Using Windows Defender Credential Guard to Protect Privileged Credentials

blog.netwrix.com/2023/02/06/using-windows-defender-credential-guard-to-protect-privileged-credentials

Joe Dibley

The compromise of a single Active Directory credential can lead to unauthorized access to your servers, applications, virtualization platforms and user files across your enterprise. One of the reasons for credential vulnerability is that Windows stores credentials in the Local Security Authority (LSA), which is a process in memory.

Handpicked related content:

[Free Guide] Active Directory Security Best Practices

Accordingly, it's vital to have a security strategy that protects Windows accounts from being compromised — especially privileged accounts that have elevated access to your company's systems and secrets. Fortunately, Microsoft provides a security tool that helps prevent credential theft in your Active Directory domain: Windows Defender Credential Guard. This article explains how it works.

Introduction to Windows Defender Credential Guard

Windows Defender Credential Guard is a security feature that was introduced by Microsoft in Windows 10 Enterprise and Windows Server 2016. Credential Guard utilizes virtualization-based security and *isolated* memory management *to ensure* that only privileged system software can access domain credentials. By running the process in a virtualized environment, user login information is isolated from the rest of the operating system and domain credentials are protected from attack. Credential Guard protects NTLM password hashes, Kerberos tickets, credentials for local logons and Credential Manager domain credentials, as well as remote desktop connections. Don't confuse Credential Guard with Device Guard; Device Guard prevents unauthorized code from running on your devices.

However, there is a cost to enabling this feature. Once Windows Defender is enabled, the Windows servers and devices in your domain can no longer use legacy authentication protocols such as NTLMv1, Digest, CredSSP and MS-CHAPv2, nor can they use Kerberos unconstrained delegation and DES Encryption.

Does Credential Guard Protect Against Mimikatz?

External threat actors can gain privileged access to an endpoint by querying the LSA for the secrets in memory and then compromise a hash or ticket. Credential Guard helps protect your organization from Pass-The-Hash and Pass-The-Ticket attacks, which are used to seize and elevate privileges during lateral movement, so every endpoint and server that is running the Windows platform and using a modern authentication protocol should have Credential Guard enabled.

Unfortunately, however, Credential Guard doesn't fully protect against a tool like Mimikatz, even though isolated LSAs can't be queried. That's because Mimikatz can capture the credentials being entered. The author of Mimikatz mentions in a tweet that if a malicious actor has control of an endpoint and a privileged user logs in after the machine has been taken over, it is possible for them to get the credentials and elevate their privileges.

Credential Guard also cannot protect against Windows insiders who use their own credentials to access IT assets, rather than trying to steal the credentials for other accounts. For example, Credential Guard cannot prevent a disgruntled employee who has legitimate access to company IP from copying it before they leave the organization.

Enabling Windows Defender Credential Guard

Prerequisites

Credential Guard uses the Windows hypervisor, so all Windows devices running it must meet the following requirements:

- 64-bit CPU
- Support for virtualization-based security

- Secure boot

In addition, Trusted Platform Module (TPM) is preferred because it provides binding to hardware; versions 1.2 and 2.0 are supported, either discrete or firmware.

Enabling Credential Guard

Windows Defender Credential Guard isn't enabled by default because it cannot run on Windows devices that still rely on legacy authentication protocols. To enable it in your domain, you can use either Intune or Group Policy.

Option 1: Enabling Credential Guard using Intune

In the Intune portal, navigate to **Endpoint Security > Account Protection**. Then create a policy, selecting the following configuration settings:

- **Platform**: Windows 10 and later
- **Profile**: Account protection (Preview)

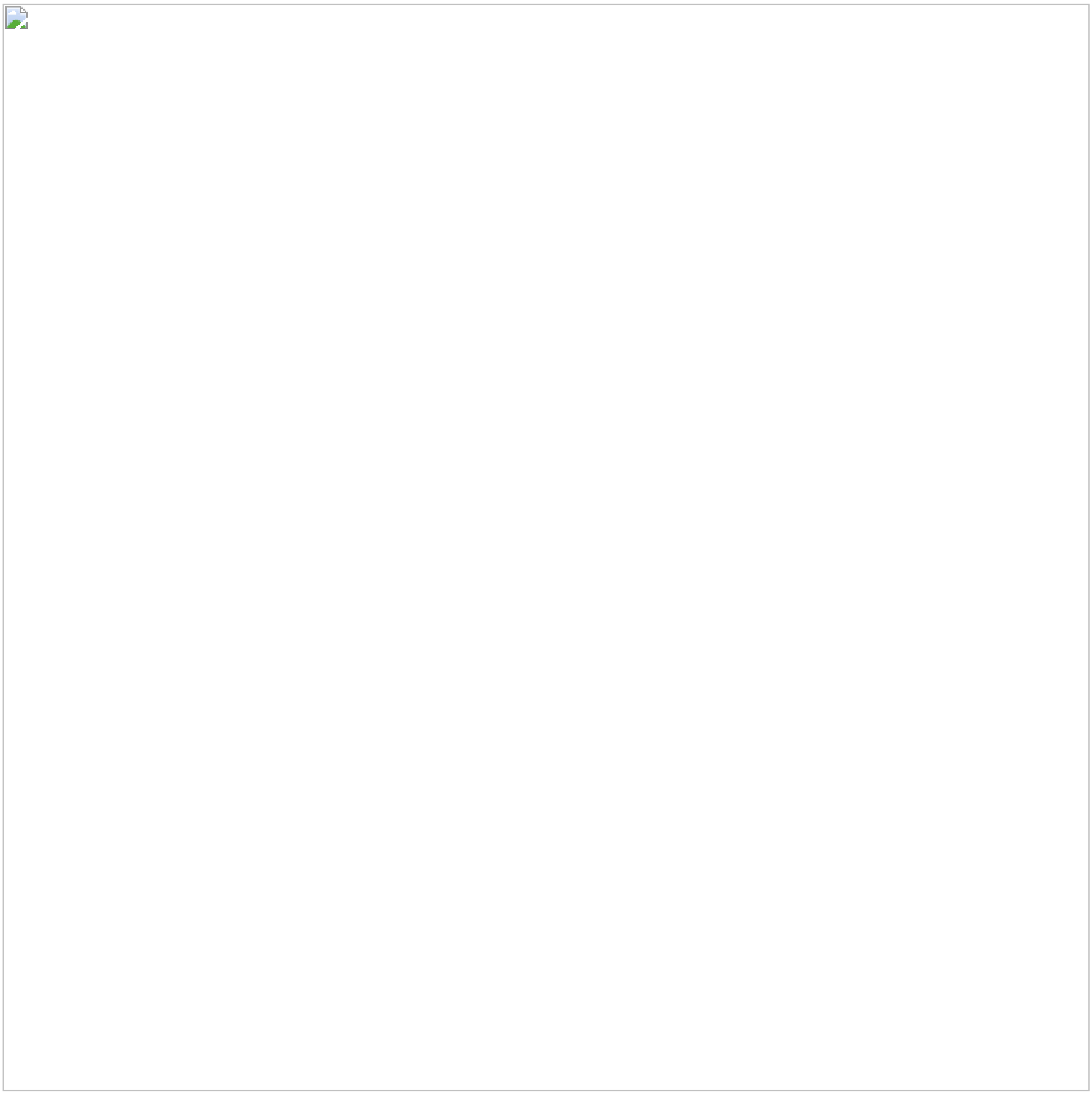


Figure 1. Creating an account protection profile

Name the policy. Then, in the Configuration settings step, set the value for **Turn on Credential Guard** to **Enable with UEFI lock**. This ensures that Credential Guard cannot be disabled remotely.

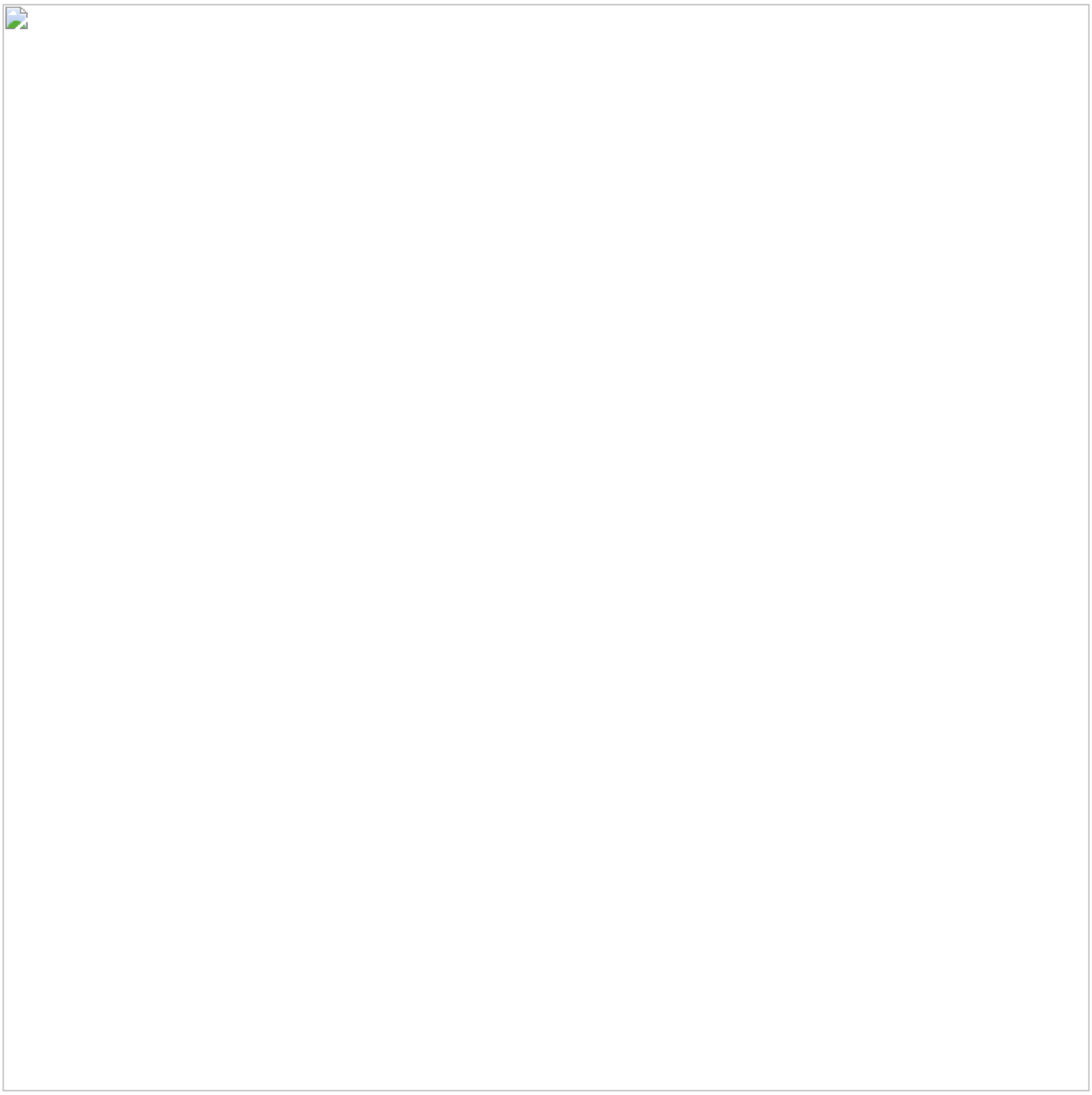


Figure 2. Configuring the account protection profile

Option 2: Enabling Credential Guard using Group Policy

Alternatively, you can use Group Policy Manager to enable Credential Guard. Create a GPO and go to Computer Configuration > Administrative Templates > System > Device Guard. Then set **Turn on Virtualization Based Security** to **Enabled**, as shown below.

Figure 3.Enabling Credential Guard using Group Policy

Verifying Enablement

Once Credential Guard has been enabled using either Intune or Group Policy, you should see the Lsalso.exe process running on all the machines assigned to the policy.

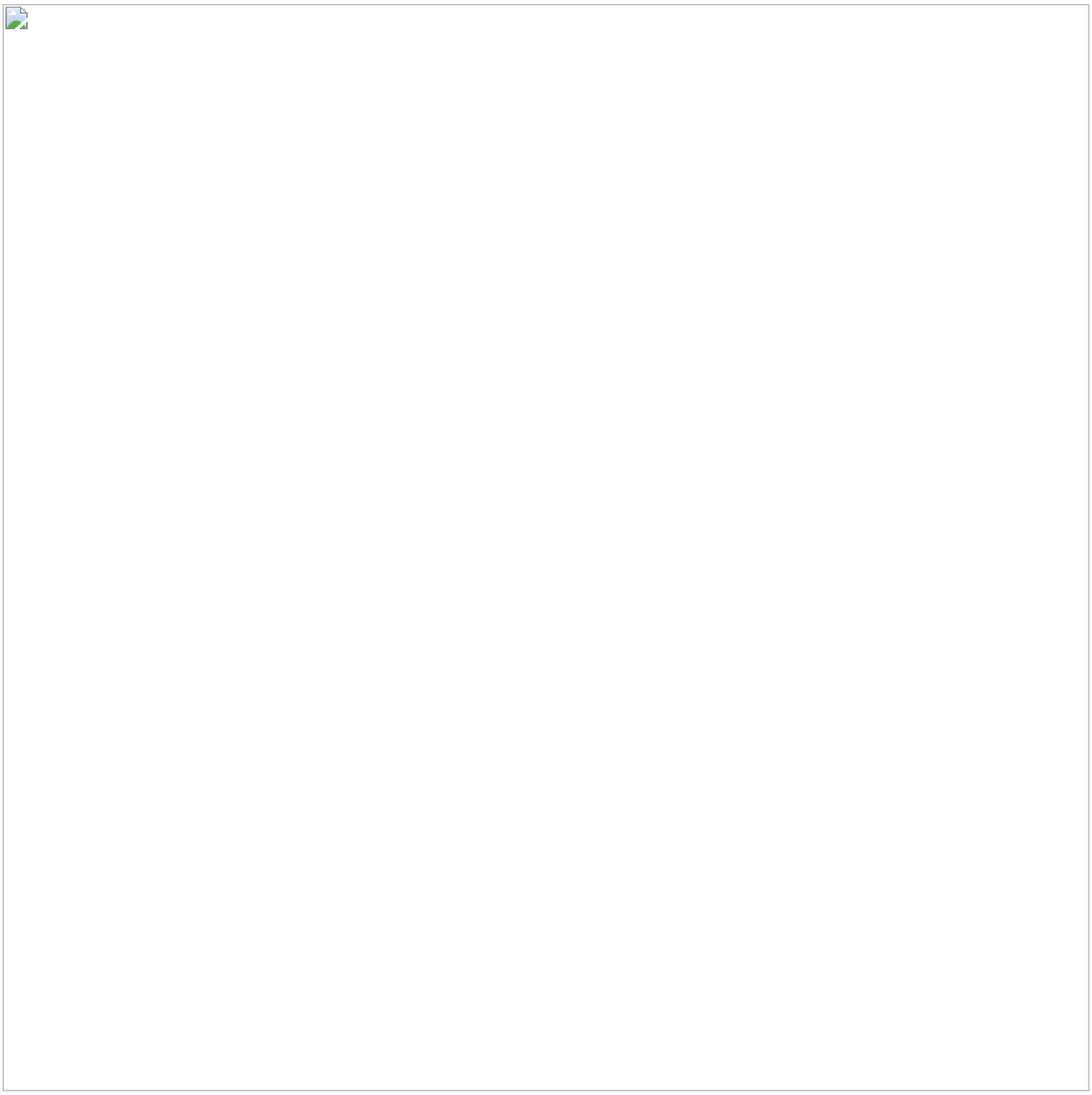


Figure 4.Verifying that Credential Guard is enabled

Credential Guard in Action

Without Credential Guard enabled, a hacker can use mimikatz to query the credentials currently stored in the LSA process to get the NTLM hash of an account remotely logged into the machine, as shown below.

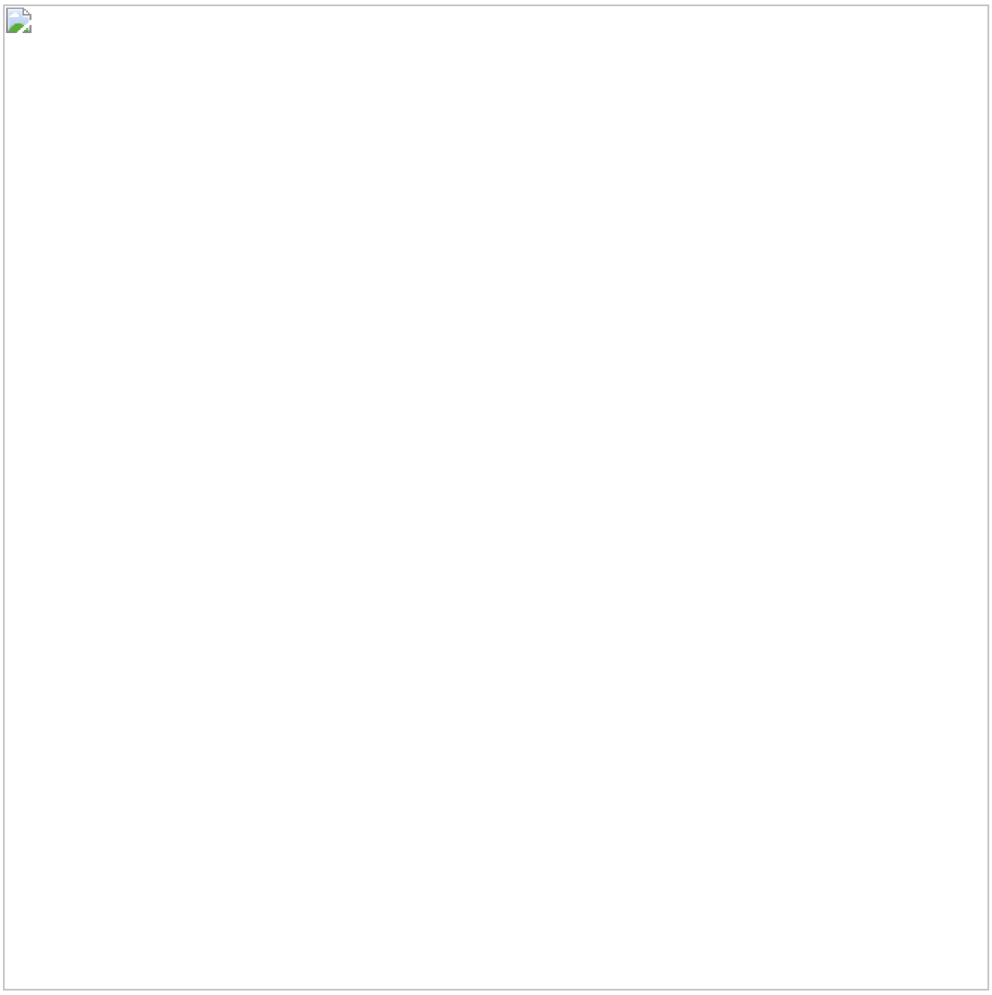


Figure 5. Without Credential Guard enabled, mimikatz can collect hashes stored in memory.

With Credential Guard enabled, however, an isolated LSA process is used to store credentials. Therefore, when we query the same server again using mimikatz, we do not get NTLM hashes in the dump.

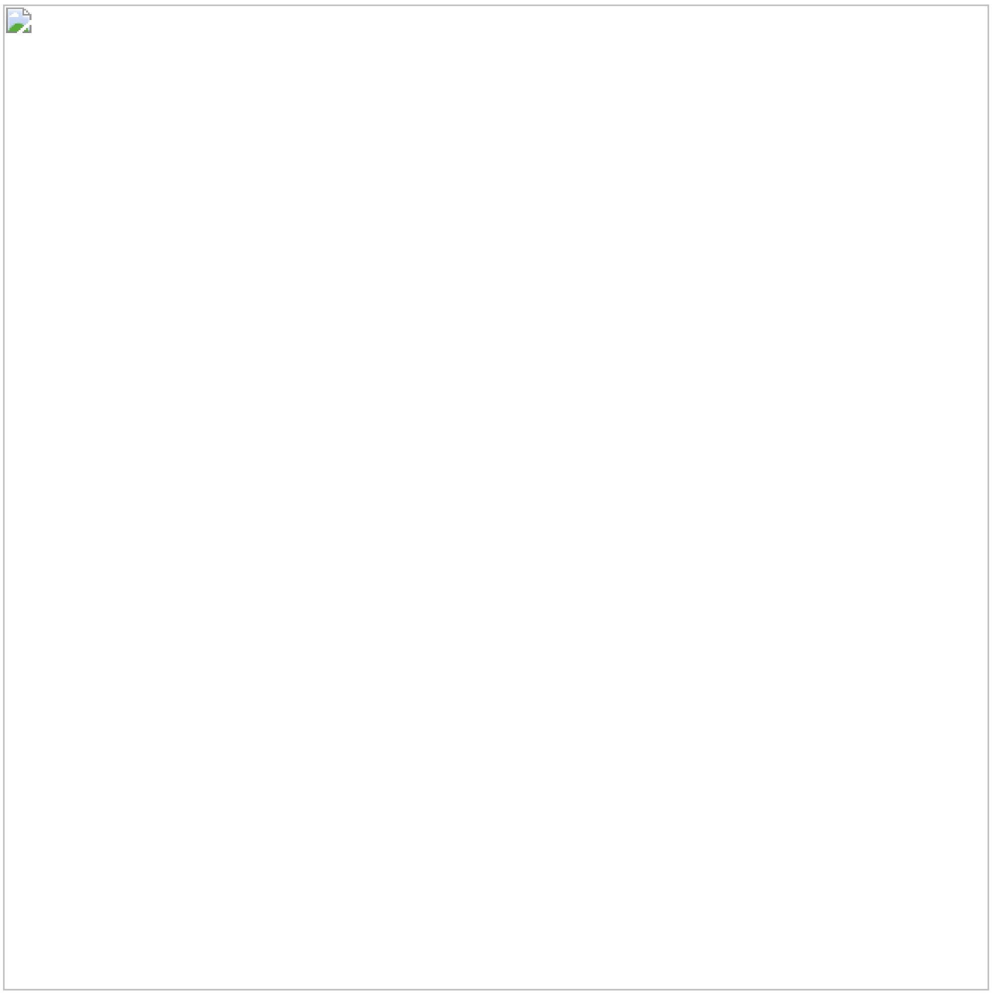
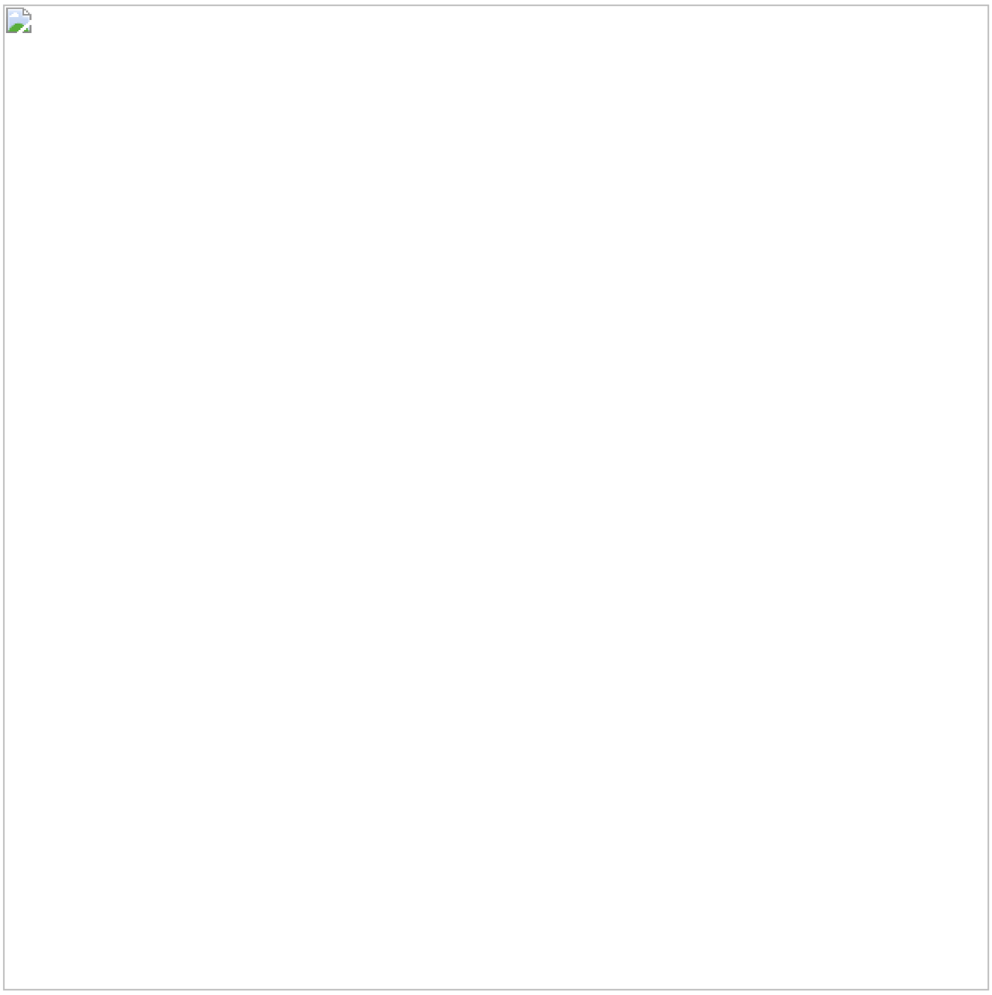


Figure 6. With Credential Guard enabled, mimikatz cannot collect hashes stored in memory.

Credential Guard is also effective against Pass-the-Ticket attacks, as shown below.



Conclusion

Limiting the attack vectors that malicious actors use to move laterally and escalate their privileges in your domain must be a top priority for any security authority. Credential Guard can help by using virtualization-based security and isolated memory management to secure credentials against attack.

Joe Dibley
Security Researcher at Netwrix and member of the Netwrix Security Research Team. Joe is an expert in Active Directory, Windows, and a wide variety of enterprise software platforms and technologies, Joe researches new security risks, complex attack techniques, and associated mitigations and detections.