How to Set Up a Dedicated Machine for AI Agents

A Practical Hardening Guide

Isolate the machine. Separate the accounts. Define the boundaries.
Then let the AI work.

2026 Edition | macOS Focus | Checklist Included

License, Attribution & Disclaimer

Copyright

© 2026 Lorant Zambori / Built by AI. All rights reserved unless explicitly granted below.

License

This work is licensed under the Creative Commons Attribution 4.0 International License (CC BY 4.0). You are free to share (copy and redistribute in any medium or format) and adapt (remix, transform, and build upon) this material for any purpose, including commercial use, under the following terms:

Attribution required. You must give appropriate credit, provide a link to the license, and indicate if changes were made.

Full license text: creativecommons.org/licenses/by/4.0/

How to Attribute

When sharing or adapting this guide, please include the following attribution:

> *"AI Agent Machine Hardening Guide" by Lorant Zambori / Built by AI. Original source: zambori.substack.com. Licensed under CC BY 4.0.*

Disclaimer

This guide is provided for informational and educational purposes only. It does not constitute professional security, legal, or IT consulting advice.

The author makes no warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the information contained herein. The security measures described may not be sufficient for all environments, use cases, or threat models.

You use this guide entirely at your own risk. The author shall not be held liable for any loss, damage, security breach, data loss, financial loss, or any other consequence arising directly or indirectly from the use or misuse of the information provided in this document.

AI agent technology is evolving rapidly. The recommendations in this guide reflect the state of available tools and practices as of March 2026. Always verify that the steps described are still current and applicable to your specific setup before implementing them.

If you are handling sensitive data, client information, or operating in a regulated industry, consult a qualified security professional before relying on this guide.

About the Author

Lorant Zambori is a technology professional with 25 years of experience in IT, digital strategy and serial entrepreneurship. He is currently running a public experiment to build a business where AI handles execution and a human handles strategy, documented in the “Built by AI” newsletter at zambori.substack.com.

Who This Guide Is For

You are about to give an AI agent real access to real tools. A browser. An email account. Maybe API keys, payment processors, or social media accounts. The AI will operate on a dedicated machine, potentially 24/7, with minimal supervision.

This guide is for anyone setting up that machine. Whether you are running an experiment, building an AI-first startup, or deploying agents for your business, the security principles are the same.

It is written for macOS (specifically Mac Mini), but the principles apply to any operating system. The focus is on practical steps, not theory.

The Threat Model

Before hardening anything, you need to understand what you are protecting against. Here are the realistic risks when running an AI agent on a dedicated machine:

Risk	What Could Happen	How This Guide Prevents It
AI accesses personal accounts	The agent browses to your Gmail, reads your messages, or takes actions in your name	Complete account separation (Section 5)
AI reaches other devices on your network	The agent discovers your NAS, printers, smart home devices, or other computers	Network isolation via VLAN (Section 1)
AI installs malicious software	A compromised prompt or hallucination leads the agent to install something harmful	Standard user account without admin rights (Section 3)
Machine is physically stolen	Someone takes the hardware and accesses all stored credentials and data	Full disk encryption with FileVault (Section 4)
External attacker targets the machine	The machine is reachable from the internet and gets probed or attacked	Firewall with blocked incoming connections (Section 5)

AI creates accounts you do not know about	The agent signs up for services, agrees to terms, or commits to payments	Weekly review of password manager and accounts (Section 8)
Blast radius spreads to your business	An AI mistake affects your consultancy, your clients, or your personal reputation	Dedicated domain and identity boundary (Section 6)

The Core Principle

The AI gets its own world. Its own network, its own accounts, its own identity. It can do anything within that world. It cannot see or touch anything outside of it. If something goes wrong, the damage is contained.

7 Mistakes People Make When Setting Up AI Agents

Before the checklist, here is what to avoid. These are the errors that turn an interesting project into a security incident.

1. Using your personal Apple ID. Shared iCloud means shared Keychain, contacts, photos, documents, and location. The AI can see everything you see.

2. Keeping the machine on your main network. If the AI is on the same subnet as your other devices, one wrong command could interact with your NAS, your printer, or your smart home.

3. Giving the AI admin privileges. An admin account can install software, change system settings, and modify security configurations. The AI does not need any of that.

4. Logging into personal accounts in the browser. One saved password, one auto-filled form, one cached session and the AI has access to your personal email, banking, or social media.

5. Sharing a password manager vault. If the AI's vault is your vault, every credential you own is one hallucination away from being used.

6. Skipping disk encryption. API keys, session tokens, and credentials stored on an unencrypted disk are trivially accessible if the hardware is compromised.

7. Never reviewing what the AI created. AI agents will sign up for services, accept terms, and create accounts. If you do not review this regularly, you lose track of your exposure.

What Do You Actually Need?

Not every setup requires every layer. Here is a quick decision framework based on your risk tolerance:

Layer	Experimenting	Building a Product	Handling Client Data
Network isolation	Recommended	Required	Required
Dedicated Apple ID	Recommended	Required	Required
Standard user account	Required	Required	Required
FileVault encryption	Optional	Required	Required
Firewall hardening	Recommended	Required	Required
Account separation	Required	Required	Required
Weekly reviews	Optional	Recommended	Required

Section 1: Network Isolation

This is the most important layer and the one most people skip because it requires router configuration.

AI agents browse the web, call APIs, send emails, and interact with cloud services. If they sit on your main network, they share a subnet with every device you own. A misconfigured agent, a prompt injection, or even a simple error could lead the AI to discover and interact with devices it was never meant to touch.

Checklist

- [ ] Create a separate VLAN on your router for the AI machine
- [ ] If your router does not support VLANs, use the guest network as a minimum
- [ ] Block inter-VLAN traffic (the AI VLAN must not route to your main LAN)
- [ ] Allow outbound internet access from the AI VLAN
- [ ] Verify isolation: from the AI machine, try to ping your main computer. It must fail.
- [ ] Verify internet works: from the AI machine, open a browser and load any website

Common mistake

Some routers label their guest network as isolated but still allow mDNS/Bonjour traffic between networks. After setup, always verify with an actual ping test. If you can reach any device on your main network, the isolation is not working.

Section 2: Dedicated Apple ID

A shared Apple ID is a shared identity. iCloud Keychain syncs passwords. iCloud Drive syncs files. Contacts, calendars, and photos all flow between devices on the same Apple ID. You do not want any of that reaching the AI machine.

Checklist

- [ ] Create a brand new Apple ID specifically for this machine
- [ ] Use a dedicated email address for the Apple ID (e.g. apple@yourdomain.com)
- [ ] Do NOT enable iCloud Keychain
- [ ] Disable iCloud sync for everything except what the AI explicitly needs
- [ ] Disable Find My Mac
- [ ] Store the Apple ID credentials in the experiment password manager, not your personal one

Section 3: macOS User Accounts

The goal is to separate human administration from AI operation. You need access to maintain the system. The AI needs access to do its work. These should be different accounts with different privilege levels.

Checklist

- [ ] Create an admin account for yourself (system updates and configuration only)
- [ ] Create a standard (non-admin) account for the AI agent
- [ ] Name the AI account something identifiable (e.g. "agent" or your chosen agent name)
- [ ] Enable automatic login for the AI account (it needs to resume after restarts)
- [ ] Set Energy Saver to never sleep (System Settings > Energy)
- [ ] Disable screen saver and lock screen for the AI account
- [ ] Optionally: enable Screen Time restrictions on the AI account for additional guardrails

Why a standard account matters

A standard (non-admin) macOS account cannot install .pkg files, modify system preferences that affect all users, change security settings, or run sudo commands. The AI can still browse, run applications, manage files in its home folder, and do everything it needs to build a business. It just cannot change the system itself.

Section 4: Full Disk Encryption

FileVault encrypts the entire startup volume. Without it, anyone with physical access to the machine can mount the drive and read everything: API keys, session tokens, credentials, business data.

Checklist

- [ ] Enable FileVault (System Settings > Privacy & Security > FileVault)
- [ ] Store the recovery key in a secure, separate location (not on the AI machine)
- [ ] Verify FileVault status: open Terminal and run fdesetup status

Section 5: Firewall Configuration

The macOS firewall adds a second layer on top of network isolation. Even if someone discovers the machine on the network, the firewall blocks unsolicited connections.

Checklist

- [ ] Enable the firewall (System Settings > Network > Firewall)
- [ ] Block all incoming connections
- [ ] Enable stealth mode (the machine will not respond to pings or port scans)
- [ ] Verify outbound connections still work (the AI needs to reach external services)

Section 6: Digital Account Separation

This is where most people make the critical mistake. The AI needs real accounts to operate: email, cloud storage, payment processing, possibly social media. Every single one of these must be completely separate from your personal and business accounts.

The boundary

The AI Gets	The AI Does NOT Get
Dedicated email (e.g. agent@yourdomain.com)	Access to your personal email
Dedicated Google Workspace	Access to your business Google account
Dedicated password manager vault	Access to your personal password vault
Its own browser profile with no saved personal data	Any browser with logged-in personal sessions
API keys for AI services under the experiment account	API keys or credentials from your other projects
Ability to create new accounts for the business	Access to your banking, investments, or financial accounts

Checklist

- [ ] Set up email on a dedicated domain (via Google Workspace, Zoho, or similar)
- [ ] Create a dedicated password manager vault for all AI/experiment credentials
- [ ] Never store personal passwords in the AI vault
- [ ] Do NOT log into any personal accounts on the AI machine browser
- [ ] Do NOT log into any existing business or client accounts on the AI machine
- [ ] Set the AI browser profile as a clean install with zero history and zero saved passwords

The blast radius test

Ask yourself: if every account and credential on this machine were leaked publicly tomorrow, what would be affected? The answer should be: only the experiment domain and its associated services. Nothing else.

Section 7: AI Agent Setup

With the security layers in place, install and configure the tools the AI will use to do its work.

Checklist

- [ ] Install your AI tool of choice (Claude, ChatGPT, or other) using the experiment account
- [ ] Enable agent/coworker features if available
- [ ] Configure remote task dispatch if available (e.g. send tasks from your phone)
- [ ] Set up a clean browser profile with only experiment bookmarks
- [ ] Install any additional tools the AI will need (code editor, terminal, design tools)
- [ ] Test the full workflow: send a task remotely and verify execution on the machine

Section 8: Ongoing Maintenance

Security degrades over time if you do not actively maintain it. These habits take 10 minutes per week and prevent the slow creep of risk.

Weekly review checklist

- [ ] Install macOS security updates
- [ ] Review what accounts the AI has created or signed up for
- [ ] Verify VLAN isolation still works (ping test from AI machine to your main machine)
- [ ] Review the AI's browser history for anything unexpected
- [ ] Back up experiment data

Do not skip this

AI agents are proactive. They will sign up for services, accept terms of service, create trial accounts, and store credentials. If you do not review this regularly, you will lose track of your exposure surface. Set a recurring weekly calendar reminder.

Quick Reference Checklist

Print this page. Check off items as you complete them.

#	Task	Done
1	Separate VLAN or guest network created	
2	Inter-VLAN traffic blocked and verified	
3	Internet access confirmed from AI machine	
4	Dedicated Apple ID created	
5	iCloud sync and Find My Mac disabled	
6	Admin account created (for you)	
7	Standard account created (for AI agent)	
8	Automatic login enabled, sleep disabled	
9	FileVault enabled and recovery key stored	
10	Firewall enabled, incoming connections blocked	
11	Stealth mode enabled	
12	Dedicated domain email set up	
13	Dedicated password manager vault created	
14	Zero personal accounts logged in on this machine	
15	AI tools installed and configured	
16	Remote task dispatch tested	
17	Browser profile clean	
18	First backup completed	
19	Weekly review reminder set in calendar	

This guide is part of the Built by AI experiment.
Follow along at zambori.substack.com