100
/ 100

MACLOCKDOWN

Partially verified

MacBook Pro de JeeyDee · Version 26.3 (Build 25D125)
Generated 2026-03-17 12:32:22

FAILED	PASSED
0	36
UNVERIFIED	**TOTAL**
3	39

ℹ️ **Partially verified:** 3 check(s) could not be verified on this macOS version and were excluded from the score.

POSTURE EVOLUTION SINCE LAST SCAN

Security posture improved since the last scan. Risk trend: **Decreasing**.

SCORE DELTA	IMPROVED	REGRESSED	NEW RISKS
+7 93 → 100	2 controls restored since last scan	0 controls that lost protection	0 new failing controls introduced

CONTROLS IMPROVED

- Firewall
- Stealth Mode

✅ PASSED (36)

System Integrity Protection

PASS

Crítico · w:10 · basic · hardened · paranoid · `CIS CIS 5.1.5` `Apple Apple Security SIP`

WHAT IT DOES
Prevents any process — even root — from modifying protected system files, directories, and kernel extensions.

WHY IT MATTERS
Malware with root access can persist indefinitely if SIP is disabled. It is the last line of defense against kernel-level attacks.

⚠ THREAT INTELLIGENCE

T1562.001 Impair Defenses: Disable or Modify Tools — Defense Evasion

Attackers disable SIP to modify signed system binaries, inject into protected processes, or install persistent kernel extensions without detection.

XCSSET	Unknown (targets macOS devs)	macOS malware via Xcode projects
OSX.Dok	Unknown	First Mac malware to bypass Gatekeeper + SIP
Silver Sparrow	Unknown	M1-native macOS implant, 30k infections

Gatekeeper

PASS

Higiénico · w:5 · basic · hardened · paranoid · `CIS CIS 2.5.1` `NIST NIST SI-7`

WHAT IT DOES
Verifies that apps are signed by an identified Apple developer and have passed notarization before running.

WHY IT MATTERS
Without Gatekeeper, any unsigned app can run silently. Most macOS malware distributed via phishing relies on Gatekeeper being disabled.

⚠ THREAT INTELLIGENCE

T1553.001 Subvert Trust Controls: Gatekeeper Bypass — Defense Evasion

Disabling Gatekeeper allows execution of unsigned or tampered binaries. Most phishing-delivered macOS malware relies on Gatekeeper being off or bypassed.

OSX.Shlayer	Cybercriminal	Most prevalent macOS malware 2019-2021, delivered via fake Flash
OSX.Bundlore	Cybercriminal	Adware/spyware dropper, Gatekeeper bypass via DMG
APT32 (OceanLotus)	Vietnam	State-sponsored, macOS backdoors against journalists and dissidents

Automatic updates

PASS

Profesional · w:5 · basic · hardened · paranoid · `CIS CIS 1.1` `NIST NIST SI-2` `PCI DSS PCI DSS 6.3.3`

WHAT IT DOES
Enables automatic download and installation of macOS security updates and system data files.

WHY IT MATTERS
Most real-world attacks exploit known vulnerabilities. Unpatched systems are the easiest targets — patches exist but were never applied.

⚠ THREAT INTELLIGENCE

T1190 Exploit Public-Facing Application — Initial Access

Unpatched systems are primary targets. Most ransomware and APT campaigns exploit known CVEs that have patches available but not applied.

APT41	China (PLA Unit 61398)	Double Dragon — espionage + financial crime
Lazarus Group	North Korea (RGB)	WannaCry, Sony hack, $1.3B in crypto theft
FIN7	Russia/Ukraine	Carbanak — $1B+ bank heists via unpatched endpoints

Secure Token enabled

PASS

Crítico · info · hardened · paranoid · `Apple Apple SecureToken` `NIST NIST IA-5`

WHAT IT DOES
Verifies that the current user account has a Secure Token, which is required for FileVault encryption and recovery key generation.

WHY IT MATTERS
Without Secure Token, a user cannot unlock FileVault or perform cryptographic operations. Accounts without it are effectively excluded from disk encryption recovery.

FileVault

PASS

Higiénico · w:10 · basic · hardened · paranoid · `CIS CIS 2.6.1` `NIST NIST SC-28` `PCI DSS PCI DSS 3.5.1`

WHAT IT DOES
Encrypts the entire startup disk using XTS-AES-128 encryption with a 256-bit key.

WHY IT MATTERS
If your Mac is lost or stolen, anyone can remove the drive and read your files without encryption. FileVault makes this impossible.

⚠ THREAT INTELLIGENCE

T1005 Data from Local System — Collection

Without disk encryption, physical access or a stolen drive gives full data access. Intelligence agencies and border crossing scenarios are documented attack vectors.

NSA ANT Catalog	USA (NSA)	Physical implants documented in Snowden leaks — target unencrypted drives
Equation Group	USA (NSA/TAO)	Most sophisticated APT — HDD firmware implants bypass encryption
APT28 (Fancy Bear)	Russia (GRU)	Physical seizure of devices in Eastern Europe operations

Auto login disabled

PASS

Profesional · w:5 · basic · hardened · paranoid · `CIS CIS 2.7.3` `NIST NIST IA-2`

WHAT IT DOES
Verifies that automatic login is not configured — the Mac requires a password every time it boots or wakes from a full shutdown.

WHY IT MATTERS
Auto login bypasses the login screen entirely. Anyone who powers on your Mac gets immediate access to your session without entering a password.

⚠ THREAT INTELLIGENCE

T1078.001 Valid Accounts: Default Accounts — Initial Access / Persistence

Auto-login bypasses authentication entirely. Any physical or remote access (via another vulnerability) gives immediate session access without credentials.

CIA Vault 7 tools	USA (CIA)	Physical access tools documented by WikiLeaks target auto-login configs
Evil Maid attacks	Various nation-states	Hotel room physical access — documented against journalists and executives

Screen password

PASS

Higiénico · w:5 · basic · hardened · paranoid · `CIS CIS 2.4.3` `NIST NIST AC-11` `PCI DSS PCI DSS 8.2.8`

WHAT IT DOES
Configures macOS to require the user password immediately when the screen lock or screensaver activates.

WHY IT MATTERS
Without screen lock, anyone with physical access to your Mac — even briefly — can access all your data and credentials.

⚠ THREAT INTELLIGENCE

T1078 Valid Accounts — Initial Access

An unlocked screen gives immediate access to all open sessions, credentials in memory, and running applications without any authentication.

Physical access operations	All major APTs	Documented in NSA, CIA, GCHQ operational playbooks for targeted access
APT29 (Cozy Bear)	Russia (SVR)	DNC hack — physical access to unlocked workstations documented

Firewall

PASS

Higiénico · w:5 · basic · hardened · paranoid · `CIS CIS 3.4` `NIST NIST SC-7` `PCI DSS PCI DSS 1.4.1`

WHAT IT DOES
Activates macOS native firewall to filter incoming network connections per application.

WHY IT MATTERS
Without a firewall, any app can accept incoming connections. Attackers on the same network can reach services running on your Mac.

⚠ THREAT INTELLIGENCE

T1046 Network Service Discovery — Discovery

Without a firewall, all listening services are reachable from the local network. Attackers on the same network (coffee shop, hotel, corporate LAN) can probe and exploit open ports.

APT10 (Stone Panda)	China (MSS)	Cloud Hopper — lateral movement via unprotected internal services
APT41	China (PLA)	Mass exploitation of open services on enterprise networks
Sandworm	Russia (GRU)	NotPetya spread via open SMB/services on unprotected networks

Stealth Mode

PASS

Profesional · w:5 · hardened · paranoid · `CIS CIS 3.5` `NIST NIST SC-7`

WHAT IT DOES
Enables firewall stealth mode so the Mac does not respond to ICMP ping requests or connection attempts on closed ports.

WHY IT MATTERS
Without stealth mode, your Mac actively responds to network probes, making it visible and enumerable to attackers scanning the network.

⚠ THREAT INTELLIGENCE

T1595.001 Active Scanning: Scanning IP Blocks — Reconnaissance

Without stealth mode, ICMP ping responses and port scan replies allow passive enumeration of your device. Attackers use this to identify targets before exploitation.

Volt Typhoon	China (PLA)	Pre-positioned in US critical infrastructure — extensive network reconnaissance
APT28 (Fancy Bear)	Russia (GRU)	Systematic scanning of government networks documented in CISA advisories

Remote Login (SSH)

PASS

Profesional · w:5 · hardened · paranoid · `CIS CIS 2.3.1` `NIST NIST AC-17` `PCI DSS PCI DSS 2.2.2`

WHAT IT DOES
Checks whether SSH remote login is enabled. If active and not needed, disables the SSH daemon.

WHY IT MATTERS
An exposed SSH port is one of the most common attack vectors. Brute force and credential stuffing rely on SSH being reachable.

⚠ THREAT INTELLIGENCE

T1021.004 Remote Services: SSH — Lateral Movement

Exposed SSH is one of the most exploited services globally. Used for brute force, credential stuffing, and as a persistent backdoor after initial compromise.

Lazarus Group	North Korea (RGB)	SSH tunneling for C2 and data exfiltration in financial heists
APT29 (Cozy Bear)	Russia (SVR)	SolarWinds — SSH used for lateral movement in compromised environments
TeamTNT	Unknown (cybercriminal)	Cryptomining worm — scans internet for exposed SSH, 50k+ infections

File Sharing disabled

PASS

Profesional · w:5 · hardened · paranoid · `CIS CIS 2.3.3`

WHAT IT DOES
Checks that the SMB file sharing daemon is not running. If active, disables it.

WHY IT MATTERS
File sharing exposes your Mac to SMB exploits and allows unauthenticated enumeration of shared resources on the network.

⚠ THREAT INTELLIGENCE

T1021.002 Remote Services: SMB/Windows Admin Shares — Lateral Movement

SMB file sharing exposes network shares to enumeration and exploitation. EternalBlue and similar exploits target SMB services on accessible networks.

Sandworm	Russia (GRU)	NotPetya — SMB exploitation destroyed $10B in infrastructure globally
WannaCry operators	North Korea (Lazarus)	EternalBlue via SMB — 200k+ systems in 150 countries
APT41	China (PLA)	SMB lateral movement in enterprise intrusions

Printer Sharing disabled

PASS

Profesional · w:5 · hardened · paranoid · `CIS CIS 2.3.4`

WHAT IT DOES
Disables printer sharing via CUPS so local printers are not advertised or accessible over the network.

WHY IT MATTERS
Shared printers expose an unnecessary network service that can be exploited for information disclosure or lateral movement.

⚠ THREAT INTELLIGENCE

T1210 Exploitation of Remote Services — Lateral Movement

CUPS vulnerabilities have allowed remote code execution via exposed printer sharing. CVE-2024-47076 (CUPS RCE) affected all Linux/macOS systems with printer sharing enabled.

Opportunistic actors	Various	CVE-2024-47076 CUPS RCE — 9.9 CVSS, affects macOS printer sharing

Remote Apple Events disabled

PASS

Profesional · w:5 · hardened · paranoid · `CIS CIS 2.3.6`

WHAT IT DOES
Ensures the Apple Events server is not running, preventing remote applications from sending commands to your Mac via AppleScript.

WHY IT MATTERS
Remote Apple Events can be used to automate and control apps on your Mac from another machine — a significant attack vector if left open.

⚠ THREAT INTELLIGENCE

T1059.002 Command and Scripting: AppleScript — Execution

Remote Apple Events allow execution of AppleScript commands from other machines. Malware uses this for inter-process control, data theft, and persistence.

OSX.Komplex	Russia (APT28)	Backdoor using AppleScript for persistence — targets aerospace
APT32 (OceanLotus)	Vietnam	macOS backdoors using AppleScript for stealth execution

Screen Sharing disabled

PASS

Profesional · w:5 · hardened · paranoid · `CIS CIS 2.3.2`

WHAT IT DOES
Verifies that the screen sharing daemon (VNC) is not running. If active, disables it.

WHY IT MATTERS
Screen sharing exposes full graphical control of your Mac over the network. A compromised credential means complete system takeover.

⚠ THREAT INTELLIGENCE

T1021.005 Remote Services: VNC — Lateral Movement

VNC/Screen Sharing gives full graphical control. Weak or default credentials make it trivially exploitable. Widely targeted by ransomware operators for initial access.

REvil / Sodinokibi	Russia (cybercriminal)	Ransomware — VNC as primary initial access vector
Dharma ransomware	Iran (cybercriminal)	Exploits exposed RDP/VNC — $24M+ in ransoms
APT38	North Korea (Lazarus)	Bank heists using VNC for remote operator control

AirDrop limited

PASS

Profesional · w:5 · hardened · paranoid · `CIS CIS 2.4.11`

WHAT IT DOES
Checks AirDrop discoverability mode. Hardened requires it set to Off or Contacts Only — not Everyone.

WHY IT MATTERS
AirDrop set to Everyone allows any nearby Apple device to send files to your Mac without authentication — a vector for malware delivery.

⚠ THREAT INTELLIGENCE

T1091 Replication Through Removable Media / Proximity — Initial Access

AirDrop set to Everyone allows any nearby device to push files without authentication. Used to deliver malicious payloads in public spaces.

OSX.Shlayer variants	Cybercriminal	Malware delivered via AirDrop in public venues documented in 2020
Unknown APT (airport attacks)	Various	NSA/GCHQ documented AirDrop-style attacks at international airports

Internet Sharing disabled

PASS

Profesional · w:5 · hardened · paranoid · `CIS CIS 2.3.7`

WHAT IT DOES
Verifies that Internet Sharing is not active — your Mac is not routing its connection to other devices.

WHY IT MATTERS
Internet Sharing turns your Mac into a router, creating a secondary network that bypasses corporate or home firewall controls.

Wake on Network disabled

PASS

Profesional · w:5 · hardened · paranoid · `CIS CIS 2.9`

WHAT IT DOES
Disables Wake on Network (WoL) so the Mac does not power on in response to network packets.

WHY IT MATTERS
Wake on Network can be exploited to remotely power on a Mac and access it before security controls are active.

Guest User Disabled

PASS

Higiénico · w:2 · hardened · paranoid · `CIS CIS 2.7.1` `PCI DSS PCI DSS 8.2.2`

WHAT IT DOES
Disables the built-in Guest account that allows anyone to use the Mac without a password.

WHY IT MATTERS
The Guest account provides Safari and partial file system access without authentication. It can be exploited for local privilege escalation.

⚠ THREAT INTELLIGENCE

T1078.001 Valid Accounts: Default Accounts — Initial Access

Guest account provides unauthenticated access to Safari and partial filesystem. Used for local privilege escalation and bypassing full-disk encryption on unattended Macs.

Physical access red teams	Various	Documented in DEF CON/Black Hat physical security assessments
Evil Maid (Thunderstrike)	Various	EFI firmware attack — guest account used as initial access vector

Ad personalization disabled

PASS

Profesional · w:5 · hardened · paranoid · `NIST NIST PT-8` `Apple Apple Privacy`

WHAT IT DOES
Disables Apple's personalized advertising system, preventing your usage data from being used for ad targeting across Apple services.

WHY IT MATTERS
Personalized advertising requires Apple to build and maintain a behavioral profile of your activity across apps and services.

⚠ THREAT INTELLIGENCE

T1119 Automated Collection — Collection

Ad tracking creates behavioral profiles usable for targeting, social engineering, and correlating identities across platforms.

APT10 (Stone Panda)	China (MSS)	Ad ecosystem exploitation for target identification in Cloud Hopper
NSO Group (Pegasus)	Israel (commercial)	Ad tracking data used to correlate device identities of targets

Siri analytics off

PASS

Profesional · w:5 · hardened · paranoid · `NIST NIST PT-1` `Apple Apple Privacy`

WHAT IT DOES
Sets Siri data sharing opt-in status to opted-out (value 2), preventing Siri interactions from being sent to Apple for analysis.

WHY IT MATTERS
Siri analytics includes audio snippets and query content. Apple has contractors who listen to Siri recordings for quality review.

⚠ THREAT INTELLIGENCE

T1123 Audio Capture — Collection

Siri analytics includes audio snippets sent to Apple. Intelligence agencies have documented interception of voice assistant data from cloud providers.

GCHQ / NSA PRISM	UK/USA	Snowden: direct collection from Apple, Google cloud services including voice data
APT40 (Leviathan)	China (MSS)	Targets voice and audio data from cloud service providers

XProtect up to date

PASS

Crítico · info · basic · hardened · paranoid · `CIS CIS 1.2` `Apple Apple XProtect` `PCI DSS PCI DSS 5.2.1`

WHAT IT DOES
Verifies that XProtect, macOS's built-in malware detection engine, has current signature definitions. XProtect silently scans files when they are opened or downloaded.

WHY IT MATTERS
Outdated signatures mean new malware variants go undetected. XProtect is the last passive line of defense for users who don't run third-party AV.

⚠ THREAT INTELLIGENCE

T1562.001 Impair Defenses: Disable or Modify Tools — Defense Evasion

Outdated XProtect signatures fail to detect new malware variants. Attackers time campaigns to exploit the window between malware release and signature update.

OSX.Shlayer	Cybercriminal	Evaded XProtect for months — Apple updated signatures retroactively
Silver Sparrow	Unknown	M1-native — operated undetected before XProtect update

MRT active

PASS

Crítico · info · hardened · paranoid · `Apple Apple MRT` `PCI DSS PCI DSS 5.2.1`

WHAT IT DOES
Checks that the Malware Removal Tool (MRT) binary is present. MRT runs automatically on login and removes known malware that has already been installed.

WHY IT MATTERS
MRT is the remediation layer — while XProtect blocks new infections, MRT removes existing ones. Its absence means infections may persist silently.

Rapid Security Response enabled

PASS

Profesional · w:5 · hardened · paranoid · `CIS CIS 1.1` `Apple Apple RSR` `PCI DSS PCI DSS 6.3.3`

WHAT IT DOES
Checks that Rapid Security Response (RSR) is enabled — Apple's mechanism to push critical security patches between full macOS updates, without requiring a restart.

WHY IT MATTERS
RSR patches actively exploited zero-days within hours of Apple's discovery. Without it, your Mac is exposed to known critical vulnerabilities between system updates.

⚠ THREAT INTELLIGENCE

T1189 Drive-by Compromise — Initial Access

RSR patches actively exploited zero-days. Disabling RSR leaves systems exposed to WebKit, kernel, and GPU vulnerabilities actively used in targeted attacks.

NSO Group (Pegasus)	Israel (commercial)	FORCEDENTRY — WebKit zero-click RCE, RSR patches were the primary mitigation
BLASTPASS	Unknown	Zero-click exploit chain — September 2023, RSR pushed within 72h of discovery

Login Items reviewed

PASS

Profesional · w:5 · hardened · paranoid · `CIS CIS 2.5.2` `NIST NIST CM-7`

WHAT IT DOES
Lists all applications and agents configured to launch automatically at login, including both user-visible Login Items and background Launch Agents.

WHY IT MATTERS
Malware and adware commonly persist by adding Login Items or Launch Agents. Unknown items launching at startup are a primary indicator of compromise.

⚠ THREAT INTELLIGENCE

T1547.015 Boot or Logon Autostart: Login Items — Persistence

Malware persistently adds itself as a Login Item. This is the most common persistence mechanism for macOS malware.

OSX.Shlayer	Cybercriminal	Login Item persistence — most prevalent macOS malware 2019-2021
OSX.XCSSET	Unknown	Spreads via Xcode — Login Item + LaunchAgent persistence
APT32 (OceanLotus)	Vietnam	macOS backdoors persist via Login Items targeting media, NGOs

Screensaver timeout ≤ 10 min

PASS

Higiénico · w:5 · basic · hardened · paranoid · `CIS CIS 2.4.1` `NIST NIST AC-11`

WHAT IT DOES
Verifies that the screensaver activates within 10 minutes of inactivity, ensuring the screen lock engages automatically when the Mac is left unattended.

WHY IT MATTERS
A Mac left unlocked for extended periods is physically accessible to anyone nearby. A short timeout is the simplest defense against opportunistic physical access.

⚠ THREAT INTELLIGENCE

T1078 Valid Accounts — Initial Access

A Mac left unlocked in a public or shared space is accessible to anyone. Physical access attacks exploit unattended sessions.

Physical access operations	All major APTs	Standard TTPs for targeted physical access — documented across CIA, NSA, GRU playbooks

Bluetooth Sharing disabled

PASS

Profesional · w:5 · hardened · paranoid · `CIS CIS 2.3.5`

WHAT IT DOES
Disables Bluetooth file sharing (OBEX), preventing other devices from browsing or transferring files to your Mac over Bluetooth.

WHY IT MATTERS
Bluetooth sharing allows nearby devices to access files without authentication. Combined with predictable device names, it is a viable attack vector in public spaces.

⚠ THREAT INTELLIGENCE

T1011.001 Exfiltration Over Bluetooth — Exfiltration

Bluetooth sharing (OBEX) allows nearby devices to browse and transfer files without user interaction if enabled.

BlueBorne	Security research (Armis)	8 CVEs — remote code execution via Bluetooth without pairing, 5B+ devices affected
KNOB attack	Academic (UCSB)	Bluetooth key negotiation attack — proximity-based MitM

Auto-join open WiFi disabled

PASS

Profesional · w:5 · hardened · paranoid · `CIS CIS 2.4.9` `NIST NIST SC-8`

WHAT IT DOES
Checks that macOS is not configured to automatically join open (unauthenticated) WiFi networks without user confirmation.

WHY IT MATTERS
Auto-joining open networks exposes your Mac to rogue access points and man-in-the-middle attacks. Attackers create hotspots with common names to intercept traffic silently.

⚠ THREAT INTELLIGENCE

T1557.003 Adversary-in-the-Middle: DHCP Spoofing — Credential Access / Collection

Auto-joining open networks allows rogue access points with common SSIDs to intercept all traffic before VPN activates.

Darkhotel	South Korea (suspected)	Luxury hotel WiFi attacks against executives — auto-join exploitation
APT28 (Fancy Bear)	Russia (GRU)	GRU Unit 26165 — rogue WiFi hotspots at OPCW, WADA, government buildings

Bonjour advertising limited

PASS

Profesional · w:5 · hardened · paranoid · `CIS CIS 2.4.12` `NIST NIST CM-7`

WHAT IT DOES
Disables mDNS/Bonjour service advertising so the Mac does not broadcast its presence and available services (printers, file shares, AirDrop) to other devices on the network.

WHY IT MATTERS
Bonjour advertisements expose the device name, OS version, and running services to anyone on the same network segment — useful intelligence for attackers doing reconnaissance.

⚠ THREAT INTELLIGENCE

T1040 Network Sniffing — Discovery / Credential Access

mDNS/Bonjour broadcasts expose device name, OS version, and running services. Used for passive fingerprinting without sending a single packet to the target.

Volt Typhoon	China (PLA)	Passive network reconnaissance before active exploitation — CISA 2024 advisory
APT28 (Fancy Bear)	Russia (GRU)	mDNS harvesting in hotel networks targeting diplomats and executives

Diagnostics sharing disabled

PASS

Profesional · w:5 · hardened · paranoid · `CIS CIS 2.6.6` `NIST NIST PT-1`

WHAT IT DOES
Disables automatic submission of crash reports, diagnostic data, and usage statistics to Apple and third-party developers.

WHY IT MATTERS
Crash reports can contain sensitive data including memory dumps, file paths, usernames, and application state. Automatic submission happens without per-report review.

⚠ THREAT INTELLIGENCE

T1020 Automated Exfiltration — Exfiltration

Crash reports contain memory dumps, stack traces, and file paths. Compromised or compelled diagnostic channels have been used to exfiltrate sensitive data.

APT10 (Stone Panda)	China (MSS)	Abuses legitimate channels (cloud sync, diagnostics) to blend exfiltration
FinFisher / FinSpy	Germany (commercial)	Sold to governments — exploits diagnostic data for target profiling

Location Services audited

PASS

Profesional · w:5 · hardened · paranoid · `NIST NIST PT-3` `Apple Apple Privacy`

WHAT IT DOES
Lists applications that have been granted access to Location Services, allowing review of which apps can determine the Mac's physical location.

WHY IT MATTERS
Location data is sensitive and persistent. Apps with background location access can track movements without obvious UI indicators.

⚠ THREAT INTELLIGENCE

T1430 Location Tracking — Collection

Apps with background location access enable persistent tracking. Intelligence operations use location data to map targets' movements and associations.

NSO Group (Pegasus)	Israel (commercial)	Zero-click location tracking — used against journalists, activists, heads of state
APT-C-23 (Two-tailed Scorpion)	Gaza (Hamas-linked)	Mobile surveillance targeting Israeli military via location-enabled apps

Remote Management disabled

PASS

Profesional · w:5 · hardened · paranoid · `CIS CIS 2.3.8` `NIST NIST AC-17`

WHAT IT DOES
Checks that Apple Remote Desktop (ARD) management is not active. ARD allows full remote control including screen viewing, file transfer, and command execution.

WHY IT MATTERS
Active ARD with weak or default credentials is a complete system takeover vector. It is frequently targeted in enterprise environments and by malware.

⚠ THREAT INTELLIGENCE

T1021.001 Remote Services: Remote Desktop Protocol — Lateral Movement

Apple Remote Desktop (ARD) gives full remote control. Exposed ARD is actively scanned and exploited by ransomware operators and APTs.

REvil	Russia (cybercriminal)	Kaseya attack — exploited remote management tools to deploy ransomware to 1500 orgs
APT41	China (PLA)	Uses ARD/RDP for persistent remote access in long-term espionage ops

Media Sharing disabled

PASS

Profesional · w:2 · hardened · paranoid · `CIS CIS 2.3.9`

WHAT IT DOES
Disables Home Sharing and Media Sharing, which advertise the Mac's Music and Photos libraries to other Apple devices on the local network.

WHY IT MATTERS
Media sharing exposes library metadata and content to any device on the network. Combined with network reconnaissance, it reveals user behavior and content.

iCloud Desktop & Documents audited

PASS

Profesional · w:5 · hardened · paranoid · `NIST NIST SC-28` `Apple Apple Privacy`

WHAT IT DOES
Checks whether iCloud Drive is configured to sync Desktop and Documents folders automatically to Apple's servers.

WHY IT MATTERS
When enabled, every file on your Desktop and in Documents — including sensitive documents, credentials files, and work files — is continuously uploaded to iCloud.

⚠ THREAT INTELLIGENCE

T1213 Data from Information Repositories — Collection

iCloud Drive continuously syncs Desktop and Documents. Cloud provider compromise or legal compulsion gives access to all synced files.

PRISM (NSA/GCHQ)	USA/UK	Direct collection from Apple iCloud — Snowden 2013
APT40 (Leviathan)	China (MSS)	Targets cloud repositories of research institutions and government contractors

Lockdown Mode available

PASS

Paranoid · info · paranoid · `Apple Apple Lockdown Mode`

WHAT IT DOES
Checks whether Lockdown Mode is enabled — Apple's extreme security mode that disables most attack surfaces including message link previews, web JIT, wired connections, and configuration profiles.

WHY IT MATTERS
Lockdown Mode is designed for journalists, activists, and individuals targeted by sophisticated nation-state attacks. It dramatically reduces the attack surface at the cost of significant usability.

Captive portal detection reviewed

PASS

Paranoid · w:2 · paranoid · `NIST NIST SC-7`

WHAT IT DOES
Disables the automatic captive network assistant that probes Apple servers when joining a new network to detect if a login page is required.

WHY IT MATTERS
The captive portal probe sends DNS and HTTP requests to apple.com immediately on network join — before VPN activates. On hostile networks, this reveals your device identity.

⚠ THREAT INTELLIGENCE

T1557 Adversary-in-the-Middle — Collection / Credential Access

Captive portal probes reveal device identity before VPN activates. On hostile networks, this leaks MAC address, hostname, and Apple ID associations.

APT28 (Fancy Bear)	Russia (GRU)	Documented MitM at international airports and conferences (OPCW, WADA)
NSA/GCHQ airport operations	USA/UK	Snowden: 'Quantum Insert' — network probes used for target identification at airports

Security audit logging active

PASS

Profesional · w:5 · hardened · paranoid · `CIS CIS 3.2` `NIST NIST AU-2` `PCI DSS PCI DSS 10.2.1`

WHAT IT DOES
Verifies that the BSM audit subsystem is active and logging security-relevant events including authentication attempts, privilege escalation, and file access.

WHY IT MATTERS
Without audit logging, there is no forensic trail of authentication failures, sudo usage, or file access. Incident response becomes guesswork.

⚠ THREAT INTELLIGENCE

T1070.001 Indicator Removal: Clear Windows Event Logs — Defense Evasion

Without audit logging, attackers can operate undetected. When logs are absent, there is no forensic trail for incident response or compromise detection.

APT29 (Cozy Bear)	Russia (SVR)	SolarWinds — operated undetected for 9+ months; log gaps key to evasion
Axiom (APT17)	China (MSS)	Systematically disables logging before long-term espionage operations

❔ UNVERIFIED (3)

Safari Suggestions disabled

UNKNOWN

Profesional · w:5 · hardened · paranoid · `NIST NIST PT-1` `Apple Apple Privacy`

WHAT IT DOES
Disables Safari Suggestions, which sends the text typed in the address bar to Apple servers in real time to generate search and website suggestions.

WHY IT MATTERS
Every URL fragment and search term typed in Safari is transmitted to Apple before you press Enter. This includes sensitive internal URLs, credentials typed accidentally, and research queries.

⚠ THREAT INTELLIGENCE

T1056.004 Input Capture: Credential API Hooking — Collection

Real-time URL transmission to Apple exposes browsing behavior, internal URLs, and accidentally typed credentials before submission.

GCHQ KARMA POLICE	UK (GCHQ)	Mass surveillance of browser URL streams — Snowden documents
NSA XKeyscore	USA (NSA)	Real-time collection of browser activity including address bar input

TCP timestamps disabled

UNKNOWN

Paranoid · w:2 · paranoid · `NIST NIST SC-7` `CIS CIS 3.6`

WHAT IT DOES
Disables TCP timestamp options, which can reveal the system's uptime and help identify the OS version to remote scanners.

WHY IT MATTERS
TCP timestamps allow passive OS fingerprinting — an attacker can determine your exact OS version and uptime without sending a single packet directly to your Mac.

⚠ THREAT INTELLIGENCE

T1592.001 Gather Victim Host Information: Hardware — Reconnaissance

TCP timestamps reveal system uptime and allow precise OS fingerprinting. Used in target profiling before tailored exploitation.

Equation Group	USA (NSA/TAO)	Passive fingerprinting via TCP timestamps documented in Snowden/Shadow Brokers
APT28 (Fancy Bear)	Russia (GRU)	Network fingerprinting in pre-operation reconnaissance

Sudo timeout configured

UNKNOWN

Profesional · w:5 · hardened · paranoid · `CIS CIS 5.4` `NIST NIST AC-6`

WHAT IT DOES
Configures sudo to require password re-entry for every command (timeout=0), preventing privilege escalation from an unattended terminal session.

WHY IT MATTERS
By default, sudo caches credentials for 5 minutes. A malicious script running in an unattended terminal can silently execute privileged commands during this window.

⚠ THREAT INTELLIGENCE

T1548.003 Abuse Elevation Control Mechanism: Sudo — Privilege Escalation

Default sudo caching (5 min) allows malicious scripts to silently execute privileged commands during an active sudo session in an unattended terminal.

OSX.Coldroot	Unknown	macOS RAT — exploits sudo caching for privilege escalation
OSX.Pirrit	Israel (Adware)	Adware abusing sudo timeout for silent privileged installation

PCI DSS COMPARE

Evidence-based mapping only. This section shows which PCI DSS requirements are supported by local macOS checks, which mapped requirements still have gaps, and which controls still need manual evidence or are out of product scope.

MAPPED SCORE	COVERED	GAPS	MANUAL / N-A
100/100 8 of 8 mapped checks passing	8 requirements supported by passing device evidence	0 mapped requirements with failing or accepted-risk evidence	5 requirements outside local device-only validation

COVERED BY DEVICE CHECKS

PCI DSS 1.4.1 Personal firewall or network security controls active — COVERED
Evidence: Firewall

PCI DSS 2.2.2 Only necessary services and insecure remote access disabled — COVERED
Evidence: Remote Login (SSH)

PCI DSS 3.5.1 PAN and sensitive data protected with strong cryptography at rest — COVERED
Evidence: FileVault

PCI DSS 5.2.1 Anti-malware mechanisms deployed and active — COVERED
Evidence: MRT active · XProtect up to date

PCI DSS 6.3.3 Security patches and system components kept current — COVERED
Evidence: Automatic updates · Rapid Security Response enabled

PCI DSS 8.2.2 Guest, shared, or unauthenticated access restricted — COVERED
Evidence: Guest User Disabled

PCI DSS 8.2.8 Session lock and re-authentication enforced — COVERED
Evidence: Screen password

PCI DSS 10.2.1 Audit logs enabled for security-relevant events — COVERED
Evidence: Security audit logging active

MANUAL EVIDENCE REQUIRED

PCI DSS 3.6.1 Cryptographic key management and custodianship — MANUAL
Requires process evidence, escrow handling, and operational controls outside a local macOS hardening check.

PCI DSS 8.3.1 Multi-factor authentication for access into the CDE — MANUAL
MFA posture depends on identity providers, VPN, MDM, and enterprise access flows not validated by MacLockdown alone.

PCI DSS 10.4.1 Daily review of security logs and exceptions — MANUAL
MacLockdown can confirm local logging, but not centralized review workflows, alerting, or documented analyst procedures.

NOT COVERED BY THIS PRODUCT

PCI DSS 11.3.1 Internal vulnerability scanning — OUT OF SCOPE
MacLockdown is not a vulnerability scanner and does not perform authenticated internal scanning.

PCI DSS 12.10.5 Incident response training and readiness — OUT OF SCOPE
Organizational incident response planning, training, and testing are outside the scope of device-local controls.