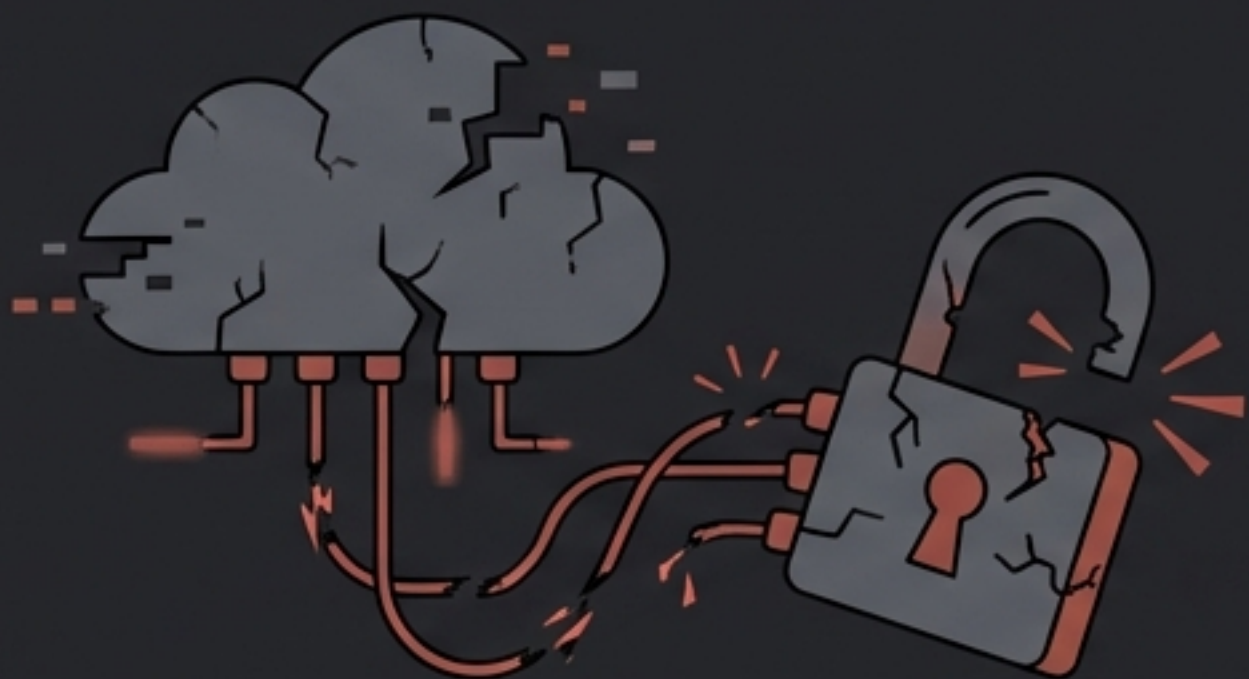


AVGVSTO 3.1.3 ■

[Hardware-Bound AES File Encryption. Destroys the Rest.]

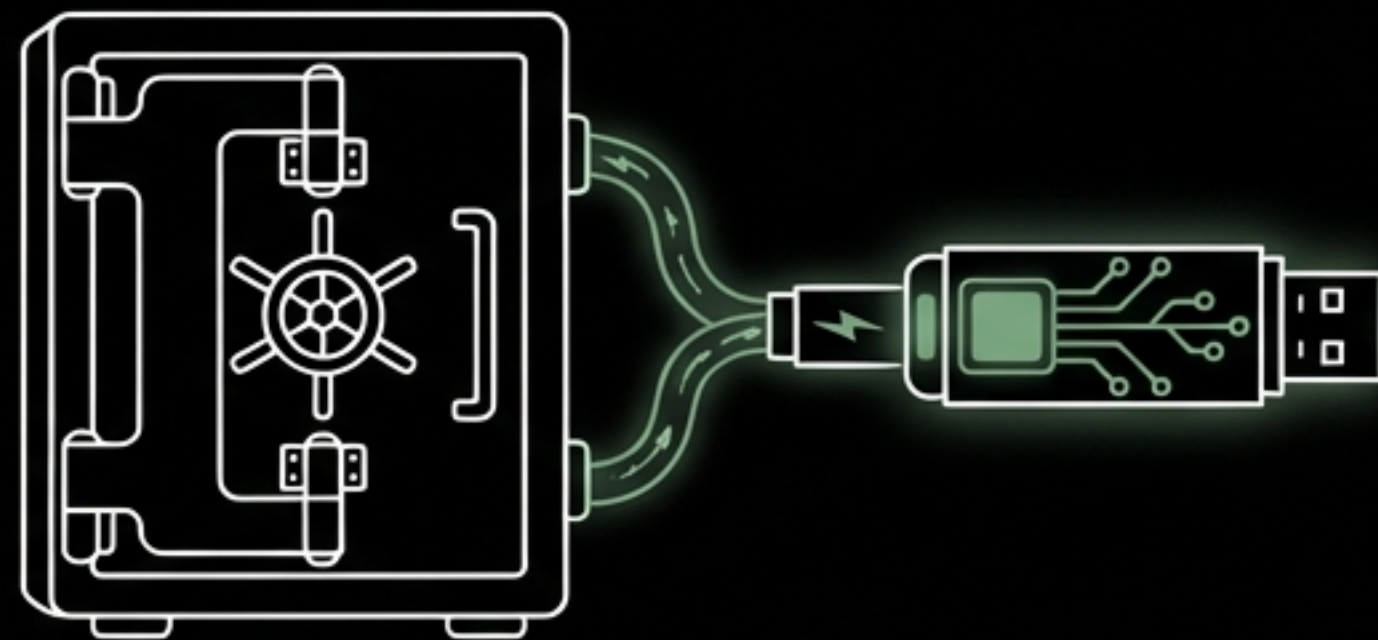
AES-256-GCM • CHACHA20-POLY1305 • PBKDF2-HMAC-SHA256 (1M) • 100% OFFLINE

Software-Only Encryption is Mathematically Insufficient.



Legacy Software Encryption: Vulnerable

Software-only solutions and cloud-reliant syncs leave cryptographic keys exposed to digital extraction and remote attacks.

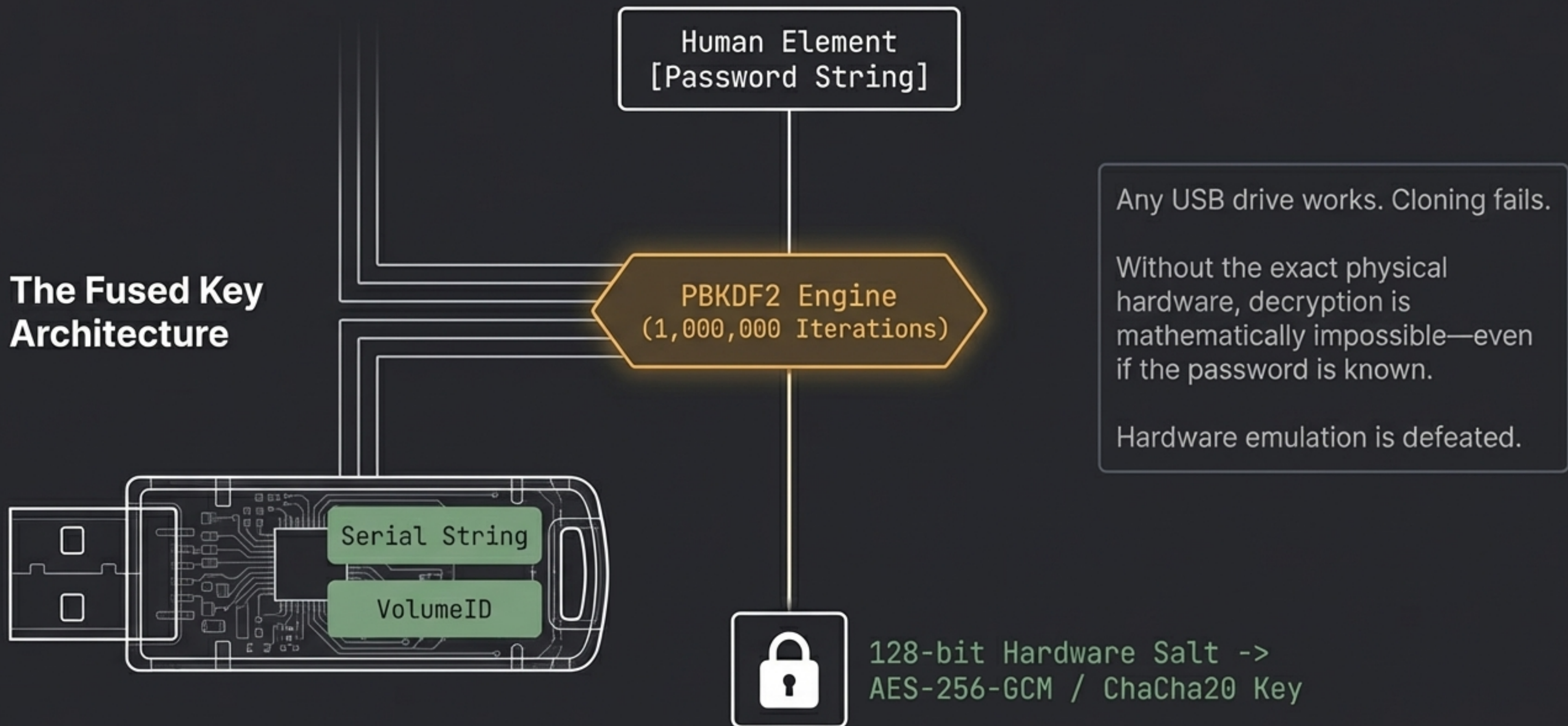


The Air-Gap Mandate: 100% Offline

True data security requires physical fusion. AVGVSTO operates entirely offline, binding your cryptographic keys directly to a physical hardware fingerprint. No cloud sync, no key escrow, no network dependency.

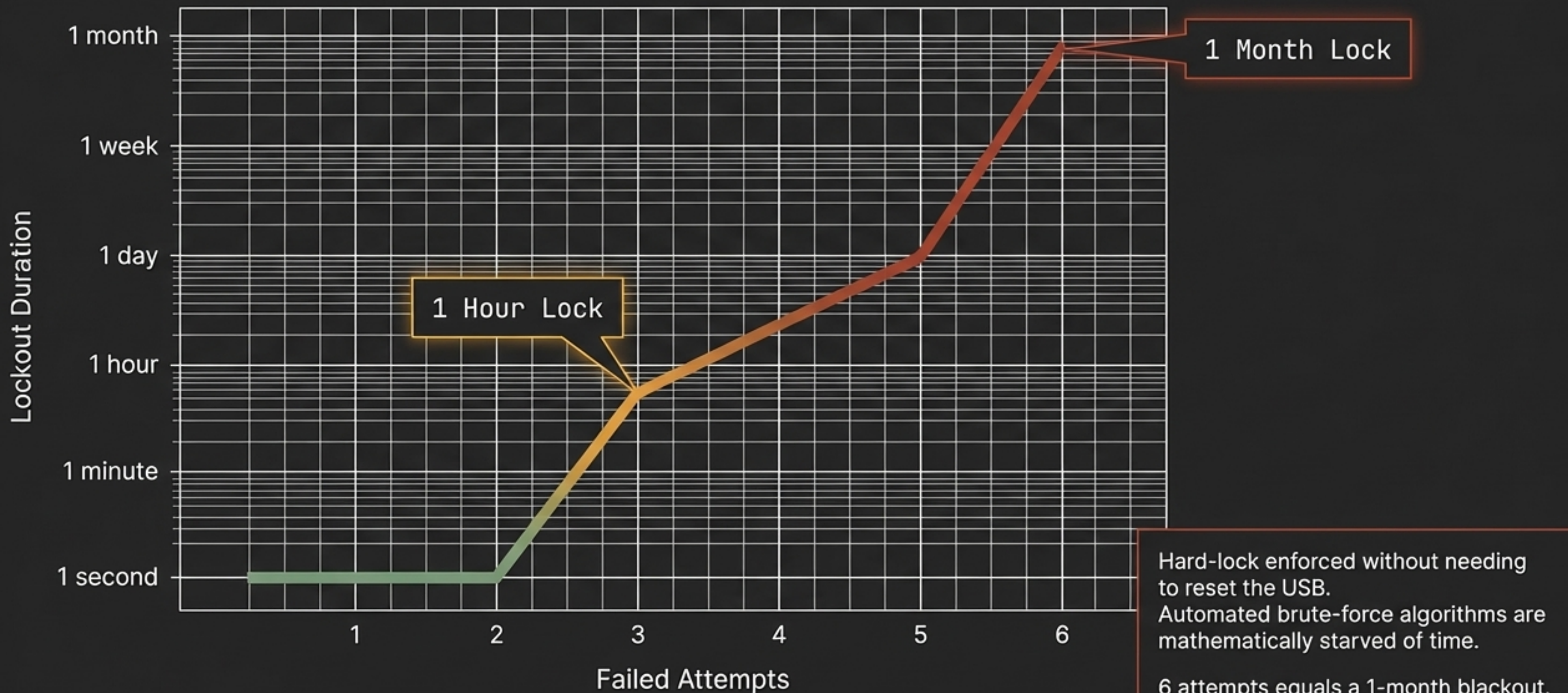
0 Network Requests
3 OS Supported (Win/Mac/Linux)
256 AES Key Bits

The Cryptographic Core: Fusing Mind and Hardware.



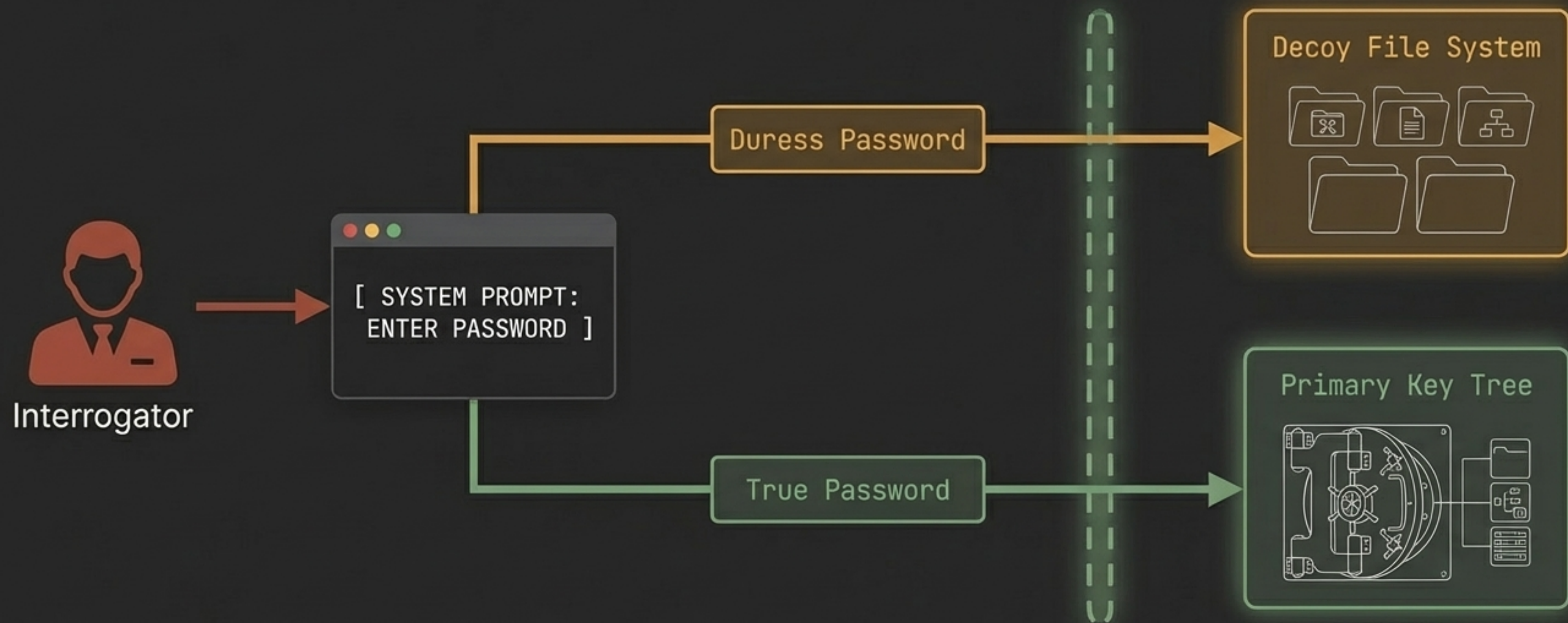
The Anti-Bruteforce Engine: Exponential Backoff

The Exponential Lockout Curve



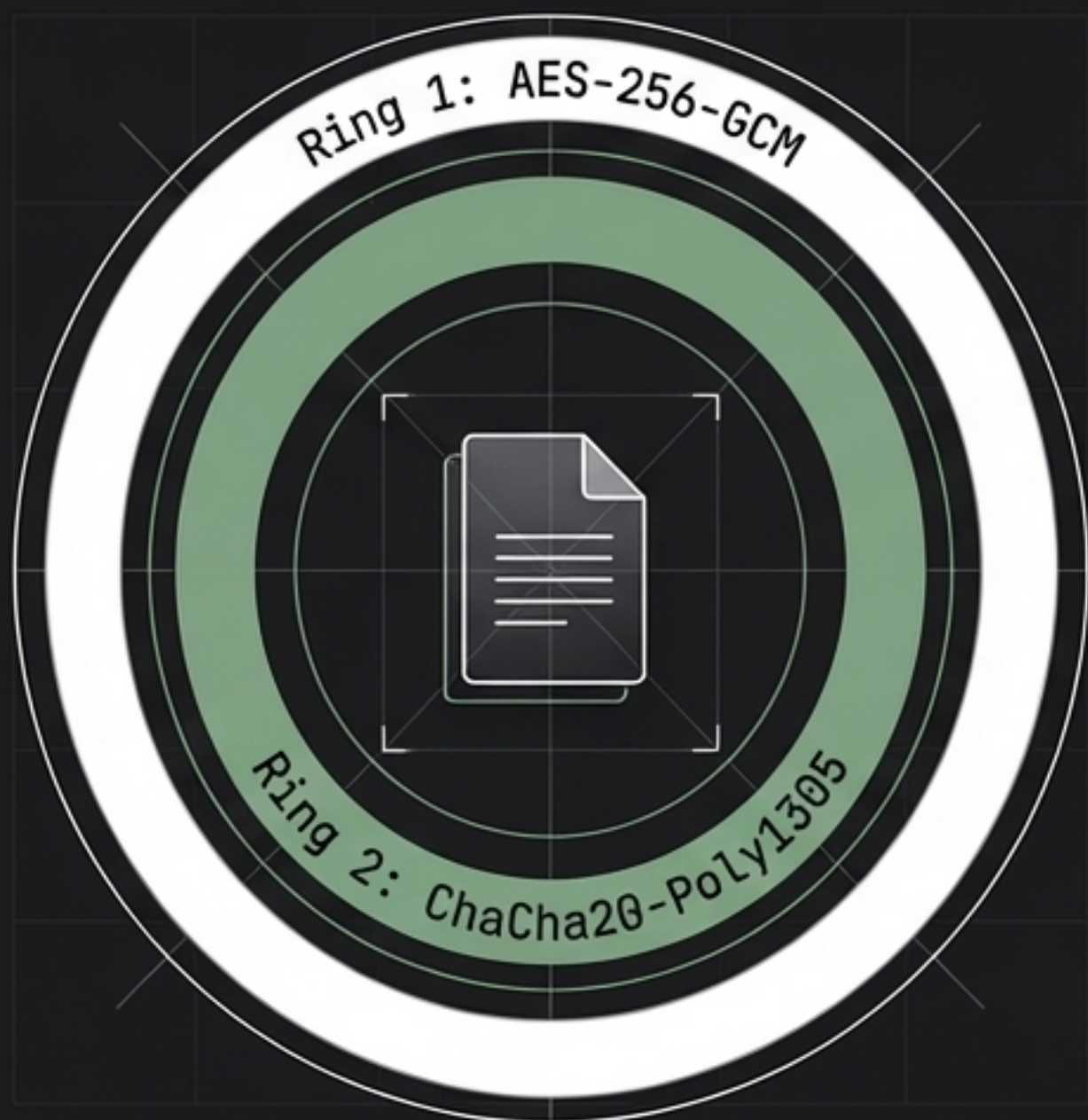
Plausible Deniability: Architectural Deception.

When coerced, provide the secondary password. AVGVSTO reveals entirely separate decoy files. The true cryptographic key tree remains mathematically hidden and unprovable.



Cascade Encryption & Immutable Auditing

Cascade Encryption



[Independent keys. 512-bit effective security.
Post-quantum resistant architecture.]

Tamper-Proof Audit



[Immutable logs of every access attempt.
Deletion is mathematically impossible.]

The Obliteration Matrix: AVGVST0 vs Pretenders

Feature	AVGVST0	VeraCrypt	BitLocker	AxCrypt
Hardware USB Binding	Serial + VolumeID	Keyfiles only	TPM only	-
Anti-Bruteforce	Exponential (1 month)	PIM delay only	TPM lock	-
100% Offline / Air-Gap	True Air-Gap	Yes	MS Account	Cloud sync
Plausible Deniability	Decoy / Duress	Hidden volumes	-	-
File-Level Limits	Yes	-	-	-

Licensing: Own Your Encryption Architecture

BUSINESS – In Dev

- Cascade Cipher (AES + ChaCha20)
- Full Audit Logs
- Silent Deployment (JSON config)
- Advanced USB Management

PRO – In Dev

- Adds ChaCha20-Poly1305
- Duress/Decoy Mode
- Full CLI Access
- Portable Mode (USB config)

FREE – €0

- AES-256-GCM
- USB Binding
- Secure Delete (3-pass)
- 5 files/batch

The Uncompromising Reality: The Three Laws of Hardware Binding

01

Absolute Loss

Lose the USB, lose the files. Your files are irrecoverable. That is the point. (Business tier supports local backup).

02

Zero Backdoors

No cloud. No key escrow. No recovery codes. We cannot restore your access, and we are not sorry.

03

Hardware Dictates

Any brand, any capacity, FAT/NTFS/exFAT. The hardware serial is read natively, totally bypassing the volume label.

Deployment Readiness: Air-Gap Ready Binaries

Native compiled. Self-contained. No runtime required.

> Windows 10/11 .exe [8.2 MB]

> Linux AppImage [7.8 MB]

> macOS 12+ [In Development]

 Also available via winget, brew, apt (community)

SHA256 (Windows): 7E2D9F4A...C8B3

GPG Signature: 0x3AFF...D717

[Download \(all platforms\)](#) | [Source & Checksums](#) | [AVGV"ST0 3.1.3](#)