

## ASM AND SECURITY COMMAND CENTER

Security Command Center continuously monitors customers' cloud environments. Therefore, Security Command Center lets you:

- gain visibility into your cloud assets
- discover vulnerabilities in resources
- detect threats targeting assets
- maintain compliance based on industry standards and benchmarks

Security Command Center Enterprise uses Mandiant Attack Surface Management to scan external attack surfaces to identify vulnerabilities and misconfigurations.



Mandiant Attack Surface Management is automatically enabled for Security Command Center Enterprise tier customers.

See the Security Command Center [Security sources documentation about Mandiant Attack Surface Management \(https://cloud.google.com/security-command-center/docs/concepts-security-sources#mandiant-asm\)](https://cloud.google.com/security-command-center/docs/concepts-security-sources#mandiant-asm) for more specific information about how to review Mandiant Attack Surface Management findings in the Google Cloud console.

### Scan Ranges

The scan range for Mandiant Attack Surface Management scans as part of Security Command Center is different than standalone Mandiant Advantage Attack Surface Management (MA-ASM) scans.

Security Command Center scan activity sources from the following IP address:

- 34.41.166.70/32

For best results, add this IP address range to your allowlist.



For information about standalone MA-ASM scans, see [ASM Scan Ranges \(https://docs.mandiant.com/home/asm-scan-ranges\)](https://docs.mandiant.com/home/asm-scan-ranges).

### Security Command Center doesn't show inferred CVE findings

Security Command Center doesn't show inferred CVE findings because that configuration option is not enabled. The configuration option for inferred CVEs cannot be enabled for individual Security Command Center customers. Enabling inferred CVEs for all customers would result in a significant increase in the number of findings.

### Security Command Center doesn't show the same findings as standalone MA-ASM

Security Command Center doesn't show the same findings as standalone MA-ASM because the scan configuration for Security Command Center and for MA-ASM are not identical. The Security Command Center scan configuration is focused on cloud assets.