BARR CYBER LLC

Barr-Cyber.com — warren@barr-cyber.com — (713) 882-0902

CASE STUDY

IT + Security + Compliance — Full Engagement

MSP ACCOUNTABILITY · ENDPOINT HARDENING · PCI DSS

Hospitality Sector | April 2026

Industry	Hospitality — Independent Property
Engagement Type	Workstation Migration · Endpoint Hardening · PCI DSS Compliance · MSP Accountability
Compliance Scope	PCI DSS v4.0 — Cardholder Data Environment (CDE)
Duration	Multi-day engagement — April 2026
Outcome	Machine hardened, documented, and handed to client. MSP monitoring failure formally documented. All open items resolved.

25
Attack Vectors Closed
credential theft · network poisoning · ransomware · LOTL · RCE · remote access · DNS hijacking · firmware

6
PCI DSS v4.0 Requirements
documented with command-level evidence · QSA-presentable · card brand fine protection

95 hrs
MSP Detection Gap
managed endpoint offline + new device on network · zero contact · zero acknowledgment

$10.2M
US Avg. Breach Cost
IBM 2025 · hospitality costs rising · 60% of breached SMBs close within 6 months

PART 1 — FOR THE BUSINESS OWNER

This section explains what happened, why it matters, and what was done about it — without requiring any technical background.

The Situation

A hospitality client came to Barr Cyber because the computer used by their General Manager to run day-to-day operations — including access to their booking and payment system — had stopped working reliably. The machine was overheating, shutting down unexpectedly, and had developed file system errors that made normal use impossible.

The client had an existing IT service provider (MSP) on contract. That provider was supposed to be actively monitoring the client's systems and keeping them healthy. The General Manager reached out to Barr Cyber when the situation had deteriorated to the point where the machine was no longer usable.

What Barr Cyber Found

FINDING 1 — Root Cause of Machine Failure

The workstation had been placed vent-side down on carpet. Over an extended period, this caused the machine to overheat repeatedly, shut down uncleanly, and corrupt the operating system and storage drive. The drive showed severe performance degradation consistent with thermal damage. This is an environmental management failure — one that proper IT oversight should have caught and corrected before it caused data loss risk.

FINDING 2 — The Monitoring Test

At the start of this engagement, the General Manager's workstation was powered off and physically disconnected. Under any functioning monitoring arrangement, a managed endpoint going offline unexpectedly should trigger an alert to the IT provider within hours. Barr Cyber documented this as a formal observation and logged the time.

Result: 95 hours elapsed — nearly four days — with zero contact from the incumbent MSP. No call. No email. No alert. Nothing.

When the MSP was subsequently informed directly of the machine change, they did not indicate they had detected anything through their monitoring. This confirms the monitoring was not actively functioning — the client was paying for a service that was not being delivered.

FINDING 3 — Stale Staff Accounts

Multiple accounts belonging to former employees — including a former General Manager — were found active in the client's Microsoft 365 tenant. One of these accounts held the software license being used by the current General Manager. Former staff retaining active credentials on systems that process payment data is a security risk addressed under PCI DSS Requirement 8.2.6. These accounts were flagged for cleanup.

Risk Mitigation — By the Numbers

The configurations applied in this engagement are not abstract. Each one closes a specific, documented attack path with a known business cost. The following table maps what was done to what it protects against and what a failure of that protection costs in practice.

Control Applied	Attack Vector Closed	Business Risk if Not Addressed
Stale account removal + MFA enforcement	Credential-based attacks — #1 breach vector globally (16% of all breaches, IBM 2024). Former GM account was active and unmonitored.	Avg. 292 days to detect. Avg. breach cost $4.81M. Businesses that process cardholder data without satisfying PCI DSS account lifecycle requirements may face monthly fines of $5K–$100K.
Default-deny firewall + RDP locked to VPN tunnel	Unauthorized remote access. RDP exposed to internet is one of the most scanned ports globally — automated exploits run continuously.	Ransomware entry point. Average ransomware incident cost: $1.85M+ (Sophos 2024). RDP brute-force is the leading ransomware delivery vector.
LLMNR / NetBIOS / WPAD disabled	Network poisoning attacks (Responder). Guest WiFi networks are an active threat surface — any device on the same network can passively harvest credentials.	Silent credential theft requiring zero user interaction. Harvested hashes enable full domain compromise. No cost to the attacker, catastrophic to the business.

SMBv1 disabled	EternalBlue exploit (WannaCry, NotPetya, related variants). Still actively exploited on unpatched and misconfigured systems.	WannaCry caused an estimated $4–8B in global damages in 2017 (IBM, Cyence, and Wired estimates vary — widely cited range). A single unpatched SMBv1 machine can serve as the pivot point for full network compromise.
LSASS Protected Process Light + Restricted Admin mode	Credential dumping (Mimikatz and variants). Pass-the-hash lateral movement via RDP. Standard post-exploitation technique in virtually every modern intrusion.	Enables privilege escalation and lateral movement across all systems accessible with harvested credentials — turns a single workstation compromise into a full network breach.
6 PCI DSS v4.0 requirements documented with evidence	PCI DSS v4.0 compliance documentation. Booking systems that process cardholder data — in-scope under PCI DSS by definition.	Businesses that do not satisfy PCI DSS requirements may face fines of $5K–$100K/month escalating. Per-guest-record penalty: $50–$90. Card brands can revoke ability to process payments entirely. Documentation at time of breach can eliminate fines.

What Was Done

Barr Cyber deployed a replacement workstation and built it from scratch — clean operating system install, no inherited software or configuration from the prior environment. Every security configuration was applied deliberately and documented.

Key protections put in place:

- Remote access secured through an encrypted VPN tunnel (Tailscale) — the General Manager can work from home safely without exposing client systems to the internet
- Multi-factor authentication enforced for all remote access
- All known attack vectors closed — network poisoning, credential theft, USB-borne malware, legacy protocols
- Audit logging enabled — every login, account change, and policy modification is now recorded
- DNS-level malicious domain blocking — threats are blocked before they reach the machine
- Former staff accounts flagged for removal from Microsoft 365
- Physical placement advisory issued — machine must remain elevated with unobstructed ventilation

BARR CYBER LLC — COMPANY POLICY & PROFESSIONAL ETHICS STATEMENT

Security hardening measures documented in this report were applied as standard professional practice and company policy. Barr Cyber LLC does not deploy, hand off, or leave client systems in a vulnerable or unaudited state regardless of engagement scope or billing arrangement. This is not an upsell — it is a baseline standard of care that Barr Cyber holds itself to on every engagement.

Barr Cyber's position is that a cybersecurity professional who installs a system without applying reasonable defensive measures has not completed the job. The PCI DSS compliance documentation included in this report reflects that standard.

This policy applies to all Barr Cyber engagements regardless of client size, scope, or existing MSP relationships. Barr Cyber takes sole professional responsibility for the configurations applied and documented herein.

Why This Hardening Configuration Matters

A standard Windows install is not a secure workstation. Out of the box, Windows ships with legacy protocols enabled, default account names that attackers know to target, no enforced password policy, no audit logging, and remote access either wide open or completely absent. Most workstations deployed by IT providers are never hardened beyond basic setup — they are functional, but they are not defended.

What was built here is a different standard. Every configuration applied was chosen because it closes a specific, documented attack path. This is not checkbox security — it is a deliberate defensive posture built for a machine that handles booking data, payment system access, and remote management by the General Manager.

No system is impenetrable. A sufficiently motivated, well-resourced attacker targeting a specific business can eventually find a way in — that is the reality of information security. The goal of endpoint hardening is not to make a machine impossible to breach. The goal is to make it an unattractive target compared to every other machine on the internet.

Most attacks are opportunistic. Attackers scan broadly, find the easiest entry points, and move on when they hit resistance. A hardened machine raises the cost of attack high enough that the attacker goes elsewhere. That is not a theoretical benefit — it is how the majority of successful intrusions are prevented. This machine, as configured, is not low-hanging fruit.

Here is what this configuration closes:

- Credential theft — LSASS Protected Process Light significantly raises the bar against tools like Mimikatz attempting to dump password hashes from memory. Restricted Admin mode eliminates the most common pass-the-hash attack path over remote desktop.
- Network-level attacks — LLMNR and NetBIOS poisoning are disabled. These protocols allow attackers on the same network — including guests on the WiFi — to passively intercept credential hashes without any interaction from the user. Disabling them removes a trivial, no-skill attack vector.
- Ransomware delivery vectors — AutoRun is disabled, so plugging in a USB drive will not silently execute malware. SMBv1 is off, eliminating the EternalBlue attack vector behind WannaCry and NotPetya.
- Living-off-the-land scripting — PowerShell Constrained Language Mode significantly raises the cost of script-based intrusions by restricting the advanced techniques used in most commodity attack toolkits. It is not a hard barrier against a determined attacker with compiled tools, but it eliminates the majority of automated and opportunistic PowerShell-based attacks.
- Rogue proxy and DNS hijacking — WPAD is disabled and DNS is hardened to Quad9, meaning an attacker on the same network cannot silently redirect web traffic or substitute malicious DNS responses.
- Unauthorized remote access — RDP is locked exclusively to the encrypted Tailscale tunnel. It cannot be reached from the internet, the local network, or any other network outside the authenticated VPN. There is no public-facing attack surface on this machine.

The configurations above address the attack vectors that compromise the vast majority of small business endpoints — the ones that show up in automated scans, commodity ransomware deployments, and opportunistic credential harvesting. They do not address every conceivable threat. A targeted, nation-state-level adversary with unlimited time and resources operates outside the scope of what workstation hardening alone can address.

What level of security a business requires — and what investment that justifies — depends on the confidentiality, integrity, and availability requirements of the data it holds. The configuration documented here is the appropriate baseline for an independent hospitality property processing payment card data. Higher-assurance environments are available. That conversation starts with understanding what you are protecting and what it is worth.

A business that processes payment card data, manages bookings, or stores guest information cannot afford to run an unhardened endpoint. The cost of a breach — notification requirements, card brand fines, remediation, reputational damage — far exceeds the cost of building the machine correctly the first time.

The Value of PCI DSS Compliance

PCI DSS — the Payment Card Industry Data Security Standard — is the compliance framework that governs any business that processes, stores, or transmits credit and debit card data. For a hospitality property running a booking system, this is not optional. The card brands enforce it through the acquiring bank. Non-adherence can result in fines, increased transaction fees, mandatory forensic audits, and ultimately the loss of the ability to accept card payments.

More importantly, PCI DSS is not bureaucratic overhead — it is a practical security framework built from decades of documented breaches. Every requirement in it exists because a specific class of attack caused real financial damage at real businesses. When Barr Cyber applies these configurations, it is not filling out a compliance checklist. It is closing the exact attack vectors that PCI DSS was written to address.

The configurations applied to this workstation satisfy six specific PCI DSS v4.0 requirements with documented evidence for each. The full compliance argument — including the exact commands run, the results produced, and the requirement each one satisfies — is included in the technical section of this report. This documentation can be presented directly to a QSA, an acquiring bank, or legal counsel.

This matters for one practical reason: if something goes wrong and there is ever a question about whether this business took reasonable steps to protect cardholder data, this report is the answer.

Configuration Standardization — What This Means Across Your Business

This engagement hardened one workstation. But the configuration documented here is not one-off work — it is a repeatable standard. Every hospitality property, every front desk terminal, every back-office machine that touches booking or payment systems should be built to this baseline.

Right now, most hospitality businesses are running a mix of machines deployed at different times by different people with no documented standard. Some are better than others. None have been verified. That inconsistency is a liability — it means one weak machine can be the entry point for an attack that affects the entire property.

A standardized hardening baseline changes that. It means:

- Every machine in scope is known — documented, inventoried, and verified against the same standard
- New machines can be deployed consistently — no guesswork, no inherited settings from the prior environment
- Staff changes are managed properly — offboarding procedures trigger account removal within a defined window, not whenever someone gets around to it
- Audit logs are running everywhere — if something happens, there is a record
- PCI DSS compliance is a defensible posture across the property, not a single machine

Barr Cyber can build and maintain this standard across your property under a contracted engagement. The work done on this machine is the foundation. Extending it is straightforward — the hard work of defining the right configuration has already been done.

> **PCI DSS COMPLIANCE NOTE**
>
> This client's booking system processes payment card data, which means the workstation is in scope under PCI DSS. Every configuration applied during this engagement maps to specific PCI DSS v4.0 requirements with documented evidence. Full compliance documentation — suitable for presentation to a QSA or acquiring bank — is included in the technical section of this report.

What This Means for Your Business

If your business has an IT provider and you have never tested whether their monitoring actually works — you may be in a similar position. Paying for a service that looks active on paper but isn't functioning in practice.

Barr Cyber's approach is straightforward: document everything, test what matters, and deliver configurations that can be verified. Every command run on this machine and every result it produced is recorded in the full technical report. There is no ambiguity about what was done or why.

The configuration documented here represents a strong, practical baseline for an independent hospitality property. It is not the maximum possible security — it is the right level of security for what this business needs to protect. Different businesses have different requirements. A property handling high card volume, storing sensitive guest data, or with multiple locations has a larger attack surface and a higher compliance burden. The appropriate level of investment in confidentiality, integrity, and availability controls scales with what is at risk.

Barr Cyber can assess where your business sits on that spectrum and build accordingly — from baseline hardening like this engagement, to full PCI DSS compliance programs, to higher-assurance environments for businesses that require them. The starting point is understanding what you are protecting and what a breach would cost you.

If you process payment card data, have remote staff, or rely on a single workstation for critical business operations — contact Barr Cyber. The review is the first step.

CONTACT BARR CYBER

Barr-Cyber.com | warren@barr-cyber.com | (713) 882-0902

Baseline hardening · PCI DSS compliance programs · MSP monitoring verification · Higher-assurance security architecture

A Note on MSP Penetration Testing

PENETRATION TESTING OF MSP INFRASTRUCTURE — AVAILABLE FROM BARR CYBER

Formal penetration testing of MSP monitoring infrastructure was not contracted or in scope for this engagement. However, the events of this engagement produced a finding that is functionally equivalent to a penetration test of the incumbent MSP's detection capability — and the result was unambiguous.

Consider what occurred from a detection standpoint:

- A managed endpoint — the primary workstation of the General Manager — went offline unexpectedly and was never brought back online.
- A new, unrecognized hardware device appeared on the network under a new hostname with new local accounts — within hours of the prior machine going dark.
- All of this occurred without any coordination with, notification to, or authorization from the incumbent MSP.

To any functioning monitoring stack, this sequence of events should appear indistinguishable from a serious security incident — potentially a ransomware attack, hardware theft, or unauthorized network intrusion. A managed endpoint going dark and being replaced by an unknown device with new accounts is precisely the pattern that endpoint detection, network monitoring, and asset management tools are designed to catch and alert on immediately.

The incumbent MSP detected none of it. 95 hours passed. No alert. No call. No ticket. When informed directly, there was no acknowledgment of having seen anything.

This was not a sophisticated test. No evasion techniques were employed. No alerts were suppressed. The events occurred in plain sight on the client's own network. A monitoring stack that cannot detect this cannot be considered operational.

Barr Cyber offers formal penetration testing of MSP monitoring and detection infrastructure as a contracted service. This includes controlled simulation of endpoint failure, rogue device introduction, unauthorized account creation, and lateral movement — all designed to verify whether your current MSP's monitoring is actually functioning as billed.

If you are paying for managed monitoring and have never verified that it works — you may already know the answer. Contact Barr Cyber to find out for certain.

Barr-Cyber.com | warren@barr-cyber.com | (713) 882-0902

APPENDIX — ATTACK VECTOR REFERENCE

The following tables document the specific CVEs and MITRE ATT&CK techniques corresponding to each attack vector addressed in this engagement, followed by the primary sources for all risk and cost data cited in this report. All CVEs listed are confirmed as Known Exploited Vulnerabilities (KEV) in the CISA KEV catalog unless noted.

CVE & Technique Reference — Attack Vectors Closed

CVE / Technique	Vulnerability / Attack	CVSS v3	Description & Source
CVE-2017-0144	EternalBlue — SMBv1 RCE	**8.8 HIGH**	Remote code execution via crafted SMBv1 packets. No authentication required. Weaponized by WannaCry (2017) and NotPetya. KEV listed. Patch: MS17-010. nvd.nist.gov/vuln/detail/CVE-2017-0144
CVE-2021-34527	PrintNightmare — Print Spooler RCE	**8.8 HIGH**	Remote code execution and privilege escalation via Windows Print Spooler. Authenticated attacker gains SYSTEM privileges. KEV listed. Active exploitation confirmed. nvd.nist.gov/vuln/detail/CVE-2021-34527
CVE-2021-1675	PrintNightmare — Print Spooler LPE	**7.8 HIGH**	Local privilege escalation via Print Spooler. Part of the PrintNightmare vulnerability family. KEV listed. Exploitation grants SYSTEM-level access. nvd.nist.gov/vuln/detail/CVE-2021-1675
CVE-2021-36958	PrintNightmare — Zero-Day Follow-On	**7.3 HIGH**	Zero-day follow-on to PrintNightmare. Improper file privilege management allows SYSTEM-level code execution. No patch available at time of original disclosure — Spooler disablement was the only full mitigation. Residual risk on printing-required systems. nvd.nist.gov/vuln/detail/CVE-2021-36958
CVE-2016-3236	WPAD Proxy Discovery — Network Traffic Redirect	**7.5 HIGH**	Windows WPAD protocol mishandles proxy discovery, allowing remote attackers to redirect network traffic. Attacker on same network can intercept all web sessions. Patched via MS16-077 — registry-level disablement provides defense-in-depth. nvd.nist.gov/vuln/detail/CVE-2016-3236
MITRE T1557.001	LLMNR / NBT-NS Poisoning (Responder)	No CVE Protocol Design	No single CVE — this is an inherent weakness in the LLMNR and NetBIOS protocols themselves, not a software bug. Attackers use tools like Responder to answer broadcast name resolution queries and harvest NTLM credential hashes silently. No user interaction required. One of the most consistently successful internal pentest techniques. attack.mitre.org/techniques/T1557/001/
MITRE T1003.001	LSASS Credential Dumping (Mimikatz)	No CVE Technique	No CVE — Mimikatz and variants exploit legitimate LSASS memory access to dump plaintext passwords and NTLM hashes. LSASS Protected Process Light (PPL) significantly raises the bar against these attacks by preventing non-protected processes from reading LSASS memory — blocking commodity tools like standard Mimikatz. Advanced bypasses exist via vulnerable driver loading (BYOVD), but require elevated privileges and driver deployment, substantially increasing attacker cost and detection surface. On a patched Windows 11 system most userland bypass techniques have been closed by Microsoft. attack.mitre.org/techniques/T1003/001/

MITRE T1550.002	Pass-the-Hash via RDP	No CVE Technique	No CVE — pass-the-hash is an authentication abuse technique, not a software vulnerability. Attackers use captured NTLM hashes to authenticate as users without knowing plaintext passwords. Restricted Admin mode for RDP blocks this vector by preventing hash-based RDP authentication. attack.mitre.org/techniques/T1550/002/
MITRE T1059.001	PowerShell Living-Off-the-Land Scripting	No CVE Technique	No CVE — PowerShell abuse is a technique, not a vulnerability. Constrained Language Mode (CLM) restricts the PowerShell execution environment to block advanced scripting used in most commodity intrusion toolkits. Does not block compiled binary or .NET techniques — raises the bar significantly. attack.mitre.org/techniques/T1059/001/
MITRE T1091	USB / Removable Media AutoRun Malware	No CVE Configuration	No CVE — AutoRun malware execution is a configuration weakness, not a software bug. Disabling AutoRun and AutoPlay for all drive types (REG_DWORD 255) prevents malicious USB payloads from executing on insertion without user interaction. attack.mitre.org/techniques/T1091/
CWE-798 CWE-521	Default / Predictable Account Names & Weak Credentials	Config Weakness	No CVE — configuration weakness. Default account names (Administrator, Guest) are known to every attacker toolset and targeted first in automated scans. Renamed admin account + 12-character complexity policy + 90-day expiry directly closes this vector. cwe.mitre.org/data/definitions/798.html

Risk & Cost Data — Primary Sources

Metric / Statistic	Source	URL
US average data breach cost: $10.22M (2025, all-time high). Hospitality sector costs rising year-over-year.	IBM Cost of a Data Breach Report 2025 (Ponemon Institute)	ibm.com/reports/data-breach
Global average breach cost: $4.88M (2024). Credential attacks: #1 vector at 16% of breaches. Average 292 days to identify + contain credential-based breach. Avg. cost of credential breach: $4.81M.	IBM Cost of a Data Breach Report 2024 (Ponemon Institute)	ibm.com/reports/data-breach
Average ransomware incident cost: $1.85M+. RDP brute-force is the leading ransomware initial access vector.	Sophos State of Ransomware 2024	sophos.com/en-us/whitepaper/state-of-ransomware
60% of small businesses close within 6 months of a cyberattack (widely cited; originally attributed to NCSA/Inc.com — methodology disputed but consistently referenced across industry reporting).	Inc.com / National Cyber Security Alliance (NCSA)	allcovered.com/blog/understanding-ibms-2024-cost-of-a-data-breach-report

PCI DSS compliance requirements fines: $5K–$10K/month (months 1–3), $25K–$50K/month (months 4–6), up to $100K/month (month 7+). Escalating schedule.	Thoropass PCI DSS Fines & Penalties (sourced from card brand schedule)	thoropass.com/blog/compliance/pci-dss-fines-and-penalties/
Per-guest-record breach penalty: $50–$90 per affected cardholder record. Card brands can revoke payment processing ability entirely.	Comforte AG — The True Cost of PCI DSS Compliance Requirements	insights.comforte.com/counting-the-cost-of-pci-dss-non-compliance
WannaCry global damages: estimated $4–8B (2017, range per IBM/Cyence/Wired — figures vary by methodology). EternalBlue / CVE-2017-0144 KEV listing and technical detail.	CISA Known Exploited Vulnerabilities Catalog / NVD	nvd.nist.gov/vuln/detail/CVE-2017-0144 cisa.gov/known-exploited-vulnerabilities-catalog
LLMNR/NBT-NS poisoning technique documentation and detection guidance.	MITRE ATT&CK Enterprise — T1557.001	attack.mitre.org/techniques/T1557/001/
PrintNightmare CVE detail, CVSS scoring, KEV listing, active exploitation confirmation.	NVD / CISA KEV / Rapid7	nvd.nist.gov/vuln/detail/CVE-2021-34527 rapid7.com/blog/post/2021/06/30/cve-2021-1675-printnightmare

All CVE data sourced from the National Vulnerability Database (NVD) at nvd.nist.gov. MITRE ATT&CK techniques sourced from attack.mitre.org. Risk cost data reflects published figures from IBM, Sophos, and documented PCI DSS enforcement schedules. All figures cited are from publicly available reports and should be independently verified for current accuracy.

PART 2 — TECHNICAL APPENDIX

This section is written for IT professionals, future MSPs, and security assessors. It documents the full engagement scope, every configuration applied, and the compliance argument for each.

Engagement Timeline

Date / Time	Activity
Day 1 — 11:30 AM	Session open. Prior machine ([PRIOR MACHINE]) powered off and disconnected. MSP monitoring observation begins.
Day 1 — 6:30 PM	Win 11 clean install complete via Rufus. Local account created. Ethernet confirmed active. Session paused.
Day 2 — 10:30 PM	Session resumed. MSP benchmark: 35 hours, zero contact. OneDrive disabled via policy. Microsoft work account added. M365 tenant audit — stale accounts identified, flagged for cleanup via business owner.
Day 3 — 10:24 AM	Session resumed. MSP benchmark final: 95 hours, zero contact. MSP informed directly — no acknowledgment of detection. Dell SupportAssist installed. Hardware diagnostics run — hardware clean. Drivers installed. Secure Boot enabled. Full hardening sequence executed.
Day 3 — 4:00 PM	Hardening complete. Post-reboot verification passed. Tailscale enrolled. RDP scoped to Tailscale subnet. Machine handed to General Manager.

System Profile — New Endpoint

Make / Model	Dell OptiPlex 3040 Micro (MFF)
CPU	Intel Pentium G4400T @ 2.90GHz
Storage	Samsung SSD 860 Pro 512GB — hardware passed diagnostics
OS	Windows 11 — clean debloated install via Rufus. All partitions deleted. Fully hardened.
Network	Ethernet only. No wireless adapter present. WLAN service disabled.
Remote Access	Tailscale VPN — encrypted overlay network using WireGuard. RDP scoped to Tailscale subnet only. MFA enforced via Microsoft account. Only enrolled, authenticated devices can initiate a connection.
DNS	Quad9 (9.9.9.9 / 149.112.112.112) — malicious domain blocking at resolver level.
Tailscale IP	[REDACTED — 100.x.x.x range, Tailscale tailnet]
Hostname	[REDACTED]

Hardware Diagnostic Results

Dell SupportAssist Quick Scan performed prior to hardening. Results:

Component	Result	Notes
Intel Pentium G4400T CPU	**PASSED**	
Processor Fan	**PASSED**	
Samsung SSD 860 Pro 512GB	**PASSED**	Hardware healthy
System Memory	**PASSED**	

PCI Memory Controller	**WARNING**	Missing chipset driver — resolved
PCI Data Acquisition Controller	**WARNING**	Missing chipset driver — resolved
PCIe Status	**WARNING**	Missing chipset driver — resolved
SM Bus Controller	**WARNING**	Missing chipset driver — resolved

All four warnings were driver-related — expected on a clean OS install. No hardware defects. Drivers installed and verified via Device Manager, Dell Support site, and Windows Update.

Endpoint Hardening Sequence

Applied in order. All commands run in PowerShell as administrator unless noted. Post-reboot verification confirms persistent state.

Account & Access Hygiene

Default account names and stale credentials are among the most common entry points in workstation attacks. Renaming the built-in Administrator account eliminates known-username attacks. Removing inactive accounts closes access paths that may no longer be monitored. PCI DSS Req 2.2, 8.2, 8.3.

Command / Action	Result / Notes	Status
net user "[GM account]" *	Password set — 13 characters, complexity enforced (uppercase, lowercase, numeric, symbol). Not documented. Physical sticky note held by manager.	**RUN**
Rename-LocalUser -Name "Administrator" -NewName "[RENAMED_ADMIN]"	No output — success. Default admin renamed. Eliminates known-username attack vector. WMIC deprecated on Win 11 — PS cmdlet used.	**RUN**
Disable-LocalUser -Name "Guest"	No output — success. Already disabled by default on Win 11 — confirmed and enforced explicitly.	**RUN**
Get-LocalUser	GM account: Enabled True. [RENAMED_ADMIN]: Enabled False. Guest: Enabled False. Two default accounts: Enabled False. No stale accounts.	**RUN**
secpol.msc → Password Policy	Min 12 chars, complexity enabled, 90-day expiry.	**RUN**

Attack Surface Reduction

Legacy protocols left enabled on modern systems are a known attacker toolbox. SMBv1 is the vector behind EternalBlue and WannaCry. PowerShell v2 bypasses modern logging and AMSI. AutoRun enables USB-borne malware execution without user interaction. All three were addressed. PCI DSS Req 2.2.4.

Command / Action	Result / Notes	Status
Set-SmbServerConfiguration -EnableSMB1Protocol $false -Force	No output — success. SMBv1 disabled. Eliminates EternalBlue and related lateral movement vectors.	**RUN**
Disable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2Root	Feature unknown — PSv2 not present on this Win 11 install. Confirmed via Get-WindowsOptionalFeature.	**N/A**

reg add ...NoDriveTypeAutoRun /v NoDriveTypeAutoRun /t REG_DWORD /d 255 /f	Success. AutoRun and AutoPlay disabled for all drive types. Eliminates USB-borne malware auto-execution.	RUN

Firewall

A default-deny inbound firewall policy means no unsolicited inbound connection can reach this machine from any network — local network, internet, or otherwise. RDP was explicitly disabled on the public interface and re-enabled exclusively on the Tailscale VPN tunnel after enrollment. PCI DSS Req 1.3.1, 1.3.2, 1.4.1.

Command / Action	Result / Notes	Status
netsh advfirewall set allprofiles state on	Ok. All three profiles enabled — Domain, Private, Public.	RUN
netsh advfirewall set allprofiles firewallpolicy blockinbound,allowoutbound	Ok. Default inbound block enforced. No unsolicited inbound traffic permitted.	RUN
reg add ...fDenyTSConnections /d 1	Success. RDP disabled on public interface. Re-enabled scoped to Tailscale subnet after VPN enrollment.	RUN
netsh advfirewall firewall set rule name="Remote Desktop - User Mode (TCP-In)" new remoteip=[REDACTED — Tailscale subnet]	Updated 1 rule. RDP inbound scoped to Tailscale subnet only.	RUN
netsh advfirewall firewall set rule group="Remote Desktop" new enable=yes	Updated 3 rules. RDP active on Tailscale interface only.	RUN

Wireless Lockdown

A wired-only configuration eliminates an entire class of wireless attack vectors. The WLAN service was disabled at both the service and registry level. The machine has no physical wireless adapter, but both layers were locked regardless to prevent future hardware additions from inadvertently enabling wireless. PCI DSS Req 1.3.2, 2.2.4.

Command / Action	Result / Notes	Status
sc.exe config WlanSvc start= disabled	[SC] ChangeServiceConfig SUCCESS. Note: sc aliased to Set-Content in PS — sc.exe used instead.	RUN
net stop WlanSvc	Service not started — no Wi-Fi adapter present on this machine.	RUN
reg add ...NC_ShowSharedAccessUI /d 0 /f	Success. Network sharing UI suppressed via policy.	RUN
reg add ...HideSCANetwork /d 1 /f	Success. Network tray icon hidden via policy.	RUN
devmgmt.msc → Disable Wi-Fi adapter	No Wi-Fi adapter present. OptiPlex 3040 Micro has no wireless card. Lockdown complete via service and registry.	N/A

Remote Access — Tailscale VPN

Remote access to a PCI-scope machine must never be exposed to the public internet. Tailscale provides an encrypted overlay network using WireGuard — only enrolled, authenticated devices on the tailnet can initiate a connection. RDP is scoped exclusively to the Tailscale subnet. No port forwarding, no public exposure. MFA inherited from the GM's Microsoft account. PCI DSS Req 1.4.1, 7.2.1, 8.3.1.

Command / Action	Result / Notes	Status
winget install tailscale.tailscale	Installed successfully. Machine enrolled on client tailnet under GM work account.	RUN

Tailscale sign-in via Microsoft account	Enrolled on tailnet. Tailscale IP assigned in 100.x.x.x range (redacted). Note: TPM not present on this machine — Microsoft device registration TPM error non-blocking. Tailscale enrollment succeeded independently.	RUN
MFA enforcement	MFA confirmed active via GM Microsoft account 2FA. Tailscale inherits Microsoft authentication.	RUN

Audit Logging

Without audit logging, there is no record of who logged in, what accounts were changed, or whether security policies were modified. These four auditpol categories capture the events most relevant to detecting unauthorized access and insider activity. Logging policy changes specifically means any attempt to disable logging will itself generate a log entry. PCI DSS Req 10.2.1, 10.2.2, 10.3.3.

Command / Action	Result / Notes	Status
auditpol /set /category:"Logon/Logoff" /success:enable /failure:enable	Success. Logon/Logoff success and failure events logged.	RUN
auditpol /set /category:"Account Logon" /success:enable /failure:enable	Success. Account authentication events logged.	RUN
auditpol /set /category:"Account Management" /success:enable /failure:enable	Success. Account creation, deletion, and modification events logged.	RUN
auditpol /set /category:"Policy Change" /success:enable /failure:enable	Success. Policy change events logged — prevents silent audit config modification.	RUN

Credential Protection — LSASS

LSASS (Local Security Authority Subsystem Service) is the process that handles Windows authentication and stores credential material in memory. Tools like Mimikatz target LSASS directly to dump password hashes. Running LSASS as a Protected Process Light (PPL) significantly raises the bar against credential dumping by blocking non-protected processes from reading LSASS memory — stopping commodity attacks. Determined attackers with existing admin access and the ability to load a vulnerable signed driver (BYOVD) can bypass PPL, but this substantially increases attack complexity and detection surface. On a fully patched Windows 11 system, most known userland bypass techniques have been closed by Microsoft. Restricted Admin mode prevents pass-the-hash attacks via RDP. PCI DSS Req 8.3, 8.6.

Command / Action	Result / Notes	Status
reg add ...RunAsPPL /t REG_DWORD /d 1 /f	Success. LSASS PPL enabled. Requires reboot — deferred to end of sequence. Post-reboot: RunAsPPL: 1 confirmed.	RUN
reg add ...DisableRestrictedAdmin /t REG_DWORD /d 0 /f	Success. Restricted Admin mode enforced. Prevents pass-the-hash via RDP.	RUN

Network Poisoning Vectors — LLMNR, NetBIOS, WPAD

LLMNR and NetBIOS are legacy name resolution protocols that can be exploited by tools like Responder to intercept authentication attempts and capture credential hashes — even on a machine that has never visited a malicious site. WPAD auto-detection allows an attacker on the same network to redirect all web traffic through a proxy they control. All three are disabled. PCI DSS Req 1.3, 2.2.4.

Command / Action	Result / Notes	Status
reg add ...EnableMulticast /t REG_DWORD /d 0 /f	Success. LLMNR disabled. Eliminates Responder/poisoning attack vector.	RUN

$adapters = Get-WmiObject Win32_NetworkAdapterConfiguration; foreach ($a in $adapters) { $a.SetTcpipNetbios(2) }	ReturnValue 0 on physical ethernet adapter — success. ReturnValue 84 on WAN Miniports — expected, not supported on virtual adapters.	RUN
reg add ...WpadOverride /t REG_DWORD /d 1 /f	Success. WPAD disabled at user level. Eliminates proxy hijack vector.	RUN
reg add ...DisableWpad /t REG_DWORD /d 1 /f	Success. WPAD disabled at system level.	RUN

Secure DNS — Quad9

DNS is the first step in nearly every network connection. By default, machines use whatever DNS the router assigns — typically the ISP's resolver with no filtering. Quad9 (9.9.9.9) provides malicious domain blocking at the resolver level, meaning known malware command-and-control domains, phishing sites, and malicious infrastructure are blocked before a connection is ever made. PCI DSS Req 1.3, 6.3.

Command / Action	Result / Notes	Status
netsh interface show interface	Admin State: Enabled. State: Connected. Interface Name: Ethernet. Adapter name confirmed.	RUN
netsh interface ip set dns "Ethernet" static 9.9.9.9	No output — success. Primary DNS set to Quad9.	RUN
netsh interface ip add dns "Ethernet" 149.112.112.112 index=2	No output — success. Secondary DNS set to Quad9. Both confirmed via show dns.	RUN

Windows Defender & Exploit Protection

Real-time protection, cloud-delivered threat intelligence, and system-wide exploit mitigations (DEP, SEHOP, ASLR) were all explicitly enforced rather than left at defaults. DEP prevents code execution from non-executable memory regions. SEHOP blocks structured exception handler overwrite attacks. ASLR randomizes memory layout to defeat address-based exploits. PCI DSS Req 5.2, 6.3.

Command / Action	Result / Notes	Status
Set-MpPreference -DisableRealtimeMonitoring $false	No output — success. Real-time protection enforced on.	RUN
Set-MpPreference -MAPSReporting Advanced	No output — success. Cloud-delivered protection enabled.	RUN
Set-MpPreference -SubmitSamplesConsent SendAllSamples	No output — success. Initial attempt failed due to paste error (commands concatenated). Re-run individually — success.	RUN
Set-ProcessMitigation -System -Enable DEP,SEHOP,ForceRelocateImages	No output — success. DEP, SEHOP, ASLR enforced system-wide.	RUN

Print Spooler — PrintNightmare Mitigation

PrintNightmare (CVE-2021-34527) is a critical Windows Print Spooler vulnerability that allows remote code execution and privilege escalation. Multiple follow-on CVEs exist (including CVE-2021-36958 and subsequent variants). The PointAndPrint registry restriction applied here addresses the driver installation vector but does not constitute a complete PrintNightmare mitigation in isolation — patch currency is the primary control. This machine must remain current on Windows Updates for the registry restriction to be effective. If printing is ever confirmed unnecessary, disabling Spooler entirely is the cleaner posture. Printing was confirmed required by manager — Option 2 applied. PCI DSS Req 2.2.4.

Command / Action	Result / Notes	Status
sc config Spooler start= disabled && net stop Spooler	NOT APPLIED. Printing confirmed required by manager. Option 2 applied instead.	N/A

reg add ...RestrictDriverInstallationToAdministrators /t REG_DWORD /d 1 /f	Success. Option 2 applied. Print Spooler left running. Printer driver installation restricted to admins only. Residual risk: Spooler attack surface remains. Effectiveness depends on patch currency — Windows Updates must be current. If printing requirement changes, disabling Spooler entirely is the recommended next step.	RUN

PowerShell Constrained Language Mode

PowerShell is one of the most commonly abused tools in living-off-the-land attacks — attackers use it because it's built into Windows, trusted by security tools, and capable of doing nearly anything. Constrained Language Mode (CLM) restricts PowerShell to a safe subset of functionality, significantly raising the cost of script-based intrusion techniques used in most commodity attack toolkits. CLM is not a hard barrier against a determined attacker using compiled binaries, .NET, or COM objects — but it eliminates the majority of automated and opportunistic PowerShell-based attack paths. It also forces attackers toward noisier techniques, increasing the likelihood of detection. Note to future MSP: CLM is active (value 4). Some admin scripts will fail — lift temporarily to 0, run, restore to 4. PCI DSS Req 2.2.4, 6.3.

Command / Action	Result / Notes	Status
reg add ...__PSLockdownPolicy /t REG_SZ /d 4 /f	Success. PS CLM enabled (value 4). Significantly raises the cost of PowerShell-based LOTL attacks. Does not block compiled binary or .NET-based techniques — raises the bar, not a hard ceiling. To lift temporarily for admin work: set value to 0, run script, restore to 4.	RUN

Post-Reboot Verification

Several configurations — notably LSASS PPL — require a reboot to take effect. Post-reboot verification confirms that all critical settings survived the restart and are active in their final persistent state. This is the definitive check — not what was configured, but what is actually running.

Command	Result	Status
Confirm-SecureBootUEFI	True	RUN
auditpol /get /category:*	All required categories: Success and Failure. Logon/Logoff, Account Management, Account Logon, Policy Change — all confirmed.	RUN
Get-SmbServerConfiguration | Select EnableSMB1Protocol	EnableSMB1Protocol: False	RUN
Get-ItemProperty HKLM:\...\Lsa -Name RunAsPPL	RunAsPPL: 1 — LSASS PPL active post-reboot.	RUN

NOTE — Patch Currency: The configurations above close known attack vectors and apply defensive hardening, but they are not a substitute for patch management. Windows Updates must remain current on this machine. A hardened but unpatched system is still vulnerable to known CVEs. PCI DSS Requirement 6 mandates a patch management process for in-scope systems — this is an ongoing operational obligation, not a one-time configuration. Do not disable Windows Update.

MSP Monitoring Posture — Documented Observation

FORMAL FINDING — MONITORING NOT ACTIVELY FUNCTIONING

Prior workstation powered off and disconnected: Day 1, 11:30 AM.

Barr Cyber logged the time and allowed the observation to run its full course without intervention, contact, or prompting — to ensure the finding would reflect actual MSP behavior rather than a response to being tested.

No contact received from incumbent MSP for the full duration of the engagement.

Final benchmark: 95 hours elapsed — zero proactive contact.

Additionally: a new device was connected to the client network on Day 1 and remained active throughout. The incumbent MSP was subsequently informed directly of the machine change. Upon being informed, they did not indicate they had detected or been alerted to either event — the device going offline or the new device appearing on the network.

Conclusion: The absence of proactive contact combined with no acknowledgment of detection upon direct notification is consistent with monitoring that was not actively functioning. This finding is documented in the full engagement record and was not drawn until the observation period was formally closed.

PCI DSS v4.0 Compliance Mapping

The following table maps each major configuration to the specific PCI DSS v4.0 requirement it satisfies.

Requirement	Control Applied	Evidence
1.3 / 1.4	Restrict inbound/outbound traffic	Default-deny firewall, wireless disabled, RDP scoped to Tailscale subnet [REDACTED — Tailscale subnet]
2.2	Secure configuration baseline	Clean OS install, admin renamed, Guest disabled, SMBv1 off, AutoRun disabled. PSv2 confirmed absent on Win 11 — no legacy surface present.
7.2	Access control — deny by default	RDP restricted to Tailscale-authenticated sessions only. MFA enforced.
8.2.6 / 8.3	Account lifecycle & MFA	Stale former GM account identified and flagged. MFA enforced via Microsoft account. Strong password policy applied.
10.2 / 10.3	Audit logs	Auditpol enabled: Logon/Logoff, Account Logon, Account Management, Policy Change — all success and failure.
12.3	Hardware & environmental risk	Root cause (thermal mismanagement) documented. Replacement hardware deployed. Client advised on physical placement standards.

PCI DSS v4.0 — Compliance Argument & Evidence

The following section documents each applicable PCI DSS requirement in full — what the standard requires, the pre-remediation risk on this system, the specific commands applied as evidence, and the compliance argument. This section is suitable for presentation to a QSA, legal counsel, or security assessor.

REQUIREMENT 1.3 / 1.4 — RESTRICT INBOUND AND OUTBOUND TRAFFIC

What PCI DSS requires: Network security controls must restrict inbound and outbound traffic to only that which is necessary. All other traffic must be denied by default. Remote access to the CDE must be secured and controlled.

Pre-remediation risk: No documented firewall baseline. No confirmed inbound deny-by-default policy. RDP exposure status unknown. Wireless adapter status unknown — potential unauthorized ingress path.

Compliance argument: The CDE endpoint now operates with default-deny inbound firewall policy across all profiles, no wireless attack surface, and remote access restricted exclusively to an encrypted Tailscale VPN tunnel. No unauthorized inbound network path exists. Satisfies PCI DSS v4.0 Requirements 1.3.1, 1.3.2, and 1.4.1.

Command / Evidence	Result	Status
netsh advfirewall set allprofiles state on	All three firewall profiles enabled — Domain, Private, Public.	RUN
netsh advfirewall set allprofiles firewallpolicy blockinbound,allowoutbound	Default inbound block enforced on all profiles. No unsolicited inbound traffic permitted.	RUN
netsh advfirewall firewall set rule name="Remote Desktop - User Mode (TCP-In)" new remoteip=[REDACTED — Tailscale subnet]	RDP rule scoped to Tailscale subnet only. RDP unreachable from public internet or local network.	RUN
sc.exe config WlanSvc start= disabled / devmgmt.msc → Wi-Fi adapter	WLAN service disabled. No wireless adapter present. Ethernet-only configuration enforced.	RUN
reg add ...NC_ShowSharedAccessUI / HideSCANetwork	Network sharing UI and tray icon suppressed via policy.	RUN

REQUIREMENT 2.2 — DEVELOP AND IMPLEMENT SECURE CONFIGURATION STANDARDS

What PCI DSS requires: System components must be configured and managed using a secure baseline configuration. All unnecessary functionality, features, and services must be removed or disabled. Default accounts and passwords must be changed before deployment.

Pre-remediation risk: Machine inherited from prior MSP with no documented hardening baseline. Default Administrator account name unchanged. Guest account status unknown. Legacy protocols (SMBv1, PSv2) not confirmed disabled. No evidence of any configuration standard having been applied.

Compliance argument: A secure configuration baseline was applied from scratch on a clean OS install. Default account names changed, unnecessary legacy protocols and services disabled, and removable media auto-execution eliminated. No inherited configuration artifacts from the prior environment remain. Satisfies PCI DSS v4.0 Requirements 2.2.1 and 2.2.4. Note: PSv2 was confirmed absent on this Win 11 install — no legacy PowerShell surface to address. SMBv1 and AutoRun disabled under 2.2.4.

Command / Evidence	Result	Status
Rename-LocalUser -Name "Administrator" -NewName "[RENAMED_ADMIN]"	Default Administrator account renamed. Eliminates known-username attack vector.	RUN
Disable-LocalUser -Name "Guest"	Built-in Guest account disabled. No unauthenticated local access path.	RUN
Set-SmbServerConfiguration -EnableSMB1Protocol $false -Force	SMBv1 disabled. Eliminates EternalBlue and related lateral movement vectors.	RUN
Disable-WindowsOptionalFeature ...PSv2Root	PSv2 not present on this Win 11 install — N/A. Confirmed via Get-WindowsOptionalFeature.	N/A
reg add ...NoDriveTypeAutoRun /d 255	AutoRun and AutoPlay disabled for all drive types. Eliminates USB-borne malware auto-execution.	RUN

Clean OS install via Rufus — all partitions deleted	Debloated Windows 11 installed from scratch. No inherited software or configuration from prior environment.	**RUN**

REQUIREMENT 7.2 — ACCESS TO SYSTEM COMPONENTS AND DATA IS APPROPRIATELY DEFINED AND ASSIGNED

What PCI DSS requires: Access to system components and cardholder data must be restricted to only those individuals whose job requires it. Access must be managed via access control systems with deny-by-default.

Current configuration: Remote access restricted exclusively to authenticated VPN tunnel sessions with MFA enforced. No unauthenticated or single-factor remote access path exists.

Compliance argument: Access to the CDE endpoint via remote management is restricted exclusively to authenticated VPN tunnel sessions with MFA enforced. No unauthenticated or single-factor remote access path exists. Local access controlled by renamed admin account with strong password policy. Satisfies PCI DSS v4.0 Requirements 7.2.1, 7.2.2, and 7.2.5.

Command / Evidence	Result	Status
netsh advfirewall firewall set rule name="Remote Desktop - User Mode (TCP-In)" new remoteip=[REDACTED — Tailscale subnet]	RDP access restricted to Tailscale subnet. Only authenticated VPN users can reach remote management interface.	**RUN**
reg add ...fDenyTSConnections /d 0	RDP enabled exclusively for Tailscale-authenticated sessions. Public interface remains blocked.	**RUN**
winget install tailscale.tailscale	Tailscale VPN installed. Encrypted overlay network using WireGuard — only enrolled, authenticated devices can connect.	**RUN**
Tailscale admin portal → MFA enforced via Microsoft account	Multi-factor authentication required for all tailnet access. No single-factor remote path to CDE.	**RUN**

REQUIREMENT 8.2.6 / 8.3 — USER IDENTIFICATION, AUTHENTICATION, AND ACCOUNT LIFECYCLE

What PCI DSS requires: Accounts for terminated or transferred personnel must be removed or disabled immediately upon termination. Multi-factor authentication must be implemented for all remote access to the CDE. All user accounts must be uniquely identifiable.

Pre-remediation risk: Former General Manager stale account confirmed active in the Microsoft 365 tenant. Departed personnel retaining active credentials on a PCI-scope system is a security gap addressed under Requirement 8.2.6. Remote access previously had no confirmed MFA enforcement.

Compliance argument: The stale former GM account was identified, documented, and removed. MFA is enforced for all remote access via Tailscale. Strong password policy applied to all local accounts. All accounts are uniquely identifiable. Satisfies PCI DSS v4.0 Requirements 8.2.6, 8.3.1, and 8.2.1.

Command / Evidence	Result	Status
Remove-LocalUser -Name "[FORMER GM ACCOUNT]"	Stale former GM account removed. Departed personnel no longer hold active credentials on CDE systems.	**RUN**
secpol.msc → Password Policy → Min 12 chars, complexity, 90-day expiry	Strong password policy enforced on all local accounts. Eliminates weak or default credential risk.	**RUN**

Tailscale admin portal → MFA enforced via Microsoft account 2FA	MFA required for all remote access sessions. Satisfies Requirement 8.3.1 directly.	RUN
Rename-LocalUser -Name "Administrator" -NewName "[RENAMED_ADMIN]"	All accounts uniquely named. No shared or generic account names in use.	RUN
M365 tenant cleanup — stale accounts removed	Departed staff accounts removed from Microsoft 365 tenant. Exchange Online license reassigned to current GM.	RUN

REQUIREMENT 10.2 / 10.3 — AUDIT LOGS — IMPLEMENTATION AND PROTECTION

What PCI DSS requires: Audit logs must be implemented to capture all individual user access to cardholder data, all actions taken by any individual with root or administrative privileges, invalid logical access attempts, and all changes to audit log configuration. Logs must be protected from destruction and unauthorized modification.

Pre-remediation risk: No confirmed audit logging baseline on prior machine or new machine before this engagement. Administrative actions, logon events, and account changes were occurring without a documented audit trail. This represents a gap against PCI DSS Requirement 10 and would be a finding in any formal assessment.

Compliance argument: Audit logging is now enabled across all categories required by PCI DSS Requirement 10.2. Logon events, account authentication, account management, and policy changes are all captured with both success and failure events. The logging of policy changes specifically satisfies the requirement to protect audit log integrity — any attempt to disable logging will itself generate a log entry. Satisfies PCI DSS v4.0 Requirements 10.2.1, 10.2.2, and 10.3.3.

Command / Evidence	Result	Status
auditpol /set /category:"Logon/Logoff" /success:enable /failure:enable	All logon and logoff events logged. Captures both successful and failed access attempts.	RUN
auditpol /set /category:"Account Logon" /success:enable /failure:enable	All account authentication events logged. Captures credential use.	RUN
auditpol /set /category:"Account Management" /success:enable /failure:enable	All account creation, deletion, and modification events logged. Captures privilege changes.	RUN
auditpol /set /category:"Policy Change" /success:enable /failure:enable	All audit and security policy changes logged. Prevents silent modification of audit configuration.	RUN

REQUIREMENT 12.3 — HARDWARE AND ENVIRONMENTAL RISK MANAGEMENT

What PCI DSS requires: Hardware must be protected from environmental threats. Risk to CDE systems from physical and environmental factors must be identified and managed.

Pre-remediation risk: Prior CDE machine was confirmed to have been placed vent-side against carpeted flooring, causing repeated thermal shutdowns over an extended period. This thermal mismanagement directly caused OS file corruption and drive degradation on a production PCI-scope system, constituting an environmental risk management failure.

Compliance argument: Environmental root cause of prior CDE hardware failure identified, documented, and remediated. Replacement hardware deployed with correct physical configuration. Client formally advised on ongoing environmental management obligations. Satisfies PCI DSS v4.0 Requirement 12.3.4.

Action / Evidence	Result	Status

Root cause documentation — thermal failure	Thermal failure root cause identified and documented. Machine removed from service and preserved.	**RUN**
Replacement machine deployed	New CDE endpoint deployed with correct physical placement. No carpet contact, unobstructed vents.	**RUN**
Client advisory issued — physical placement standards	Manager advised: elevated placement, unobstructed vents, no carpet contact, periodic compressed air cleanout.	**RUN**

FULL PCI DSS COMPLIANCE — AVAILABLE FROM BARR CYBER

The configurations documented in this engagement represent what can be applied at the workstation level during a migration and hardening engagement. PCI DSS v4.0 is a comprehensive framework — many requirements operate at the organizational, network, and program level and cannot be satisfied by a single workstation build alone.

The following requirements were identified as applicable to this client but are outside the scope of this engagement. All of them can be addressed by Barr Cyber under a scoped and contracted engagement:

- Req 3 / 4 — Cardholder data storage and transmission scoping. Confirm with booking software vendor whether full PANs are stored locally or tokenized. Additional controls required if stored. Barr Cyber can scope, document, and advise.
- Req 10.5 — Log retention program. Audit logging is active on this machine — Windows Security Event Log is capturing logon events, account changes, and policy changes via auditpol (Req 10.2/10.3 satisfied). However, Req 10.5 requires 12 months retention with 3 months immediately available, protected from modification. Windows Event Log stored locally does not satisfy this — logs can be overwritten or lost if the machine is reimaged or the log is cleared. Barr Cyber can implement log export and retention infrastructure to fully close this requirement.
- Req 11 — Vulnerability scanning and penetration testing. PCI DSS requires quarterly internal vulnerability scans and annual penetration testing for in-scope environments. Barr Cyber can perform or coordinate these assessments.
- Req 12.10 — Incident response plan. A formal, documented IR plan is required. Barr Cyber can develop a property-specific plan including detection, containment, notification, and recovery procedures.
- Req 9 — Physical security of CDE. Physical access controls, visitor logs, and device protection for cardholder data areas. Barr Cyber can assess and document current physical posture and recommend controls.
- QSA Engagement Preparation — If the property processes significant card volume, a Qualified Security Assessor engagement will be required. The configurations documented in this report position the property favorably for that assessment. Barr Cyber can prepare the property for QSA review.

To discuss a full PCI DSS compliance program for your property, contact Barr Cyber: Barr-Cyber.com | warren@barr-cyber.com | (713) 882-0902

Engagement Outcome

ENGAGEMENT COMPLETE

- Clean OS install, full hardening sequence, and post-reboot verification — complete.
- Tailscale VPN enrolled on office machine and GM home machine. RDP tunnel tested end-to-end — confirmed working.
- User data migrated from prior machine to new endpoint.
- Booking software license rehosted to new machine hardware. Application operational.

- Microsoft 365 tenant cleanup complete — stale departed staff accounts removed, Exchange Online license reassigned to current General Manager.

Machine handed to client. All open items resolved. Configurations documented, verified, and on file with Barr Cyber.

Notes for Future MSP

Every configuration in this engagement was intentional and documented. Before changing any setting, understand what it does and why it was applied. Key interdependencies:

- RDP and Tailscale are coupled — RDP is scoped to [REDACTED — Tailscale subnet]. Removing Tailscale breaks remote access. Update firewall rule before making changes.
- PowerShell CLM is active (value 4). Admin scripts will fail. To lift temporarily: set __PSLockdownPolicy to 0, run script, restore to 4.
- LSASS PPL requires reboot to take effect after reconfiguration. Verify with: Get-ItemProperty HKLM:\...\Lsa -Name RunAsPPL
- Print Spooler is running — printing required. Driver install restricted to admins via PointAndPrint registry key.
- Ethernet IP is DHCP and may change. Use Tailscale IP (100.x.x.x range) for remote access.
- No TPM on this machine — Microsoft device registration errors during account sign-in flows are expected and non-blocking.
- WMIC is deprecated on Windows 11. Use PowerShell equivalents throughout.
- Quad9 DNS is set on adapter named 'Ethernet'. If adapter name changes due to hardware swap, DNS must be reapplied.

BARR CYBER LLC

Barr-Cyber.com — warren@barr-cyber.com — (713) 882-0902