



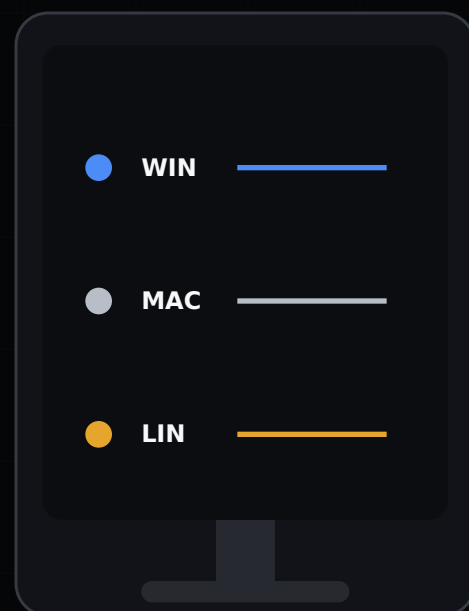
2026 FIELD GUIDE

RED.ONE DEVICE SECURITY

DESKTOP PRIVACY & SECURITY

WINDOWS PC + macOS + LINUX

A practical, protection-minded field guide for reducing exposure, securing data, and preparing workstations for everyday and higher-risk use.



COMBINED GUIDE

Three systems. One security baseline.

Start with the shared priorities below, then follow the section for each operating system you use. Exact labels can vary by version, edition, desktop environment, and organizational policy.

SHARED PRIORITIES

- Install security updates promptly
- Encrypt the system and backups
- Use strong authentication and MFA
- Limit apps, permissions, and services
- Harden browsers and network access
- Lock quickly and control the device
- Maintain tested offline recovery
- Use a dedicated travel device when warranted

01

Windows PC

12 focused configuration areas

02

macOS

10 focused configuration areas

03

Linux

12 focused configuration areas

01

Windows PC

WINDOWS 11 PRIVACY AND SECURITY

Why these settings matter

A Windows 11 system contains personal data, credentials, communications, browsing history, and sensitive work product. Default settings are insufficient for strong privacy when a PC supports professional, travel, or executive-level operations.

Use the pathways below to reduce telemetry, limit cloud and application exposure, and harden the machine against unauthorized access. Some settings trade convenience for protection; align them with your threat model and operational needs.

01

Software Updates

Purpose: Maintain current patches to reduce exposure to known exploits.

RECOMMENDATIONS

- Go to Settings > Windows Update > Check for updates.
- Enable Settings > Windows Update > Advanced options > Receive updates for other Microsoft products.
- Enable downloads over metered connections only if operational needs require it.
- Remove unused applications to reduce the attack surface.

02

Microsoft Account, Sign-in and Recovery

Purpose: Secure synchronization, account recovery, and cloud access.

- Use a strong, unique Microsoft account password under Settings > Accounts > Your info.
- Enable two-step verification at account.microsoft.com/security.
- Disable Dynamic Lock if it is not required. Use facial recognition or fingerprint only when operational benefits outweigh biometric privacy concerns.
- Review and remove old or unknown devices at account.microsoft.com/devices.

03

Local Account Option

A local account can reduce cloud-level telemetry and remote recovery linkages.

- Convert at Settings > Accounts > Your info > Sign in with a local account instead.
- Maintain a strong password and a secure recovery process for a local-only configuration.

04

Device Encryption and BitLocker

Purpose: Protect data at rest if the computer is lost, stolen, or accessed physically.

- Windows 11 Pro or Enterprise: Control Panel > System and Security > BitLocker Drive Encryption > Turn on BitLocker.
- Windows 11 Home, when supported: Settings > Privacy & security > Device encryption > Enable.
- For strongest protection, configure TPM + PIN through gpedit.msc > Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Require additional authentication at startup.
- Store recovery keys offline in secure physical storage.

05

Privacy Controls and Telemetry Reduction

Windows collects diagnostic and personalization data by default. Reduce collection that is not operationally necessary.

- Settings > Privacy & security > General: turn off advertising and tracking toggles.
- Turn off Online speech recognition and Inking & typing personalization when not needed.
- Diagnostics & feedback: choose Required only; disable Improve inking & typing and Tailored experiences.
- Activity history: stop storing history on the device and clear existing history.
- Location: disable it entirely or restrict it to essential applications.
- App permissions: review Camera, Microphone, Contacts, Phone calls, Messages, Videos, and File system; deny unnecessary access.

06

Account Sync, Cloud and OneDrive

Cloud synchronization increases the impact of remote account compromise.

- Settings > Accounts > Windows backup: turn off Remember my apps and Remember my preferences if unnecessary.
- Disable synchronization features that are not required.
- In OneDrive settings, review synchronized folders and exclude sensitive documents where practical.
- Consider disabling OneDrive entirely when it is not essential.

07

Web Browser Hardening

Browsers are major vectors for tracking, credential theft, and exploitation.

- Edge > Settings > Privacy, search, and services: set Tracking prevention to Strict and turn off personalization and advertising.
- Review the Do Not Track option based on operational need; it is only a request and may add fingerprinting uniqueness.
- Block third-party cookies, require confirmation for downloads, and remove unused extensions.
- Consider a hardened Firefox configuration for sensitive work.

08

Firewall and Network Controls

- Windows Security > Firewall & network protection: verify Domain, Private, and Public firewalls are enabled.
- Use Advanced settings > Outbound Rules to restrict unnecessary applications when appropriate.
- Forget Wi-Fi networks that are no longer used. Disable Wi-Fi and Bluetooth when not needed.
- On public networks, set the network profile to Public.

09

Application Control and Exploit Protection

- Windows Security > App & browser control: enable Reputation-based protection.
- Enable SmartScreen for Microsoft Edge and Microsoft Store apps.
- Windows Security > Device security > Core isolation: enable Memory integrity when compatible.
- App & browser control > Exploit protection: keep system-level mitigations enabled.

10

Physical Security and Lockdown

- Require sign-in every time and set a short screen timeout.
- Use a strong alphanumeric password rather than relying only on a simple PIN.
- When the threat model warrants, disable external boot in firmware security settings and use tamper-evident seals during travel.
- Avoid public USB charging stations; use your own power supply.

11

Backup, Monitoring and Incident Response

- Use BitLocker-encrypted external drives and configure local or offline backups. Test recovery and delete unneeded data regularly.
- Avoid automatic cloud backup for sensitive content unless mission-critical.
- Review Windows Security > Protection history and Event Viewer > Windows Logs > Security for abnormal events.
- If compromise is suspected: disconnect the network, change critical passwords from a trusted device, restore from a known-good offline backup, and review Microsoft account sessions.

12

High-Risk User Adjustments

- Use a dedicated travel laptop with minimal installed software.
- Disable unused wireless radios, use FIDO2 hardware authentication keys, and use a hardened browser or sandbox for sensitive operations.
- Avoid long-term storage of sensitive files on the device; use encrypted removable media when needed.
- Inspect the device for tampering during travel.

● Configuration takeaway

Windows 11 can be secured to a high level with correct configuration and discipline. Reducing telemetry, limiting cloud exposure, controlling permissions, and enforcing strong physical and network controls materially improves privacy. Consistent monitoring and operational awareness make these protections effective.

02

macOS

MAC PRIVACY AND SECURITY

Why these settings matter

A Mac holds identity data, communications, credentials, network access, and sensitive work. A protection-minded configuration maps each setting to a clear purpose and balances privacy with operational requirements.

Some steps reduce convenience. Choose the controls that match your threat model, then review them regularly as macOS and installed applications change.

01

Software Updates

Purpose: Patch vulnerabilities and stay ahead of adversary tools.

- System Settings > General > Software Update: turn Automatic updates on.
- Open Software Update > Advanced and enable relevant system files, security updates, and application updates. Use beta updates only when specifically required.
- Update App Store applications and check non-App Store applications manually.
- Uninstall software you no longer use.

02

Apple Account, iCloud and Account Security

- System Settings > Apple Account > Sign-In & Security: enable two-factor authentication and use a strong, unique password.
- Review the Devices list and remove anything unrecognized or no longer used.
- Review what iCloud synchronizes. Disable unnecessary categories and enable Advanced Data Protection when available and appropriate.
- If minimal cloud exposure is the priority, limit iCloud to essential services or disable it.

03

User Accounts and Disk Encryption

- System Settings > Privacy & Security > FileVault: enable full-disk encryption.
- Use a Standard account for daily work and reserve the administrator account for elevated tasks.
- Require the password immediately after sleep or the screen saver begins.
- On Apple silicon, restrict external and network boot unless specifically needed.

04

Application and System Privacy Controls

- Review Location Services, Camera, Microphone, Files and Folders, Accessibility, and Full Disk Access. Permit only applications that genuinely require access.
- Under Location Services > System Services, disable Significant Locations, Networking & Wireless, Product Improvement, and Suggestions unless required.
- Restrict Bluetooth and Local Network access to necessary applications.
- Under Analytics & Improvements, disable Mac analytics, developer sharing, and other telemetry that does not provide sufficient benefit.

05

Web Browsing and Tracking Mitigation

- Use a privacy-focused browser or harden Safari under Settings > Privacy.
- Enable Prevent cross-site tracking and available fingerprinting protection. Disable cross-app tracking requests where presented.
- Remove unused extensions and clear browsing history and website data regularly.
- Consider a privacy-focused search engine plus reputable tracker blocking or network-level DNS filtering.

06

Network and Connectivity Security

- For Wi-Fi networks, enable Private Wi-Fi Address and Limit IP Address Tracking when available.
- Disable Bluetooth when not needed. Enable the built-in firewall; consider LuLu or Little Snitch for application-level outbound monitoring.
- Use a trusted VPN with a strong protocol such as WireGuard on untrusted networks.
- Forget old Wi-Fi networks and disable unnecessary Sharing services such as File Sharing, Remote Login, and AirDrop.

07

Physical Security and Device Use

- Use a short lock-screen timeout and require the password immediately after sleep or screen saver activation.
- Consider a webcam cover or microphone blocker in high-risk environments.
- Restrict external boot and require administrator authentication for startup security changes.
- Avoid untrusted USB charging; use a trusted adapter or power bank. Keep the Mac under direct control and consider tamper-evident seals during travel.

08

Backup, Encryption and Data Lifecycle

- Use Time Machine with an encrypted backup disk and consider offline or air-gapped backups for highly sensitive data.
- Review iCloud Drive synchronization and exclude sensitive folders where practical.
- Keep Full Disk Access limited to approved applications.
- Review and delete data from unused applications and folders; remove sensitive photo metadata before sharing.

09

Incident Response and Monitoring

- Use Console.app to review system, kernel, and application logs. Establish a baseline for normal applications, network connections, and performance.
- If compromise is suspected: disconnect from networks, change key credentials from a trusted device, wipe and restore from a clean image, and review Apple Account sessions and device logins.
- Maintain tested backups and current incident-response contacts.

10

High-Risk and Targeted Users

- Use a dedicated travel Mac with minimal applications and separate accounts.
- Disable wireless radios when not needed. Use hardware MFA keys for critical accounts and consider strong alphanumeric passwords instead of biometric unlock.
- Use a hardened browser sandbox for sensitive tasks and restrict background services.
- Inspect for tampering, interceptors, keyloggers, and unauthorized peripherals during travel.

● Configuration takeaway

Hardening a Mac is a strategic process, not a one-time checklist. Align the configuration with the threat model, reduce unnecessary exposure, and maintain consistent habits. Regular review and discipline keep the protection effective.

03

Linux

PRACTICAL WORKSTATION HARDENING

Why these settings matter

Linux is often considered secure, but no platform is secure by default. A protected workstation depends on configuration, maintenance, strong authentication, and limiting unnecessary exposure.

These practices provide a strong baseline across Ubuntu, Linux Mint, Fedora, Debian, Arch, openSUSE, and other mainstream distributions. Confirm distribution-specific commands and policies before making changes.

01

Keep the System Updated

Install security updates promptly and keep the operating system, kernel, browser, applications, and firmware current.

- Debian / Ubuntu / Mint: `sudo apt update`, then `sudo apt upgrade`
- Fedora: `sudo dnf upgrade`
- Arch Linux: `sudo pacman -Syu`
- Avoid unsupported distributions and remove obsolete or untrusted software repositories.

02

Encrypt the Device

- Use LUKS full-disk encryption, preferably during installation.
- Choose a strong encryption passphrase, encrypt removable media, and keep recovery information separate from the device.
- Encryption provides its strongest protection when the computer is fully powered off.

03

Use Strong Authentication

- Use a strong, unique login password and do not routinely work as root.
- For online accounts, use a password manager, unique passwords, and multifactor authentication.
- Prefer passkeys or hardware security keys for high-value accounts.
- Enable automatic screen locking after roughly five to ten minutes of inactivity.

04

Enable the Firewall

A workstation generally should not accept unsolicited inbound connections.

- UFW baseline: `sudo ufw default deny incoming; sudo ufw default allow outgoing; sudo ufw enable`
- Review listening services with: `sudo ss -tulpn`
- Disable SSH, remote desktop, file sharing, web servers, databases, and other network services when not required.

05

Keep AppArmor or SELinux Enabled

Mandatory access controls constrain what compromised applications can do.

- Ubuntu, Mint, and many Debian-based systems commonly use AppArmor.
- Fedora and RHEL-family systems commonly use SELinux.
- Investigate and correct policy problems instead of disabling the security framework.

06

Reduce the Attack Surface

- Review active services: `systemctl --type=service --state=running`
- Review enabled units: `systemctl list-unit-files --state=enabled`
- Remove unused applications, disable unnecessary startup programs, and avoid unknown repositories or unverified installation scripts.

07

Secure Wi-Fi and Bluetooth

- Treat public networks as untrusted. Disable automatic connection to unknown networks and remove obsolete saved profiles.
- Prefer WPA2 or WPA3, a trusted hotspot, and an approved VPN on untrusted networks.
- Disable Bluetooth when not needed.
- Review saved NetworkManager connections with: `nmcli connection show`

08

Secure the Browser

- Keep the browser updated and minimize extensions; treat extensions as privileged software.
- Restrict camera, microphone, location, and notification permissions. Limit third-party tracking.
- Consider separate browser profiles for work, personal use, and research.

09

Protect Sensitive Files and Credentials

- Use restrictive permissions: `chmod 600 sensitive-file` and `chmod 700 private-directory`.
- Do not routinely use broad permissions such as `chmod 777`.
- Protect SSH keys, API credentials, VPN profiles, and other secrets.
- Do not place passwords or tokens directly in command-line instructions where shell history may record them.

10

Control USB and Removable Media

- Never trust unknown USB devices; they can impersonate storage, keyboards, network adapters, or several devices at once.
- Encrypt removable drives that contain sensitive information.
- Consider USB authorization controls in higher-security environments.

11

Maintain Secure Backups

- Maintain encrypted backups and periodically verify that they can be restored.
- Timeshift, Btrfs, or ZFS snapshots can recover from failed updates or configuration changes, but do not replace independent backups of important data.

12

Be More Restrictive During Travel

- Consider a dedicated travel laptop with minimal local data, full-disk encryption, and hardware security keys.
- Disable Bluetooth and automatic Wi-Fi connections; use an organization-controlled VPN and restrict USB access.
- Fully shut down the computer whenever physical custody is uncontrolled.
- Conduct pre-travel and post-travel security reviews.

● Configuration takeaway

Linux provides a strong foundation, but protection comes from configuration and operating practices rather than the operating system name. Reduce unnecessary exposure while keeping the system secure, reliable, understandable, and recoverable.