SHA-1 - what it is, why it’s weak now, and what to use instead

Gridinsoft Help Center

What it is

SHA-1 is a one-way math function that turns any input (a file, a message, a certificate) into a short fingerprint called a hash. The output is always 160 bits long, no matter how big the input is. It’s great for quick "did this change?" checks because the same input should always give the same hash. But SHA-1 is old and weak now: attackers can create two different inputs with the same hash (a collision), so it’s no longer safe for things like digital signatures or TLS certificates. It’s a hash, not encryption-you can’t "decrypt" a hash to get the original.

Why it matters

If you trust SHA-1 for signatures or certificates, an attacker could fake a file or web certificate that appears legit. That breaks trust in downloads, updates, and secure websites.

How it works

- Takes your data and processes it in chunks.
- Produces a fixed 160-bit hash (a hex string).
- Tiny input changes -> very different output (avalanche effect).
- Collisions are now practical, so two different inputs can share a hash.

Red flags

- Software updates or downloads still signed with SHA-1.
- TLS/SSL certificates using SHA-1 for the signature.
- Policies or build pipelines that accept SHA-1 as "secure."

Do it right

- Use modern hashes: SHA-256 or SHA-3 for integrity checks and signatures.
- Update certificate chains and code-signing to SHA-256+.
- Block SHA-1 in security policies and scanners; alert on its use.
- Re-hash old integrity lists (checksums) with SHA-256 when possible.