Mandiant

ATTACK SURFACE MANAGEMENT CREDENTIAL SECURITY DETAILS

To help strengthen security, Mandiant Advantage Attack Surface Management (MA-ASM) leverages Google Cloud Secret Manager for the storage of all customer-provided credentials. This allows our platform to be built upon a foundation of enterprise-grade security controls that are managed directly by Google.

Security controls for credential storage in MA-ASM

When you provide a credential to MA-ASM for an inbound integration, it is stored within Secret Manager. This provides the following safeguards to ensure its confidentiality and integrity at rest:

- ### Confidentiality through encryption at rest

  Protecting the secrecy of your credentials is the primary objective. Secret Manager provides robust, automatic encryption.

  - **Automatic encryption**: Every secret you entrust to MA-ASM is immediately and automatically encrypted at rest using the industry-standard Advanced Encryption Standard with a 256-bit key (AES−256). This is not an optional feature; it is enabled by default for all data.
  - **Layered key management**: The encryption keys that are used to protect your secrets are themselves encrypted with a set of master keys that are regularly rotated by Google. This layered approach provides defense in depth against unauthorized access to the raw credential data.

- ### Integrity and granular access control

  We ensure that your credentials are not only encrypted but are also protected from unauthorized access or modification.

  - **Principle of least privilege**: MA-ASM adheres strictly to the principle of least privilege using Google Cloud's Identity and Access Management (IAM). This means that only the specific, authorized components of the MA-ASM platform required to perform an inbound integration scan can request access to your credentials. Access is granular and purpose-driven.
  - **Data integrity verification**: Google Cloud's infrastructure employs multiple layers of checksums and cryptographic verification. When the MA-ASM platform retrieves your credential for a scan, these checks ensure the data has not been corrupted or tampered with while at rest.

- ### Verifiable security through auditing

  To provide you with the necessary validation and transparency, all access is logged and auditable.

  - **Immutable audit trail**: Every administrative action or access attempt made by the MA-ASM platform to your secrets is recorded in Cloud Audit Logs. This creates a detailed and immutable record, providing a verifiable trail of when, and for what purpose, your credentials were used by our service. This is one of the critical components for both security assurance and compliance requirements.
  - **Secure credential management**: The underlying use of Secret Manager supports best practices like credential versioning. This facilitates the secure rotation of your tokens and keys without service disruption, empowering you to maintain a strong security posture.

In summary, using Secret Manager as the secure vault for your integration credentials, MA-ASM ensures that your sensitive data is protected by Google's security infrastructure. This provides you with verifiable assurance that the confidentiality, integrity, and controlled availability of your credentials are comprehensively safeguarded.