ORing

書き込みは、許可制。
すべてを検証してから。

Plug in anywhere. Scans before it writes. Trust nothing.

SEMI E187 · IEC 62443 · NERC CIP · HIPAA · FDA 21 CFR Part 11 · ISO 27001 · NIST SP 800-171 · CMMC 2.0 · IEC 62443-3-3 · GDPR · SOC 2 Type II · NIS2

HOW IT WORKS

5つのチェックポイント。抜け道はゼロ。

すべてのファイルは、お客様の環境に入る前に検証されます。

01 **接続**

OPS Portable ShieldをUSB-CまたはUSB-Aで任意のエンドポイントに接続。ドライバ不要、インストール不要、管理者権限不要。

02 **認証**

管理者が事前に作成したアカウントのみがOPSを操作可能。各セッションはホストOSのログインと紐付けされ、すべての転送が追跡・監査可能。

03 **スキャン**

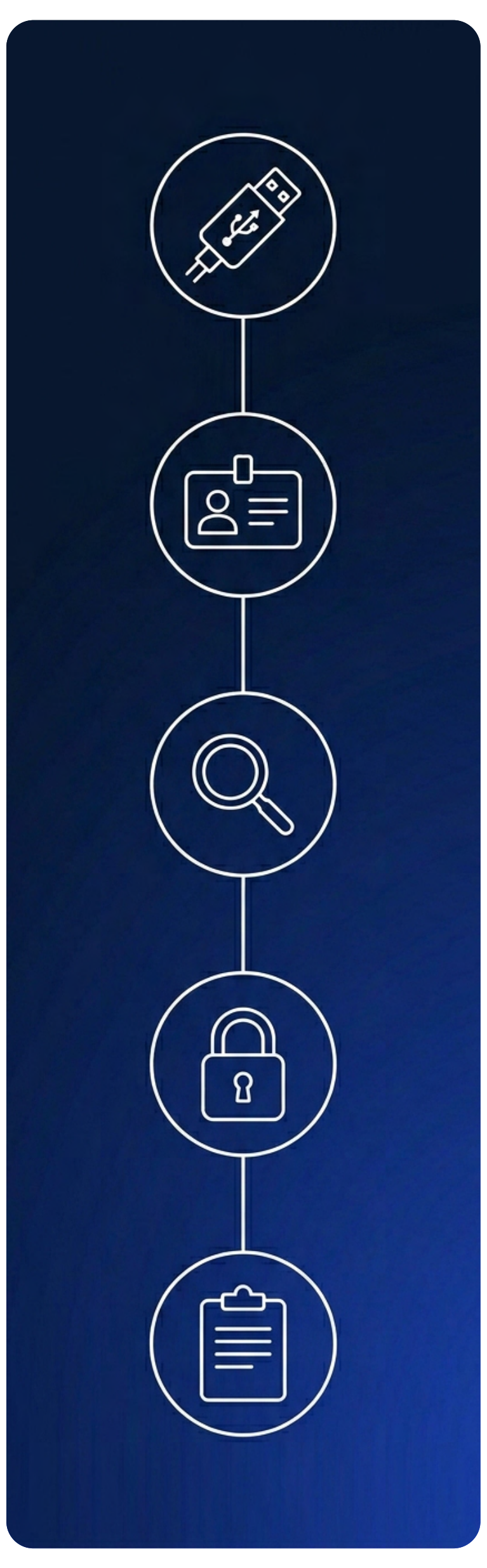
すべてのファイルをデバイス上でローカルスキャン — クラウド不要、外部サーバー不要。AVエンジンはAV-TESTトップランクベンダーから提供され、組織の要件に合わせて構成可能。暗号化アーカイブはデフォルトでブロック。

04 **暗号化・保存**

保存データはすべてフラッシュレベルでAES-256暗号化。ホストOSはボリュームを読み取れますが、直接書き込むことはできません — すべての書き出しはOPSを経由する必要があります。

05 **レポート**

OPSは12の規制フレームワークに対応したPDFコンプライアンスレポートを生成 — SEMI E187からHIPAA、CMMC 2.0まで。各レポートはフレームワーク固有のコントロールに対するエンドポイントの証拠を文書化し、次回の監査に対応。



YOUR INDUSTRY

1台で、あらゆる業界に。

USB禁止？ もう過去の話です。

SEMICONDUCTOR

SEMI E187

エアギャップ環境のFabツールネットワーク全体でUSBポリシーを実施。ベンダーファイルは装置に触れる前にすべてスキャン。

ENERGY

NERC CIP

重要インフラ向けリムーバブルメディア管理義務に対応。OT環境のための一元管理・完全監査可能な転送ポイント。

HEALTHCARE

HIPAA Security Rule

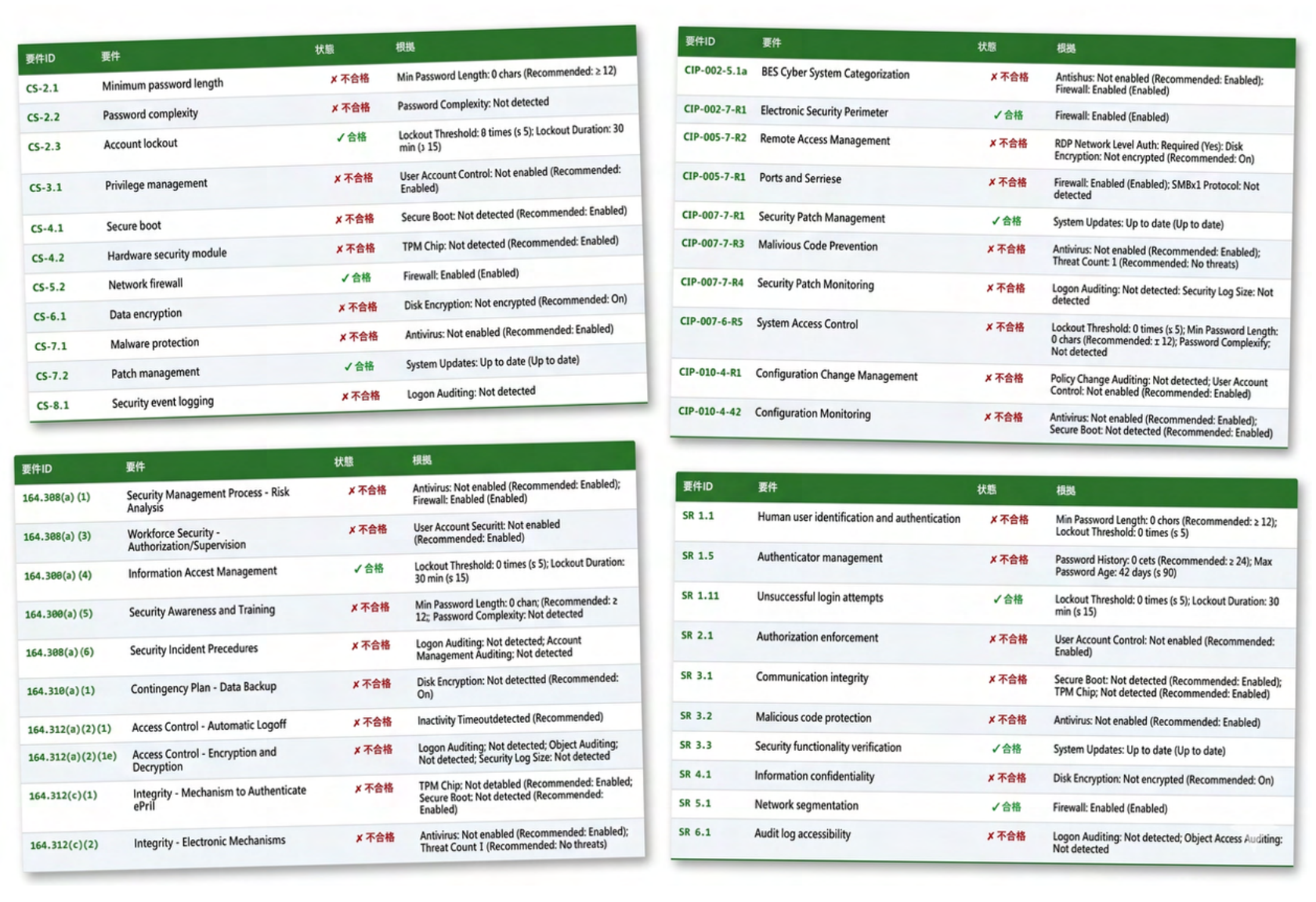
USB転送ごとにePHIを保護。HIPAAおよびFDA 21 CFR Part 11に適合する監査証跡を提供。

MANUFACTURING

IEC 62443

ITゾーンとOTゾーン間の安全な橋渡し。ICS環境向けのゾーン＆コンジットメディア制御。

12 のコンプライアンスフレームワークに対応 — こちらは4つの例。



要件ID	要件	状態	根拠
CS-2.1	Minimum password length	✗ 不合格	Min Password Length: 0 chars (Recommended: ≥ 12)
CS-2.2	Password complexity	✗ 不合格	Password Complexity: Not detected
CS-2.3	Account lockout	✓ 合格	Lockout Threshold: 8 times (≤ 5); Lockout Duration: 30 min (≥ 15)
CS-3.1	Privilege management	✗ 不合格	User Account Control: Not enabled (Recommended: Enabled)
CS-4.1	Secure boot	✗ 不合格	Secure Boot: Not detected (Recommended: Enabled)
CS-4.2	Hardware security module	✗ 不合格	TPM Chip: Not detected (Recommended: Enabled)
CS-5.2	Network firewall	✓ 合格	Firewall: Enabled (Enabled)
CS-6.1	Data encryption	✗ 不合格	Disk Encryption: Not encrypted (Recommended: On)
CS-7.1	Malware protection	✗ 不合格	Antivirus: Not enabled (Recommended: Enabled)
CS-7.2	Patch management	✓ 合格	System Updates: Up to date (Up to date)
CS-8.1	Security event logging	✗ 不合格	Logon Auditing: Not detected

要件ID	要件	状態	根拠
CIP-002-5.1a	BES Cyber System Categorization	✗ 不合格	Antishus: Not enabled (Recommended: Enabled); Firewall: Enabled (Enabled)
CIP-002-7-R1	Electronic Security Perimeter	✓ 合格	Firewall: Enabled (Enabled)
CIP-005-7-R2	Remote Access Management	✗ 不合格	RDP Network Level Auth: Required (Yes): Disk Encryption: Not encrypted (Recommended: On)
CIP-005-7-R1	Ports and Serriese	✗ 不合格	Firewall: Enabled (Enabled); SMBx1 Protocol: Not detected
CIP-007-7-R1	Security Patch Management	✓ 合格	System Updates: Up to date (Up to date)
CIP-007-7-R3	Malivious Code Prevention	✗ 不合格	Antivirus: Not enabled (Recommended: Enabled); Threat Count: 1 (Recommended: No threats)
CIP-007-7-R4	Security Patch Monitoring	✗ 不合格	Logon Auditing: Not detected: Security Log Size: Not detected
CIP-007-6-R5	System Access Control	✗ 不合格	Lockout Threshold: 0 times (≤ 5); Min Password Length: 0 chars (Recommended: ≥ 12); Password Complexity: Not detected
CIP-010-4-R1	Configuration Change Management	✗ 不合格	Policy Change Auditing: Not detected; User Account Control: Not enabled (Recommended: Enabled)
CIP-010-4-42	Configuration Monitoring	✗ 不合格	Antivirus: Not enabled (Recommended: Enabled); Secure Boot: Not detected (Recommended: Enabled)

要件ID	要件	状態	根拠
164.308(a)(1)	Security Management Process - Risk Analysis	✗ 不合格	Antivirus: Not enabled (Recommended: Enabled); Firewall: Enabled (Enabled)
164.308(a)(3)	Workforce Security - Authorization/Supervision	✗ 不合格	User Account Securitt: Not enabled (Recommended: Enabled)
164.308(a)(4)	Information Accest Management	✓ 合格	Lockout Threshold: 0 times (≤ 5); Lockout Duration: 30 min (≤ 15)
164.308(a)(5)	Security Awareness and Training	✗ 不合格	Min Password Length: 0 chan; (Recommended: ≥ 12; Password Complexity: Not detected
164.308(a)(6)	Security Incident Precedures	✗ 不合格	Logon Auditing: Not detected; Account Management Auditing: Not detected
164.310(a)(1)	Contingency Plan - Data Backup	✗ 不合格	Disk Encryption: Not detectted (Recommended: On)
164.312(a)(2)(1)	Access Control - Automatic Logoff	✗ 不合格	Inactivity Timeoutdetected (Recommended)
164.312(a)(2)(1e)	Access Control - Encryption and Decryption	✗ 不合格	Logon Auditing: Not detected; Object Auditing: Not detected; Security Log Size: Not detected
164.312(c)(1)	Integrity - Mechanism to Authenticate ePril	✗ 不合格	TPM Chip: Not detabled (Recommended: Enabled; Secure Root: Not detected (Recommended: Enabled)
164.312(c)(2)	Integrity - Electronic Mechanisms	✗ 不合格	Antivirus: Not enabled (Recommended: Enabled); Threat Count 1 (Recommended: No threats)

要件ID	要件	状態	根拠
SR 1.1	Human user identification and authentication	✗ 不合格	Min Password Length: 0 chors (Recommended: ≥ 12); Lockout Threshold: 0 times (≤ 5)
SR 1.5	Authenticator management	✗ 不合格	Password History: 0 cets (Recommended: ≥ 24); Max Password Age: 42 days (≤ 90)
SR 1.11	Unsuccessful login attempts	✓ 合格	Lockout Threshold: 0 times (≤ 5); Lockout Duration: 30 min (≤ 15)
SR 2.1	Authorization enforcement	✗ 不合格	User Account Control: Not enabled (Recommended: Enabled)
SR 3.1	Communication integrity	✗ 不合格	Secure Boot: Not detected (Recommended: Enabled); TPM Chip; Not detected (Recommended: Enabled)
SR 3.2	Malicious code protection	✗ 不合格	Antivirus: Not enabled (Recommended: Enabled)
SR 3.3	Security functionality verification	✓ 合格	System Updates: Up to date (Up to date)
SR 4.1	Information confidentiality	✗ 不合格	Disk Encryption: Not encrypted (Recommended: On)
SR 5.1	Network segmentation	✓ 合格	Firewall: Enabled (Enabled)
SR 6.1	Audit log accessibility	✗ 不合格	Logon Auditing: Not detected; Object Access Auditing: Not detected

+ ISO 27001 · NIST CSF 2.0 · NIS2 · EU CRA · FDA 21 CFR Part 11 · PCI DSS 4.0 · CMMC 2.0 · GCB/CIS

DATA SECURITY

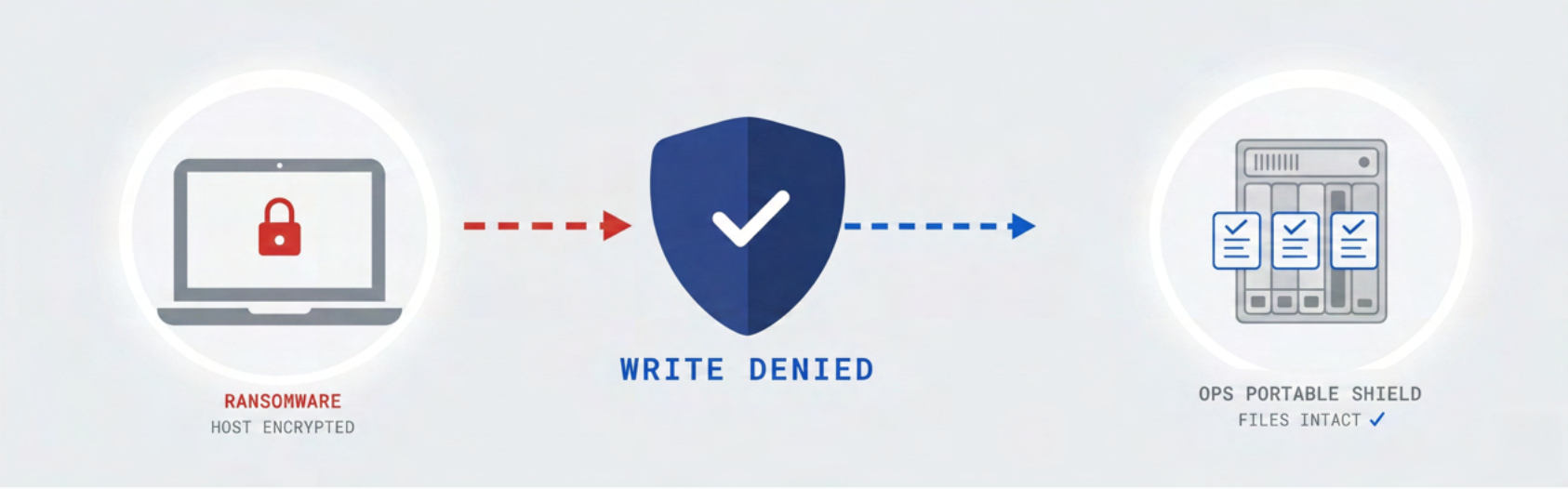
あなたのファイル。誰にも触れさせない。

ホストOSは読み取り専用 – 書き込み・変更・暗号化は一切不可。

ランサムウェア耐性ストレージ

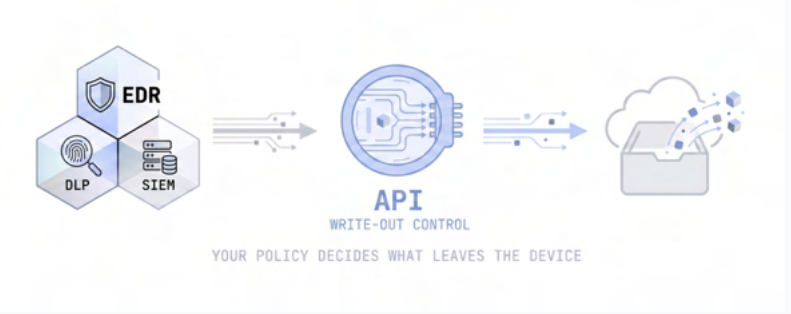
ランサムウェアがホストを暗号化しても、あなたのファイルは無事です。OPSはUSBファームウェアレベルで読み取り専用を強制 — ドライバ不要、ソフトウェア不要、ホスト側のマルウェアにデータを書き込み・暗号化・削除する手段を与えません。新たにクリーンなデバイスにて接続する事でそのまま作業を再開できます。

FIRMWARE-LEVEL WRITE PROTECTION · ZERO INSTALL · ZERO TRUST



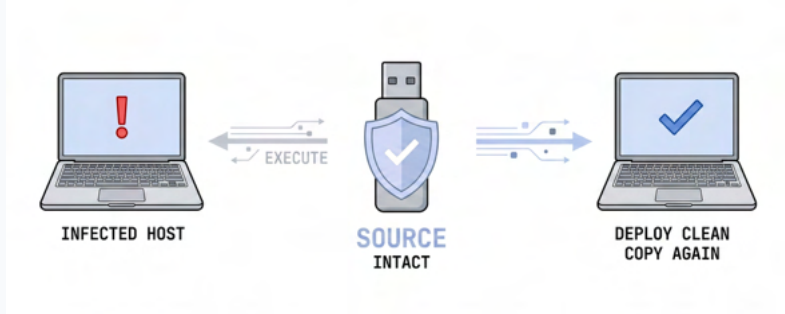
パートナー連携用オープンAPI

OPSは書き出し制御用のローカルAPIを公開。お客様のEDR、DLP、または資産管理プラットフォームがデバイスからのデータ書き出しを制御 — 既存のセキュリティポリシーを単一のUSBエンドポイントで実施。



改ざん防止ツールストレージ

診断ユーティリティ、インストーラー、フィールドサービスツールをOPSに保存。ホストが侵害されても、ソースファイルはバイト単位で完全に保持。常に既知の安全なコピーからデプロイ。



SPECIFICATIONS

完全なプラットフォームをたったの1台で。

フラッシュレベル暗号化

フラッシュ層でAES-256暗号化。ホストOSは読み取り専用ボリュームのみ表示。書き出しはOPS経由のみ。

AV-TESTトップランクエンジン

デバイス上でローカルスキャン。AV-TESTトップランクベンダーの構成可能なエンジン。暗号化アーカイブはデフォルトでブロック。

アカウントベースアクセス

管理者が作成したアカウント。セッションはホストOSログインと紐付けられ、すべての転送が追跡・監査可能。

12コンプライアンスフレームワーク

SEMI E187、HIPAA、NERC CIP、IEC 62443など12の規制フレームワークに対応したPDFレポート。

ゼロインストール

エージェント不要、ドライバ不要、管理者権限不要。エアギャップ環境でもそのまま動作。

ファームウェア書き込み保護

ファームウェアレベルでホストOSは読み取り専用。ドライバ不要。ランサムウェア耐性を標準装備。

ストレージ	128 GB MLC Flash	動作温度	0°C – 70°C
暗号化	AES-256-XTS (Hardware)	書き込み保護	Firmware-level
インターフェース	USB-C/A · USB 3.2 Gen 1	コンプライアンス	12 frameworks
セキュアエレメント	CC EAL5+	レポート形式	PDF
外形寸法	76 × 20.5 × 10 mm	認証	CE · FCC · RoHS · VCCI · FIDO2-ready
対応OS	Windows 7 SP1 and later	インストール	Zero install

www.oringnet.com
ethanchuang@oringnet.com