Windows 10 credential theft mitigation guide

Assume breach: two words that should change the way defenders think about compromise in their organization. Microsoft investigations of attacks on customers all too often reveal success in compromising user and administrator account credentials, including domain and enterprise administrator credentials. Technical features and capabilities alone are not enough: the most effective solution requires a planned approach as part of a comprehensive security architecture that includes proper system administration and operation.

### In this topic:

* Introduction
* Attacks that steal credentials
* Credential protection strategies
* Primary technical countermeasures for credential theft
* Additional technical countermeasures for credential theft
* Other potential countermeasures for credential theft
* Detecting credential attacks
* Responding to suspicious activity

### See also:

* For more details on Microsoft Passport and Windows Hello, see the [Microsoft Passport guide](https://technet.microsoft.com/en-us/library/mt589441(v=vs.85).aspx).
* For an explanation of Kerberos technologies and concepts, see [Kerberos Explained](https://msdn.microsoft.com/en-us/library/bb742516.aspx) and [Microsoft Kerberos](https://msdn.microsoft.com/en-us/library/windows/desktop/aa378747(v=vs.85).aspx).
* For a description of credential theft mitigation in Windows 10, see <https://channel9.msdn.com/Blogs/Seth-Juarez/Mitigating-Credential-Theft-using-the-Windows-10-Isolated-User-Mode>.
* For a detailed description of Credential Guard protection, see [Protect derived domain credentials with Credential Guard](https://technet.microsoft.com/itpro/windows/keep-secure/credential-guard).

Copyright

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

© 2016 Microsoft. All rights reserved.

Please refer to [Microsoft Trademarks](http://www.microsoft.com/en-us/legal/intellectualproperty/Trademarks/EN-US.aspx) for a list of trademarked products.

## Introduction

As the tools and techniques criminals use to carry out credential theft and reuse attacks improve, malicious attackers are finding it easier to achieve their goals. In fact, one example of such an attack—the pass-the-hash (PtH) attack—is the most popular credential theft and reuse attack Microsoft has seen to date. Credential theft attacks like PtH use a technique in which an attacker captures account logon credentials or, in the case of a PtH attack, the user-derived credentials used for single sign-on (SSO) from a compromised computer, and then uses those captured credentials to authenticate to other computers on the network from the attacker’s computer. This type of attack is used in the majority of significant security breaches and enables the attacker to maximize the breach’s security compromise.

[Mitigating PtH Attacks and Other Credential Theft Techniques](https://www.microsoft.com/en-us/download/details.aspx?id=36036) recommended simple, practical, and widely applicable mitigations that every organization should implement. This paper builds on those recommendations, providing key strategies and mitigations designed to help organizations limit the impact of the intrusions that will inevitably occur. It is critical that organizations make proactive investments in the identification of high-value assets, detection, response, and recovery processes.

The first part of this paper provides information about credential risks generally. It explains both technical attacks such as PtH and social engineering– and hardware-based attacks. The second part describes strategies and considerations to help prevent attacks and overcome challenges related to identification, protection, detection, response, and post–compromise recovery scenarios. To ensure a resilient defense, organizations must protect, detect, respond to, and recover continuously. These strategies use several features new to the Windows 10 operating system and features that Microsoft implemented in previous versions of Windows.

You can never assume that a technical countermeasure will be 100 percent effective at eliminating or solving a problem. Most security strategies factor in people, process, and technology controls to reduce risk comprehensively. For this reason, the strategies that this paper describes also include nontechnical controls, such as not sharing administrator passwords and prioritizing countermeasures based on a risk assessment.

Security-focused systems administrators, security architects, and security managers who understand IT security concepts and risk management make up the target audience for this paper, which focuses on advanced credential security topics and assumes that you are technically knowledgeable with IT security. Its purpose is to help you understand risks to credentials, and then create a comprehensive defense plan based on the recommended strategies.

### Assume breach

Traditional security approaches focus on hardening the outermost network perimeter to protect against a breach, but a legitimate user account that has inadvertently been compromised or authorized personnel purposefully acting in a malicious capacity can bypass even the most stringent perimeter protections. In today’s pervasive threat environment, you must assume that this perimeter can be breached and protect key assets against internal and external threats.

Assuming breach requires a shift in mindset from prevention alone to containment after breach. One reason for this shift is that shared long-term secrets (for example, privileged account passwords) are frequently used to access anything from print servers to domain controllers, representing a risk that transcends the technique or protocol your organization currently uses. To contain attackers, you need rapid detection and remediation of initial breaches. You can achieve such a level of responsiveness only through preparation.

In addition, most threat-modeling efforts stop at the point where the attacker gains administrative access, in effect declaring “game over.” In reality, organizations must continue to do business, respond to the attack, and plan to recover from security compromises. According to the New York Times blog post [The Year in Hacking, by the Numbers](http://bits.blogs.nytimes.com/2013/04/22/the-year-in-hacking-by-the-numbers/?_php=true&_type=blogs&_php=true&_type=blogs&_php=true&_type=blogs&_r=4&)), an often-repeated adage among security experts is, “There are two types of companies today, those that have been hacked and those that don’t know they’ve been hacked.” Assumption of breach represents a maturing of defenses to meet this reality and shifts the focus from if to when an attacker gets inside your organization’s network.

### Build a security portfolio

Microsoft has made significant technology advances in Windows 10 that help thwart credential attacks. Yet even as Microsoft improves strategies for detection and provides new features that help protect against these attacks, organizations cannot solve the problem simply by implementing one strategy or deploying a single feature. As Scott Culp originally wrote in [Ten Immutable Laws of Security](https://technet.microsoft.com/en-us/library/hh278941.aspx), technology is not a panacea.

Credential theft often relies on operational practices or user credential exposure, so effective mitigations require a holistic approach that addresses people, processes, and technology. In addition, these attacks rely on the attacker stealing credentials after compromising a system to expand or persist access, so organizations must contain breaches rapidly by implementing strategies that prevent attackers from moving freely and undetected in a compromised network. Realistically, mitigations increase the effort that a determined attacker needs to apply to remain inconspicuous. When an organization implements an effective program, attackers may find too many barriers and trigger detection mechanisms that could help the organization stop the attack.

Realistically, no security mitigations on a complex system can stop all attacks permanently, but they can significantly increase the effort and cost per attack on your organization, reducing the likelihood of attack success and stealth. When an organization implements an effective program, attackers may find too many barriers and trigger detection mechanisms that could help the organization stop the attack.

Most organizations have unique deployments and specific requirements, so every organization must tailor the strategies this document describes to its needs. Above all, every organization must consider a portfolio of mitigations and strategies to reduce the risk of credential theft. When implemented correctly, these strategies and mitigations will ultimately make credential theft even more difficult, but attackers may still be able to capture credentials after gaining access to an organization’s network. Even heavily restricted environments can have weak links that a determined adversary can exploit. In such cases, containment is possible only if several layers of obstacles restrict the attacker’s ability to achieve his or her goal. The strategies and mitigations this white paper describes are meant to enable the deployment of such obstacles, although they often require trade-offs.

### Plan for compromise

Technical features and capabilities alone will not prevent PtH and other credential theft attacks because operational practices typically shape the attack surface. Therefore, Microsoft encourages its customers to use Microsoft security strategies and the features in Windows to create a comprehensive plan prior to deploying a security architecture program. To create resilience to PtH and related attacks, identify and investigate possible threats, and recover from a compromise, Microsoft encourages customers to consider the stages shown in Figure 1 during architecture planning efforts. These stages map to the functions in the National Institute of Standards and Technology’s [Framework for Improving Critical Infrastructure Cybersecurity](http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf).

Figure . Security stages

Let’s look at each stage:

* **Identify all high-value assets.** When planning for and prioritizing security investments, identify your organization’s most valuable resources. Although assets critical to each organization will vary, assets in control of domain or forest consistently have direct influence over all IT assets, which makes securing these resources a top priority for any organization. When you have taken these assets into account, the next priority is to identify which IT assets host the most important business- or mission-critical information or services, including proprietary intellectual property and sensitive communications. Identifying accounts that provide access to all these systems is key during this stage. The more detailed and accurate the identification process, the more effective other strategies will be.

|  |
| --- |
| **Note:** |
| Although prioritizing high-value assets is the right approach, remember that the least interesting assets also become the beachhead for attacks. So, you ultimately need to prioritize everything on the network, including the least valuable assets, and you start by protecting the most important assets first. |

* **Protect against known and unknown threats.** To protect against attacks, organizations must undergo a planning exercise in which they closely examine how they currently protect their infrastructure and business assets. Planning for protection is a critical task prior to deploying mitigations, and it requires that organizations understand how their users and administrators are authenticated to perform daily tasks. Understanding these requirements helps the business develop a containment strategy that mitigates risk.
* **Detect PtH and related attacks.** Detective controls are a critical part of any complete security strategy. Windows 10 helps you detect attacks by defining authorized scope, which creates cases of unauthorized use that the operating system can monitor, alerting you when trouble occurs. Although detection can be a challenge, the mitigations and strategies this paper describes can help you detect anomalies if an attacker attempts to use an account that has constrained scope.
* **Respond to suspicious activity.** Create a response strategy that prepares defenders to respond appropriately when suspicious activity occurs. If an incident triggers detection mechanisms, it’s possible that a breach has occurred and an attacker may be attempting to move laterally or escalate privileges. False positives help update the configuration of detection mechanisms to prevent reoccurrence. Update plans after analyzing attacker behavior, the compromised account, and the scope of attack to help prevent future attacks.
* **Recover from a breach.** Recovery from credential theft attacks is not trivial. Although you can update credentials and secrets with new passwords or new certificates, attackers may have installed rootkits or other malware on the affected computers during the compromise. If so, they may be able to regain access and compromise these accounts again. Detection plays an important role in efficient recovery because it may define the scope of an attack.

This paper considers each of these stages to help with system planning and design prior to deploying specific mitigations. It recommends only one approach, however, along with considerations for those areas Microsoft believes are important.

## Attacks that steal credentials

Credential theft has a broad definition: the attacker obtains or uses credentials that he or she should not be able to use. Certainly, that definition applies to traditional password-stealing attacks.

As authentication has become more resilient, however, attackers have begun to attack not just the password but the credential itself—a distinction from traditional password cracking in that the attacker may not obtain a password or other authentication factor. Instead, he or she uses the target’s credentials without performing authentication. This is the primary aspect of credential theft that this white paper examines. This paper also highlights a few of the more effective low-tech credential theft techniques and provides several countermeasures to help thwart them.

### Pass the hash

A password hash is a direct, one-way mathematical derivation of the password that changes only when the user’s password changes. Depending on the authentication mechanism, a user can present either a password hash or a plain-text password as a credential to serve as proof of the user’s identity to the operating system. Depending on the authentication type, a password hash or other password-equivalent credential can be stored in the computer’s memory to support SSO and could be subject to theft.

The PtH attack is one of the most popular types of credential theft and reuse attack. This and other, similar attacks use an iterative, two-stage process. First, an attacker obtains elevated read/write permission to privileged areas of volatile memory and file systems, which are typically accessible only to system-level processes on at least one computer. Second, the attacker attempts to increase access to other computers on the network by:

* Stealing one or more authentication credentials from the compromised computer.
* Reusing the stolen credentials to access other computer systems and services.

The intruder often repeats this sequence multiple times during the attack to increase the level of access he or she has to an environment.

After an attacker has stolen a user name and corresponding authenticator, he or she is effectively in control of that account. An attacker who has stolen a user account’s credentials has access to all the resources, rights, and privileges of that account. If the compromised account is a privileged account, such as a domain administrator account, the attacker gains domain administrative rights. He or she can steal any other account credentials stored on the compromised computer, including those for local user accounts, domain user accounts, service accounts, and computer accounts, although the attacker cannot steal domain accounts that have never been used to sign on to the compromised computer.

For an attacker to reuse a stolen password hash on another host, he or she must meet the following requirements:

* The attacker must be able to contact the remote computer over the network, and the computer must have listening services that accept network connections.
* The account and corresponding password hash value the attacker obtained from the compromised computer must be valid on the computer to which the attacker is authenticating (for example, if both computers are in the same domain or local accounts with the same user name and password exist on both computers).
* The compromised account must have the **Network logon** user right on the remote computer.

|  |
| --- |
| **Note:** |
| You can use password hashes only for network logons; you can use-plain text passwords to authenticate interactively. Plain-text passwords can allow an attacker to access other services and features, as well, such as Remote Desktop. |

Table 1 lists the types of PtH attack activities an attacker can perform after the initial compromise.

Table 1. PtH Attack Activities

| **Attack activities** | **Description** |
| --- | --- |
| Lateral movement | The attacker uses the credentials he or she obtained from a compromised computer to gain access to another computer of the same value to the organization. For example, the attacker could use stolen credentials for the built-in local Administrator account from the compromised computer to gain access to another computer that has the same user name and password. |
| Privilege escalation | The attacker uses the credentials he or she obtained from a compromised computer to gain access to another computer of greater value to the organization. For example, an attacker who has compromised a workstation computer could gain administrative access to a server computer by stealing the credentials of server administrators who log on to the compromised workstation. |

It is important to reiterate that the attacker must have administrative access on the initial compromised computer to steal these credentials. Administrative access to a computer can include the ability to run a program or script with an account in the local Administrators group, but attackers can also achieve this type of access through administrator-equivalent privileges, such as those used to debug programs, loading and unloading device drivers, and take ownership privileges.

With administrative access, an attacker might be able to steal credentials from several locations on the computer, including:

* The Security Accounts Manager (SAM) database.
* Local Security Authority Subsystem (LSASS) process memory.
* Active Directory database (domain controllers only).
* The Credential Manager store.
* LSA Secrets in the registry.

The locations from which an attacker might steal credentials vary depending on the operating system. For example, Windows 10 implements Credential Guard, which inhibits some previously attackable credential locations. Credential Guard and other countermeasures are explored later in this paper.

It’s difficult to distinguish the activities of attackers who are using stolen credentials from those of authorized users. If system and event logging are enabled, all authentication activity, malicious or not, will appear as normal logons; therefore, administrators who attempt to detect malicious activities should focus on “authorized” activity that is unexpected.

### Kerberos pass the ticket

Kerberos attacks occur less frequently than PtH attacks, but proofs of concept and tools dedicated to them have already been published. One type of Kerberos attack is the pass-the-ticket (PtT) attack, which resembles a PtH attack in its execution. As with a PtH attack, this type of credential theft and reuse attack requires that the attacker obtain local administrative access to capture the stored ticket-granting tickets (TGTs) before reusing them with the Kerberos protocol.

For an explanation of Kerberos technologies and concepts like TGT and session tickets (STs), see [Kerberos Explained](https://msdn.microsoft.com/en-us/library/bb742516.aspx).

A Kerberos TGT and the associated session key together make up a reusable credential for the Kerberos protocol. TGTs have a default lifespan of about 10 hours and a default total lifetime of 7 days if that TGT is always renewed before it expires. Attackers can steal TGTs and associated session keys and request new STs, which are the credentials used to connect to a specific resource. Attackers can continue this cycle until the TGTs have reached the renewal lifetime, which means that a compromised TGT may allow an attacker to use stolen credentials for up to 7 days, assuming that you have configured the default Kerberos TGT lifetime. Because of the limited lifetime, attackers often collect many TGTs so that as one expires they can use another and continue the attack.

When companies use smart cards for authentication and the TGT has expired, users must insert their smart cards, and then type their corresponding PIN. Otherwise, the TGT is renewed automatically with the same credentials used for SSO authentication.

A significant difference in the attack value between the NT hashes that NT LAN Manager (NTLM) authentication uses and TGTs is the useful lifetime of the compromise. Password hashes are reusable until the user’s password changes, while TGTs expire in a matter of hours according to their configurable lifetime.

|  |
| --- |
| **Note:** |
| An additional risk in Kerberos authentication may arise if the organization trusts sensitive domain accounts for delegation. If the service or server to which a user is authenticating is trusted for unconstrained delegation, the client sends a TGT and session key to the server. An attacker who has compromised the target computer can then use that TGT to impersonate clients. |

### Kerberos golden ticket and silver ticket

A different type of Kerberos credential attack occurs when an attacker can craft a fraudulent TGT or ST. Imagine that a nefarious attacker obtains a trustworthy ST in your organization: that theft has the potential to do harm, but the harm is limited. The ST would provide authentication on only one host, would be time-bound to prevent reuse, and would be restricted to the authorization that that ST grants. Beyond that, if the attacker obtained a TGT, he or she would be able to obtain STs for many hosts but would still be limited in time.

In contrast, if an attacker could craft his or her own TGT, with custom values for all parameters, such an attack would provide nearly unlimited authentication and authorization within the organization. The attacker could specify parameters such as:

* TGT lifetime.
* Group membership.
* User identity.

This method is known as the Kerberos golden ticket attack, and it has the potential to be devastating to an organization’s security because it can achieve nearly unlimited access. In the Kerberos golden ticket attack, an attacker begins by attacking the KRBTGT account, which is the special service account that runs the Kerberos service in the Windows Server operating system. The attacker compromises the KRBTGT account’s credentials by examining Active Directory memory or Local Security Authority (LSA) memory, password cracking, or other means. This provides the attacker with the cryptographic keys required for the attack. The attacker next crafts a TGT with parameters that specify a long lifetime and membership in trusted groups like Enterprise Admins. Then, the attacker uses the stolen KRBTGT account credentials to encrypt the TGT, which results in the attacker in possession of a TGT that can access most resources within a target domain.

A slightly less impactful yet still worrisome vector is the Kerberos silver ticket attack. This attack focuses on forging an ST. The forged ST, with parameters of the attacker’s choosing, could provide unlimited access for an unlimited amount of time but is restricted to the host the ST specifies.

Kerberos itself is designed to prevent this type of attack and to limit the damage a fraudulent TGT or ST can do. So, how does an attacker create a golden or silver ticket? The Kerberos TGT and ST encryption keys are based on the password of the accounts involved: the KRBTGT account for a golden ticket and the service’s account for the silver ticket. An attacker needs the cryptographic keys for one of these two account credentials to perform the attacks. When an attacker has the KRBTGT keys, he or she can create a TGT and use it to create new STs. When the attacker has the service’s account, he or she cannot create a TGT but can create a new ST.

Fortunately, countermeasures for the golden and silver ticket attacks are available. They include:

* Regularly changing the KRBTGT password manually or with a script (see [KRBTGT Account Password Reset Scripts now available for customers](http://blogs.microsoft.com/cybertrust/2015/02/11/krbtgt-account-password-reset-scripts-now-available-for-customers/))
* Monitoring for and responding to credential attacks on the KRBTGT account and on the trusted host’s machine accounts.
* Regularly changing service account passwords manually or with a script.

This white paper discusses all these countermeasures.

### Key loggers

Some credential attacks do not target Kerberos or NTLM authentication directly; instead, they attack the authentication process itself by intercepting the proof of identity. Two important attacks that target the proof of identity process are key loggers and shoulder surfing, which the next section explains.

Consider a simplified authentication process on a Windows PC:

1. Windows prompts the user for credentials.
2. The user types his or her user name and password on a keyboard connected to the PC.
3. The user name and password pass through an electrical connection (typically USB) to the PC.
4. The PC hardware provides the input to the Windows authentication process.
5. The Windows authentication process verifies the information, proving the identity and completing the authentication process.

Key loggers intercept the user name and password at weak points in this process. The most effective form of key logger is the hardware key logger. The attacker connects this device between the keyboard and the PC. The key logger then monitors the electrical signal the keyboard sends and stores it, effectively recording everything the user types on the keyboard without interrupting it. The attacker either retrieves the key logger at a later date or, for more advanced devices, the key logger periodically sends the attacker a report of all keystrokes it records.

This type of attack can be effective because:

* The attack is stealthy.
* The key logging device is inexpensive.
* Malware scanners cannot detect the device because the device does not add or modify software.
* It works on most operating systems and versions.

Figure 2 shows a typical hardware key logger. Notice that the device hides in plain sight, blending into the cacophony of connectors and plastic at the back of a typical PC.

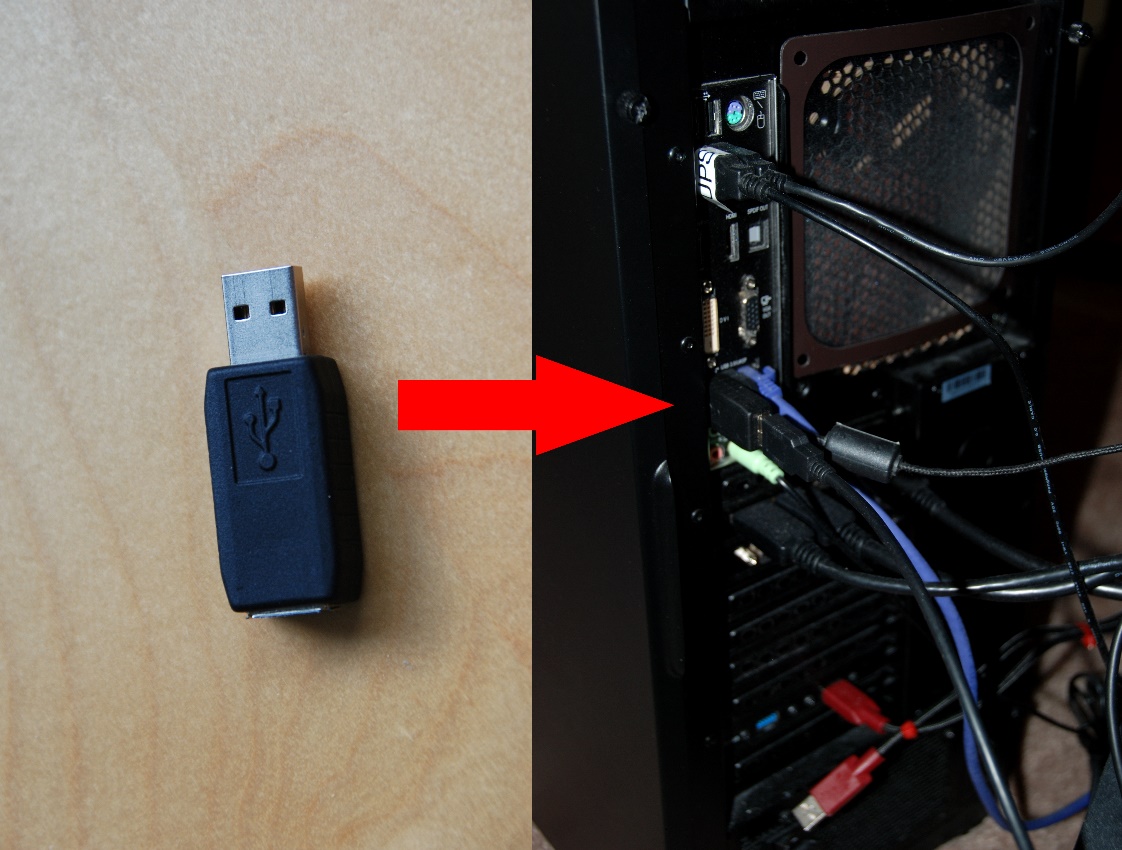


Figure 2. A hardware key logger both on its own and attached to a computer’s USB port

Several mitigations are covered later in this paper that may reduce the impact of hardware key loggers. The primary mitigation is to use multifactor authentication (MFA), including at least one factor that doesn’t use the keyboard, like a smart card or a biometric factor.

|  |
| --- |
| **Note:** |
| Software key loggers also exist and are easier for an attacker to implement than a hardware key logger. In addition, software key loggers present less risk of capture to the attacker. That said, software key loggers are easier to detect. Many antimalware and software-protection solutions automatically detect or block software key loggers, which makes them both a more common and a less successful attack than hardware key loggers. |

### Shoulder surfing

Shoulder surfing is an attack in which an attacker watches a user type his or her user name and password. It is a low-tech attack that requires no special hardware or software: the only real requirements are close physical proximity to the target and the target’s lack of awareness of his or her surroundings.

Shoulder surfing attacks can happen in any location where a user authenticates. The classic examples are employees logging in to their PCs in public places like coffee shops, restaurants, and airports where an attacker can be nearby yet not arouse suspicion. Shoulder surfing also happens in office environments, where an insider wants to impersonate another user without arousing suspicion.

### Credential theft attack risk markers

An organization is at greater risk of a PtH or other credential theft attack if one or more of the following risk factors are present:

* Organizational personnel use high-privilege domain accounts to log on to workstations and servers.
* Applications or services run with high-privilege accounts.
* Scheduled tasks run with high-privilege accounts.
* You grant ordinary user accounts (local or domain) membership to the local Administrators group on their workstations.
* Users can use highly privileged user accounts to browse the Internet from workstations, domain controllers, or servers.
* You configure the same password for the built-in local Administrator account on most or all workstations and servers.

|  |
| --- |
| **Note:** |
| Since the release of the Windows Vista operating system, the built-in Local Administrator account has been disabled by default in Windows operating systems. |

* You don’t enforce account termination for accounts in the Domain Admins, Enterprise Admins, or other high-privilege groups when they are no longer needed.
* You don’t apply security updates quickly to operating systems and applications.
* Users can use privileged accounts that are potentially compromised to log on to less secure computers.
* Operations, processes, and personnel share privileged account credentials.
* Too many administrators use high-privilege accounts for administrative tasks.
* Service accounts have domain administrative privileges.

Recognizing one or more of these risk factors in your organization doesn’t necessarily mean that your organization is vulnerable or has been compromised, but you should consider them when working to protect your organization.

## Credential-protection strategies

You can’t protect what you don’t know or understand, so a critical first step is to identify and prioritize high-value IT and business assets. Such assets may provide access to multiple computers with or without administrative rights or access to sensitive data or resources, or they may allow attackers to perform lateral movement or privilege escalation. (See [Prioritize high-value accounts and computers](#_Prioritize_High-value_accounts) for examples.)

### Consider the attacker mindset

You have to understand your network from the attacker’s perspective, especially during identification and planning. When attackers gain a foothold on a new network, they typically ask:

* What are the assets we want access to (for example., domain controller, certification authority [CA], email server, jump server, Remote Desktop server, file server)?
* Who has access to those assets (who are the administrators on these servers)?
* Where can we get access to those credentials (what servers can we compromise to capture the credentials of a target user or administrator)?
* What do I need to compromise first?

Attackers see a network as a graph of dependencies between computers and accounts (Figure 3). Their goal is to identify a path between a compromised computer and a target computer, account, or group. They will gather as many credentials as possible; each stolen credential grows the graph and puts them closer to their goal. They repeat this process multiple times until they can reach their target.

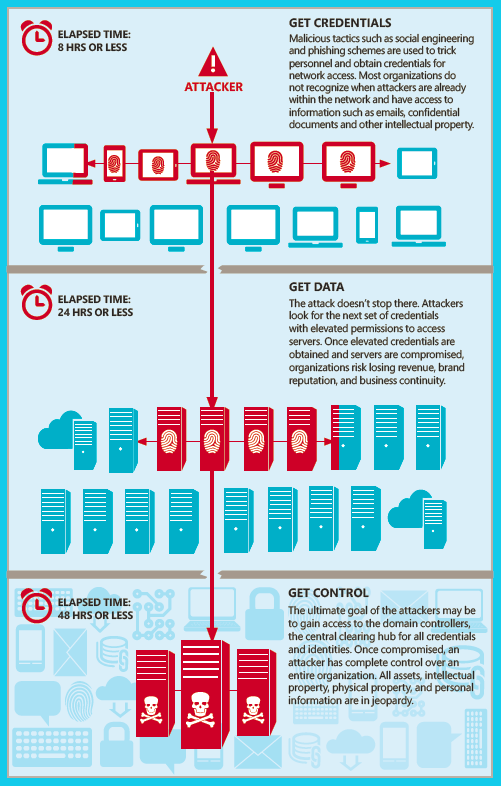


Figure 3. Attack graph

In many cases, an attack graph will look different from normal usage patterns because the attackers may not care about the legitimate access pattern, only what they can use a compromised account or resource to access.

An attacker’s first step is to understand his or her target, so you must take a similar approach. By identifying both legitimate and possible unauthorized access patterns, you can more effectively tailor the strategies this paper describes to your organization.

### Prioritize high-value accounts and computers

Eventually, you need to protect all assets in your organization. Realistically, though, you can’t implement strong security simultaneously across the board. You need to know which assets should come first to help you build an implementation plan. A good place to start when identifying high-value assets is with the accounts and hosts you use to manage IT assets: these elements are the assets attackers target to escalate privileges. Attackers may target other hosts and services for sensitive information or people of interest, however. Examples of targeted high-value accounts and hosts include:

* Hosts that are expected to use high-value accounts:
  + Computers used for administration
  + Computers used for support, such as help desk
  + Patch management servers
  + Security scanners
* Domain administrator and domain administrator–equivalent account members of the following [Active Directory security groups](http://technet.microsoft.com/en-us/library/dn579255.aspx):
  + Domain Administrators
  + Enterprise Administrators
  + Schema Administrators
  + Account Operators
  + Backup Operators
  + BUILTIN\Administrators
* Accounts that administrators use to manage domain controllers. For example, if Microsoft System Center Operations Manager or System Center Configuration Manager runs on domain controllers or any server that a domain administrator–equivalent account logs on to, then System Center Operations Manager and System Center Configuration Manager administrators are effectively domain administrators.
* When a server that contains domain administrator–equivalent credentials is connected to an out-of-band management device (such as a baseboard management controller) that gives physical-equivalent access to a domain controller, the device administrators are domain administrator equivalents.
* Other accounts that have elevated permissions on numerous systems:
  + Service accounts used for software installation or updates
  + Service accounts used for security scans
  + Service accounts for backup
  + Service accounts for third-party agents
  + Shared local administrator accounts
  + Accounts that have access to high-value business assets
  + Email systems
  + File shares
  + Content management systems (such as Microsoft SharePoint)
  + Other important infrastructure
  + Non-IT users who access high-value business assets
  + Executives and directors
  + Researchers
  + Administrative assistants

This list is just a sample of the more common high-value accounts. The specific list of high-value accounts and criteria are different in each organization. You need to consider which apply to your organization. For additional guidance on identifying and prioritizing assets, see [the Privileged Access Workstations page](aka.ms/cyberPAW).

|  |
| --- |
| **Note:** |
| Although prioritizing high value assets is the right approach, you ultimately need to address the security of everything on the network, including the least valuable assets, because these can be weak points that attackers use as leverage. These assets include all user accounts, all service and computer accounts, and all devices, regardless of how the devices are used or by whom. |

### Identify normal behavior

To properly implement mitigations and enable detective controls later, you must identify the current state of existing administrative practices and how you use other high-value accounts. This process may include identifying:

* Who has access to what resource.
* How resources are being accessed.
* Which applications should be run on high-value hosts.

Understanding how these high-value accounts and computers should behave helps you define cases of unauthorized use. You can monitor normal behavior for deviation and protect your systems through mitigations.

### Protect against known and unknown threats

Organizations must consider protection holistically to protect against credential theft. This means implementing controls that protect against two general categories of threats:

* Specific, known threats that you have identified and specific controls mitigate
* Unknown threats that may arise in the future and can be defeated in advance through good security practices and closely monitored hygiene

Your focus should be on attacker containment while ensuring that you deploy mitigations in a meaningful, usable manner. To achieve this, it’s important that you create a containment model as well as reshape credential use and administrative practices. The following section discusses general practices and considerations for architecting a credential theft defense to support this approach prior to implementing and deploying mitigations.

#### Architect a credential theft defense

To create environments resilient to credential theft, you must consider all aspects of credential use and storage. Limit the availability of credentials throughout the life cycle shown in Figure 4 as you use or store them, and ensure that they are transmitted securely.

Figure 4. Credentials use and storage life cycle

In particular, consider credentials that are:

* Stored outside Windows (for example, on sticky notes, in plain-text files, in a credential vault).
* Used during Windows authentication (for example, on keyboards, in smart card readers).
* Being used or cached for later use (on clients or servers).
* In transit over network connections.
* Stored on authoritative stores such as domain controllers and local account databases on local computers.

|  |
| --- |
| **Note:** |
| Be sure to consider any storage systems and devices that contain copies of the operating system, such as storage of virtual hard disks and backups. |

For more information about locally stored credentials, see the Microsoft TechNet article [Cached and Stored Credentials Technical Overview](http://technet.microsoft.com/en-us/library/hh994565.aspx).

Because this white paper assumes a certain degree of account compromise, the remainder of this section focuses on containment, administrative practices, and supplemental general recommendations.

**The value of containment**

Today, large ships are designed with compartments to ensure that no one leak sinks the ship. IT environments should be designed the same way to contain the compromise of any one asset so that it doesn’t lead to a direct loss of confidentiality, integrity, or availability of all assets in the environment.

Because Internet-facing and internal hosts can be compromised at any time, organizations must design an architecture that prevents initial compromises and is adept at containing internal lateral movement and privilege escalations. To establish a strategy to contain such risk, consider segmentation. Segmentation limits the privileges, access, and exposed credentials that an attacker can gain when he or she compromises a resource*.* Segmentation of accounts and networks also enables easier detection of an attacker who tries to remain inconspicuous through captured credentials.

|  |
| --- |
| **Note:** |
| This paper provides detailed account segmentation and containment information. For detailed information about network segmentation using Internet Protocol security (IPsec), see [Microsoft’s IPsec page](https://technet.microsoft.com/en-us/network/bb531150.aspx). |

**Establish a containment model for account privileges**

Consider using this simple model to classify existing resources quickly and set up zones to limit account use. This model adapts the Biba and Bell-LaPadula hierarchical access control models to administrative control and uses three tiers of administrative privilege. Specific business needs may require other tiers or additional segmentation, but this model offers a starting point:

* **Tier 0: Forest admins.** Direct or indirect administrative control of the Active Directory forest, domains, or domain controllers
* **Tier 1: Server admins.** Direct or indirect administrative control over a single or multiple servers
* **Tier 2: Workstation admins.** Direct or indirect administrative control over a single or multiple devices

**Tier definition**

The model is intended to prevent an escalation-of-privilege path for an attacker who is using stolen credentials. It is defined by the following rules:

* Each administrative resource (group, account, server, workstation, Active Directory object, or application) is classified as only one tier.
* Personnel who have responsibilities at multiple tiers will have separate administrative accounts for each required tier. Split any account that currently logs on to multiple tiers into multiple accounts, each of which fits within only one tier definition. Require that each of these accounts have its own password.
* Administrative accounts cannot control higher-tier resources through administrative access such as access control lists, application agents, or control of service accounts. Accounts that control a higher tier cannot log on to lower-tier computers because logging on to such a computer may expose and inadvertently grant control of the account credentials and privileges assigned to that account. Under some exceptions, an attacker could use a feature that supports the Remote Desktop Protocol (RDP) with restricted admin mode without exposing credentials.
* Administrative accounts can control lower-tier resources if their role requires it but only through management interfaces that are at the higher tier and that do not expose credentials—for example, domain admin accounts (tier 0) managing server admin Active Directory account objects (tier 1) through Active Directory management consoles on a domain controller (tier 0).

Figure 5 shows the logon restrictions for this tiered model.



Figure 5. Tiered model showing administrative logon restrictions

#### Implement administrative practices

Containing credential theft risk for administrative accounts typically requires reshaping administrative practices to limit exposure to attackers. As a first step, Microsoft recommends that you:

* Limit the number of hosts on which administrative credentials are exposed.
* Limit role privileges to the minimum required.
* Ensure that IT pros don’t perform administrative tasks on hosts used for standard user activities (for example, email and web browsing).

The next step is to implement logon restrictions and enable processes and practices that adhere to the tier model requirements. Ideally, reduce credential exposure to the least privilege required for the role within each tier (that is, isolation of business groups).

Enforce logon restrictions to ensure that:

* Domain admins (tier 0) cannot log on to enterprise servers (tier 1) and standard user workstations (tier 2).
* Server administrators (tier 1) cannot log on to standard user workstations (tier 2).

|  |
| --- |
| **Note:** |
| Do not add server administrators to the Domain Admin group. Personnel who are responsible for managing domain controllers and enterprise servers should have separate accounts to do so. |

You can enforce logon restrictions through:

* Group Policy logon rights restrictions:
  + Deny access to this computer from the network
  + Deny logon as a batch job
  + Deny logon as a service
  + Deny logon locally
  + Deny logon through Remote Desktop
* Authentication policies and silos.
* Selective authentication (if the account is in another domain, such as a dedicated admin forest).

For more information about these policy settings, see [User Rights Assignment](http://technet.microsoft.com/en-us/library/dn221963.aspx) and [Authentication Policies and Authentication Policy Silos](http://technet.microsoft.com/en-us/library/dn486813.aspx).

In addition, consider other enterprise solutions to manage accounts and restrict access to applications, hosts, and servers:

* Implement temporary admin privileges and passwords.
* Implement mechanisms to rotate password or just-in-time access.
* Implement a dedicated administrative forest.
* Implement network segmentation for client, server, and domain isolation.
* Implement an integrated MFA solution, such as Microsoft Passport.
* Implement a physically separated MFA solution. (See [Azure Multi-Factor Authentication](http://azure.microsoft.com/en-us/services/multi-factor-authentication/?WT.mc_id=azurebg_us_sem_bing_ub_mfa_solutions_mfa&WT.srch=1) for more information.)

#### Harden and restrict hosts for administrative purposes

Any hosts on which administrators enter credentials or perform administrative tasks are entrusted with the privileges associated with the account that administrator uses, even if only temporarily. The act of physically typing a password, smart card PIN, or other verifier or connecting a physical authentication device grants the user permissions to that computer. You should measure the risk to a system by the highest-risk activity a user performs on it, such as Internet browsing, sending and receiving email, or running applications that process unknown or untrusted content.

Administrative hosts include:

* A hardened administrator desktop on which users physically enter credentials.
* Administrative “jump servers” on which users run administrative sessions or tools.
* Servers that host applications that you must administer and that you don’t access through RDP with restricted admin mode or Windows PowerShell remoting. (See [Enable-PSRemoting](http://technet.microsoft.com/en-us/library/hh849694.aspx) for more information about Windows PowerShell remoting.)
* All hosts on which you perform administrative actions, including those that use a standard user desktop running an RDP client to remotely administer servers and applications.

|  |
| --- |
| **Note:** |
| The root of trust must extend from keyboard to server. Just putting a trusted server in the middle without considering the rest of the system is an incomplete solution. If the entry point of the chain—the workstation—is used for higher-risk activities, you must harden and restrict it, as well. |

**Create hardened and restricted administrative hosts**

Although inconvenient, separate hardened workstations dedicated to users who have high-impact administrative credentials may be required to provide a host with a level of security equal to or greater than the level of the privileges entrusted to the credentials. Maintaining security against a determined and talented adversary may require additional measures, such as:

* **Verifying that all media in a build are clean** to defend against malware installed in a master image or injected into an installation file during download or storage.
* **Security baselines**, which you should use as starting configurations. Use the [Microsoft Security Compliance Manager](http://technet.microsoft.com/en-us/library/cc677002.aspx) (SCM) and System Center Configuration Manager to configure the baselines on the administrative hosts.
* **The Unified Extensible Firmware Interface (UEFI) with Secure Boot** and **Measured Boot** to defend against attackers or malware attempting to load unsigned code into the boot process. (See the [Windows 10 security overview](https://technet.microsoft.com/en-us/library/mt601297(v=vs.85).aspx) for more information.)
* **App control** to ensure that only authorized administrative software executes on the administrative hosts. Device Guard provides comprehensive administrative control over software execution on devices. In addition, AppLocker helps prevent malicious software and unsupported applications from executing. Additional information is available in the [Windows 10 security overview](https://technet.microsoft.com/en-us/library/mt601297(v=vs.85).aspx) and the [AppLocker Design Guide](http://www.microsoft.com/en-us/download/details.aspx?id=40330).
* **Disk encryption** to defend against physical loss of computers, such as administrative laptops used remotely. (See [BitLocker](http://technet.microsoft.com/en-us/library/dn641993.aspx) for more information.)
* **USB restrictions** to protect against physical infection vectors. (See [Control Read or Write Access to Removable Devices or Media](http://technet.microsoft.com/en-us/library/cc730808(v=ws.10).aspx) for more information.)
* **Network isolation** to protect against network attacks and inadvertent administrator actions. Host firewalls should block all incoming connections except those explicitly required and block all outbound Internet access.
* **Antimalware software** such as Windows Defender to protect against known threats and malware.
* **Conducting attack surface analysis** to prevent introduction of new attack vectors to Windows during installation of new software. The [Attack Surface Analyzer](http://www.microsoft.com/en-us/download/details.aspx?id=24487) helps you assess configuration settings on a host and identify attack vectors that software or configuration changes introduce.
* **Implement virtualization-based security (VBS) including Device Guard and Credential Guard to more comprehensively isolate critical security components from potential malware threats. These features are described later in this document.**

Some of these measures might seem extreme, but public revelations in recent years have illustrated the significant capabilities that skilled adversaries possess to compromise targets.

#### Considerations for securing forests and domains

A domain or enterprise administrator account has the technical ability by default to exercise control over all resources on a domain, regardless of whether it operates with malicious or benign intent. This control includes the ability to create accounts; read, write, or delete data; install or alter applications; and erase operating systems. If you know that any administrative host you use to manage a domain is compromised, you must consider the entire domain and forest compromised, as well.

#### Recommended credential management practices

You should implement the general recommendations this section provides to ensure that administrative staff are trained, administrative tasks and actions are visible to security personnel, and administrative operations are usable.

**Ensure that users, especially administrators, are well trained**

Organizations should design administrative use processes that are effective and secure, and then educate administrators on the threats to their accounts and privileges as well as how to use these processes to avoid risk. You must apply comprehensive security practices consistently to ensure their effectiveness. Informing and training personnel appropriately increases the chances that they will execute these practices appropriately rather than working around the controls.

**Ensure the visibility and accountability of administrative practices**

Windows records administrative account usage in the Event Log, but you may want to increase the visibility and control of that usage. You can use an identity management tool such as Microsoft Forefront Identity Manager (now [Microsoft Identity Manager](http://blogs.technet.com/b/server-cloud/archive/2014/04/23/forefront-identity-manager-vnext-roadmap-now-microsoft-identity-manager.aspx)) to manage access to privileged groups through workflows. You can also use Microsoft or third-party tools to control and review access to privileged accounts, several of which are described in the white paper [Best Practices for Securing Active Directory](http://www.microsoft.com/en-us/download/details.aspx?id=38785). Increasing visibility and control of administrative practices allows organizations to hold individuals accountable and spot anomalous activity that may indicate compromise.

#### Establish security configurations

To ensure that a weak security configuration doesn’t undermine the credential theft mitigation architecture, be sure to follow and regularly verify recommended security configurations from manufacturers and security vendors.

**Ensure that security configurations are implemented**

Windows hosts can use the [SCM](http://technet.microsoft.com/en-us/library/cc677002.aspx) and System Center Configuration Manager to verify the implementation of host and domain baselines. You should ensure that exceptions are made only when required and that they are applied only after you have reviewed the risks in the tool. Always document the reasons for each exception, and review them regularly to determine whether the reasons are still applicable. If not, remove the exception and apply the baseline.

#### Usability as a security feature

Usability is critical to security, processes, and technology. Design your administrative and maintenance tasks to be both secure and usable. All systems, processes, and configurations can degrade over time. Systems that are difficult to use will accelerate this degradation process significantly because they create incentives for administrators to find easier ways to accomplish daily tasks with little or no regard for security.

To establish usability as a security feature:

* Follow a sample set of users in their daily tasks to identify their important and frequent duties, which aspects of those duties are security sensitive, and how to align security and usability.
* When designing systems, make usability a priority.
* Measure how many steps it takes to accomplish a task, and automate or eliminate steps where possible.
* Perform user acceptance testing of administrative and security systems with administrators and security personnel.
* Repeat these tasks periodically to keep your strategies and countermeasures current.

You can see from the details in this section that credential protection is a complex process. Effective protection requires implementing security countermeasures with people, process, and technology assets. This strategy section covered all three of these asset types. The following sections focus primarily on the technical countermeasures that help prevent and limit the impact of credential theft.

## Primary technical countermeasures for credential theft

This section provides mitigation strategies that you can use in your organization to help prevent both lateral movement and privilege escalation by decreasing the impact of credential theft or illicit reuse on computers running Windows operating systems in your environment. Microsoft has chosen these mitigations from a larger list of considerations because they are effective, practical, and broadly applicable to different domain configurations. In addition, these recommended mitigations don’t have significant prerequisites, so you can deploy them relatively quickly to mitigate credential theft attacks and other, related threats.

|  |
| --- |
| **Notes:** |
| Although the recommended mitigations should have a minimal negative impact for most organizations, Microsoft strongly recommends testing your systems before implementing any mitigation in a production environment. Test each mitigation before implementing it; identify relevant rollback plans, and then gradually deploy any changes to minimize the impact on your organization’s daily IT and business operations. These recommendations are not a substitute for updating and securing your computers against compromise by attackers; rather, they are defense-in-depth measures designed to ensure that your environment is protected even if some measures fail. |

### Use Windows 10 with Credential Guard

An important design consideration for Windows 10 was mitigating credential theft—in particular, derived credentials such as NTLM hashes. A new feature called Credential Guard provides significantly improved security against derived credential theft and reuse by implementing a significant architectural change in Windows designed to help eliminate hardware-based isolation attacks rather than simply trying to defend against them.

Credential Guard protects credential derivatives by running the Windows authentication service known as the Local Security Authority (LSA), and then storing the user’s derived credentials (for example, NTLM hashes, Kerberos keys) within the VBS environment. This environment uses the same type 1 hypervisor technology used to run virtual machines in Microsoft Hyper‑V to isolate LSA in a virtualization-based, protected container. The hypervisor separates the Windows 10 environment from the VBS environment and tightly controls any interaction between the two.

As Figure 6 shows, Credential Guard uses VBS to isolate the LSA process and the user’s derived credentials from both user mode and kernel mode. This means that an attacker who has compromised the operating system core will still be unable to tamper with authentication or access derived credential data. Credential Guard prevents PtH and PtT attacks, which are central to the success of most major network breaches you’ve read about, making Credential Guard one of the most impactful and important features to deploy in your environment.

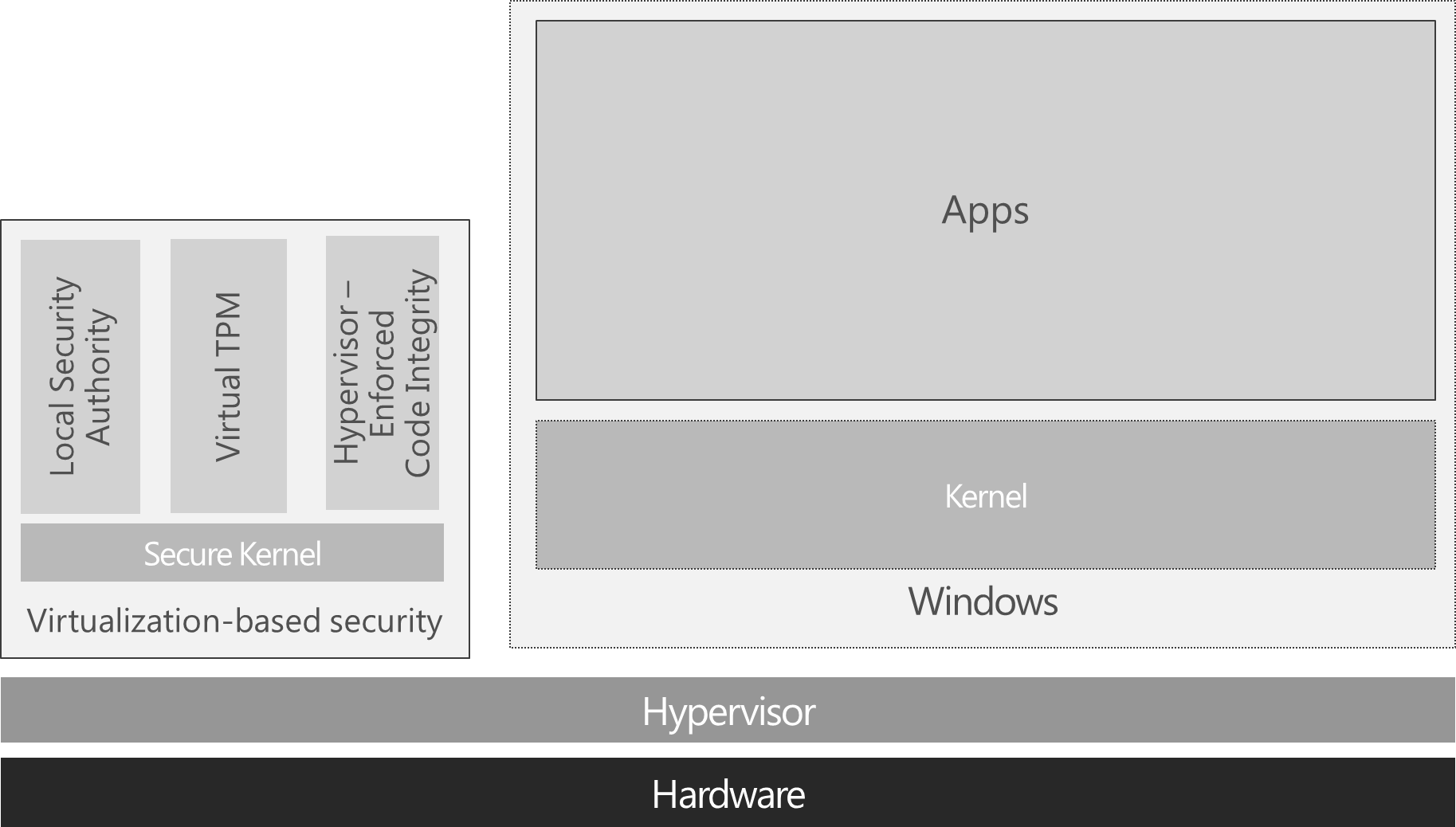


Figure 6. The architecture of VBS

|  |
| --- |
| **Note:** |
| Credential Guard protects against credential theft, preventing an attacker from reading and passing credential derivatives. It does not protect against credential use on a compromised device, however, or against hardware key loggers. |

**Main objective.** This mitigation reduces an attacker’s ability to access and reuse credential derivatives.

**How.** Credential Guard is simple to set up. First, verify that the computers on which domain administrator account and other privileged account logon occurs meet the requirements for Credential Guard:

* UEFI firmware version 2.3.1 or higher, with UEFI Secure Boot and Platform Secure Boot (optionally with a third-party UEFI CA removed from the UEFI database)
* Virtualization support enabled by default in the system firmware (BIOS): virtualization extensions (for example., Intel VT‑x, AMD RVI), second-level address translation (for example, Intel EPT, AMD RVI), and input/output memory management unit (for example., Intel VT‑d, AMD Vi)
* UEFI BIOS configured to prevent an unauthorized user from disabling Device Guard–dependent hardware security features (for example, Secure Boot)
* Kernel mode drivers signed and compatible with hypervisor-enforced code integrity
* Windows 10 Enterprise (x64)
* Windows 10 Hyper‑V and Isolated User Mode features enabled
* In domain environments, computers configured for Credential Guard prior to joining the domain

For details about Device Guard hardware requirements, see the [Device Guard deployment guide](https://technet.microsoft.com/en-us/itpro/windows/keep-secure/device-guard-deployment-guide).

After verifying that the computer meets these requirements, use Group Policy, Local Security Policy, or Unattend settings to enable Credential Guard. For additional details on setting up Credential Guard and its requirements, see [Protect derived domain credentials with Credential Guard](https://technet.microsoft.com/en-us/library/mt483740%28v=vs.85%29.aspx).

**Outcome.** Credential derivatives are isolated against arbitrary access from attackers and are accessible only from trusted Windows components in a strictly managed way. This configuration greatly reduces the potential for credential access or theft from nefarious code and malicious hackers. Other benefits of Credential Guard include preventing authentication downgrade attacks for NTLM and Kerberos, encrypting domain account passwords that Credential Manager stores, and preventing the Terminal Services Security Support Provider (TSPkg) from using the default credentials.

### Restrict and protect high-privilege domain accounts

Some organizations allow high-privilege accounts like those that are members of the Domain Admins group to perform general administrative tasks or log on to user desktops or other systems used for email and Internet browsing, exposing these credentials to potential attackers. Microsoft recommends restricting highly privileged accounts so that they can be used only to log on to sufficiently secured systems that require them. In addition, allowing the use of delegation with privileged accounts can make it easier for an attacker to reuse those accounts to access additional network resources. For details about delegation, see [Delegating authentication](http://technet.microsoft.com/en-us/library/cc739740(v=WS.10).aspx).

**Main objective.** This mitigation restricts administrators’ ability to inadvertently expose privileged credentials to higher-risk computers.

**How.** Complete the following tasks to successfully implement this mitigation:

1. Restrict domain administrator accounts and other privileged accounts from authenticating to lower-trust servers and workstations.
2. Give administrators accounts separate from their typical user accounts that they can use to perform administrative duties.
3. Assign dedicated workstations for administrative tasks.
4. Mark privileged accounts as Sensitive and do not allow them to be delegated in Active Directory.
5. Do not configure services or schedule tasks that use privileged domain accounts on lower-trust systems, such as user workstations.

**Outcome.** An attacker cannot steal credentials for an account if no one uses those credentials on the compromised computer. This mitigation significantly reduces the risk of attackers compromising highly privileged accounts.

For additional guidance on restricting high-privilege domain accounts, see [Privileged Access Workstations](aka.ms/cyberPAW).

### Restrict and protect local accounts with administrative privileges

Attackers can use accounts that offer administrative access on a computer to take full control of that computer. With the computer compromised, the attacker can use the accounts to access other credentials stored on the computer.

|  |
| --- |
| **Recommendation:** |
| If possible, instead of implementing this mitigation, disable all local administrator accounts. |

In addition, many organizations have deployment and operational processes that store the same local administrator account and password on many computers. Identical passwords make it significantly easier for attackers to compromise all computers that use them and obtain all credentials stored on these computers. IT support processes typically don’t require the built-in local administrator account to log on over a network connection, which is a common attack vector for lateral movement based on credential theft.

**Main objective.** This mitigation restricts attackers’ ability to use local administrator accounts or their equivalents for lateral movement PtH attacks.

**How.** Complete one or a combination of the following tasks to implement this mitigation successfully on all computers in your organization:

* Use the [Local Administrator Password Solution (LAPS)](http://aka.ms/laps) to manage local account passwords of domain-joined computers.
* Enforce the restrictions available in Windows that prevent use of local accounts for remote administration.
* Explicitly deny network and Remote Desktop logon rights for all local administrative accounts.
* Create unique passwords for accounts that have local administrative privileges.

**Outcome.** An attacker who successfully obtains local account credentials from a compromised computer won’t be able to use those credentials to move laterally on the organization’s network.

### Restrict inbound network traffic

For an attacker attempting to carry out lateral movement or privilege escalation, he or she must be able to contact other computers on the network.

**Main objective.** This mitigation restricts attackers from moving laterally from a compromised workstation by using the local Windows Firewall to block inbound connections on all workstations.

You can use Windows Firewall on local workstations to restrict inbound traffic to specific services, servers, and trusted workstations you use for desktop management. To do so, deny all inbound access unless explicitly specified in a rule.

Using Windows Firewall to restrict inbound traffic is a simple and robust mitigation that can help prevent attackers from using captured hashes for lateral movement or privilege escalation. This mitigation significantly reduces the attack surface of your organization’s network resources to a PtH attack and other credential theft attacks because it disables an attacker’s ability to authenticate from any given host on a network. Because you may have configured firewall rules that differ from the default rules, this mitigation isn’t universal or fully prescriptive.

|  |
| --- |
| **Note:** |
| Exercise caution when updating or rolling out new firewall rules to prevent outages or connectivity issues with applications that depend on inbound connections to client computers. Don’t follow these instructions if your organization uses another host firewall instead of or in addition to Windows Firewall. |

**How.** This mitigation restricts all inbound connections to all workstations except for those that have expected traffic originating from trusted sources, such as help desk, workstations, security compliance scanners, and management servers.

**Detailed steps.** The recommended strategy for this mitigation is to:

* Block all inbound traffic, and then use rules to allow inbound traffic only by exception. In Windows Firewall, you can use the **Block (Default)** setting to configure all profiles that appear in the snap‑in, as shown in Figure 7.

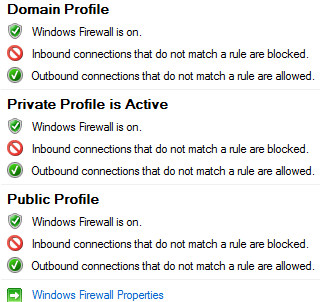


Figure 7. The Block (Default) setting in Windows Firewall

* Enable inbound exceptions for authorized hosts that your organization uses to manage workstations. To enable authorized inbound rules, you must provide IP addresses or subnets on the expected ports and protocols.

|  |
| --- |
| **Note:** |
| Most management software today, including System Center Configuration Manager, use agents that run locally on the organization’s client computers that connect to the management server to receive policy and software updates over the network. These pull operations don’t usually require an inbound firewall exception. Ensure that you test your specific management software and configuration. |

Review your organization’s current inbound rules to ensure that none allows connections from peer workstations that you don’t use to manage computers in your environment.

**Outcome.** This mitigation prevents an attacker from using any type of stolen credentials to connect to other workstations on the network.

#### Use a Group Policy object to set up Windows Firewall rules

Configure a Group Policy object (GPO) to block inbound connections that don’t match a rule, create an allow rule for management servers, and identify whether any other inbound rules can allow inbound authenticated connections. To accomplish this task, you must enable and configure a policy, configure an exception, and then deploy the policy. The following sections provide instructions.

**To enable and configure Windows Firewall inbound policy**

1. As a domain administrator, open the Group Policy Management Console (GPMC).
2. Expand the Group Policy Management node; then, expand Forest, Domains, Domain, and then Group Policy Objects.
3. Right-click **Group Policy Objects**, and then click **New** (Figure 8).

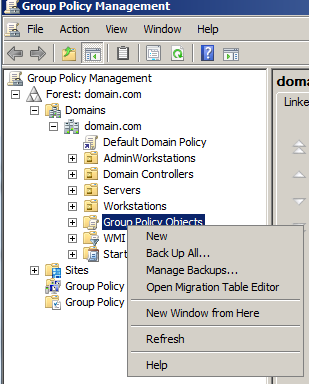


Figure 8. Creating a new GPO

1. Name the new GPO that you will use to configure Windows Firewall settings.
2. Right-click the new GPO, and then click **Edit**.
3. Navigate to Computer configuration\Windows Settings\Security Settings, and then expand Windows Firewall with Advanced Security.
4. Right-click **Windows Firewall with Advanced Security – LDAP://path***,* and then click **Properties** (see Figure 9).

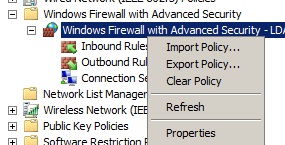


Figure 9. Configuring Windows Firewall properties

1. Enable Windows Firewall, and set inbound connections to **Block (default)** for each profile, as shown in Figure 10.

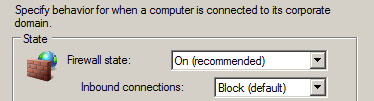


Figure 10. Enabling the firewall and setting connections

1. Select **Settings**; then, under **Rule Merging**, select **No** to prevent local administrators from creating rules that can bypass incoming connection restrictions (allowing all incoming connections).

|  |
| --- |
| **Important:** |
| Allowing firewall rules to merge negates the effect of this mitigation. |

1. Click **OK** to complete the configuration.

**To configure an inbound exception for remote management hosts**

1. As a domain administrator, open GPMC, navigate to Windows Firewall with Advanced Security, and then expand Windows Firewall with Advanced Security – LDAP:// path.
2. Right-click **Inbound Rules**, and then click **New**.
3. For **Rule type**, select **Custom**, and then click **Next**.
4. Select **All Programs**, and then click **Next**.
5. If you know the inbound ports for the management application, configure them at this location. Otherwise, click **Next** to allow all traffic from the management hosts.
6. On the **Scope** page, click **Add** to enter the remote hosts that will initiate network connections to these hosts (see Figure 11).

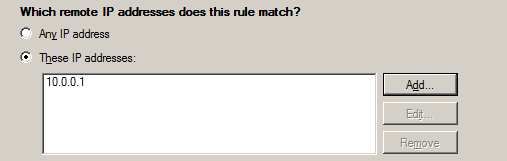


Figure 11. Matching rules to IP addresses

|  |
| --- |
| **Important:** |
| Do not select **Any IP address**. This option leaves this dialog box blank, allowing traffic from any host and thereby defeating the purpose of this mitigation. |

1. Select **Allow the connection**, and then click **Next**.
2. Select all the profiles (**Domain**, **Private**, and **Public**), and then click **Next**.
3. Name the rule, and then create a description that includes which remote applications are allowed to connect through the firewall based on this rule (see Figure 12).

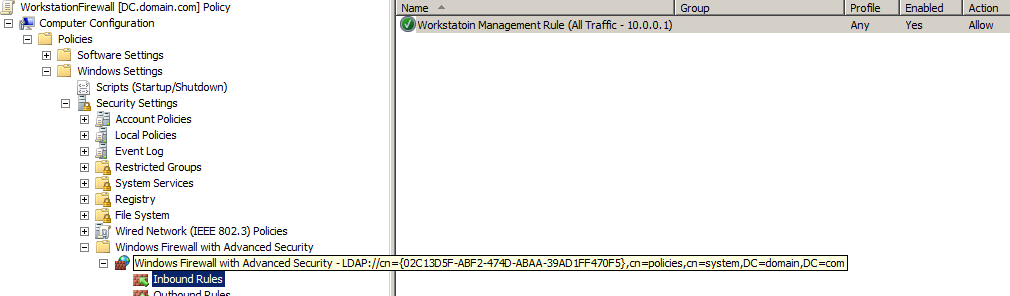


Figure 12. Naming and describing the new rule

**To deploy the GPO**

1. Link the GPO to the first Workstations organizational unit (OU):
2. Navigate to Forest\Domains\Domain\OU Path.
3. Right-click the **Workstation** OU, and then click **Link an existing GPO** (see Figure 13).

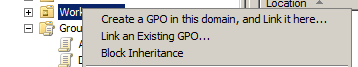


Figure 13. Linking an existing GPO to an OU

1. Select the GPO that you just created, and then click **OK**.
2. Test the functionality of management and other applications on the workstations in the first OU, and resolve any issues the new policy causes.
3. Create links to all other existing OUs that contain workstations.

## Additional technical countermeasures for credential theft

This section discusses additional recommendations for protecting computers against other types of credential theft attacks. These recommendations may not directly protect against PtH attacks or be as effective, practical, or broadly applicable in different domain configurations, but Microsoft strongly encourages you to use them because they significantly increase organizations’ security posture and indirectly protect organizations against these types of attacks.

### Do not allow Internet browsing from highly privileged accounts

Internet activities, such as browsing websites and reading email, are inherently high-risk activities because they process content accessed from the Internet that is potentially malicious or dangerous. If people use user accounts that have administrative rights to perform these activities, a potential compromise on the computer or application can lead to immediate attacker control of those administrative rights. For these reasons, Microsoft recommends that you separate administrative rights from Internet access where possible. To do so:

* Remove standard users from the local Administrators group.
* Configure outbound proxies to deny Internet access to privileged accounts.
* Ensure that administrative accounts do not have email accounts or mailboxes associated with them.

These measures help to separate untrustworthy Internet content and code from trusted corporate assets.

### Remove standard users from the local Administrators group

Microsoft recommends that you not grant membership in the local Administrators group on organization workstations to standard user accounts that run Internet applications, such as those used for web browsing and email. Many organizations have already implemented this configuration, and others are implementing it as they deploy the latest Windows operating systems.

This strategy strengthens an organization’s resilience to a PtH attack by increasing the barrier an attacker must overcome to obtain the local administrative access required to start a credential theft attack. An attacker who has compromised a standard domain user account must overcome the additional operating system security boundary to elevate him- or herself to the administrator level and steal credentials. If the user isn’t a member of the local Administrator group, attackers who attempt to compromise a user account must find a different way to elevate their privileges locally.

Although restricting administrative rights is a strong defense against PtH attacks and credential theft, it may not be feasible to apply this mitigation in some organizations. For example, some organizations may not have a robust management infrastructure designed to handle administrative tasks that users can no longer perform. Other organizations may depend on legacy applications that don’t work correctly without administrative rights.

|  |
| --- |
| **Note:** |
| The latest Windows operating systems include a set of technologies known as User Account Control (UAC), which are designed to help users run tasks without administrative privileges, thereby mitigating the impact of malicious programs. For more information about UAC, see the [User Account Control Technical Reference](http://technet.microsoft.com/en-us/library/dd835546(v=ws.10).aspx). |

If a large number of standard users in your organization are currently operating with local administrative privileges, converting these users to standard privileges should include the following activities:

* Use application compatibility testing to ensure that legacy applications continue to operate correctly for standard users.
* Use deployment processes and tools to deploy new software and updates without administrative rights.
* Update help desk and support processes to ensure that support is available for users who don’t have local administrative rights.

### Use remote management tools that don’t place reusable credentials on a remote computer’s memory

Some remote authentication methods allow you to perform administrative tasks on the remote computer without storing the administrator account password hash, Kerberos tickets, or other reusable credentials in the remote computer’s memory. Therefore, use only management tools that include these authentication mechanisms to help reduce the risk of PtH attacks.

See [Securing Privileged Access Reference Material](http://aka.ms/logontypes) for more information about these logon types and tools.

|  |
| --- |
| **Note:** |
| This mitigation is most effective when you use a dedicated administrative workstation. |

### Update applications and operating systems

Applications or operating systems that have not been updated contribute to credential theft attacks because they provide an avenue for well-known, published exploits to circumvent security controls or elevate privileges. By applying updates to operating systems and applications, you force attackers to find unknown vulnerabilities or other means of attack that require user interaction.

Numerous solutions can automate the deployment of operating system and application updates. Beyond the basic Windows Update feature built into all current versions of Windows, Windows Server Update Services and System Center Configuration Manager automate and provide centralized administration of Microsoft product updates. Other, third-party products can be highly effective, as well.

### Limit the number and use of privileged domain accounts

By granting membership in the Administrators, Domain Admins, or Enterprise Admins group in a domain or forest, you inadvertently create high-value targets for attackers. The greater the number of members in these groups, the greater the likelihood that a privileged user may inadvertently misuse these credentials and expose them to attackers.

Every workstation to which a privileged domain user logs on provides another location from which an attacker can steal privileged credentials. Microsoft strongly advises that you reduce membership in privileged groups and stringently control where and how privileged accounts are used.

### Secure and manage domain controllers

Because domain controllers store the credential password hashes of all accounts in the domain, they are a high-value target for attackers. If you don’t stringently update and secure your domain controllers, attackers may compromise them and the domain (and possibly the forest) through a vulnerability that you haven’t addressed. Microsoft recommends that you ensure that the domain controllers in your environment don’t run unnecessary software, that you update them promptly and regularly, and that you configure them with the appropriate security settings.

Installed applications and management agents on domain controllers may provide a privilege escalation path by which attackers can compromise the management service or administrators of that service. Consider the management tools and services your organization uses to manage domain controllers and their administrators equally important to the security of the domain controllers and domain administrator accounts. Secure these services and administrators with equal effort.

For more information, see [Microsoft Security Compliance Manager](http://technet.microsoft.com/en-us/library/cc677002.aspx).

### Remove LAN Manager hashes

Disable and remove LAN Manager (LM) hashes in your computer’s local SAM and Active Directory domain databases to reduce the risk of attackers obtaining these legacy password hashes. You may have LM hashes for one or more user accounts if either of the following conditions is true:

* You used a pre–Windows Server 2008 operating system to create your domain.
* You have replaced the Group Policy setting **Default Domain Policy Group policy object** with **Network security: Do not store LAN Manager hash value on next password change**.

When a user changes his or her password, Active Directory always stores a copy of the NT hash. Active Directory can also store an LM hash if the password is compatible with LM and the setting **Network security: Do not store LAN Manager hash value on next password change** is disabled. This setting is enabled by default in Windows operating systems, starting with the release of Windows Vista and Windows Server 2008. Note, however, that using a GPO that has this setting disabled may cause it to persist in a domain upgraded from the Windows Server 2003 operating system or earlier. In addition, any user who has not changed his or her password since the setting was enabled still has an LM hash in his or her account if the password is LM compatible.

To ensure that your Active Directory and SAM databases no longer store LM hash values, complete the following tasks:

* Enable the **Network security: Do not store LAN Manager hash value on next password change** setting in the Default Domain Policy.
* Ensure that all users change their passwords.

For more information about this GPO, see [Network security: Do not store LAN Manager hash value on next password change](http://technet.microsoft.com/en-us/library/cc757582(v=WS.10).aspx).

|  |
| --- |
| **Note:** |
| Some older applications, operating systems, and services may still rely on LM hashes for authentication, so Microsoft recommends that you test this change before you implement it. To test for incompatibility, configure an account with a password or passphrase that is longer than 15 characters. This configuration prevents storage of the LM hash for the account, which you can use to test applications for compatibility. |

### Disable the NTLM protocol

Restricting NTLM completely in an environment helps mitigate PtH attacks and offers added security benefits. However, this restriction doesn’t qualify as a mitigation that Microsoft recommends because most organizations cannot easily implement it and it doesn’t mitigate theft and reuse of Kerberos tickets or passwords.

The requirements for most organizations to restrict and effectively disable NTLM include, at a minimum, the following tasks:

* Extensive discovery analysis for incompatible devices and applications
* Discovery of non-Windows operating system dependencies (if applicable)
* Planning, testing, and implementing changes to address all discovered compatibility issues (potentially including hardware and software replacements)
* Ensuring that all Kerberos prerequisites have been met completely and configured for all applications and services in the environment

Even with extensive NTLM restrictions in the environment that mitigate PtH attacks, attackers may still be able to steal and reuse other credentials, including Kerberos TGTs and plain-text passwords. Disabling NTLM doesn’t constitute a proposed mitigation, but Microsoft still encourages you to implement Kerberos, if possible, because it does not plan to enhance the NTLM protocol.

For more information about how to restrict NTLM, see the [Auditing and restricting NTLM usage guide](http://technet.microsoft.com/en-us/library/jj865674(v=ws.10).aspx).

## Other potential countermeasures for credential theft

This section discusses other commonly proposed mitigations that don’t provide a meaningful mitigation of credential theft and reuse directly but may have other positive security or operational impacts on an Active Directory domain environment.

### Use MFA for user accounts

MFA methods such as smart cards can greatly strengthen the proof of the user’s identity if the host is secure, but these methods don’t provide absolute immunity from credential theft attacks. Although multiple factors are required for initial logon, Windows uses standard Kerberos and NTLM authentication protocols that exchange single-factor authenticators to communicate with other domain computers, as the protocol standards require. When a computer in the domain is compromised and a user uses MFA to log on to it, the attacker can steal these authenticators’ LSASS process memory and reuse them in exactly the same way as a user logged on with a password.

|  |
| --- |
| **Note:** |
| If the account is enabled for smart card use and still has a valid password, the NT hash in LSASS process memory is the hash of the user’s password. If you have configured the account with the attribute **Smart Card required for interactive logon**, then the NT hash is a random value calculated when that attribute was enabled for the account. LSASS provides this password hash to the client computer during the smart card logons that the domain controller processes. The password hash that is automatically generated when the attribute is set doesn’t change. For more information, see [[MS-PAC]: Privilege Attribute Certificate Data Structure](http://msdn.microsoft.com/en-us/library/cc237917(prot.20).aspx). |

Another factor to consider is that MFA is typically available only for interactive logons, including local logons (Interactive) and RDP (RemoteInteractive) logons, so the account attribute can enforce smart card MFA only for those logon types.

### Use Microsoft Passport and Windows Hello

Windows 10 delivers two new authentication components that work together: Microsoft Passport and Windows Hello. Microsoft Passport provides strong two-factor authentication (2FA), fully integrated into Windows, and replaces passwords with the combination of an enrolled device and either a PIN or Windows Hello. Microsoft Passport is, from a security perspective, similar to smart cards but more flexible. Authentication is performed by using an asymmetric key pair instead of a string comparison (for example, password), and you can use hardware to secure the user’s key material.

Unlike smart cards, Microsoft Passport doesn’t require the extra infrastructure components required for smart card deployment. In particular, you don’t need a public key infrastructure (PKI) for client keys. If you already use PKI—for example, in virtual private network (VPN) authentication—you can use the existing infrastructure with Microsoft Passport. Microsoft Passport combines the major advantages of smart card technology—deployment flexibility for virtual smart cards and robust security for physical smart cards—without any of their drawbacks.

Microsoft Passport offers three significant advantages over the current state of Windows authentication: it’s more flexible, it’s based on industry standards, and it effectively mitigates risks. The sections that follow look at each advantage in more detail.

#### It’s flexible

Microsoft Passport offers unprecedented flexibility. Although the format and use of passwords and smart cards is fixed, Microsoft Passport gives both administrators and users options to use and manage authentication.

First and foremost, Microsoft Passport works with biometric sensors and PINs. Next, you can use your PC or even your phone as one of the factors to authenticate on your PC. Finally, your user credentials can come from your PKI infrastructure, or Windows can create the credential itself.

Microsoft Passport gives you options beyond long, complex passwords. Instead of users memorizing and retyping often-changed passwords, Microsoft Passport enables PIN- and biometrics-based authentication through Windows Hello to securely identify users. These benefits deliver simplified MFA solutions that together provide stronger security than any single factor. For example, a PIN by itself is not a strong proof of identity, but as part of an MFA solution it is quite valuable.

With Microsoft Passport, you gain flexibility in the data center, too. You can either add on-premises Windows Server 2016 Preview domain controllers or use Microsoft Azure Active Directory (Azure AD) to deploy Microsoft Passport to your network. The choice of which users to enable for Microsoft Passport is completely up to you: you choose which authentication factors you want to support. This flexibility makes it easy to use Microsoft Passport to supplement existing smart card or token deployments: simply add convenient 2FA or deploy Microsoft Passport in scenarios that call for extra protection for sensitive resources or systems. Microsoft plans to offer client updates to support additional scenarios in the future.

#### It’s standardized

Both software vendors and enterprise customers have come to realize that proprietary identity and authentication systems are a dead end: the future lies with open, interoperable systems that allow secure authentication across a variety of devices, line-of-business applications, and external applications and websites. To this end, a group of industry players formed FIDO, the Fast IDentity Online Alliance. The FIDO Alliance is a nonprofit organization intended to address the lack of interoperability among strong authentication devices as well as the problems users face in creating and remembering multiple user names and passwords. The FIDO Alliance plans to change the nature of authentication by developing specifications that define an open, scalable, interoperable set of mechanisms that supplant reliance on passwords to securely authenticate users of online services. This new standard for security devices and browser plug‑ins will allow any website or cloud application to interface with a broad variety of existing and future FIDO-enabled devices that the user has for online security.

In 2014, Microsoft joined the board of [the FIDO Alliance](https://fidoalliance.org/). FIDO standards enable a universal framework that a global ecosystem delivers for a consistent and greatly improved user experience of strong password-less authentication. The FIDO 1.0 specifications, published in December 2014, provide for two types of authentications: password-less (known as *UAF*) and second factor (U2F). The FIDO Alliance has completed the 2.0 specification, which incorporates the best ideas from its U2F and UAF FIDO 1.0 standards and of course new ideas. Microsoft contributed Microsoft Passport technology and design to the FIDO 2.0 specification workgroup, which later ratified the design in the 2.0 specification. Interoperability of FIDO products is a hallmark of FIDO authentication. Microsoft believes that bringing a FIDO solution to market will help solve a critical need for enterprises and consumers alike. Microsoft has built Microsoft Passport as a reference implementation of the draft FIDO 2.0 specification and continues to work with the FIDO Alliance as the FIDO 2.0 specification moves forward.

#### It’s effective

Microsoft Passport effectively mitigates two major security risks. First, it eliminates the use of passwords for logon and so reduces the risk that a nefarious attacker will steal and reuse the user’s credentials. The user device’s Trusted Platform Module (TPM) generates and protects user key material, when present, which protecting it from attackers who want to capture the key material and reuse it. Second, because Microsoft Passport uses asymmetrical key pairs, users credential can’t phished or stolen in cases where the identity provider or websites the user accesses have been compromised.

To compromise a Microsoft Passport credential that a TPM protects, an attacker must have access to the physical device, and then must find a way to spoof the user’s biometrics or guess his or her PIN—and all of this must be done before TPM anti-hammer capabilities lock the device. This technology sets the bar much higher than password phishing attacks.

### Windows Hello

Windows Hello is the name given to the new biometric sign-in option for Microsoft Passport. Because biometric authentication is built directly into the operating system, Windows Hello allows users to unlock their devices and credential store by using their face or fingerprint. From here, Windows performs authentication by using the Microsoft Passport credential, which is effectively the device itself.

The user’s biometric data used for Windows Hello is considered a local gesture and consequently doesn’t roam among a user’s devices and is not centrally stored. The biometric image of the user that the sensor takes is converted into an algorithmic form that cannot be converted back into the original image that the sensor took. If multiple users share a device, each user will be able to enroll and use Windows Hello for his or her Windows profile.

Windows Hello supports two biometric sensor options that are suitable for enterprise scenarios:

* **Facial recognition** uses special infrared (IR) cameras to reliably tell the difference between a photograph or scan and a living person. Several vendors are shipping external cameras that incorporate this technology, and major manufacturers are already shipping integrated devices with facial-recognition technology.
* **Fingerprint recognition** uses a fingerprint sensor to scan the user’s fingerprint. Although fingerprint readers have been available for computers running Windows for years, the detection, antispoofing, and recognition algorithms in Windows 10 are more advanced than in previous Windows versions. Most existing fingerprint readers (whether external or integrated into laptops or USB keyboards) can be used with Windows Hello.
* **Iris scanning** uses cameras designed to scan the user’s iris, the colorful and highly detailed portion of the eye. Because the data must be accurate, iris scanning uses a combination of an IR light source and a high-quality camera. Microsoft Lumia 950 and 950 XL devices support this technology.

Windows Hello offers several major benefits. First, it addresses the problems of credential theft and sharing because an attacker must obtain the device and impersonate the user’s biometric identity, which is more difficult than stealing a password by shoulder surfing. Second, the use of biometrics gives users an authenticator that’s always with them—there’s nothing to forget, lose, or leave behind. Instead of worrying about memorizing long, complex passwords, users can take advantage of a convenient, secure method for logging in to all their Windows devices. Finally, there’s nothing additional to deploy or manage. Because Windows Hello support is built directly into the operating system, there are no additional drivers to deploy.

For more information about Microsoft Passport and Windows Hello in Windows 10 see the [Microsoft Passport guide](https://technet.microsoft.com/en-us/library/mt589441(v=vs.85).aspx).

### Use jump servers to administer isolated network segments

Jump servers are special-purpose computers typically used for administrative access to isolated or segmented networks. These servers consolidate administrative tools and activities, and you can use them to restrict access to different security zones.

Although jump servers can provide utility in security architectures, they don’t directly mitigate credential theft and reuse attacks. You cannot maintain security integrity if a user connects to an administrative jump server from a lower-trust workstation. In other words, if the host connecting to a jump server is already sufficiently trusted, the jump server doesn’t provide additional security. These servers can provide value as part of a more comprehensive security architecture, however. For example, you can use them as part of a strategy for monitoring unauthorized activity. If policy requires administrators to perform all administrative tasks from jump servers, authentication that doesn’t originate from those jump servers would be immediately suspicious.

### Restart computers after logoff

Restarting computers after privileged administrators have logged off may have a positive mitigating effect prior to a PtH attack. Restarting computers after use is the most effective way to remove credentials from stale or leaked logon sessions from memory.

|  |
| --- |
| **Note:** |
| For this option to be effective, the restart must be a full reboot, or “cold boot.” Warm reboots (restarting the device without a power-down) can result in system memory retaining information from the prior boot sequence, which attackers can access. A cold boot is much less likely to retain accessible information in system memory. |

Such restarts are useful for limiting risk in the event an attacker later compromises a running computer, but restarting isn’t a recommendation in this document because it has no meaningful effect on an already-compromised computer. Attackers can capture credentials as soon as a logon has succeeded, and they can easily automate the capture of credentials. For these reasons, limiting the duration of the logon session or any potential lingering stale session—even signing out of the account—may have a limited effect on preventing a PtH attack.

## Detecting credential attacks

Detection is an important part of a security strategy because it provides an alert that suspicious activity is happening in addition to the data needed to investigate and evaluate that activity. Detective controls are a key dependency for proper response and remediation because you need data to understand what attackers are targeting and the extent of their network reach.

PtH and other credential theft attacks typically consist of two steps: the attacker steals the credentials, and then uses them to obtain unauthorized access to resources and extend control over the network. The attacker may also use a compromised user (nonadministrative) session to obtain access to a resource for which that user has administrative rights, and then escalate privileges.

Detective controls are more effective for credential use because credential theft detection relies on retrieving events from a compromised computer. An attacker who uses stolen credentials may trigger suspicious events in a network while accessing resources. Detecting this illicit credential use is possible but requires that you separate attacker activity from high volumes of legitimate events.

In most scenarios, it’s important that you prioritize deploying detection for high-value accounts or computers that attackers are more likely to target. Note that each network environment is different, and high-value accounts are not necessarily just domain-privileged accounts; nonprivileged domain accounts may have access to sensitive information, as well.

### Detect use of stolen credentials

Attackers who use stolen credentials to navigate networks are impersonating valid users, which makes detection on complex networks difficult. The key is that these attackers use these stolen credentials for unauthorized access, which may provide an opportunity for detection.

Detection is most efficient when performed on well-structured networks in which high-value account usage is clearly defined. Every activity that’s outside the previously observed or approved use of a high-value account should generate a report for analysis and possible correction of the detection pattern. Detection can also complement mitigations by ensuring that you applied them correctly.

Microsoft Advanced Threat Analytics (ATA) is an effective solution that helps you detect the use of stolen credentials as well as identify breaches and threats. For more information about ATA, see the [Microsoft Advanced Threat Analytics page](https://www.microsoft.com/en-us/server-cloud/products/advanced-threat-analytics/overview.aspx).

Specific indicators for detecting anomalous activity may include:

* Where the account was used (source or destination).
* When the authentication occurred (such as when a user is on leave or vacation or outside working hours).
* Unusual or unexpected account creation (for example, domain accounts created outside the provisioning system or local accounts are created on a server).
* The account being used to perform unusual activity (for example, to change settings, authentication policy failures).
* Detection of known and unknown malicious executables.
* Multiple unrelated high-value accounts used from the same host (for example, domain admin credentials and service accounts used from same host).
* Multiple accounts from different owners authenticating within a short period of time from the same computer in the same session.
* Modification of sensitive objects (for example, a change in Domain Admins membership).
* Mismatches between an account used for perimeter access, such as a VPN, and the account used to access resources.

### Collect computer events

This section provides a list of recommended events worth collecting from computers to help you detect credential theft. Many events are available on different versions of Windows, and it's important to assess which events you should collect for specific environments to enable detection as well as to make response and remediation easier.

#### Data collection

Events to collect include:

* Application execution events (on any monitored computer):
  + Event ID 4688 – A new process has been created
  + Key fields: Account Name, New Process Name
* Authentication events (on any monitored computer):
  + Event ID 4648 – A logon was attempted using explicit credentials
  + Key fields: Account Name (Subject), Account Name (account whose credentials were used), Process Name
  + Event ID 4624 – An account was successfully logged on
  + Key fields: Account Name, Logon type
* Kerberos events on domain controllers:
  + Event ID 4769 – A Kerberos service ticket was requested
  + Key fields: Account Name, Service Name, Client Address
  + Event ID 4768 – A Kerberos authentication ticket (TGT) was requested
  + Key fields: Account Name, Service Name, Client Address
  + Event ID 4776 – The domain controller attempted to validate the credentials for an account
  + Key fields: Logon Account, Source Workstation
* Authentication policies and authentication policies silo events on domain controllers:
  + In Applications and Services logs at Microsoft\Windows\Authentication
  + Under **ProtectedUserFailures-DomainController**
* Events generated when an account that is a member of the Protected users security group tries to use blocked authentication options:
  + Event ID 100 – NTLM usage attempted
  + Event ID 104 – DES or RC4 attempted for Kerberos Authentication
  + Under **AuthenticationPolicyFailures-DomainController**
* Events that are generated when someone uses an account outside the allowed authentication policy silos:
  + Event ID 101 – NTLM usage attempted
  + Event ID 105 – Kerberos authentication from a particular device was not permitted
  + Event ID 106 – The user or device was not allowed to authenticate to the server
  + Event ID 305 – Kerberos TGT request did not meet access control restrictions
  + Event ID 306 – User, device, or both do not meet the access control restrictions
* Events that are generated by Credential Guard:
  + Event ID 13 – Credential Guard (LsaIso.exe) was started and will protect LSA credentials.
  + Event ID 14 – Credential Guard (LsaIso.exe) configuration: 0x1, 0
  + The first value: 0x1 means Credential Guard is enabled. 0x0 means it’s disabled.
  + The second value: 0 means Credential Guard is configured to run in protect mode. 1 means it’s configured to run in test mode. This value should always be 0.
  + Event ID 15 – Credential Guard (LsaIso.exe) is configured but the secure kernel is not running; continuing without Credential Guard.
  + Event ID 16 – Credential Guard (LsaIso.exe) failed to launch
  + Event ID 17 – Error reading Credential Guard (LsaIso.exe) UEFI configuration

#### Detect LSA plug-ins and drivers that fail to run as a protected process

If you have enabled audit mode for the LSASS, you will see a generated event when Lsass.exe attempts to load an unauthorized driver. See the TechNet article [Configuring Additional LSA Protection](http://technet.microsoft.com/en-us/library/dn408187.aspx) for details.

* In Applications and Services Logs\Microsoft\Windows\CodeIntegrity:
  + Event ID 3065 – Code integrity check determined that a process attempted to load a particular driver that did not meet the security requirements for Shared Sections. However, due to the system policy that is set, the image was allowed to load.
  + Event ID 3066 – This event records a code integrity check that determined that a process (usually lsass.exe) attempted to load a particular driver that did not meet the Microsoft signing level requirements. However, due to the system policy that is set, the image was allowed to load.

#### Other events

Observe systems that run applications to restrict software or monitor system changes, antimalware, or other applications that may provide relevant information about PtH and related attacks. In addition, monitor access logs for supporting infrastructure, such as firewalls and VPNs. Evaluate what other software and infrastructure events are relevant when you implement your detection strategy. This information will be invaluable when investigating attacks and successful breaches.

If your organization uses Azure AD, it can also benefit from machine learning and other geo-location detection of malicious activities for Azure AD cloud accounts. See [Azure Active Directory Identity and Access Management for the Cloud](http://azure.microsoft.com/en-us/services/active-directory/) for more information.

#### Manage event collection and alerts

Multiple options exist for centralized event log collection and management, including [Windows Event Collector](http://msdn.microsoft.com/en-us/library/windows/desktop/bb427443(v=vs.85).aspx) and [Audit Collection Services](http://technet.microsoft.com/en-us/library/bb381258.aspx). Third-party solutions such as security information and event management solutions may provide agents for collection and alerting for specific events. Enable log collections for as many computers as possible, and configure these logs to push the events from these computers quickly. For example, you could configure the Windows Event Collector with a latency time of 0 to ensure that events are sent as soon as possible to the collector.

For additional information about detection, see the National Security Agency/Central Security Service document [Spotting the Adversary with Windows Event Log Monitoring](http://www.nsa.gov/ia/_files/app/Spotting_the_Adversary_with_Windows_Event_Log_Monitoring.pdf).

## Responding to suspicious activity

A key element of a comprehensive security strategy is the ability to respond to suspicious activity quickly and ensure that you engage the right resources to evaluate, prioritize, investigate, and act on events. Some alerts may warrant immediate response, while you can give others lower priority to ensure that you reserve resources for the most important events.

Microsoft recommends that you integrate the following elements in an incident response process:

* Regularly update protection and detection mechanisms to limit false-positive alerts from reoccurring.
* After each significant security event or compromise, update protection and detection mechanisms to prevent future attacks from reoccurring.
* After a compromise, continue with close observation of affected hosts and accounts to ensure that the attacker is not able to regain access.
* If a compromise has occurred, proceed to recovery plans and ensure that you have properly addressed attack vectors.
* Consider delaying recovery efforts to track attacker behavior and uncover the intent or attack details. This information could lead to a better recovery strategy.

### Investigate attacks

The most important part of developing an investigation strategy is to obtain enough details about an attack to determine the scope of the breach. Adversaries typically obtain a keychain of valid domain credentials in an attack, and any individual credential compromise could be a sign of a larger problem.

Attackers typically need to reacquire credentials periodically: their keychain of stolen credentials will naturally degrade over time because of password changes and resets. Therefore, attackers frequently maintain a foothold in the compromised organization by installing backdoors and maintaining credentials from a number of computers in the environment. This pattern supports both the reacquisition of credentials and other functions, like remote access. Tracing the access chain backwards may lead to the discovery of other computers involved in the breach. Sometimes, an attacker’s presence is limited to a single compromised host; other times, a large number of compromised hosts harvest credentials, and a smaller number of hosts “manage” these compromised hosts.

When investigating activity on compromised hosts, you may want to use command-line auditing. Command-line auditing may provide further insight into what an attacker is doing on each host. It provides command-line information for every process logged in plain text in the security event log as part of the Audit Process Creation event 4688 – A new process has been created on the workstations and servers on which you have applied this policy setting.

|  |
| --- |
| **Note:** |
| For security and privacy reasons, Microsoft does not recommend enabling command-line auditing permanently. When you enable this policy setting, any user who has read access to security events will be able to read the command-line arguments for any successfully created process. Command-line arguments can contain sensitive or private information, such as passwords or user data. |

To enable this feature for a computer or user, set **Software\Microsoft\Windows\CurrentVersion\Policies\System\Audit\ProcessCreationIncludeCmdLine\_Enabled**to **1** or establish a policy change. For more information, see the TechNet article [Command line process auditing](http://technet.microsoft.com/en-us/library/dn535776.aspx).

Microsoft ATA is another tool you should consider. ATA can help you detect the use of stolen credentials as well as identify breaches and threats. For more information about ATA, see [Microsoft Advanced Threat Analytics](https://www.microsoft.com/en-us/server-cloud/products/advanced-threat-analytics/overview.aspx).

### Recover from a breach

After a successful credential attack, the highest priority should be to recover control over the compromised assets. Unfortunately, the traditional disaster recovery approach of restoring from a recent backup is often ineffective because organizations typically don’t detect attacks immediately. This section provides considerations for recovering accounts and domain integrity when restoring from a backup isn’t viable.

### Recover accounts

In the event of a compromise, you must take action to recover control of the compromised accounts. These practices are effective only if you’re extremely confident that attack didn’t compromise the domain.

The following recovery practices have limitations, and you should evaluate them carefully before executing them. It is also imperative that you identify the root cause of a breach for the following recommendations to be effective and prevent attackers from regaining access.

#### Change compromised account passwords

The idea is straightforward: the adversary has user and computer credentials, so changing the affected accounts’ passwords reclaims control of these accounts.

**Methods:**

* Set passwords to require a change at the next logon. One benefit of doing so is that other types of credentials such as smart cards will be unusable until users have reset their passwords.
* Manually change passwords in Active Directory Domain Services (AD DS). Additional use of the previously compromised credentials will result in failed logon attempts.
* Consider resetting computer account credentials if a computer has been compromised.

|  |
| --- |
| **Note:** |
| Windows uses computer account passwords to prove the computer’s and the domain controller’s identity to each other. Attackers can use these secrets for attacks that restrict access based on the machine account (for example, authentication policies). |

For more information, see [Reset a Computer Account](http://technet.microsoft.com/en-us/library/cc753596.aspx).

* Reset NT hashes for smart card–enforced accounts by disabling and re-enabling the account attribute **Smart card is required for interactive logon**.

For more information, see [Settings for default local accounts in Active Directory](http://technet.microsoft.com/en-us/library/dn745899.aspx#Sec_Account_Settings).

**Considerations:**

* This approach is effective only against future authentications. Resources such as shares and named pipes that the attacker used the compromised credentials to access will remain available until the logon session that granted access is terminated.
* If the host is offline during this practice, the attacker can still use cached logon password verifiers locally.
* This action will likely inform the attacker that the organization has detected the breach.
* The attacker can persist on a compromised host by using keystroke loggers or other malware and may be able to steal the new password.
* The attacker can persist in the context of the user by using malware installed in the user’s profile.

#### Disable an account, and remove group memberships

The idea here is to restrict or remove the privileges associated with the compromised account.

**Methods:**

* Disable the account in AD DS.
* Remove the account from Active Directory security groups and any local security groups.

**Considerations:**

* This approach is effective only against future authentications. When Windows creates the security token, it hard-codes the group membership in the token. Therefore, any process that is already running with that token will run with the original permissions of the account even after you remove the account from the security group.
* This action will likely inform the attacker that the organization has detected the breach.

### Restore the integrity of the domain and forest

Because many AD DS implementations have been in operation for years and so at risk of credential theft, organizations should assume breach and consider the very real possibility that they may have an undetected compromise of domain or enterprise administrator credentials. If your organization suspects domain compromise, consider engaging professional incident response services.

Recovering the integrity of a large and complex IT environment is a particularly challenging undertaking because such systems consist of many individual nodes, each of which is itself complex and difficult to assess or clean quickly. If your organization is planning a full recovery, you must address several requirements:

* **Disrupt an adversary’s current operation.** It’s a daunting task to remove the elements of control that an adversary who has domain administrator access can implant—a task that requires incident details. In some scenarios, you might not want to disable an attacker’s account immediately because leaving it intact can help you better understand the attacker’s actions or intent. In other scenarios, you might want to block a compromised account immediately to observe the attackers use of another account or to prevent further damage.

|  |
| --- |
| **Note:** |
| If an attacker has compromised a domain controller, it’s possible that he or she has stolen the KRBTGT password hash and is now using it to obtain access. In such a case, you may have to plan and execute a reset of the key stored in the password hash for the KRBTGT account. This action requires planning because it can disrupt all authentication. See [Reset the KRBTGT account](#_Reset_the_KRBTGT) at the end of this section for more information. |

* **Prevent the same attack from working again.** Attackers typically use techniques that were successful in the past, and then move to other available techniques. The use of backdoors and other attacks may also allow an attacker to regain access.

Ultimately, there are two valid approaches to achieving meaningful recovery of accounts in large, complex environments:

* **Tactical recovery.** This short-term operation is designed to disrupt a known adversary operation currently present in an environment. This approach doesn’t guarantee recovery but can be effective at breaking an attacker’s link to controlling an environment and preventing additional operations in a compromised state. A tactical operation relies on the following factors for success:
  + **Useful intelligence about the attacker’s presence.** To disrupt an attacker’s operation, you must understand how that operation is configured. Missing or overlooking an element of redundant adversary control can negate the effect of the operation.A tactical recovery typically requires the involvement of an experienced investigative team.
  + **A stealth operation about which the attacker is unaware.** Attackers frequently monitor email and other communications so that they can modify their presence on a network, if necessary, to defeat a cleanup operation.
  + **A properly scoped defender operation.** The scope has to be sufficiently comprehensive to be effective and small enough that you can execute it in a short period of time—a difficult balance to achieve.
* **Strategic recovery.** This approach is a long-term plan that consists of multiple operations focused on recovering integrity at a high assurance level, often for a large number of assets. Strategic recoveries can take months to plan and fully execute. A strategic recovery plan must address the following factors:
  + **Risk of migration.** Carefully conduct migrations to avoid transitioning the attacker’s malware implants and compromised accounts to a new, clean environment during the migration of legitimate users. In addition, assess the way migration tools and processes are designed and operated to help ensure that an attacker cannot exploit these tools or processes to move into the new organization.
  + **Risk of coexistence.** Organizations that are moving resources to a new environment frequently need users to be able to connect with the compromised environment to perform some job tasks until migration of all resources and users is complete. Therefore, take care to ensure that no one can use any credentials the migration exposes to the old environment to gain access to the new environment.
  + **Planned end state.** Consider the relative cost and benefit of the options for the strategic recovery end state, which range from recovering only the current forest to separating business-critical functions into a separate forest to create and migrate to a new forest (and many other variations). Consider these options in light of such factors as the business value of assets in the forest, available budget, ability to separate business-critical resources from lower-value resources, and the ability to detect and respond to incidents.

### Reset the KRBTGT account

The KRBTGT account stores a secret that the Kerberos service uses to issue and validate TGTs in a domain. In a compromised domain, an attacker can use publicly available tools to steal this secret and generate arbitrary valid TGTs as described in the golden ticket attack section of this document. This technique allows the attacker to obtain long-term access to the infrastructure as any user, including domain administrators, if you don’t reset the KRBTGT account after compromise. By initiating a password reset for the KRBTGT account, you instruct the system to generate a new random key for this value. This action invalidates the currently issued Kerberos TGTs but can also cause authentication errors throughout the domain and forest, so plan your approach carefully. For more information, see [KRBTGT account](http://technet.microsoft.com/en-us/library/dn745899.aspx#Sec_KRBTGT).