

HOW ATTACK SURFACE MANAGEMENT DIFFERS FROM VULNERABILITY MANAGEMENT TOOLS

As its name states, Mandiant Advantage Attack Surface Management (MA-ASM) is an attack surface management tool and shouldn't be confused with vulnerability management tools. While both MA-ASM and vulnerability management tools both perform vulnerability analysis against a network range, there are several differentiating points, as described in the following table.

	Mandiant Advantage Attack Surface Management	Vulnerability management tools
Scope	Sophisticated scoping mechanisms to automatically decide whether an asset should be scoped.	Must be pointed at a network range, and has no concept of scope beyond this.
Vulnerability Scanning	Focuses on unauthenticated techniques (like an attacker would), on hosts, apps, APIs, and more.	Focuses on authenticated and unauthenticated techniques, only on hosts.
Asset Inventory	Broad scope, including hosts, apps, cloud resources, networks).	Narrow scope, limited to only hosts.
	In-depth enrichment and information available for discovered assets.	Limited, often incorrect or inferred information about each host.
Technology Inventory	In-depth technology discovery capabilities and tech inventory across all assets.	Does not identify technologies beyond what's needed for vulnerability scanning.
	Searchable technology directory.	Not available.
Third Party Inventory	Utilizes global intelligence to identify third-party services and applications.	Does not do anything to identify third-party services or supply chain.