Mandiant

Ransomware Protection and Containment Strategies

Practical Guidance for Hardening and
Protecting Infrastructure, Identities and Endpoints

Overview

Ransomware is a common method of cyber extortion or disruption for financial gain. This type of attack can instantly disrupt access to files, applications or systems until the victim pays the ransom (and the attacker restores access with a decryption key) or the organization restores and reconstitutes from backups. Once ransomware is invoked within an organization, most variants utilize privileged accounts and trust relationships between systems for lateral dispersion.

Ransomware is commonly deployed across an environment in two ways:

1. Manual propagation by a threat actor after they have established access and have administrator-level privileges broadly across the environment:

   • Manually running encryptors on target systems.

   • Staging and deploying encryptors across the environment using scripting (e.g., mount C$ shares, copy the encryptor, and execute it with the Microsoft PsExec tool).

   • Deploying encryptors using Active Directory Group Policy Objects (GPOs).

   • Deploying encryptors using existing software deployment or endpoint management tools utilized by the victim organization.

   • Gaining access to virtualization infrastructure and encrypting localized virtual machines and mounted storage.

2. Automated propagation:

   • Credential or Windows token extraction from disk or memory.

   • Trust relationships between systems — and leveraging methods such as Windows Management Instrumentation (WMI), SMB, or PsExec to bind to systems and execute payloads.

   • Unpatched exploitation methods (e.g., EternalBlue — addressed via Microsoft Security Bulletin MS17-010).

The purpose of this document is to provide practical security strategies and enforcement measures which can limit the capability for an attacker leveraging ransomware or other destructive means to impact a large scope of systems within an environment. If an organization is the victim of an active ransomware attack, depending upon the propagation method that the variant is leveraging, implementing many of the recommendations within this document can potentially disrupt and contain the event.
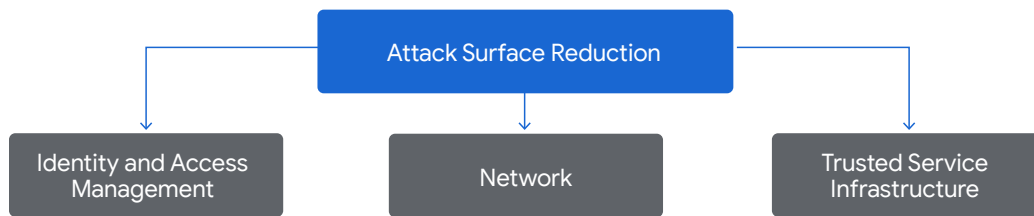
Category	Coverage Areas
Attack Surface Identification and Reduction	Identity and Access Management Network Infrastructure Trusted Service Infrastructure
Endpoint Hardening	Endpoint Segmentation Remote Desktop Protocol Hardening Administrative / Hidden Shares Restrictions SMB Hardening WinRM Hardening
Credential Protections	Local Accounts Privileged and Service Accounts Cleartext Password Protections
Domain Controllers	Isolation and Recovery Planning Domain Controller Backup Strategies
Group Policy Objects (GPOs)	Permissions Monitoring Strategies
Virtualization Infrastructure Protections	Identity Segmentation Network Segmentation / Infrastructure Hardening Visibility and Monitoring Virtualization Recovery Preparation
Backup Infrastructure Protections	Dependency and Interconnectivity Identification Backup Architecture Design Segmentation and Hardening Strategies

While the scope of recommendations contained within this document are not all encompassing, they represent the most practical proactive strategies based upon Mandiant's frontline visibility and expertise in helping organizations secure and defend their infrastructure from destructive attacks.

Attack Surface Identification and Reduction

An organization's attack surface consists of various components, including managed identities, network footprint, and supporting infrastructure that a threat actor can abuse to gain initial access, maintain persistence, escalate privileges, and potentially abuse to deploy ransomware at-scale.

This section covers different strategies to reduce overall attack surface across three major focus areas: identity, network, and trusted service infrastructure.

```
                        ┌─────────────────────────┐
                        │ Attack Surface Reduction │
                        └─────────────────────────┘
              ┌──────────────────┼──────────────────┐
              ▼                  ▼                  ▼
   ┌─────────────────┐  ┌─────────────────┐  ┌─────────────────┐
   │ Identity and    │  │                 │  │ Trusted Service │
   │ Access          │  │    Network      │  │ Infrastructure  │
   │ Management      │  │                 │  │                 │
   └─────────────────┘  └─────────────────┘  └─────────────────┘
```

Across all three focus areas, Mandiant included targeted recommendations for organizations to consider as part of proactive cyber readiness and also during incident containment workstreams. These recommendations can enable organizations to:
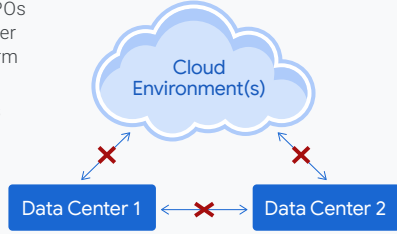
• Prevent a threat actor with initial access from moving laterally to further expand their scope of access and persistence;

• Protect against the risk of threat actors exploiting an externally accessible vector for unauthorized remote access and additional lateral movement;

• Limit access to platforms and technologies that (if compromised) could lead to destructive attacks.

Focus Area #1 - Identity and Access Management (IAM) Attack Surface Reduction		
Focus Area	**Action**	**Additional Details**
Identity Attack Reduction	Privileged Account Identification and Reduction	Identify and reduce the number of accounts assigned highly privileged roles. Accounts assigned highly privileged roles can be determined by the following criteria: • Accounts or nested groups that are assigned default privileged roles. • Accounts or groups assigned permissions for modifying or linking group policy objects (GPOs). • Accounts or groups assigned explicit permissions on Domain Controllers or Tier 0 endpoints. • Accounts or groups that are assigned privileged roles for virtualization platforms / infrastructure. • Account or groups that are assigned permissions to invoke processes as SYSTEM on a large scope of endpoints. • Accounts or groups with local administrative access on all (or a large scope of) endpoints in a domain.
	Privileged Account Password Rotations	Rotate credentials for all identified privileged accounts. Enforce long and complex passwords. If there is evidence of an active attacker with access into an environment, until the incident has been contained, the organization should not store updated passwords within the existing Privileged Access Management (PAM) or password vault solution. If a password cannot be rotated for a privileged account, the organization should temporarily disable the account, or temporarily reduce the scope of access.
	Use Local Accounts for Administrative Access	Organizations should proactively create isolated and segmented identities that are used for administrative access. During an active incident, organizations should sever integrations between on-premises identity store (e.g., Active Directory) and infrastructure platforms and services. Examples include: 1. Active Directory integration with VMware Virtualized Infrastructure (VCenter) 2. Active Directory integration with Privileged Access Management solution 3. Active Directory integration with Backup solution 4. Active Directory integration with Cloud IAM services During an incident containment phase, access to the organizations infrastructure platforms and services should be conducted using local administrator accounts (e.g., local VMware VCenter Admin account). Local administrator accounts should adhere to the following principles: 1. Created with long and complex passwords 2. Passwords should not be stored within your password management or vault solution 3. Multi-Factor Authentication enforced 4. Create at least two distinct local accounts

Focus Area #1 - Identity and Access Management (IAM) Attack Surface Reduction		
Focus Area	**Action**	**Additional Details**
	Identify and Harden Single-Factor Authentication Access Methods	Proactively audit and identify external access channels that allow for single-factor authentication methods. Common externally accessible technologies that may allow for single-factor authentication can include: • Remote access platforms (e.g., VPNs) • Virtualized Desktop Infrastructure (VDIs) • Cloud platforms and infrastructure • SaaS applications • Administrative consoles for application / technology platforms Externally accessible platforms that allow for single-factor authentication should have multi-factor authentication (MFA) enforced. If MFA enforcement is not achievable, at a minimum, the external exposure of the platform should be reduced to a small subset of trusted IP ranges.
	Harden Password Reset Processes	Identify and validate security controls for organizational-wide password reset self-service methods. Organizations should proactively create detections focused on monitoring password modifications across the infrastructure. If an organization leverages on-premises Active Directory integrated with Microsoft Entra ID, specific detections use-cases should include:

Identity Store	Audit Log	Audit Log Description
Active Directory	Event ID 4723	User-initiated password reset
	Event ID 4724	Administrator initiated password reset
Entra ID	Reset password (self-service)	User-initiated password reset
	Reset password (by admin)	Administrator initiated password reset

Table 1. Detections use-cases

If there is a suspected incident, organizations should align playbooks and response processes that enforce additional guardrails and positive identity verification methods for self-service password processes. This may even include temporarily disabling the ability for self-service password reset methods to be available from external locations until the incident has been fully contained.

At a minimum, any identities assigned a privileged role should be excluded from leveraging self-service password reset tools for managing the password for the associated account(s).

	Review / Restrict MFA Device Self-Registration Processes	Review and validate security controls for MFA device registrations and modifications. If there is a suspected incident, the ability for users to register or modify MFA authentication devices / methods may need to be restricted. Organizations may even need to require users to go through a verification process such as requiring live video verification of the user in order to modify MFA device / methods criteria. Alternatively, an organization may need to restrict MFA modifications and registrations to only be permissible from trusted physical network locations. At a minimum, any identities assigned a privileged role should be excluded from leveraging self-service methods for MFA device / method registration and modifications.
	Implement Credential Exposure Hardening Controls	Further identity-based controls are critical to reduce the overall exposure of identities across the infrastructure. Reference the following sections for additional details: • Restrict Remote Usage of Local Accounts • Reduce Exposure of Privileged and Service Accounts • Implement Protected Users Security Group • Implement Cleartext Password Protections controls

Focus Area #2 - Network Infrastructure Attack Surface Reduction		
Pillar	**Action**	**Additional Details**
Network Attack Reduction	Perform an external network scan to identify exposed resources.	Leverage Mandiant Attack Surface Management or a third-party vulnerability scanning technology to perform an external unauthenticated scan against the organization's domains, public IPs, and CIDR IP ranges. This scan should help determine the scope of applications and organization-managed services that are externally exposed and accessible. Organizations should cautiously review the output of the external scan. Unintended services or applications that are publicly exposed should be immediately isolated and reviewed. Additionally, organizations should review exposed and accessible applications and organization-managed services for any vulnerabilities and misconfigurations. Any identified vulnerabilities and misconfigurations should not only be patched and hardened, but the identified technology platforms should also be reviewed to ensure that evidence of suspicious activity or technology/device modifications have not already occurred.
	Sever Site-to-Site Integrations	Threat actors commonly deploy ransomware through the use of GPOs and other automated mechanisms. These methods allow an attacker to quickly encrypt a large number of endpoints from a single platform based upon the interconnectivity of infrastructure resources. To protect against ransomware propagation at-scale, organizations should align playbooks that allow for the quick segmentation and isolation of environments, which can minimize the potential impact of ransomware being deployed across specific boundaries. This strategy should also include isolating on-premises networks from cloud networks and other data centers, as seen in Figure 1 (e.g., disconnecting Site-to-Site VPN tunnels). **Figure 1.** Isolating networks
	Hunt and Block Remote Access Tools (RATs)	"Remote Access Tools" are software applications that allow remote management and control of endpoints (Laptops and Servers). Attackers will often deploy remote access tools as a means to establish and maintain persistence within a compromised network. Organizations should hunt for remote access tools through the following mechanisms: *See Table 2 below* **Table 2.** Mechanisms to hunt for remote access tools If an organization detects logs indicating traffic flows or process creations/installations of RATs, the following containment measures should be considered: *See Table 3 below* **Table 3.** Containment measures Additionally, servers and critical assets should have restrictions enforced that only allow egress communications to allow-listed domains. Organizations should also consider proactively blocking domains and ports/protocols associated with common remote access tools.
	Restrict or Shutdown Virtual Private Network (VPN)	Organizations should proactively review existing VPN and other technologies allowing remote connectivity into the environment. Organizations should also review the scope of accounts that are permitted to use these platforms for remote access. Only human / user accounts requiring MFA and associated with authorized personnel with should be allowed remote access to the environment (i.e., no shared accounts or service accounts).
	Restrict or Shutdown Streaming technologies (e.g., Citrix)	Additionally, organizations should implement "Host Integrity Posture" (HIP) checks to validate the integrity of endpoints used to access these technologies. Examples include: • Certificate Validation: verifying that an organization-issued certificate is installed on the endpoint • Domain validation: verifying the system is joined to the organization's domain • Operating System (OS) & Patch level: validating that the OS level and security patches adhere to the organizations standard • EDR: validating that the organizations EDR agent is installed and service actively running on the endpoint If systems do not pass HIP checks, their ability to connect-to or communicate to the corporate environment should be restricted. This method of quarantining can be a detection opportunity that should trigger a review and investigation of the system to determine the root cause of the non-compliant state. If there is a suspected incident, Organizations should limit the usage of VPN and streaming technologies to dedicated security and IT personnel who have reset their password and re-registered their MFA method. Until the incident has been contained, access for non-critical / end users should be temporarily revoked.
	Consider blocking ALL outbound internet	If there is a suspected incident, organizations should align playbooks and response processes to block / limit all outbound internet connections. While performing this action could introduce operational impacts, this level of communication restriction may be necessary to remove an attacker's interactive access until further investigation and containment measures can be conducted.

Log Source	Description
Network Logs	Network Traffic flow indicating traffic to a RAT Domain/IP or traffic over specific RAT ports/protocols
Endpoint Detection and Response (EDR) Logs	EDR logs indicating process creation or installation of a RAT
Asset Inventory Technologies	Installation of RAT application across endpoints and servers

Table 2. Mechanisms to hunt for remote access tools

#	Recommended Action
1	Block the RAT URL / call-back domain or the specific port/protocols at the Edge Firewall .
2	Add a block rule within endpoint detection and response (EDR) tooling to prevent the RAT from loading / executing.
3	Contain impacted endpoints and perform a comprehensive investigation.

Table 3. Containment measures

Focus Area #3 - Trusted Service Infrastructure Attack Surface Reduction		
Pillar	**Action**	**Additional Details**
Trusted Service Infrastructure Attack Reduction	Patch Management Tools	The terminology of "Trusted Service Infrastructure" is typically associated with management interfaces for platforms and technologies that provide core services for an organization. Examples include: • Asset and Patch Management Tools • Network Management Tools and Devices • Virtualization Platforms • Backup Technologies • Security Tooling • Privileged Access Management Systems
	Security Tools	
	Asset Inventory Tools	
	Privileged Access Management	
	Backup Infrastructure and Services	
		As the administrative trusted service infrastructure is already associated with "trusted" infrastructure within an environment, attackers will often target these platforms for persistence, lateral movement, and to abuse their intended functionality. For any trusted service infrastructure, organizations should: • Limit accounts allowed to authenticate and access infrastructure tooling. Reference "Use Local Accounts for Administrative Access" for additional details. • Review and validate MFA enforcement. Reference" Audit and Expand Multi-Factor Authentication Enforcement" for additional details • Implement network restrictions to allow authentication and access from trusted IPs/networks only. • Create detections focused on monitoring authentications and activity performed within trusted service infrastructure.
	Active Directory	Organizations should not only proactively backup Active Directory Domain Controllers (System State), but also ensure isolation and protection of the backup configuration data. Reference "Domain Controller Isolation and Recovery Planning" section of this document for additional details. Organizations should also review, reduce, and closely monitor the scope of accounts allowed to create, modify, or link GPOs. Prioritize review of accounts assigned the following roles: {{TABLE}} Reference the Group Policy Object (GPO) Permissions and Monitoring section of this document for additional details.
	Virtualization Infrastructure	Threat actors often target virtualization infrastructure as part of their reconnaissance, data theft, and ransomware deployment objectives. Direct access to the underlying components of the virtualization infrastructure should be protected, with only a specific subset of identities and devices provisioned for access. Reference the Virtualization Infrastructure Hardening and Protections section of this document for additional details.

Table embedded in the "Active Directory" cell:

#	Role Name
1	Domain Admins
2	Enterprise Admins
3	Group Policy Creator Owners
4	Delegated Permissions to — Create GPOs — Link GPOs — Edit GPOs

Attack surface reduction requires a multi-layered approach - implementing targeted restrictions, hardening measures, response actions, and detections across the different layers of an organization's managed identity, network, application, and trusted service infrastructure to successfully contain and limit the blast radius. The high-level recommendations listed above should be tested and verified to not impact operations. In the event of an active incident where ransomware deployment may be imminent, it's important to consider all potential hardening measures to prevent prolonged impact and outages. Additional strategies for protecting on-premises environments from a ransomware event are detailed below.

Endpoint Hardening

Endpoint Segmentation

```
Tactic: Lateral dispersion amongst systems using standard
Windows Operating System protocols
```

Windows Firewall

During a ransomware event, many variants utilize privileged and trusted accounts to bind to systems within an environment. Commonly, Server Message Block (SMB) is utilized for the communication channel between systems. While SMB is typically required within a Windows operating environment (e.g., workstation to Domain Controllers or File Servers), the scope of SMB communications permitted directly between systems can be restricted and minimized (e.g., workstation-to-workstation).

During a ransomware event, a Windows Firewall policy can be configured to restrict the scope of communications permitted between common endpoints within an environment. This firewall policy can be enforced locally or centrally via Group Policy. At a minimum, the common ports and protocols that should be blocked between workstation-to-workstation—and workstations to non-Domain Controllers and non-File Servers include:

• SMB (TCP/445, TCP/135, TCP/139)
• Remote Desktop Protocol (TCP/3389)
• Windows Remote Management / Remote PowerShell (TCP/80, TCP/5985, TCP/5986)
• WMI (dynamic port range assigned through DCOM)

Using Group Policy, the settings listed in Table 4 can be configured for the Windows Firewall to restrict inbound communications for endpoints in a managed environment.

Group Policy Setting Path:
Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security

Profile Setting	Firewall State	Inbound Connections	Log Dropped Packets	Log Successful Connections	Log File Path	Log File Maximum Size (KB)
Domain	On	Block all connections that do not match a preconfigured rule	Yes	Yes	%systemroot%\system32\LogFiles\Firewall\pfirewall	4,096
Private	On	Block all connections	Yes	Yes	%systemroot%\system32\LogFiles\Firewall\pfirewall.log	4,096
Public	On	Block all connections	Yes	Yes	%systemroot%\system32\LogFiles\Firewall\pfirewall.log	4,096

TABLE 4. Windows Firewall recommended configuration state

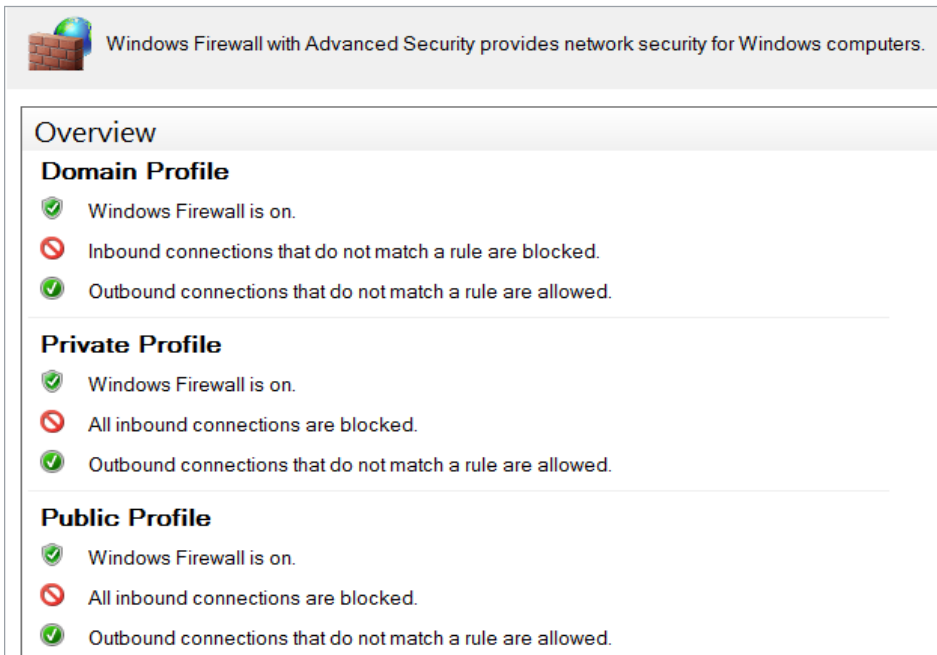**FIGURE 2.** Windows Firewall recommended configurations

Additionally, to ensure that only centrally managed firewall rules are enforced during a containment event (and cannot be overridden by a nefarious actor), the settings for "Apply local firewall rules" and "Apply local connection security rules" can be set to "No" for all profiles.
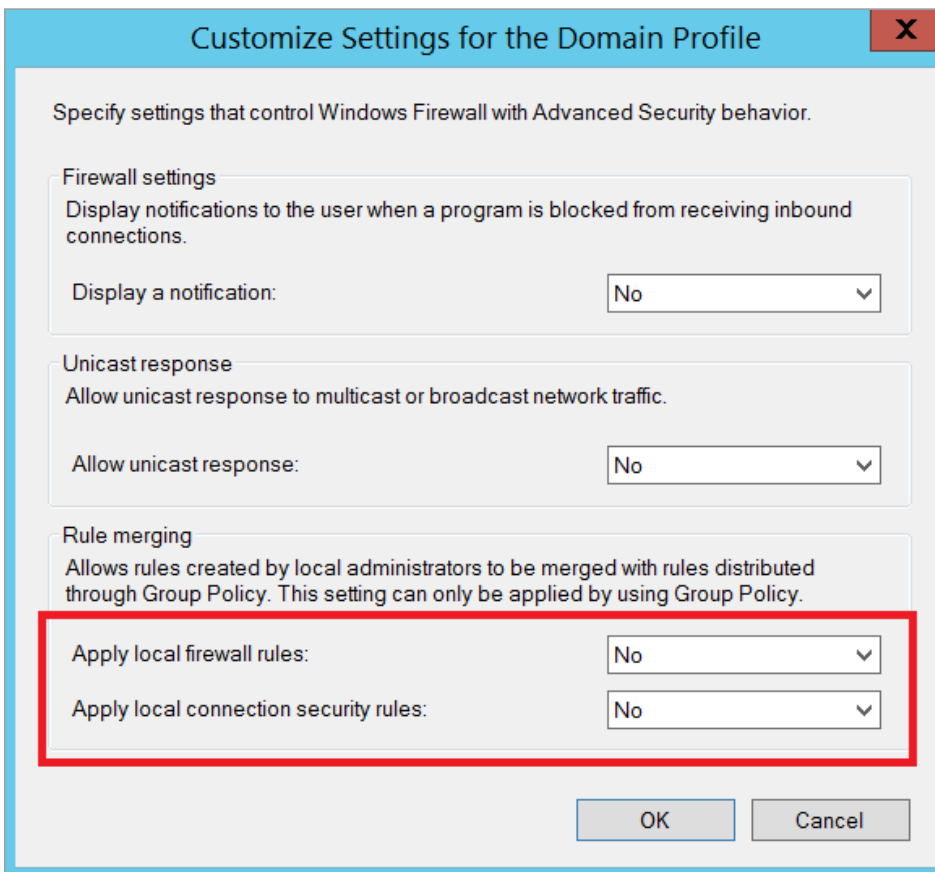

FIGURE 3. Windows Firewall domain profile customized settings

To quickly contain and isolate systems, the centralized Windows Firewall setting of "Block all connections" (Figure 4) will prevent any inbound connections from being established to a system. This is a setting that can be enforced on workstations and laptops, but will likely impact operations if enforced for servers; although if ransomware is spreading throughout an environment, it may be a necessary step for quick containment.

Note: Once the event has been contained and deemed "safe" to re-establish connectivity amongst systems within an environment, via Group Policy, the "Inbound Connections" setting can be changed back to "Allow" if necessary.
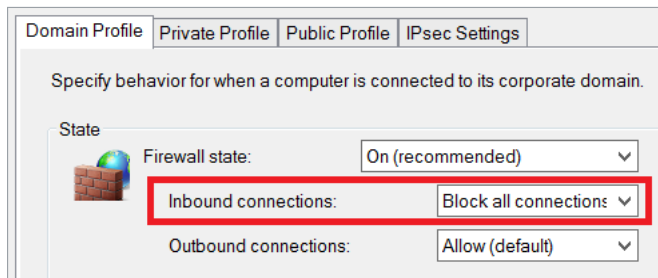

FIGURE 4. Windows Firewall - "Block all connections" settings

The protocols and ports listed in Table 5 represent the most common avenues for lateral movement and propagation. If blocking all inbound connectivity for common endpoints is not practical for containment, at a minimum, the protocols and ports listed in Table 5 should be considered for blocking using the Windows Firewall.

For any specific applications that may require inbound connectivity to end-user endpoints, the local firewall policy should be configured with specific IP address exceptions for origination systems that are authorized to initiate inbound connections to such devices.

Protocol/Port	Windows Firewall Rule	Command Line Enforcement
SMB TCP/445, TCP/139, TCP/135	Predefined Rule: • File and Print Sharing	`netsh advfirewall firewall set rule group="File` `and Printer Sharing" new enable=no`
Remote Desktop Protocol TCP/3389	Predefined Rule: • Remote Desktop	`netsh advfirewall firewall set rule group="Remote` `Desktop" new enable=no`

WMI	Predefined Rule:
	• Windows Management Instrumentation
		`netsh advfirewall firewall set rule`
		`group="windows management instrumentation`
		`(wmi)" new enable=no`

Windows Remote Management/ PowerShell Remoting
 	
TCP/80, TCP/5985, TCP/5986
	Predefined Rule:
	• Windows Remote Management
	• Windows Remote Management (Compability)
	Port Rule:
	• 5986
		`netsh advfirewall firewall set rule`
		`group="Windows Remote Management" new`
		`enable=no`
		
		Via PowerShell:
		`Disable-PSRemoting -Force`

TABLE 5. Windows Firewall suggested block rules

Name	Group ▲	Profile	Enabled	Action
🚫 WinRm via HTTPs - Block Inbound		All	Yes	Block
🚫 File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	All	Yes	Block
🚫 File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	All	Yes	Block
🚫 File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	All	Yes	Block
🚫 File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	All	Yes	Block
🚫 File and Printer Sharing (NB-Name-In)	File and Printer Sharing	All	Yes	Block
🚫 File and Printer Sharing (NB-Session-In)	File and Printer Sharing	All	Yes	Block
🚫 File and Printer Sharing (SMB-In)	File and Printer Sharing	All	Yes	Block
🚫 File and Printer Sharing (Spooler Service - RPC)	File and Printer Sharing	All	Yes	Block
🚫 File and Printer Sharing (Spooler Service - RPC-EPM...	File and Printer Sharing	All	Yes	Block
🚫 Remote Desktop - Shadow (TCP-In)	Remote Desktop	All	Yes	Block
🚫 Remote Desktop - User Mode (TCP-In)	Remote Desktop	All	Yes	Block
🚫 Remote Desktop - User Mode (UDP-In)	Remote Desktop	All	Yes	Block
🚫 Windows Management Instrumentation (ASync-In)	Windows Managemen...	All	Yes	Block
🚫 Windows Management Instrumentation (DCOM-In)	Windows Managemen...	All	Yes	Block
🚫 Windows Management Instrumentation (WMI-In)	Windows Managemen...	All	Yes	Block
🚫 Windows Remote Management (HTTP-In)	Windows Remote Ma...	All	Yes	Block
🚫 Windows Remote Management (HTTP-In)	Windows Remote Ma...	All	Yes	Block

FIGURE 5. Windows Firewall suggested rule blocks via Group Policy

Additionally, the Windows Firewall can be configured to block specific binaries from making outbound connections on endpoints. During ransomware response engagements, Mandiant has identified legitimate Windows binaries being leveraged to download backdoors and encryptors from both internal and external locations. To protect against this tactic, an organization can leverage a series of Windows Firewall rules to block specific binaries from making outbound connections from an endpoint.

Using powershell.exe and bitsadmin.exe as examples, Figure 6 provides configurations of leveraging Windows Firewall rules to deny the ability for specific binaries to establish outbound connections from an endpoint.

FIGURE 6. Windows Firewall rule example to block specific binaries from making outbound connections on an endpoint

RDP Hardening

Remote Desktop Protocol (RDP) is a common method used by malicious actors to remotely connect to systems, laterally move from the perimeter onto a larger scope of systems, and deploy malware. External-facing systems with RDP open to the Internet have elevated risk. Malicious actors may exploit RDP to gain initial access into an organization, perform lateral movement, invoke ransomware, and potentially access and steal data.

Proactively, organizations should scan their public IP address ranges to identify systems with RDP (TCP/3389) and other protocols (SMB: TCP/445 or SSH: TCP/22) open to the Internet. At a minimum, RDP, SMB and SSH should not be directly exposed for ingress and egress access to/from the Internet. If required for operational purposes, explicit controls should be implemented to restrict the source IP addresses which can interface with systems using these protocols.

Enforce Multi-Factor Authentication

If external-facing RDP must be utilized for operational purposes, multi-factor authentication should be enforced for connectivity. This can be accomplished either via the integration of a third-party multi-factor authentication technology or by leveraging a Remote Desktop Gateway and Azure Multi-Factor Authentication Server using RADIUS.

Leverage Network Level Authentication

For external-facing RDP servers, Network Level Authentication (NLA) provides an extra layer of pre-authentication before a connection is established. NLA is also useful for protecting against brute force attacks, which often target open internet-facing RDP servers.

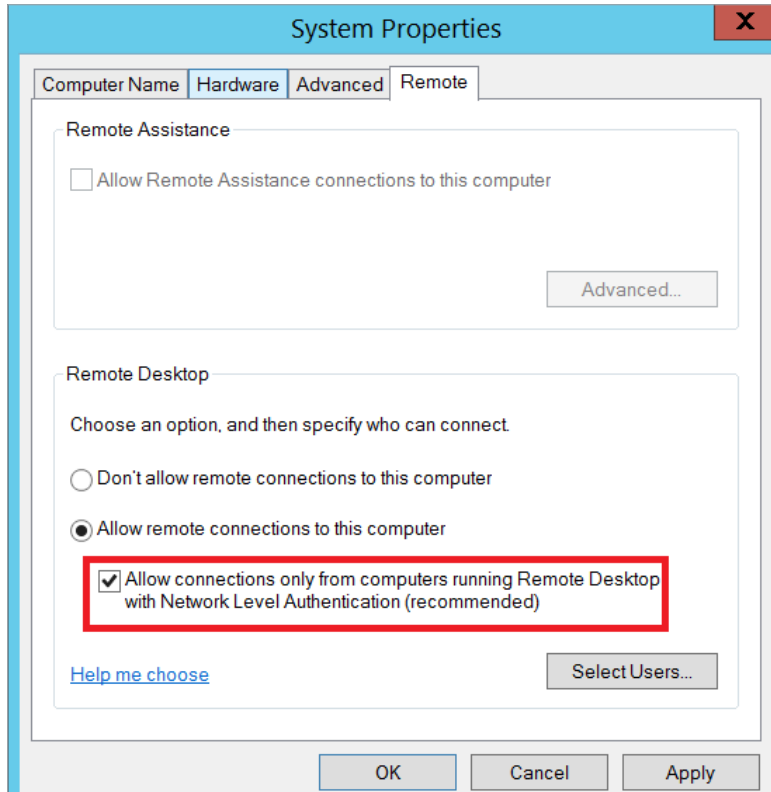NLA can be configured either via the User Interface (UI) (Figure 7) or via Group Policy (Figure 8).

FIGURE 7. Enabling NLA via the UI

Using Group Policy, the setting for NLA can be enabled via:

- Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Security > Require user authentication for remote connections by using Network Level Authentication

Setting	State	Comment
Server authentication certificate template	Not configured	No
Set client connection encryption level	Not configured	No
Always prompt for password upon connection	Not configured	No
Require secure RPC communication	Not configured	No
Require use of specific security layer for remote (RDP) connections	Not configured	No
Do not allow local administrators to customize permissions	Not configured	No
Require user authentication for remote connections by using Network Level Authentication	Enabled	No

FIGURE 8. Enabling NLA via Group Policy

Some caveats about leveraging NLA for RDP:

- The Remote Desktop client v7.0 (or greater) must be leveraged.

- NLA utilizes CredSSP to pass authentication requests from the initiating system. CredSSP stores credentials in LSA memory on the initiating system—and these credentials may remain in memory even after a user logs off from the system. This provides a potential exposure risk for credentials in memory on the source system.

- On the RDP server, users permitted for remote access using RDP must be assigned the "Access this computer from the network" privilege when NLA is enforced. This privilege is often explicitly denied for user accounts to protect against lateral movement techniques.

Restrict Administrative Accounts from Leveraging RDP on Internet-Facing Systems

For external-facing RDP servers, highly-privileged domain and local administrative accounts should not be permitted access to interface with the servers using RDP (Figure 9).

This can be enforced using Group Policy, configurable via the following setting:

- Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment > Deny log

Local Policies/User Rights Assignment

Policy	Setting
Deny access to this computer from the network	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on as a batch job	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on as a service	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on locally	MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on through Terminal Services	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts

FIGURE 9. Group Policy configuration for restricting highly privileged domain and local administrative accounts from leveraging RDP

Disable Administrative / Hidden Shares

> Tactic: Lateral dispersion amongst systems via binding to
> administrative shares for tool or malware deployment

Some ransomware variants will attempt to identify administrative or hidden network shares, including those that are not explicitly mapped to a drive letter—and use these for binding to endpoints throughout an environment. As a containment step, an organization may need to quickly disable default administrative or hidden shares from being accessible on endpoints. This can be accomplished by either modifying the registry, stopping a service, or by using the "Microsoft Security Guide" Group Policy template from the Microsoft Security Compliance Toolkit.

Common administrative and hidden shares on endpoints include:

• ADMIN$
• C$
• D$
• IPC$

Note: Disabling administrative and hidden shares on servers, specifically Domain Controllers, may significantly impact the operation and functionality of systems within a domain-based environment.

Additionally, if PsExec is utilized in an environment, disabling the admin (ADMIN$) share can restrict the capability for this tool to be utilized to remotely interface with endpoints.

Registry Method:

Using the registry, administrative and hidden shares can be disabled on endpoints (Figure 10 and Figure 11).

Workstations:

```
HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
DWORD Name = "AutoShareWks"
Value = "0"
```

FIGURE 10. Registry value for disabling administrative shares on workstations

Servers:

```
HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
DWORD Name = "AutoShareServer"
Value = "0"
```

FIGURE 11. Registry value for disabling administrative shares on servers

Service Method:

By stopping the "Server" service on an endpoint, the ability to access any shares hosted on the endpoint will be disabled (Figure 12).
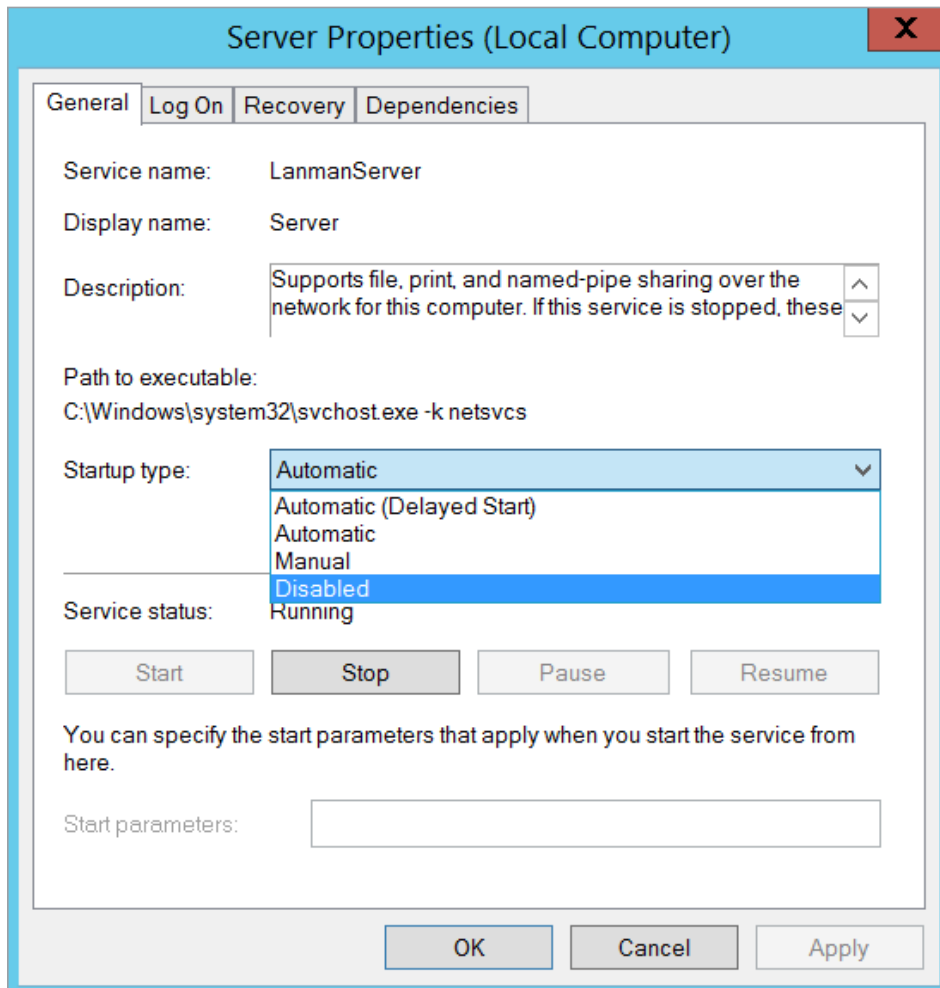
FIGURE 12. "Server" Services Properties

Group Policy Method:

Using the "MSS (Legacy)" Group Policy template, administrative and hidden shares can be disabled on either a server or workstation using Group Policy settings (Figure 13).

- Computer Configuration > Policies > Administrative Templates > MSS (Legacy) > MSS (AutoShareServer)

- Computer Configuration > Policies > Administrative Templates > MSS (Legacy) > MSS (AutoShareWks)

Setting	State	Comment
MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)	Not configured	No
MSS: (AutoReboot) Allow Windows to automatically restart after a system crash (recommended e...	Not configured	No
MSS: (AutoShareServer) Enable Administrative Shares (recommended except for highly secure envi...	Disabled	No
MSS: (AutoShareWks) Enable Administrative Shares (recommended except for highly secure enviro...	Disabled	No

FIGURE 13. Disabling administrative and hidden shares via the "MSS (Legacy)" Group Policy template

Disable SMBv1

```
Tactic: Lateral dispersion amongst systems via vulnerability
exploitation or legacy protocol abuse
```

In addition to patching for known vulnerabilities impacting common protocols (e.g., SMB), disabling SMBv1 on endpoints can reduce the mass propagation methods used by specific ransomware variants.

SMBv1 can be disabled on Windows 7 and Windows Server 2008 R2 (and above) using either PowerShell (Figure 14), a registry modification, or by using the "Microsoft Security Guide" Group Policy template from the Microsoft Security Compliance Toolkit.

PowerShell Method:

```
Set-SmbServerConfiguration -EnableSMB1Protocol $false
```

FIGURE 14. PowerShell command to disable SMBv1

Registry Method:

Using the registry, SMBv1 can be disabled on endpoints (Figure 15 and Figure 16).

Disable SMBv1 Server:

```
HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
Registry entry: SMB1
REG _ DWORD = "0" (Disabled)
```

FIGURE 15. Registry key and value for disabling SMBv1 server (listener)

Disable SMBv1 Client:

```
HKLM\SYSTEM\CurrentControlSet\services\mrxsmb10
Registry entry: Start
REG _ DWORD = "4" (Disabled)
HKLM\SYSTEM\CurrentControlSet\Services\LanmanWorkstation
Registry entry: DependOnService
REG _ MULTI _ SZ: "Bowser","MRxSmb20","NSI"
```

FIGURE 16. Registry key and value for disabling SMBv1 client

Group Policy Method:

Using the "Microsoft Security Guide" Group Policy template, SMBv1 can be disabled using the settings noted as follows.

• Computer Configuration > Policies > Administrative Templates > MS Security Guide > Configure SMBv1 Server

Setting	State	Comment
Configure SMB v1 server	Disabled	No
Configure SMB v1 client driver	Enabled	No
Configure SMB v1 client (extra setting needed for pre-Win8.1/2012R2)	Enabled	No

FIGURE 17. Disabling SMBv1 server via the "MS Security Guide" Group Policy template

• Computer Configuration > Policies > Administrative Templates > MS Security Guide > Configure SMB v1 Client Driver
  ◦ Enabled
    ▪ Configure MrxSMB10 driver
      • Disable driver

Setting	State	Comment
Configure SMB v1 server	Disabled	No
Configure SMB v1 client driver	Enabled	No
Configure SMB v1 client (extra setting needed for pre-Win8.1/2012R2)	Enabled	No

FIGURE 18. Disabling SMBv1 client driver via the "MS Security Guide" Group Policy template

FIGURE 19. Disabling SMBv1 client driver via the "MS Security Guide" Group Policy template—additional setting

- Computer Configuration > Policies > Administrative Templates > MS Security Guide > Configure SMB v1 Client (extra setting needed for pre-Win8.1/2012R2)
  - Enabled
    - Configure LanmanWorkstation Dependencies
      - Bowser
      - MrxSMB20
      - NSI

Setting	State	Comment
Configure SMB v1 server	Disabled	No
Configure SMB v1 client driver	Enabled	No
Configure SMB v1 client (extra setting needed for pre-Win8.1/2012R2)	Enabled	No

FIGURE 20. Disabling SMB v1 client extra settings via the "MS Security Guide" Group Policy template

FIGURE 21. Disabling SMB v1 client driver via the "MS Security Guide" Group Policy template—additional settings ensuring that the "MRxSmb10" option is not present

Windows Remote Management (WinRM) Hardening

> Tactic: Lateral dispersion between systems via Windows Remote Management (WinRM) and PowerShell remoting

Manual operators may leverage Windows Remote Management (WinRM) to propagate ransomware throughout an environment. WinRM is enabled by default on all Windows Server operating systems (since Windows Server 2012 and above), but disabled on all client operating systems (Windows 7 and Windows 10) and older server platforms (Windows Server 2008 R2).

PowerShell Remoting (PS Remoting) is a native Windows remote command execution feature that's built on top of the WinRM protocol.

If WinRM has ever been enabled on a client (non-server) operating system, then the following configurations will exist on an endpoint, and will not be remediated solely through the PowerShell command noted in Figure 22.

• WinRM listener configured
• Windows Firewall exception configured

These items will need to be disabled manually through the commands in Figure 24 and Figure 25.
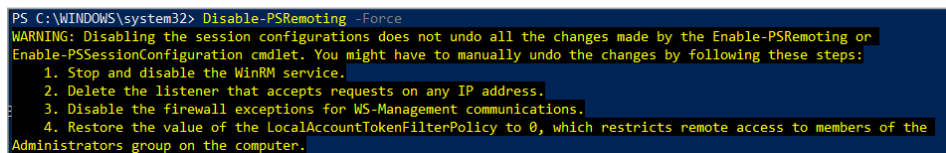
PowerShell:

```
Disable-PSRemoting -Force
```

FIGURE 22. PowerShell Command to disable WinRM / PowerShell Remoting on an endpoint

Note: Disabling PowerShell Remoting does not prevent local users from creating PowerShell sessions on the local computer - or for sessions destined for remote computers.

After running the command, the message recorded in Figure 23 will be displayed.

FIGURE 23. Warning message after disabling PSRemoting

Figures 24-27 show how to enforce the additional steps for disabling WinRM via PowerShell.

Stop and disable the WinRM Service:

```
Stop-Service WinRM -PassThruSet-Service WinRM -StartupType
Disabled
```

FIGURE 24. PowerShell command to stop and disable the WinRM Service

Disable the listener that accepts requests on any IP address:

```
dir wsman:\localhost\listener
Remove-Item -Path WSMan:\Localhost\listener\<Listener name>
```

FIGURE 25. PowerShell commands to delete a WSMAN listener

Disable the firewall exceptions for WS-Management communications:

```
Set-NetFirewallRule -DisplayName 'Windows Remote Management
(HTTP-In)' -Enabled False
```

FIGURE 26. PowerShell command to disable firewall exceptions for WinRM

Restore the value of the LocalAccountTokenFilterPolicy to "0" (zero), which enforces UAC token filtering (admin approval mode) for the built-in administrator (RID 500) account:

```
Set-ItemProperty -Path
HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system
-Name LocalAccountTokenFilterPolicy -Value 0
```

FIGURE 27. PowerShell command to configure the registry key for LocalAccountTokenFilterPolicy

Group Policy Method:

• Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Remote Management (WinRM) > WinRM Service > Allow remote server management through WinRM

If the aforementioned Group Policy setting is configured as "Disabled", the WinRM service will not respond to requests from a remote computer, regardless of whether or not any WinRM listeners are configured.

• Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Remote Shell > Allow Remote Shell Access

This Group Policy setting will manage the configuration of remote access for all supported shells to execute scripts and commands.

Credential Exposure and Usage Hardening

Remote Usage of Local Accounts

> Tactic: Lateral movement and propagation using the built-in local administrator account on endpoints

Local accounts that exist on endpoints are often a common avenue leveraged by attackers to laterally move throughout an environment. This tactic is especially impactful when the password for the built-in local administrator account is configured to the same value across multiple endpoints. To mitigate the impact of local accounts being leveraged for lateral movement, Microsoft Security Advisory KB2871997 introduced two (2) well-known SIDs that can be leveraged within Group Policy settings to restrict the usage of local accounts for lateral movement.

• S-1-5-113: NT AUTHORITY\Local account
• S-1-5-114: NT AUTHORITY\Local account and member of Administrators group

Specifically, the SID "S-1-5-114: NT AUTHORITY\Local account and member of Administrators group" is added to an account's access token if the local account is a member of the BUILTIN\Administrators group. **This is the most beneficial SID to stop an attacker (or ransomware variant) that propagates using credentials for any local administrative accounts.**

Note: For SID "S-1-5-114: NT AUTHORITY\Local account and member of Administrators group", if Failover Clustering is utilized, this feature should leverage a non-administrative local account (CLIUSR) for cluster node management. If this account is a member of the local Administrators group on an endpoint that is part of a cluster, blocking the network logon permissions can cause cluster services to fail. Be cautious and thoroughly test this configuration on servers where Failover Clustering is utilized.

Step 1 – Option 1: S-1-5-114 SID

To mitigate the usage of local administrative accounts from being used for lateral movement, utilize the SID "S-1-5-114: NT AUTHORITY\Local account and member of Administrators group" within the following settings:

• Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment

  ◦ Deny access to this computer from the network (SeDenyNetworkLogonRight)
  ◦ Deny log on as a batch job (SeDenyBatchLogonRight)
  ◦ Deny log on as a service (SeDenyServiceLogonRight)
  ◦ Deny log on through Terminal Services (SeDenyRemoteInteractiveLogonRight)
  ◦ Debug Programs (SeDebugPrivilege)—permission used for attempted privilege escalation and process injection

Step 1 – Option 2: UAC Token-Filtering

An additional control that can be enforced via Group Policy settings pertains to the usage of local accounts for remote administration and connectivity during a network logon. If the full scope of permissions (referenced in Option 1) cannot be implemented in a short timeframe, consider applying the UAC token-filtering method to local accounts for network-based logons.

These configurations can be enforced via the previously mentioned "Microsoft Security Guide" Group Policy template from the Microsoft Security Compliance Toolkit.

Group Policy Setting:

• Computer Configuration > Policies > Administrative Templates > MS Security Guide >
  Apply UAC restrictions to local accounts on network logons

Once enabled, the registry value (Figure 28) will be configured on each endpoint:

```
Set-ItemProperty -Path
HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system
-Name LocalAccountTokenFilterPolicy -Value 0
```

FIGURE 28. Registry key and value for enabling UAC restrictions for local accounts

When set to "0", remote connections with high integrity access tokens are only possible using either the plaintext credential or password hash of the RID 500 local administrator, dependent upon the setting of "FilterAdministratorToken."

The "FilterAdministratorToken" setting can either enable (1) or disable (0) (default) "Admin Approval" mode for the RID 500 local administrator. When enabled, the access token for the RID 500 local administrator account is filtered and therefore User Account Control (UAC) is enforced for this account (which can ultimately stop attempts to leverage this account for lateral movement across endpoints).

Group Policy Setting:

• Computer Configuration > Policies > Windows Settings > Security Settings > Local
  Policies > Security Options > User Account Control: Admin Approval Mode for the
  built-in Administrator account

Once enabled, the registry value (Figure 29) will be configured on each endpoint:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\
FilterAdministratorToken
REG _ DWORD = "1" (Enabled)
```

FIGURE 29. Registry key and value for requiring admin approval mode for local administrative accounts

Note: It's also prudent to ensure that the default setting for "User Account Control: Run all administrators in Admin Approval Mode" ("EnableLUA" option) is not changed from Enabled (Default) to Disabled. If this setting is disabled, all UAC policies are also disabled. With this setting disabled, it is possible to perform privileged remote authentication using plaintext credentials or password hashes with any local account that is a member of the local administrators group.

Group Policy Setting:

• Computer Configuration > Policies > Administrative Templates > MS Security Guide >
  User Account Control: Run all administrators in Admin Approval Mode

Once enabled, the registry value (Figure 30) will be configured on each endpoint. This is the default setting.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\
EnableLUA
REG _ DWORD = "1" (Enabled)
```

FIGURE 30. Registry key and value for enabling UAC restrictions for local accounts

UAC access token filtering will not affect any domain accounts in the local Administrators group on an endpoint.

Step 2: LAPS

Once the usage of local accounts has been blocked for remote authentication and access to remote endpoints, an organization must align a strategy to enforce password randomization for the built-in local administrator account. For many organizations, the easiest way to accomplish this task is by deploying and leveraging Microsoft Local Administrator Password Solutions (LAPS).

Reduce the Exposure of Privileged and Service Accounts

```
Tactic: Lateral movement and propagation using
domain-based accounts
```

Privileged Account Logon Restrictions

For ransomware to be deployed throughout an environment, privileged and service accounts credentials are commonly utilized for lateral movement and mass propagation. Until a thorough investigation has been completed, it may be difficult to determine the specific credentials that are being utilized by a ransomware variant for connectivity to a large scope of systems within an environment.

For any accounts that have privileged access throughout an environment, the accounts should not be utilized on standard workstations and laptops, but rather from designated systems (e.g., Privileged Access Workstations (PAWS)) that reside in restricted and protected VLANs and Tiers. Explicit privileged accounts should be defined for each Tier, and only utilized within the designated Tier.

The recommendations for restricting the scope of access for privileged accounts is based upon Microsoft's guidance for securing privileged access.

As a quick containment measure, consider blocking any accounts with privileged access from being able to login (remotely or locally) to standard workstations, laptops, and common access servers (e.g., virtualized desktop infrastructure).

The settings referenced as follows are configurable via the Group Policy path of:

• Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment

Accounts delegated with local or domain privileged access should be explicitly denied access to standard workstations and laptop systems within the context of the following settings (which can be configured using Group Policy settings similar to what are depicted in Figure 31):

Deny access to this computer from the network (also include S-1-5-114: NT AUTHORITY\ Local account and member of Administrators group)

• Deny access to this computer from the network (also include S-1-5-114: NT AUTHORITY\Local account and member of Administrators group)
• Deny log on as a batch job
• Deny log on as a service
• Deny log on locally
• Deny log on through Terminal Services

Local Policies/User Rights Assignment	
Policy	**Setting**
Deny access to this computer from the network	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on as a batch job	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on as a service	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on locally	MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on through Terminal Services	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts

FIGURE 31. Example of Privileged Account access restrictions for a standard workstation using Group Policy settings

Service Account Logon Restrictions

Organizations should also consider enhancing the security of domain-based service accounts to restrict the capability for the accounts to be used for interactive, remote desktop, and where possible, network-based logons.

On endpoints where the service account is not required for interactive or remote logon purposes, Group Policy settings can be used to enforce recommended logon restrictions for limiting the exposure of service accounts.

• Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment

  ◦ Deny log on locally (SeDenyInteractiveLogonRight)
  ◦ Deny log on through Terminal Services (SeDenyRemoteInteractiveLogonRight)

Additional recommended logon hardening for service accounts (on endpoints where the service accounts is not required for network-based logon purposes):

• Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment

  ◦ Deny access to this computer from the network (SeDenyNetworkLogonRight)

If a service account is only required to be leveraged on a single endpoint to run a specific service, the service account can be further restricted to only permit the account's usage on a predefined listing of endpoints.

• Active Directory Users and Computers > Select the Account Tab

  ◦ "Log On To" button > Select the proper scope of computers for access (Figure 32)
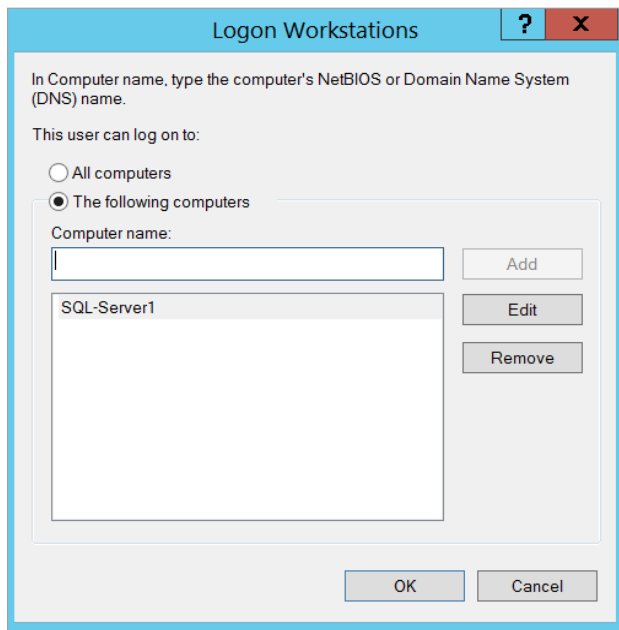
FIGURE 32. Option to restrict an account to logon to specific endpoints

Protected Users Security Group

By leveraging the "Protected Users" security group for privileged accounts, an organization can minimize various risk factors and common exploitation methods for exposing privileged accounts on endpoints.

Beginning with Microsoft Windows 8.1 and Microsoft Windows Server 2012 R2 (and above), the "Protected Users" security group was introduced to manage credential exposure within an environment. Members of this group automatically have specific protections applied to their accounts, including:

- The Kerberos ticket granting ticket (TGT) expires after 4 hours, rather than the normal 10-hour default setting.
- No NTLM hash for an account is stored in LSASS since only Kerberos authentication is used (NTLM authentication is disabled for an account).
- Cached credentials are blocked. A Domain Controller must be available to authenticate the account.
- WDigest authentication is disabled for an account, regardless of an endpoint's applied policy settings.
- DES and RC4 can't be used for Kerberos pre-authentication (Server 2012 R2 or higher); rather Kerberos with AES encryption will be enforced.
- Accounts cannot be used for either constrained or unconstrained delegation (equivalent to enforcing the "Account is sensitive and cannot be delegated" setting in Active Directory Users and Computers).

To provide Domain Controller-side restrictions for members of the "Protected Users" security group, the domain functional level must be Windows Server 2012 R2 (or higher). Microsoft Security Advisory KB2871997 adds support for the protections enforced for members of the "Protected Users" security group to Windows 7, Windows Server 2008 R2, and Windows Server 2012 systems.

Note: Service accounts (including Managed Service Accounts) should NOT be added to the "Protected Users" security group, as authentication will fail.

Cleartext Password Protections

> Tactic: Obtaining cleartext credentials in memory for credential harvesting

In addition to restricting access for privileged accounts, controls should be enforced that minimize the exposure of credentials and tokens in memory on endpoints.

On older Windows Operating Systems, cleartext passwords are stored in memory (LSASS) to primarily support WDigest authentication. WDigest should be explicitly disabled on all

Windows endpoints where it is not disabled by default.

By default, WDigest authentication is disabled in Windows 8.1+ and in Windows Server 2012 R2+.

Beginning with Windows 7 and Windows Server 2008 R2, after installing Microsoft Security Advisory KB2871997, WDigest authentication can be configured either by modifying the registry or by using the "Microsoft Security Guide" Group Policy template

from the Microsoft Security Compliance Toolkit.

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\
WDigest\UseLogonCredential
REG _ DWORD = "0"
```

FIGURE 33. Registry key and value for disabling WDigest authentication

Registry Method:

Another registry setting that should be explicitly configured is the "TokenLeakDetectDelaySecs" setting (Figure 33), which will clear credentials in memory of logged off users after 30 seconds, mimicking the behavior of Windows 8.1 and above.

```
Another registry setting that should be explicitly configured
is the "TokenLeakDetectDelaySecs" setting (Figure 34), which
will clear credentials in memory of logged off users after 30
seconds, mimicking the behavior of Windows 8.1 and above.
```

FIGURE 34. Registry key and value for enforcing the "TokenLeakDetect DelaySecs" setting

Group Policy Method:

Using the "Microsoft Security Guide" Group Policy template, WDigest authentication can be disabled via a Group Policy setting (Figure 35).

• Computer Configuration > Policies > Administrative Templates > MS Security Guide > WDigest Authentication

Setting	State	Comment
Configure SMB v1 server	Not configured	No
Configure SMB v1 client driver	Not configured	No
Configure SMB v1 client (extra setting needed for pre-Win8.1/2012R2)	Not configured	No
Extended Protection for LDAP Authentication (Domain Controllers only)	Not configured	No
Turn on Windows Defender protection against Potentially Unwanted Applications (DEPRECATED)	Not configured	No
Enable Structured Exception Handling Overwrite Protection (SEHOP)	Not configured	No
Apply UAC restrictions to local accounts on network logons	Not configured	No
WDigest Authentication (disabling may require KB2871997)	Disabled	No
Lsass.exe audit mode	Not configured	No
LSA Protection	Not configured	No
Remove "Run As Different User" from context menus	Not configured	No
Block Flash activation in Office documents	Not configured	No

FIGURE 35. Disabling WDigest authentication via the "MS Security Guide" Group Policy template

Additionally, an organization should verify if any applications are explicitly listed in the

"Allow" keys (Figure 36), as this would permit the tspkgs / CredSSP providers to store cleartext passwords in memory.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Credssp\
PolicyDefaults
```

FIGURE 36. Additional registry key for hardening against cleartext password storage

As Microsoft Security Advisory KB287199713 is not applicable for Windows XP, Windows Server 2003, and Windows Server 2008, to disable WDigest authentication on these platforms, prior to a system reboot, WDigest needs to be removed from the listing of LSA security packages within the registry (Figure 37 and Figure 38).

```
HKLM\System\CurrentControlSet\Control\Lsa\Security Packages
```

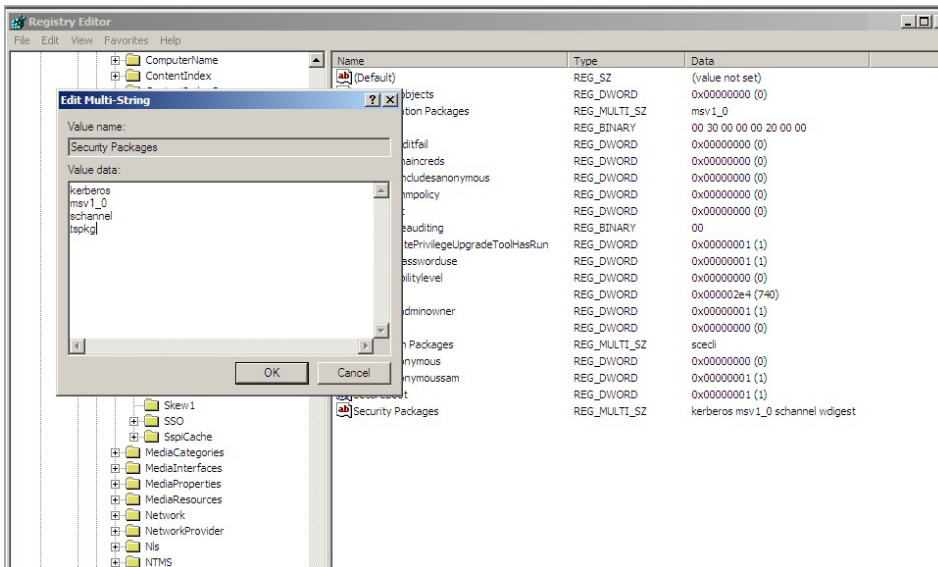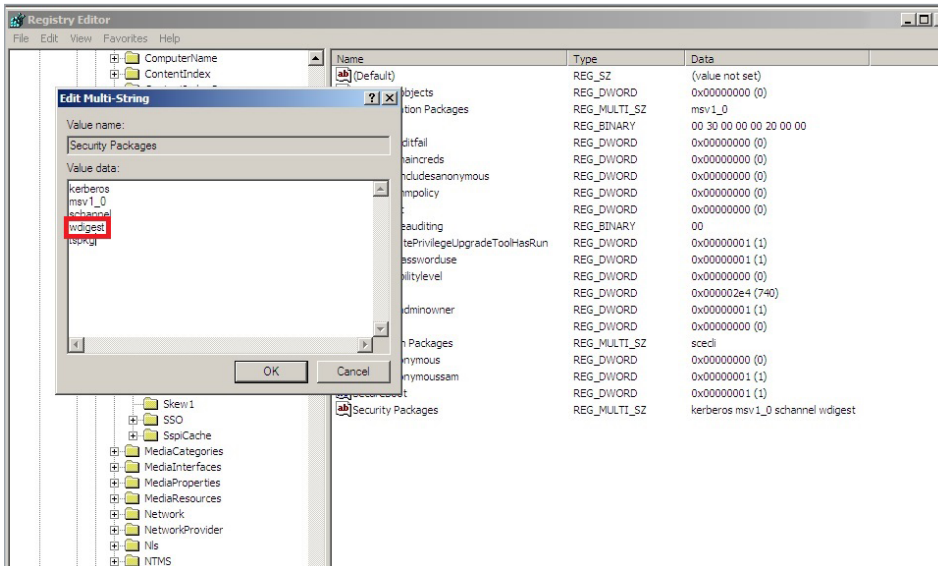**FIGURE 37.** Registry key to modify LSA security packages

FIGURE 38. LSA security package registry key before and after the removal of WDigest authentication from the listing of providers

By default, Group Policy settings are only reprocessed and reapplied if the actual Group Policy was modified prior to the default refresh interval.

Many attackers will manually "enable" WDigest authentication on endpoints by directly modifying the registry (UseLogonCredential configured to a value of "1"). Even on endpoints where WDigest authentication is automatically disabled by default, it is recommended to enforce the Group Policy settings noted in Figure 35—and configure automatic policy reprocessing for the configured settings on an automated basis.

• Computer Configuration > Policies > Administrative Templates > System > Group Policy
  > Configure security policy processing
  – Enabled - Process even if the GPOs have not changed

• Computer Configuration > Policies > Administrative Templates > System > Group Policy
  > Configure registry policy processing
  – Enabled - Process even if the GPOs have not changed

Domain Controllers

Isolation and Recovery Planning

In the event of a ransomware outbreak, an organization must ensure that they have a practiced plan in place to quickly isolate key systems, and ensure that at least one Domain Controller can be quickly taken offline and safely isolated for each domain within managed and trusted forests. If the disk partition that houses the Active Directory database (%SYSTEMROOT%\ntds\ntds.dit) and SYSVOL (%SYSTEMROOT%\SYSVOL) on all Domain Controllers were to be encrypted, this will impact the availability of domain services and functionality for all domain-based applications and services, including authentication, name resolution, and GPO processing. If Domain Controller backups are either encrypted or are not current, an organization may be faced with a complete rebuild of an entire forest, which can further impact downtime.

When Mandiant is engaged to help contain an active ransomware deployment, the first steps recommended that an organization take are to isolate at least one Domain Controller (preferable one that holds FSMO roles) and ensure that offline backups of SYSVOL (%SYSTEMROOT%\SYSVOL*) and GPOs are available and current.

```
netdom query fsmo
```

FIGURE 39. Command to determine a Domain Controller that holds a FSMO role

```
backup-gpo –domain "domain.local" –all –path "c:\temp\gpo-
backups"
```

FIGURE 40. PowerShell command to backup all GPOs in a domain

Proactively, in the event that either an authoritative or non-authoritative Domain Controller restoration is required, an organization should ensure that the Directory Services Restore Mode (DSRM) password is set to a known value on all Domain Controllers. If an organization does not have the DSRM password available, the password can be set to a known value by following the process outlined in Figure 41. The steps will need to be initiated on each Domain Controller.

```
PS C:\Windows\system32> ntdsutil
C:\Windows\System32\ntdsutil.exe: set drsm password
Reset DRSM Administrator Password: reset password on server
null
Please type password for DS Restore Mode Administrator
Account: *****************
Please confirm new password: **************
Password has been set successfully.

Reset DRSM Administrator Password: q
C:\Windows\System32\ntdsutil.exe:
```

FIGURE 41. Command to set the DSRM password on a Domain Controller

Domain Controller Backup Strategies

When restoring Active Directory from previous Domain Controller backups is the only viable option to restore domain services, an organization must first ensure that they have a working and tested backup plan and strategy to guarantee the availability and integrity of the schema and domain services that need to be reconstituted. The following best practices should be proactively reviewed by an organization:

- **Offline backups:** ensure that offline Domain Controller backups (System State) are secured and stored separately from online system state backups.

- **Encryption:** backup data should be encrypted both during transit (over the wire) and when at rest or mirrored for offsite storage.

- **Configure alerting for backup operations:** backup products and technologies should be configured to detect and provide alerting for operations that are critical to the availability and integrity of backup data (e.g., deletion of backup data, purging of backup metadata, restoration events, media errors).

- **Data Retention:** backup products and technologies should ensure that backups are retained for a pre-defined period-of-time before overwriting or purging data.

- **Enforce role-based access control:** Access to backup media and the applications that govern and manage data backups should utilize role-based access controls, to restrict the scope of accounts that have access to the stored data and configuration parameters.

- **Testing and verification:** An organization should periodically test and verify that data can be restored and reconstituted from both online and offline media sources. Both authoritative and non-authoritative Domain Controller restoration processes should be documented and tested.

Group Policy Objects (GPOs)

Permissions

A common tactic utilized by ransomware operators is to deploy encryptors by modifying an existing GPO configuration, or by creating a new GPO, and linking either at the root of the domain or to a large scope of Organizational Units (OUs) that contain computer objects. By leveraging scheduled tasks, startup / logon scripts, or software installation package settings within GPOs, ransomware operators are able to leverage native functionality within Active Directory to accomplish their mission, without the need to directly interface with each endpoint to invoke encryptors across an enterprise environment.

Proactively, organizations should review the scope of configured GPOs, and the last modified timestamp of a GPO to ensure that all modifications align to authorized and expected activities.

```
get-gpo -all | export-csv -path "c:\temp\gpo-listing-all.csv"
-NoTypeInformation
```

FIGURE 42. PowerShell command to review the scope of configured GPOs, including the last modified timestamp

Additionally, organizations should review permissions for existing GPOs—specifically focusing on the scope of accounts and groups that have the ability to modify GPOs within a domain. Any

accounts or security groups that have the ability to modify a large scope of GPOs, or GPOs that are linked-to and enforce security settings for a large scope of endpoints (e.g., Default Domain

Policy) should be carefully protected, and deemed to be privileged within a domain.

```
$permissions = Foreach ($GPO in (Get-GPO -All | Where {$ _ .
DisplayName -like "*"}))
     {
         Foreach ($Permission in (Get-GPPermissions $GPO.
DisplayName -All | Where {$ _ .Permission -like "*"}))
         {
             New-Object PSObject -property @{GPO=$GPO.
DisplayName;Trustee=$Permission.Trustee.
Name;Permission=$Permission.Permission}
         }
     }
$permissions | Select GPO,Trustee,Permission | Export-CSV c:\
temp\GPO-Permissions.csv -NoTypeInformation
```

FIGURE 43. PowerShell commands to list existing GPOs and assigned permissions

Monitoring Strategies

GPO modifications can be proactively detected by reviewing Security event logs on Domain Controllers for Event ID 5136, which requires that "Audit Directory Service Changes" auditing be enabled. Figure 44 provides an example of a Security event log detection for the Default Domain Policy GPO (well-known GUID of 31B2F340-016D-11D2-945F00C04FB984F9) being modified, and a Scheduled Task (client side extension of AADCED64-746C-4633-A97C-D61349046527) being added.

FIGURE 44. Event ID 5136 detection for GPO modifications

Virtualization Infrastructure Hardening and Protections

The widespread adoption of virtualization technologies for hosting critical applications, services, and operational processes has yielded an attractive target for threat actors seeking to deploy ransomware. Attackers understand that the potential impact of disrupting virtualized environments can lead to significant financial and operational pressure on victim organizations, especially when multiple systems and workloads may reside on a single physical host. Common tactics attackers leverage for impacting virtualized environments include:

• Encrypting a large-scope of virtual machines at scale.

• Accessing guest virtual machines (using a virtualization administrative console) for data theft / encryption.

• Changing the credentials for local administrative accounts within the virtualization platform, therefore restricting the ability for an organization to gain access for effective recovery and reconstitution.

• Joining VMware ESXi hosts to on-premises Active Directory to access ESXi hosts at scale using identities created in Active Directory

• Encrypting VMware ESXi host logs and disabling Virtual Machine logs in ESXi to evade defense controls

Additionally, virtualization platforms typically won't have endpoint detection and response (EDR) software installed, resulting in low visibility and an optimal target for attackers. Organizations must proactively align proper defenses, segmentation strategies, hardening efforts, and detection mechanisms to minimize the risks related to ransomware deployment within virtualization environments.

For organizations that are facing the threat of potential ransomware deployment or compromise, the following checklist (Table 6) should be considered to isolate and protect virtualization platforms.

Virtual Infrastructure Attack Surface Reduction Category	Actions
Network Segmentation	• Isolate and restrict access to virtualization hosts / servers / applications. • Ensure that backups of virtual machines are isolated and secured.
Identities	• Unbind authentication for accessing virtualization platforms from the centralized identity provider (e.g., Active Directory). • Proactively rotate local root / administrative passwords for privileged identities associated with virtualization platforms. • Enforce randomized passwords for local root / administrative identities correlating to each virtualized host that is part of an aggregate pool.
Virtualization Platforms	• Disable / restrict SSH (shell) access to virtualization platforms. • Enhance monitoring to identify potential malicious / suspicious authentication attempts and activities associated with virtualization platforms.

Table 6. Considerations to isolate and protect virtualization platforms

Identity Segmentation and Isolation

Organizations should proactively create isolated, dedicated, and segmented identities that are assigned administrative permissions for managing virtualization platforms. This strategy should avoid assigning privileged roles to identities originating from **a centralized identity store** (e.g., Active Directory or LDAP authentication providers). Integrating a virtualization platform with a centralized identity provider for administrative access introduces a potential privilege escalation path for attackers. If a user account within the identity store is compromised, attackers could leverage those credentials to gain administrative control of the virtualization platform.

In addition to utilizing dedicated and isolated accounts for privileged access to virtualization platforms, organizations should also:

- Use unique and strong passwords for all local accounts for the virtualization infrastructure.
    - For VMware environments, this should include leveraging a randomized password for the root account on each ESXi host and vCenter Server Appliance.
- Enforce multi-factor authentication (MFA) for the identities that require privileged access
- Store the credentials for the identities (including root account password) in a secured Privileged Access Management (PAM) system.

If completely separating user identities for privileged access within the virtualization platform might not be possible, organizations should review the scope of identities assigned privileged roles and utilize dedicated groups within the identity provider to manage and store unique accounts for accessing the virtualization platform. To reduce the attack surface and exposure, any accounts assigned privileged roles should be separate from accounts used for other administrative purposes and should be:

- Configured with a strong / randomized password
- Configured for MFA enforcement
- Governed by operational controls that restrict how and where the account(s) can be utilized (e.g., denying the accounts the ability to be leveraged for remote or interactive logons on endpoints throughout the environment).

If VMware vCenter Server is utilized, this platform provides a centralized capability to manage and control multiple ESXi hosts that are part of an aggregate pool. VMware vCenter also supports single sign-on capabilities via integration with an external identity provider. Organizations should review the scope of domains where identities are stored that are also assigned privileged roles in vCenter, and ensure that the correlating accounts are secured following the guidelines of a Tier 0 identity. An example of privileged roles when single sign-on domain integration is used within vCenter include:

- `Administrators`
- `Vclsadmin`
- `VM Power User`

Vpxuser Account

If an attacker is able to access VMware vCenter, this provides the capability to control virtual machines running across all ESXi hosts that are part of a managed pool. The interaction between ESXi hosts and vCenter leverages the `vpxuser` account. Harvesting credentials for the `vpxuser` service account from a vCenter server will provide root privileges across all ESXi hosts managed by the vCenter server. It is therefore critical to restrict and limit access to the vCenter application and server(s) hosting the application. This strategy should include both identity and network-layer segmentation controls.

If there is a suspected compromise of the `vpxuser` account, the following measures should be considered:

- Do not manually reset the password for `vpxuser` account - as this will break functionality between vCenter and ESXi hosts. Rather, organizations should modify the default expiry time in vCenter for the `vpxuser` account to a shorter timeframe (e.g., 24 hours). This will automatically reset the account password based upon the desired interval (default password change = 30 days for the `vpxuser` account).

- If an organization is leveraging ESXi v8.0 (or later), the `vpxuser` account can be deactivated from having shell access on the ESXi hosts.

Network Segmentation / Infrastructure Hardening

Attackers commonly gain direct access to virtualization platforms using the following connectivity methods:
- SSH (TCP/22)
- Administrative consoles (using a web browser) (TCP/443)
- Web-based APIs (TCP/443)
- VMware vSphere web client (TCP/902)

Organizations should configure virtualized kernel network adapters to be resident on dedicated management and communication networks, where either Layer 3 network configurations or local firewall settings (e.g., VMware ESXi host firewall) enforce isolation from the greater organization infrastructure. This architecture design can also be leveraged for traffic management and routing for dependent technologies such as storage communications, replication, and administrative access to the virtualization platform. Additionally, the network architecture should require that direct access to the virtualization platform (e.g, SSH connectivity, web access to the virtualization management console) only be accessible from network segments that contain isolated management systems, which have additional segmentation and hardening controls enforced to minimize their exposure and attack surface.

As an additional hardening measure, remote SSH and shell access capabilities to the virtualization platforms should be disabled, as attackers will commonly leverage SSH connectivity as a means to gain access and stage ransomware binaries for encrypting data stores and images associated with the virtualization stack. If SSH connectivity cannot be fully disabled, at a minimum, organizations should configure an allow list to limit the source IP addresses that can bind to the virtualization platform using SSH or web API (which can be used to remotely start SSH services if disabled). The allow list should only permit access from isolated and hardened management systems (previously referenced).

VMware ESXi Lockdown Mode

If VMware ESXi is leveraged as the virtualization platform, enabling lockdown mode can reduce the risk of an attacker bypassing access controls and accessing the ESXi host(s) directly. Lockdown mode requires that all ESXi management and access must occur through a vCenter Server and console, where roles and access controls are centrally defined and enforced for the child ESXi hosts. This provides a capability to centralize management, privileges, and auditing for a distributed collection of ESXi hosts.

Visibility and Monitoring

Organizations should ensure that centralized SIEM / logging aggregation platforms are capturing authentication, authorization, access events, and configuration changes related to virtualization platforms. Proactively, organizations should baseline and normalize authentication and access events for the virtualization stack, and alert on any potential access attempts when privileged identities and access is being leveraged.

The following VMware articles cover the locations of log locations for both vCenter and ESXi. For syslog forwarding configurations for these architectures, reference:

- Configuring Syslog on ESXi Hosts
- ESXi Syslog Options

Virtualization Recovery Preparation

Attackers with a goal of disruption or ransomware deployment will often modify root passwords on virtualization platforms as part of their attack chain. In addition to the hardening strategies previously outlined, organizations should plan and practice for recovery of access to virtualization platforms as part of proactive technical and process validation exercises.

For organizations that leverage VMware ESXi, the processes for consideration outlined in Table 7 should be exercised and validated.

ESX / ESXi Version	Steps to Regain Access
ESXi 4.0+	If the host is managed by vCenter and is still connected, the host profile feature within vCenter can be utilized to reset the root password. This method requires an **Enterprise Plus** license.
	If the ESXi host is integrated and joined to an on-premises Active Directory, an account that is a member of the ESX Admins Active Directory group can be used to reset the root password of an ESXi host.
	Reinstalling the ESXi host.
ESXi version 3.5 - 7.0 (Update 1)	Booting an ESXi host using a Linux boot disk and either:
	• Modifying the /etc/shadow file
	• Copying the /etc/shadow file from another ESXi host (replacing the stage.tgz archive)
ESX 3.x and 4.x	Rebooting the ESX host into the Service Console to set a new root password.

TABLE 7. VMware ESXi processes for consideration

Backup Infrastructure Protections

Organizations must align protections for the underlying infrastructure, servers, and applications that are part of backup and recovery operations. Not only is it important to protect the integrity of backups, but the availability of the backup infrastructure is a key component for any restoration strategy. If the backup infrastructure (and underlying data elements) were to become inaccessible or encrypted, rebuilding or recovering the infrastructure will become a dependency to restoration efforts, prolonging recovery and reconstitution time frames.

Dependency and Interconnectivity Identification

Organizations must identify dependencies and the interconnectivity requirements for the backup infrastructure to be available and accessible. Common dependencies include, but are not limited to:

• An Identity Provider (IdP) such as Active Directory
• Multi-factor authentication platforms
• Any administrative platforms such as secure access workstations or bastion hosts
• Access to emergency access account credentials
• DNS communications
• Storage Connectivity (on-premises + cloud)
• Data at rest (online + offline)
• Physical or Virtualization Infrastructure
• Licensing and trusted software binaries (if backups software needs to be reinstalled)
• Encryption keys (for decrypting backup data)
• SLAs with backup vendors for expedited assistance and technical support

Backup Architecture Design

The effectiveness and timeliness of an organization's backup and recovery workstreams will be dependent on the design of the overall backup architecture. Common design considerations are outlined in Figure 45.

CapEx / OpEx	Backup / Recovery Architecture	Pros	Cons	Recovery Time
Highest $	**Isolated Recovery Environment**	• Backup data unlikely to be directly accessible by an attacker • Backup systems and dependent infrastructure is isolated and pre-staged • Integrated validation capabilities for assurance	• High capital and operational expenses • Additional operation and administrative requirements	**Shortest**
	Isolated Data Vault **Offline + Immutable Backups**	• Backup data unlikely to be directly accessible by an attacker	• Moderate capital and operational expenses • Requires functioning (available) production backup servers to access backup data • If suspected to be compromised forensic examination may delay availability of production systems for secure data restoration • Restoration of backup platforms (and dependent systems) will likely delay restoration efforts.	
Lowest $	**Online / Production Integrated Backups**	• Low capital and operational expenses • Ease of integration and management	• Could provide direct access to backups for an attacker, based upon the interconnected nature of the backup platforms and credentials that are integrated with a centralized IdP. • Requires functioning (available) production backup servers to access backup data. • If suspected to be compromised, forensic examination may delay availabilty of production systems for secure data restoration. • Restoration of backup platforms (and dependent systems) will likely delay restoration efforts.	**Longest**

Figure 45: Common backup and recovery designs

Additionally, organizations must align a recovery and reconstitution sequencing strategy, where business and operational criticality are essential drivers to the order of restoration actions. In the event of a large-scale ransomware attack where many applications, services, and data libraries need to be restored, without a pre-defined order of restoration, competing priorities amongst business units will likely contribute to prolonged restoration challenges.

Validated Recovery and Reconstitution Planning

Following a ransomware event, if an attacker's initial access date and ransomware malware self-propagation capability has not been determined, recovering from backups may pose a significant risk of an attacker's malware, backdoors, or malicious code being reintroduced into an environment. Organizations should plan for a strategy for secure and validated restoration of systems using isolated network enclaves, which do not permit direct access to the larger operating environment(s). This strategy can allow for an organization to:

- Ensure that restored endpoints and applications are configured using a secured (clean) baseline image
- Patch and harden systems and applications according to the organization's standards and requirements
- Validate that restored endpoints and application do not have identified indicators of compromise present
- Ensure that the appropriate security tooling, telemetry, and detection visibility is present

Segmentation and Hardening Strategies

Similar to the strategies outlined in the Virtualization Infrastructure Hardening and Protections section, key protections for ensuring the integrity and availability of backup infrastructure should include:

Focus Areas	Strategies
Identities	• Leveraging unique and separate (non-identity provider integrated) credentials for accessing and managing backup infrastructure, in addition to the enforcement of MFA for the accounts.
	• Securing offline copies of any emergency access (break glass) credentials used for administrative interactive access to backup systems.
	• For programmatic service accounts that are integrated with the backup infrastructure, leverage unique and separate accounts for this automation. Additionally, the passwords for the programmatic accounts should be proactively rotated on a 30-day basis.
Network Infrastructure	• Implementing firewall rules or access controls lists restricting inbound administrative traffic and protocols to the backup environment to a backup administration environment.
Backup Servers	• Ensuring that backup servers are isolated from the production environment, residing within dedicated, isolated backup networks on virtualization infrastructure isolated from the production environment.
Backup Data	• Protecting the integrity and availability of backup data - such as leveraging immutable backups or "write once, read many" (WORM) capabilities of some backup solutions. This process should also include aligning security controls and governance for backup retention policies, which can be leveraged as additional enforcement criteria for immutable backup protection strategies.
	• Securing offline copies of backup data.
Access Management	• Restricting administrative access to backup infrastructure via the use of secure access workstations / privileged access workstations, where protections are enforced at both the identity and endpoint layers.
Visibility and Monitoring	• Creating detection strategies and playbooks to identify and stop any illegitimate modifications to backup retention and purge policies
Planning	• Recovery preparation and testing of reconstituting backup infrastructure and associated applications.

Conclusion

Ransomware poses a serious threat to organizations, as attackers continue to utilize this tactic to monetize breaches. This white paper provided practical guidance on protecting against ransomware attacks and containing ongoing ransomware events. This white paper should not be considered a comprehensive guide on every tactic and control that can be used for this purpose, but it can serve as a valuable resource for organizations faced with this challenge. It is based on years of experience of helping our clients protect against and recover from ransomware attacks—and it can help your organization do the same.