# ForteFide

CMMC Level 2 Compliance Scanner Sales & Licensing Guide

| | |
|---|---|
| **Version** | 1.4.2 |
| **Product** | ForteFide |
| **Framework** | CMMC Level 2 / NIST 800-171 |
| **Website** | densedefense.com |



## Executive Summary

ForteFide is a standalone compliance scanner and automated remediation platform purpose-built for organizations pursuing CMMC Level 2 certification. It scans Windows and Linux endpoints against all 110 NIST SP 800-171 Rev 2 controls, identifies gaps, and remediates findings with a single click.

Delivered as a single installer (Windows .exe or Linux .deb), ForteFide runs entirely on-premises with no cloud dependency. It operates air-gapped, requires no internet connection, and stores all data locally with AES-256-GCM encryption.

## Key Features

- **7-Step Guided Workflow**From network discovery through signed evidence collection -- zero guesswork
- **110 CMMC L2 Controls**Full coverage of all 14 NIST 800-171 control families
- **Dual-OS Scanning**Windows (WinRM) and Linux (SSH) from a single dashboard
- **Auto OS Detection**Probes ports 5985/22 to determine target OS automatically
- **Zero-Credential Scanning**SSH key or certificate auth deployed during preparation -- no passwords in scan
- **Endpoint Preparation**Automated service account creation with key/cert deployment
- **Bulletproof Remediation**Smart ordering, lockout detection, auto-rollback, 90s timeouts
- **DANGER MODE**Manual-intervention controls with confirmation overlay and rollback
- **Signed Evidence**23-document package with SHA-256 hashes and Ed25519 digital signatures
- **Baseline + Final Delta**Auto-collected baseline evidence shows C3PAO exactly what improved
- **Session Persistence**F5-safe encrypted SQLite -- never lose scan results
- **Scheduled Scans**HallMonitor continuous monitoring with compliance drift alerts
- **REST API**55 routes for CI/CD integration and automation
- **Air-Gap Ready**No internet required. No cloud. No telemetry. Fully offline.
- **Ed25519 Licensing**Cryptographic license validation - tamper-proof, offline-verified

## Pricing & Licensing

### Tier Comparison

| Feature | Free | Starter | Professional | Enterprise |
|---|---|---|---|---|
| Price (Monthly) | $0 | $599/mo | $1,799/mo | $4,999/mo |
| Price (Annual) | $0 | $499/mo | $1,499/mo | $4,166/mo |
| Compliance Scanning | Yes | Yes | Yes | Yes |
| Controls Assessed | 110 | 110 | 110 | 110 |

| | | | | |
|---|---|---|---|---|
| Windows + Linux | Yes | Yes | Yes | Yes |
| Auto OS Detection | Yes | Yes | Yes | Yes |
| Dual Credentials | Yes | Yes | Yes | Yes |
| Max Endpoints | Unlimited | 25 | 100 | Unlimited |
| Auto Remediation | No | Single-host | Batch | Batch |
| Rollback | No | Yes | Yes | Yes |
| Evidence Package | No | Basic | Full (signed ZIP) | Full (signed ZIP) |
| Scheduled Scans | No | No | Yes | Yes |
| API Access | Read-only | Full | Full | Full |
| Priority Support | Community | Email | Email + Phone | Dedicated |
| License Duration | Forever | Monthly/Annual | Monthly/Annual | Monthly/Annual |

### Free Tier

The Free tier provides full compliance scanning with no time limit. Organizations can assess their CMMC readiness across unlimited endpoints before committing to a paid tier. Scan results include per-control findings, compliance scores, and remediation guidance - but automated remediation requires a paid license.

### Starter Tier - $599/month

Designed for small teams with up to 25 endpoints. Includes single-host automated remediation, rollback capability, and basic evidence collection. Ideal for small contractors beginning their CMMC journey.

### Professional Tier - $1,799/month

The most popular tier for mid-size organizations. Supports up to 100 endpoints with batch remediation, full signed evidence package generation, scheduled scans, and phone support. Everything needed for C3PAO assessment readiness.

### Enterprise Tier - $4,999/month

Unlimited endpoints with dedicated support. For large organizations and MSPs managing multiple client environments. Includes all features plus dedicated support engineer.

> **Trial License**
> A 10-day trial license provides Professional-equivalent features so you can evaluate remediation and evidence collection before purchasing. Trial is a license type, not a pricing tier.

## License System

ForteFide uses Ed25519 digital signatures for tamper-proof license validation:

- License keys are cryptographically signed and verified offline
- No phone-home, no activation server, no internet requirement
- Each license encodes: organization ID, tier, endpoint limit, expiration date
- Machine binding optional (prevents license sharing between systems)
- License import via dashboard UI or file placement in ProgramData directory

> **Try Before You Buy**
> Download the Free tier and scan your entire environment. When ready to remediate, purchase a license and import it - no reinstall needed. The same binary serves all tiers.

## Technical Specifications

| Specification | Detail |
|---|---|
| Supported OS (Scanner) | Windows 10/11, Server 2016-2025, Ubuntu 20.04+, Debian 10+, RHEL 8+ |
| Supported OS (Targets) | Windows 10/11, Server 2012R2-2025 (WinRM), Any Linux with SSH |
| Dashboard Port | TCP 5000 (configurable) |
| Scan Protocol (Windows) | WinRM over HTTP (5985) with NTLM authentication |
| Scan Protocol (Linux) | SSH (22) with password or key authentication |
| Binary Size | Windows: 42 MB installer, Linux: 54 MB .deb |

| | |
|---|---|
| RAM Required | 512 MB minimum, 2 GB recommended |
| Disk Required | 200 MB + scan data |
| Database | SQLite (local, encrypted, no external DB required) |
| Encryption | AES-256-GCM (scan data), Ed25519 (license), SHA-256 (integrity) |
| Network | No internet required. Outbound to targets only. |
| Compilation | Nuitka standalone binary - no Python runtime needed |

## Why ForteFide

- **Single Binary**One .exe or .deb - no agents, no cloud, no dependencies
- **Air-Gap Native**Built for classified and disconnected environments
- **Instant ROI**Free scanner finds gaps today. Remediation license fixes them tomorrow.
- **Assessment Ready**23-document evidence package accepted by C3PAOs
- **Proven Results**89%+ compliance on hardened systems, 47% on vanilla Ubuntu
- **Mixed OS**Single scan covers Windows DCs, Linux servers, and everything between

## 7-Step Compliance Workflow

ForteFide guides customers through a structured 7-step process from zero to assessment-ready:

| Step | Name | Description |
|---|---|---|
| 1 | Network Recon | CIDR discovery finds all hosts on the network |
| 2 | Prepare Endpoints | Create service accounts, deploy SSH keys or certificates |
| 3 | Configure & Execute | Zero-credential scan using deployed keys |
| 4 | Baseline Evidence | Auto-collected signed evidence package |
| 5 | Review & Attest | Review findings, attest 11 manual controls, document exceptions |
| 6 | Remediate & Rescan | One-click remediation with safety engine, then verify |
| 7 | Final Evidence | Collect post-remediation package, teardown service accounts |

## Get Started

1. Download the free scanner from densedefense.com
2. Run a full 7-step workflow against your CUI boundary
3. Review your compliance score and gap analysis
4. Contact sales for licensing: info@dense.media