Leaked credentials stay valid for years because teams fear what a revoke will break



GitGuardian's State of Secrets Sprawl 2026 found over 64% of valid secrets found in 2022 still worked in January 2026. Teams hesitate over what a revoke might break.

- More than 64% of valid secrets discovered in 2022 were still valid in January 2026, per GitGuardian's State of Secrets Sprawl 2026.
- Teams stall because they do not know what a revocation will break.
- Triage based only on whether a secret is valid misses 46% of critical secrets.
- The source recommends prioritizing by impact: what the credential can access and whether it leaked publicly.

What the report found

GitGuardian's State of Secrets Sprawl 2026 reports that most valid secrets discovered in 2022 were still working in January 2026, with more than 64% remaining valid after four years. The reason given is not a lack of detection but hesitation: teams stall because they cannot tell what a revocation will break.

Why validity alone is a weak filter

The source notes that triaging only by whether a secret is still valid misses 46% of critical secrets. It recommends ranking by impact instead, weighing what the credential can access and whether it was exposed publicly. The remainder of the source text, including its material on identity exposure and attack paths, is promotional teaser content and gives no further detail.

What this means for regulated institutions

For risk and compliance leaders, the lesson is that a long-lived exposed credential is often an unmapped dependency problem. If nobody knows which services rely on a secret, revocation is delayed and the exposure persists. Building that knowledge before an incident makes remediation faster and less disruptive.

What to do now

1. Maintain an inventory of secrets and API keys with the owner and dependent services for each.
2. Rank exposed credentials by what they can access and whether they leaked publicly, not by validity alone.
3. Define a tested rotation procedure with rollback so revocation does not depend on guesswork.
4. Set target timelines for revoking exposed secrets and track overdue items to closure.
5. Review older findings from secret scanning that are still unremediated.