

What happens when a program tries to access identity data it shouldn't?

Short answer: It depends on whether the program is trusted and whether it has been compromised. A legitimate application that simply overreaches is given fake data or quietly denied. An unknown or compromised application is rejected or suspended. The real credential is never handed over in any of those cases.

Why a single response would be wrong

The obvious design is "block anything that touches a credential store." It fails immediately in practice, because legitimate software touches those stores constantly — browsers, password managers, VPN clients, sync tools, and backup agents all have real reasons to be there.

Blocking everything breaks the machine. Allowing everything trusted means an exploited browser gets whatever it asks for. The useful question is narrower: **is this program behaving the way it should be?**

The four outcomes

1. Allowed. A known, unexploited application accessing what it legitimately needs. Nothing changes.

2. Fake data returned. A known, unexploited application that exceeds its appropriate access. Privacy behavioral rules apply: the program receives plausible but false data. It continues running normally, and the real credential never leaves storage. From the program's perspective nothing failed — which is precisely why this works without breaking workflows.

3. Access denied. The same situation, where returning fake data isn't appropriate. The request is refused; the application keeps running.

4. Rejected or suspended. The program is unknown, or a known program whose process or libraries show signs of exploitation. Here the concern isn't overreach, it's that the program is no longer acting as itself. Whether it's rejected or suspended depends on the behavioral engine's assessment and your configured settings.

Why deception rather than blocking

Returning fake data is a deliberate choice. A blocked request tells an attacker they've been detected and prompts them to try another route. Fake data that looks real does not — the tooling proceeds with credentials that unlock nothing, and the operator may not learn anything is wrong for some time.

This is the same principle behind canary files in ransomware defense: give the attacker something convincing to grab that costs you nothing.

Configurability

The boundary between rejection and suspension is tunable. Environments with low tolerance for interruption — clinical systems, production lines — can weight toward denial and fake data over suspension, while high-security environments can be more aggressive.

Revision #3

Created 2026-07-20 19:24:22 UTC by Dennis Underwood

Updated 2026-07-21 19:32:36 UTC by Dennis Underwood