What is Credential Guard?

Credential Guard is a Windows security feature that uses virtualization-based security (VBS) to move the secrets normally held in LSASS, NTLM hashes and Kerberos tickets, into an isolated container that even an administrator on the machine cannot read. It blocks the most common credential-dumping path (Mimikatz-style LSASS reads) and blunts Pass-the-Hash and Pass-the-Ticket. It is a strong control, though not a complete answer, so it works best alongside LAPS, Protected Users, and tiering.

HOW IT WORKS

01 How to deploy it

- Enable Credential Guard on supported endpoints with the required virtualization-based security settings.
- Combine with the Protected Users group so the most privileged accounts get extra Kerberos hardening.
- Pair with LAPS so any credential that is captured does not unlock other machines.
- Keep Domain Admins off ordinary workstations, the deepest fix, since the best credential is the one never present.
- Verify it is running, since misconfiguration can silently leave it off.

HOW TO DEFEND

- Mimikatz `sekurlsa::logonpasswords` can no longer read protected hashes from LSASS.
- Pass-the-Hash and Pass-the-Ticket lose their easy source of harvested material.
- It protects domain credentials cached in LSASS, not every secret on the machine, and it does not stop keyloggers or attacks that capture credentials as they are typed.
- It needs the hardware and configuration for VBS, and it does not apply to Domain Controllers in the same way.

SOURCES

[1] MITRE ATT&CK Enterprise Matrix

[2] Microsoft: Kerberos Authentication Overview

[3] NIST SP 800-115 Technical Guide to Security Testing

Test your Active Directory before an attacker does.

securelayer7.net/learn/active-directory/what-is-credential-guard

Open online