiant.com/home/asm-create-a-collection), or use case they want to solve for, and then adding a starting Entity, known as a Seed. For example, a domain name such as `mandiant.com` is considered a Seed. Using this Seed, MA-ASM is able to generate an inventory of related Entities, including known assets and surprise, unmanaged assets.
  - Customers may add other types of **Seeds** (https://docs.mandiant.com/home/asm-seeds) to help populate the discovery process. Seeds are enumerated to help MA-ASM uncover additional assets that the organization might own. Seeds can include domain names, network services, URLs, nameservers, GitHub repositories and accounts, DNS records, certificates, and more.

- **Issue detection**: Once the assets are collected and discovered, MA-ASM continuously monitors the assets, detecting **Issues** (https://docs.mandiant.com/home/asm-how-issues-work) where they exist for each Entity. Issues are generated when vulnerabilities, misconfigurations, exposures, or data leaks are identified. Issues can come from known Common Vulnerabilities and Exposures (CVEs) or can be based on custom rules. Issues give customers a high-level understanding of the risks that currently exist in their environment. Issues are rated on a five-point scoring system, with Issues labeled with a “1” as critical, and those labeled with a “5” as informational.
  - Types of Issues range from expired certificates, exposed development systems, and insecure cookies, to more severe problems like misconfigurations of automated build systems such as Jenkins, Microsoft Remote Desktop CVEs, and AWS S3 buckets accessible to unauthenticated users. A full list of Issues can be found on the **Library > Issues page** (https://asm.advantage.mandiant.com/library/issues) in MA-ASM.
  - Issues are then tackled by the organization's security team, and when resolved, become 'inactive' upon the next scan. Scans run either every day or every week, depending on the agreed upon configuration.

    In cases where an Issue is resolved between the scans, the Issue still populates as 'active' until the next scan is completed.

MA-ASM is used by pen-testers, red teams, security analysts, and anyone who needs to keep their attack surface secure. At the tactical level, MA-ASM is commonly used to:

- determine if there are any ports open to the internet
- uncover any vulnerable technologies in use
- monitor supply chain vendors and services
- assess API endpoints
- identify application endpoints that don't allow 2FA
- find unknown or unmanaged assets

MA-ASM is available as both a free and a paid application. To learn more about the differences, see **Comparing ASM versions** (https://docs.mandiant.com/home/asm-versions).

- Learn how ASM helps you automate external asset discovery and analysis to uncover vulnerabilities, misconfigurations and exposures.
- Provide an overview of Issues, Entities and Technologies.
- Define the scope of the attack surface to help ASM find critical sources and exposures.
- Learn how to leverage, search, sort, filter, and ask questions of the attack surface.