VIPER Q PRO

Security Whitepaper

Architecture, threat model, controls, limitations, and operational guidance

Product	Viper Q Pro
Version	3.7.1
Document type	Security Whitepaper
Release status	Customer release documentation
Purpose	Clear, readable, operational documentation for installation, use, troubleshooting, and security review.

Read this before deployment or customer release. This document is written for real customers, not internal developers.

1. Executive Summary

Viper Q Pro is an offline-first encrypted vault for Windows users who need sensitive data protected without handing plaintext to a cloud provider. The product combines authenticated encryption, password-derived keys, hardware binding, local audit evidence, backup discipline, and optional high-risk operating modes such as hidden volume, decoy vault, tripwires, remote wipe, and travel mode.

The design principle is simple: the most sensitive data should be encrypted before it touches storage, should remain useless when copied to another machine, and should never require a third-party server to decrypt it. VQPro is not a magic shield. It is a layered security system. Its strength depends on correct installation, strong passwords, safe backups, and disciplined use.

Plain-English position: VQPro is built to reduce exposure, not to excuse reckless behaviour. If a user stores their password in a screenshot, ignores backups, exports unencrypted files to cloud storage, or runs malware as administrator, no vault can honestly promise perfect protection.

2. Security Goals

- Protect files, notes, credentials, keys, recovery material, identity documents, legal documents, business records, and private archives.
- Keep protected material usable offline without requiring a cloud account, subscription server, or vendor-held decryption key.
- Make stolen vault copies difficult or impossible to open on unauthorised hardware when machine binding is enabled.
- Detect tampering through hash-based integrity monitoring and signed audit events.
- Give high-risk users emergency tools such as decoy vaults, panic actions, travel mode, and wipe paths.
- Keep customer guidance clear enough that a non-technical user can install, back up, restore, and troubleshoot the product.

3. Threat Model

VQPro is designed around realistic threats. The main threat classes are device theft, casual snooping, cloud exposure, password database compromise, unauthorised file copying, insider access, ransomware touching vault files, and coercion scenarios where the user may need a decoy or emergency wipe path.

The system assumes the user controls their Windows account and can install/run the application. It does not assume Windows itself is invincible. If a machine is already fully compromised by administrator-level malware before the vault is opened, that malware may observe user actions. VQPro reduces risk with clipboard wipe, lockouts, audit logging, tripwires, and offline isolation, but endpoint hygiene still matters.

4. Architecture Overview

The architecture has four major zones: the user interface, the cryptographic engine, the vault storage layer, and the local security monitoring layer. The interface never needs cloud plaintext access. The cryptographic engine derives keys from user-controlled secrets and machine identity. The storage layer keeps vault material encrypted. The monitoring layer records important actions and identifies tampering indicators.

- User interface: dashboard, vault operations, chambers, settings, reports, manual, and alerts.
- Cryptographic engine: authenticated encryption, key derivation, key wrapping, salts, nonces, and integrity checks.

- Vault storage: encrypted containers, chamber structure, file metadata, audit material, backup material, and restore state.
- Security monitoring: failed attempts, lockouts, tripwires, file integrity checks, health scoring, SIEM-style events, and access certificates.

5. Cryptographic Design

VQPro uses authenticated encryption as the core protection pattern. Authenticated encryption is important because confidentiality alone is not enough: the system must also detect tampering. A vault that decrypts modified data without warning is not acceptable for serious use.

Argon2id is used as the password-based key derivation model. It is memory-hard, which means attackers cannot cheaply test large numbers of passwords without paying a real hardware and memory cost. This makes password strength meaningful, but it does not make weak passwords safe.

Post-quantum key wrapping, represented in the website as ML-KEM, is positioned as a future-resilience layer. It should be understood as part of the layered design rather than a claim that every possible attack is permanently impossible.

Important limitation: No honest security paper should claim absolute invincibility. VQPro can be strong, layered, and well-designed while still requiring good passwords, safe computers, controlled backups, and cautious exporting.

6. Authentication and Access Control

Access control is layered. The master password is the main secret. Optional controls include TOTP, Windows Hello, YubiKey, machine binding, hidden volume passwords, chamber passwords, lockout policy, and time or location restrictions. The purpose is to avoid one weak point becoming total failure.

- Master password: the primary user-held secret.
- TOTP: time-based one-time codes from an authenticator app.
- Windows Hello: local biometric or PIN-backed convenience factor.
- YubiKey: physical possession factor for stronger authentication.
- Machine binding: blocks vault copies from opening freely elsewhere.
- Lockout policy: slows brute force attempts after repeated failure.
- Chamber permissions: compartmentalises access inside the vault.

7. The 12 Crown Jewels

Crown Jewel 01: Hidden Volume

Plausible deniability through an outer vault and a hidden vault. The outer vault can hold harmless decoy material; the hidden vault is designed to be indistinguishable from random encrypted data.

Operational value: this feature exists to reduce a specific real-world risk. It should be configured deliberately, documented by the owner, and tested with non-critical data before being trusted with live data.

Crown Jewel 02: Cascade Cipher

A layered encryption option where data is processed through multiple independent encryption layers. The purpose is defence in depth: no single layer is relied upon as the only barrier.

Operational value: this feature exists to reduce a specific real-world risk. It should be configured deliberately, documented by the owner, and tested with non-critical data before being trusted with live data.

Crown Jewel 03: Hardware RNG

Key material and cryptographic salts are generated using strong operating system randomness and available hardware entropy sources. The goal is to avoid predictable seeds and weak random generation.

Operational value: this feature exists to reduce a specific real-world risk. It should be configured deliberately, documented by the owner, and tested with non-critical data before being trusted with live data.

Crown Jewel 04: File Integrity Monitor

Protected vault files are tracked with cryptographic hashes and metadata so unexpected modification, deletion, or replacement can be detected between sessions.

Operational value: this feature exists to reduce a specific real-world risk. It should be configured deliberately, documented by the owner, and tested with non-critical data before being trusted with live data.

Crown Jewel 05: Dead Man's Switch

A configurable check-in and contingency mechanism for high-risk users. It can be used for inheritance workflows or emergency response settings depending on configuration.

Operational value: this feature exists to reduce a specific real-world risk. It should be configured deliberately, documented by the owner, and tested with non-critical data before being trusted with live data.

Crown Jewel 06: Remote Wipe

A controlled emergency wipe path designed to destroy vault keys and vault material when an authenticated wipe command or token is accepted.

Operational value: this feature exists to reduce a specific real-world risk. It should be configured deliberately, documented by the owner, and tested with non-critical data before being trusted with live data.

Crown Jewel 07: Local SIEM

A local security event monitor that scores access attempts, anomalies, policy changes, tamper events, and other vault activity without sending private data to the cloud.

Operational value: this feature exists to reduce a specific real-world risk. It should be configured deliberately, documented by the owner, and tested with non-critical data before being trusted with live data.

Crown Jewel 08: Cryptographic Tripwires

Canary records, honey files, shadow hashes, and other planted indicators used to detect unauthorised browsing or extraction attempts.

Operational value: this feature exists to reduce a specific real-world risk. It should be configured deliberately, documented by the owner, and tested with non-critical data before being trusted with live data.

Crown Jewel 09: Staged Self-Destruct

A progressive protection sequence that can lock the vault, wipe keys, destroy selected chambers, or perform full destruction depending on the confirmed threat state.

Operational value: this feature exists to reduce a specific real-world risk. It should be configured deliberately, documented by the owner, and tested with non-critical data before being trusted with live data.

Crown Jewel 10: Geofencing + Time-Lock

Optional access policy controls that restrict when and where the vault can open. These controls are intended to reduce risk from stolen credentials and travel exposure.

Operational value: this feature exists to reduce a specific real-world risk. It should be configured deliberately, documented by the owner, and tested with non-critical data before being trusted with live data.

Crown Jewel 11: M-of-N Threshold Auth

A split-authorisation model using threshold keyholding. A configured number of approved keyholders must participate before access is granted.

Operational value: this feature exists to reduce a specific real-world risk. It should be configured deliberately, documented by the owner, and tested with non-critical data before being trusted with live data.

Crown Jewel 12: Travel Mode

A reduced-exposure operating mode for border crossings, device inspections, or travel risk. Selected chambers can be hidden from the interface until Travel Mode is disabled.

Operational value: this feature exists to reduce a specific real-world risk. It should be configured deliberately, documented by the owner, and tested with non-critical data before being trusted with live data.

8. The 49 Security Stages

The website presents VQPro as a 49-stage security architecture. Some rows cover multiple numbered stages where the controls belong to the same layer. The table below keeps the same customer-facing structure and explains the role of each layer in plain English.

S01-S03 - AES-256-GCM Encryption

Layer: FOUNDATION. Every file encrypted individually before touching disk. Authenticated encryption - tampering detected instantly. Individual keys per file derived via Argon2id. Intelligence-grade cipher. No exceptions, no shortcuts.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S04 - Argon2id Key Derivation

Layer: KEY FORGE. Memory-hard key derivation function. Your password is transformed into a 256-bit cryptographic key using Argon2id with high memory and iteration parameters. Brute force attacks become computationally infeasible - even with purpose-built hardware.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S05 - SHA-256 Hardware Lock

Layer: MACHINE BINDING. Vault is cryptographically bound to your exact hardware fingerprint - CPU serial, motherboard UUID, volume serial. Copy the vault files to any other machine - they will not open. There is no key that unlocks them elsewhere.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S06 - Decoy Vault Trap

Layer: HONEYPOT GATE. Under duress, enter a separate password. Opens a convincing decoy vault. Real vault remains hidden and untouched. Attacker sees realistic-looking data and believes they have succeeded.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S07 - Kill Switch

Layer: NUCLEAR OPTION. One command destroys the vault instantly. Nothing recoverable. Panic hotkey Ctrl+Shift+K, panic phrase at Gate I, or destroy button. Full 7-pass wipe. No second chances.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S08 - Public Drop Slot

Layer: BLIND DEPOSIT. Accept encrypted files without opening the vault. Zero exposure during deposit. Asymmetric key design - anyone can deposit, only you can retrieve. Public key distributable safely.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S09 - Multi-Chamber Vault

Layer: SEALED CHAMBERS. Separate encrypted chambers with independent passwords and keys. Different access levels. Compartmentalise everything. Each chamber completely invisible to all other chambers.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S10 - Ed25519 Forensic Audit Log

Layer: EVIDENCE CHAIN. Every action signed and timestamped with Ed25519 cryptographic signatures. Hash-chained - like a blockchain for your audit trail. Any tamper, deletion, or insertion detected instantly.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S11 - Post-Quantum ML-KEM

Layer: FUTURE-PROOF. ML-KEM-768 (NIST PQC standard) wraps your encryption keys. Quantum computer resistant today and tomorrow. Your data remains secure against attacks that do not yet exist.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S12 - 24-Hour Lockout Protection

Layer: LOCKOUT. 5 failed attempts triggers a full 24-hour lockout. No bypass. No reset without authorisation. Brute force attacks rendered useless.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S14 - ZK Cloud Sync

Layer: CLOUD COMPATIBLE. Encrypted before it leaves your machine. Cloud provider sees only ciphertext - never file structure or content. Identical encryption engine to the main vault. Fully offline compatible.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S15 - Vault Personality

Layer: IDENTITY. Custom vault name, tagline, and colour theme. Replaces all VQPro branding with your chosen identity. Six colour presets plus manual hex entry. The vault becomes indistinguishable from a legitimate custom application.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S16 - Full ZK Vault Backup

Layer: DISASTER RECOVERY. Full zero-knowledge backup to any local folder or external drive. Backup is encrypted before it leaves your machine. Restore with cryptographic integrity verification. Completely offline, zero server dependency.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S17 - Windows Hello Unlock

Layer: BIOMETRIC. Face recognition and fingerprint authentication via Windows Hello API. Hardware-backed biometric tied directly to your vault key. Falls back to master password if hardware unavailable.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S18 - YubiKey Support

Layer: HARDWARE KEY. HMAC-SHA1 challenge-response authentication via YubiKey OTP slot. Physical hardware key required to open vault. Without the YubiKey present the vault will not open regardless of password.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S19 - Remote Wipe Token

Layer: REMOTE. Generates a one-time wipe token stored offline. Present the token to trigger complete vault destruction from any location. QR code displayed in Settings. Full 7-pass wipe sequence executed on token presentation.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S20 - Access Certificate

Layer: EVIDENCE. Ed25519-signed PDF proof of vault access - date, time, machine fingerprint, signed cryptographic hash. Tamper-evident chain of custody documentation designed to assist evidentiary review.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S21 - Machine-Bound Licence

Layer: LICENCE. HMAC-SHA256 licence key cryptographically bound to your machine hardware fingerprint. Licence is non-transferable by design - it will not activate on any other machine.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S22 - ZK Cloud Sync

Layer: CLOUD. Exports an encrypted blob to any local folder, network share, or cloud storage. Zero-knowledge - the cloud provider sees only encrypted data, never file structure or content.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S23 - TOTP Authentication

Layer: 2FA. Time-based one-time password two-factor authentication. Compatible with Google Authenticator, Authy, and any TOTP app. Required at Gate II in addition to master password.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S24 - Vault Clone

Layer: PORTABILITY. Duplicate your entire vault to a second USB drive or backup location. Full cryptographic clone including all chambers, files, audit trail, and keys.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S25 - Custom Branding

Layer: WHITE LABEL. Single JSON configuration file rebrands the entire product. Deploy VQPro under your own brand identity. Used for white-label enterprise deployments.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S26 - Team Vault

Layer: MULTI-USER. Owner plus up to 5 named users with independent roles and permissions. Each user has their own password and access scope. Full audit trail per user identity.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S27 - Encrypted File Preview

Layer: PREVIEW. View images, PDFs, and text files directly inside the vault without extracting them. Decrypted in memory only - file never written to disk unencrypted.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S28 - Vault Health Score

Layer: HEALTH. Live 0-100 security score calculated on every dashboard open. AT RISK warnings with specific remediation guidance. Scores authentication strength, hardware binding, backup currency, and 2FA status.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S29 - Deposit Alerts

Layer: NOTIFICATIONS. Badge indicator on Deposits tab showing new files deposited since last open. Never miss an incoming encrypted file deposit. Zero performance overhead.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S30 - Vault Lock Screen

Layer: AUTO-LOCK. Idle timeout re-locks the vault to the full animated Gate I screen. Configurable timeout period. No data exposed during unattended periods.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S31 - Clipboard Wipe

Layer: CLIPBOARD. Automatically wipes the clipboard N seconds after any copy action performed inside the vault. Prevents clipboard sniffing tools from capturing copied passwords or keys.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S32 - Vault Export Report

Layer: REPORTING. One-click encrypted PDF summary of complete vault state. Ed25519 signed. Tamper-evident audit record designed to assist evidentiary review.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S33 - Time Lock

Layer: TIME LOCK. Vault locked until a future date and time you set. Cannot be opened before the unlock datetime regardless of correct password. Used for timed release of sensitive documents.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S34 - Stealth Mode

Layer: STEALTH. Ctrl+Shift+H toggles a convincing fake application overlay. To any observer the vault appears to be a different application entirely. Real vault continues running underneath.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S35 - Panic Broadcast

Layer: PANIC. Fires on panic phrase entry before vault wipe. Sends encrypted emergency broadcast to configured contacts. Designed for duress situations where silent alert is required before destruction.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S37 - Sound Fingerprint

Layer: BIOMETRIC. Microphone captures a 3-second ambient sound sample as an environmental biometric. Unusual acoustic environment triggers alert. Detects vault being opened in unfamiliar locations.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S38 - USB Auto-Launch

Layer: PORTABILITY. Registers vault to autorun on USB insertion. Vault launches automatically on any authorised machine. Combined with hardware binding - auto-launches only on bound machines.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S39 - Stealth Shortcut

Layer: ACCESS. Ctrl+Shift+S spawns the vault from anywhere without it appearing in the taskbar or window switcher. Invisible to screen recording software during spawn.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S40 - Built-in Manual

Layer: GUIDANCE. Full user manual and troubleshooting guide built directly into the vault interface. Accessible from the Manual tab without internet connection.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S41 - Hidden Volume

Layer: ♛ CROWN JEWEL #1. True plausible deniability. One container file - two completely separate encrypted vaults. Outer volume opened with outer password reveals decoy data. Hidden volume is mathematically indistinguishable from random data. No header, no signature, no marker - forensic tools cannot detect it.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S42 - Cascade Cipher

Layer: ♛ CROWN JEWEL #2. Triple-layer AES-256-GCM. Three independent encryptions nested inside each other, each with its own independently derived 256-bit key. Mathematically equivalent to 768-bit authenticated encryption. An attacker must break all three simultaneously.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S43 - Hardware RNG

Layer: ♛ CROWN JEWEL #3. True entropy key generation from hardware sources. Windows BCryptGenRandom via TPM/RDRAND/RDSEED, CPU RDRAND and RDSEED instructions directly via ctypes, and os.urandom() - all three XOR-mixed.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S44 - File Integrity Monitor

Layer: ♛ CROWN JEWEL #4. Watches all vault files on disk between sessions. Builds a cryptographic manifest - SHA-256 hash, file size, and last-modified timestamp per file. Manifest encrypted with machine-bound key. Any mismatch triggers tamper alert.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S46 - Remote Wipe

Layer: ♛ CROWN JEWEL #6. Multi-channel remote vault destruction. Trigger via file drop, email command, or network URL poll. 7-pass wipe sequence. Sends receipt confirmation email to owner after wipe completes.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S47 - Local SIEM

Layer: ♛ CROWN JEWEL #7. Lightweight local Security Information and Event Management system. Monitors, correlates, and scores ALL security events in real time. Threat scoring 1-10 per event. Critical threshold triggers automatic forensic capture.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S48 - Cryptographic Tripwires

Layer: ♛ CROWN JEWEL #8. Hidden fake credentials - canary tokens, honey files, shadow hashes. If an attacker reads, copies, or uses any tripwire - silent alarm fires instantly. Attacker cannot distinguish tripwires from real credentials.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

S49 - Self-Destruct + Geo + M-of-N + Travel

Layer: ♛ CROWN JEWELS #9-12. Staged Self-Destruct: 7-stage progressive vault destruction on confirmed attack. Geofencing + Time-Lock: vault refuses to open outside approved location and hours. M-of-N Threshold Auth: require M of N keyholders via Shamir Secret Sharing. Travel Mode: instantly hide selected chambers on demand.

Operational meaning: this control is one part of the defence-in-depth chain. It should not be viewed alone; its value comes from combining password strength, machine binding, encryption, monitoring, backup, and user discipline.

9. Audit, Evidence and Integrity

A serious vault must do more than encrypt. It must help the owner understand what happened. VQPro uses audit events, signed records, file integrity checks, and optional access certificates to show when the vault was opened, when sensitive actions occurred, and when tamper indicators appeared.

- Audit logs should be reviewed after failed access attempts or system alerts.
- Access certificates should be generated when proof of access is needed for review or evidence handling.
- File integrity alerts should be treated as serious until explained.
- Manual editing of audit material defeats the purpose and should never be done.

10. Backup, Restore and Continuity

Backup is not optional. Strong encryption without backup discipline can permanently lock out the rightful owner. The safest routine is to create a backup after important vault changes, keep at least one offline copy, and periodically test restore using non-destructive steps.

1. Create a backup from inside VQPro after important changes.

2. Store the backup on a separate external drive or strongly protected location.

3. Write down recovery notes and keep them away from the computer.

4. Test that the backup is visible and complete.

5. Do not delete the original vault until a restore has been confirmed.

11. Safe Deployment and Distribution

Customers must receive the complete VQPro_Setup.zip, not loose files. They must extract the ZIP first, keep the VQPro folder together, and launch from the extracted folder. The Netlify site should serve the official customer ZIP after the Stripe success flow verifies payment.

- Do not run the EXE directly from inside the ZIP preview.
- Do not move VQPro.exe away from its folder and support files.
- Create shortcuts only from the real VQPro.exe inside the extracted VQPro folder using Windows Send to -> Desktop (create shortcut).
- Do not upload internal development files, keys, audit logs, or vault config files to the website.
- Do not replace the clean website with a stripped placeholder page.

12. Known Limitations

- Unsigned Windows applications may trigger SmartScreen until code-signing reputation is established.
- If a computer is already infected with administrator-level malware, any vault can be attacked at the endpoint.
- If the master password and recovery material are lost, zero-knowledge design may make recovery impossible.
- Hardware binding improves theft resistance but can complicate migration after hardware replacement.
- Static hosting is convenient, but fully private download enforcement is stronger with protected backend storage.
- Users must not export decrypted files to insecure folders or cloud drives by mistake.

13. Owner Checklist Before Release

1. Confirm the website looks like the proper Viper Q Pro product page.

2. Confirm the payment buttons use the correct live Stripe links.

3. Confirm Stripe redirects to thank-you.html?session_id={CHECKOUT_SESSION_ID}.

4. Confirm Netlify has STRIPE_SECRET_KEY set as an environment variable.

5. Confirm /api/verify-download exists and the thank-you page calls it.

6. Download the customer ZIP from the final deployed site and extract it on a clean Windows machine.

7. Run VQPro.exe from inside the extracted VQPro folder, then create a normal Windows desktop shortcut using right-click VQPro.exe -> Show more options -> Send to -> Desktop (create shortcut).

8. Open the whitepaper and user manual and confirm they are readable at 100% zoom.

14. Security Conclusion

VQPro is strongest when used as designed: offline-first, extracted correctly, backed up properly, protected by a strong master password, and operated by a user who understands the difference between encrypted vault data and unencrypted exported files. The layered architecture is the product advantage. The documentation is part of that architecture because poor instructions create security failures.

Verified Customer Launch Method

The official customer package must be extracted before use. VQPro.exe must remain inside the extracted VQPro folder with its support files. The verified launch path is: extract ZIP -> open VQPro folder -> double-click VQPro.exe with the VQPro logo/icon.

Desktop shortcuts must be created manually through Windows: right-click VQPro.exe -> Show more options -> Send to -> Desktop (create shortcut). Do not drag or move VQPro.exe to the Desktop. Do not use a shortcut that fails or points to the wrong location.