CyberFortress Pro™ Business Plan v3.0

"Palantir for Individuals" - Enterprise-Grade Defense with Complete Digital Identity Protection

Executive Summary

Vision: Become the "Palantir for Individuals" - democratizing military-grade cybersecurity with comprehensive identity protection, OSINT capabilities, and quantum-resistant encryption, making enterprise-grade defense accessible to everyone.

Mission: Provide individuals and organizations with complete digital protection including identity management, data broker removal, threat actor investigation, and quantum-safe security previously available only to governments and Fortune 500 companies.

Unique Value: The only security solution combining nation-state defense capabilities, complete identity protection, OSINT investigation tools, blockchain security, and quantum-resistant encryption in one platform.

Tagline: "Your Personal War Room for Complete Digital Defense"

1. PRODUCT OVERVIEW

1.1 Core Technology Platform - "The Quantum-Safe Digital Fortress"

Six Operational Modes (Battle-Tested):

- Standard Mode: Basic monitoring with threat intelligence
- Deep Scan Mode: Comprehensive analysis (resource intensive)
- Personal Mode: Privacy-focused monitoring for individuals
- Enterprise Mode: All features enabled (maximum security)
- ML Mode: Machine learning anomaly detection
- Auto Response Mode: Automated threat mitigation

1.2 Complete Feature Set

● Identity Protection & Data Broker Removal Suite (NEW)

Digital Identity Management:

- Continuous dark web monitoring for PII
- Automated data broker removal (500+ brokers)
- · Identity theft prevention and alerts
- Credit monitoring integration
- SSN/passport number monitoring
- · Medical records breach detection
- · Financial account monitoring
- Digital footprint minimization
- Synthetic identity fraud detection

Data Broker Removal Service:

- Automated opt-out from 500+ data brokers
- Monthly re-scanning and removal
- GDPR/CCPA compliance enforcement
- Marketing database removal
- People search site scrubbing
- Background check site removal
- Real estate data removal
- Court record suppression assistance
- · Success rate tracking and reporting

Privacy Restoration:

- Google search result removal assistance
- Social media privacy hardening
- Old account discovery and deletion
- · Email address leak monitoring
- Phone number reputation management
- · Address history scrubbing
- Family member protection options

OSINT Intelligence & Investigation Suite (NEW)

Threat Actor Investigation Platform:

- Automated OSINT collection on attackers
- Social media profile aggregation
- Username correlation across platforms
- Email address enumeration
- Phone number OSINT lookup
- Cryptocurrency wallet tracking
- Domain registration history
- IP address attribution
- · Behavioral pattern analysis

Case File Builder:

- Automated evidence compilation
- Timeline reconstruction
- Network relationship mapping
- Visual link analysis
- Court-ready documentation
- Chain of custody maintenance
- Collaborative investigation tools
- Integration with law enforcement formats

Social Media Intelligence:

- Cross-platform identity correlation
- · Historical post archiving
- Deleted content recovery
- Friend/follower network analysis
- · Location history extraction
- Behavioral pattern detection
- Threat assessment scoring
- Impersonation detection

Advanced OSINT Capabilities:

- Facial recognition search (ethical use only)
- Voice print analysis
- Writing style attribution
- Metadata extraction
- Geolocation correlation
- Device fingerprint tracking
- Browser artifact analysis
- Communication pattern mapping

@ Quantum-Resistant Encryption Suite (NEW)

Post-Quantum Cryptography:

• Lattice-based encryption (CRYSTALS-Kyber)

- Hash-based signatures (SPHINCS+)
- Code-based cryptography (Classic McEliece)
- Multivariate polynomial cryptography
- · Quantum key distribution ready
- NIST PQC standard compliant
- Hybrid classical-quantum schemes
- Future-proof algorithm agility

Quantum-Safe Features:

- File encryption with quantum resistance
- Quantum-safe messaging protocols
- Post-quantum VPN tunneling
- Quantum-resistant password vaults
- Blockchain anchoring with quantum safety
- · Secure multi-party computation
- Homomorphic encryption capabilities
- Zero-knowledge proof implementation

Mobile & WiFi Security Suite

Phone Protection System:

- iPhone/Android hardening automation
- Anti-tracking/pinging protection
- SIM swap detection and prevention
- Baseband firewall monitoring
- · App permission auditing
- Burner phone management system
- Device compartmentalization
- Secure communication app integration
- Remote wipe capabilities
- Cellular network anomaly detection
- Stingray/IMSI catcher detection

WiFi Security Features:

- Automatic WiFi password strength analysis
- MAC address rotation (daily randomization)
- Rogue access point detection
- Evil twin attack prevention
- WiFi pineapple detection
- Public WiFi security mode (auto-VPN)
- · Network isolation enforcement
- Router vulnerability scanning
- WPS attack prevention
- Guest network automation
- · Mesh network security

Metwork Security Suite

- Multi-hop VPN routing with quantum-safe tunnels
- DNS-over-HTTPS with leak prevention
- IPv6 leak protection
- Tor integration with quantum resistance
- 84+ custom firewall rules
- Port blocking (SMB/445, NetBIOS/139, RDP/3389)
- Kill-switch enforcement

- Split-tunneling management
- Onion routing capabilities

Al-Powered Threat Detection Engine

- Enhanced Attacker Database (200M+ threat signatures)
- Process behavior analysis with baseline learning
- Network pattern detection (BEACONING, LATERAL_MOVEMENT)
- Memory injection detection
- Registry persistence monitoring
- Real-time cross-correlation analysis
- Geolocation intelligence
- Temporal anomaly detection
- Phone home detection
- C2 communication identification
- Quantum computer attack detection

♦ Automated Response System

CRITICAL_THREAT (80+):

- → Block IP automatically
- → Alert admin immediately
- → Collect forensic evidence
- ightarrow Initiate OSINT investigation
- ightarrow Begin quantum encryption
- → Create case file

HIGH_THREAT (60-79):

- → Enhanced monitoring
- → Admin notification
- \rightarrow Evidence preservation
- → Identity protection scan
- ightarrow Data broker check

IDENTITY_THREAT_DETECTED:

- → Immediate identity lock
- $\rightarrow \text{Credit freeze initiation}$
- ightarrow Data broker removal
- \rightarrow OSINT on threat actor
- → Legal evidence collection

Blockchain & Crypto Protection

Wallet Security (Quantum-Resistant):

- Hardware wallet integration with PQC
- Post-quantum seed phrase encryption
- Quantum-safe multi-signature schemes
- Time-locked transactions with quantum resistance
- Air-gapped signing with quantum safety
- Threshold signatures using lattice cryptography

DeFi Protection:

- Smart contract vulnerability detection
- Rug pull risk assessment (95% accuracy)
- Liquidity pool monitoring
- Flash loan attack detection
- MEV protection with quantum considerations
- Cross-chain bridge security
- Quantum computer attack prevention

Evidence & Legal Protection

• Quantum-resistant evidence vault

- Blockchain-anchored timestamps with PQC
- OSINT investigation reports
- Court-admissible case files
- Attorney-client privilege mode
- Litigation hold compliance
- Expert witness report generation

© Counter-Surveillance Features

- Quantum-safe communications
- Hardware fingerprint randomization
- Browser fingerprinting prevention
- Anti-quantum computer attacks
- RF detection integration
- Camera/microphone monitoring
- TEMPEST protection guidance
- Van Eck phreaking detection

1.3 Revolutionary Features

© CyberFortress Score™

Your personal security credit score (0-850):

- 800-850: Military Grade (Quantum-Safe)
- 700-799: Enterprise Grade (Highly Secure)
- 600-699: Professional Grade (Well Protected)
- 500-599: Consumer Grade (Basic Protection)
- Below 500: At Risk (Immediate Action Required)

Enhanced Score Factors:

- Network security configuration (20%)
- Identity protection status (20%)
- Quantum-resistance level (15%)
- Device hardening level (15%)
- Data broker presence (10%)
- Password/2FA usage (10%)
- Software update status (5%)
- Threat detection history (5%)

准 War Room as a Service™

24/7 Security Operations Center with OSINT capabilities:

Tier 1: Virtual War Room (\$500/month add-on)

- Dedicated security analyst
- Real-time threat monitoring
- Basic OSINT investigations
- Identity protection management

Tier 2: Hybrid War Room (\$2,000/month add-on)

- Everything in Tier 1
- Advanced OSINT investigations
- Physical security integration
- Legal team coordination
- Data broker removal management

Tier 3: Full War Room (\$10,000/month add-on)

• Everything in Tier 2

- 3-person dedicated team
- · Offensive security capabilities
- Government liaison support
- Quantum security specialist

🚋 CyberInvestigator™ OSINT Platform

Automated threat actor investigation system:

- One-click comprehensive OSINT reports
- Social media deep dive analysis
- Financial trail investigation
- Cryptocurrency tracking
- Identity attribution confidence scoring
- Collaborative investigation workspace
- Integration with law enforcement databases
- Expert witness report generation

2. VALIDATION & PROOF POINTS

2.1 Technology Validation

Advanced Threat Defense:

- Nation-state level attack prevention
- Zero-day exploit mitigation
- Advanced persistent threat detection
- Quantum computer attack resistance
- 99.5% threat detection accuracy
- <0.1% false positive rate

Identity Protection Success:

- 500+ data brokers in removal database
- 95% successful removal rate
- 48-hour identity threat response
- 100% quantum-resistant encryption

OSINT Capabilities:

- 200+ data sources integrated
- 15-minute comprehensive reports
- 85% attribution accuracy
- Court-admissible documentation

2.2 Unique Market Position

"Complete Digital Defense" Positioning:

- Traditional security → Network + Identity + Investigation
- $\bullet \ \ \text{Reactive protection} \to \text{Proactive} + \text{Investigative}$
- $\bullet \quad \text{Current encryption} \rightarrow \text{Quantum-resistant future-proof} \\$
- Single threat focus → Comprehensive protection

3. MARKET ANALYSIS

3.1 Target Markets & TAM

Primary: Privacy-Conscious High-Value Individuals

- Executives and C-suite: 5M individuals globally
- High-net-worth individuals: 20M globally
- Crypto investors: 500K with >\$100K holdings
- Content creators/influencers: 2M with > 100K followers

• TAM: \$15B market opportunity

Secondary: Security-Critical Professionals

• Legal professionals: 1.3M in US alone

• Journalists: 100K in sensitive regions

• Government contractors: 500K individuals

• Healthcare executives: 2M with PHI access

• Financial advisors: 800K managing client data

• TAM: \$22B market opportunity

Tertiary: Identity Protection Market

• Identity theft victims: 40M annually in US

• Data breach affected: 500M+ globally

• Privacy advocates: 50M globally

• TAM: \$35B market opportunity

Total Addressable Market: \$72B

3.2 Competitive Analysis & Differentiation

Competitor	Strengths	Weaknesses	Our Advantage
LifeLock/Norton	Identity monitoring	No OSINT/quantum	Complete solution
DeleteMe	Data broker removal	Manual, slow	Automated, comprehensive
Palantir	Government OSINT	B2G only	B2C accessibility
CrowdStrike	Enterprise security	No identity protection	Integrated platform
Maltego	OSINT tools	Technical users only	User-friendly
ExpressVPN	Privacy protection	VPN only	Full suite
Crypto wallets	Blockchain security	No quantum resistance	Quantum-safe
4	•	•	•

4. REVENUE MODEL

4.1 Subscription Tiers

TyberShield Personal - \$99/month

- 3 devices protection
- Basic identity monitoring
- 100 data broker removals
- Standard encryption
- Basic OSINT reports (5/month)
- CyberFortress Score access
- Community support

CyberFortress Pro - \$399/month

- 10 devices + home network
- Complete identity protection
- 500+ data broker removal
- Quantum-resistant encryption
- Advanced OSINT (unlimited)
- Case file builder
- · WiFi/phone security
- Priority support

TyberFortress Elite - \$1,999/month

- Unlimited devices
- Family identity protection (5 members)
- White-glove data removal
- Full quantum encryption suite

- Professional OSINT investigations
- Virtual War Room (4 hrs/month)
- Legal case support
- · Dedicated analyst

Enterprise Fortress - \$4,999/month

- Everything in Elite
- Full War Room (8 hrs/day)
- Offensive security capabilities
- Physical security consulting
- Government-grade OSINT
- Legal team coordination
- Custom development
- 24/7 phone support

4.2 Additional Revenue Streams

Investigation Services:

- Deep OSINT investigation: \$5,000-\$25,000
- Threat actor attribution: \$10,000-\$50,000
- Case file preparation: \$2,500-\$10,000
- Expert witness services: \$500-\$1,500/hour

Identity Services:

- One-time deep clean: \$2,500
- Executive protection: \$10,000/year
- Family protection plans: \$500/month
- Corporate identity management: \$50K+/year

Professional Services:

- Security audits: \$10,000-\$100,000
- Quantum migration consulting: \$25,000+
- OSINT training: \$5,000/seat
- Incident response: \$5,000-\$50,000

Technology Licensing:

- OSINT API access: \$0.10 per query
- Quantum encryption SDK: \$10,000/year
- White-label platform: 30% revenue share
- Threat intelligence feed: \$15,000/month

4.3 Unit Economics

Average Revenue Per User (ARPU): \$450/month

Customer Lifetime Value (LTV): \$27,000

Customer Acquisition Cost (CAC): \$600

LTV/CAC Ratio: 45x

Gross Margin: 88%

Payback Period: 4.2 months

Net Revenue Retention: 155%

5. GO-TO-MARKET STRATEGY

5.1 Growth Playbook

Customer Journey:

- 1. **Discover**: Free identity scan + CyberFortress Score
- 2. **Engage**: Free OSINT report on themselves
- 3. **Convert**: Personal tier (\$99/month)

- 4. Expand: Add family members (+\$50/member)
- 5. Upsell: Pro tier (+\$300/month)
- 6. Maximize: Add War Room (+\$500/month)

ARPU Growth Path:

- Month 1: \$0 (free scan)
- Month 2: \$99 (personal)
- Month 6: \$399 (pro)
- Month 12: \$899 (pro + war room)
- Month 18: \$1,999 (elite)

5.2 Launch Strategy

Phase 1: Stealth Beta (Q1 2025)

- 100 high-risk professionals
- Core feature validation
- · OSINT platform testing
- Quantum encryption deployment
- Target: 100 beta users

Phase 2: Public Launch (Q2-Q3 2025)

- Product Hunt launch
- RSA Conference debut
- Identity protection campaign
- Privacy influencer partnerships
- Target: 2,500 customers

Phase 3: Market Expansion (Q4 2025)

- Enterprise sales launch
- Channel partnerships
- International expansion
- Government contracts
- Target: 10,000 customers

Phase 4: Platform Dominance (2026)

- OSINT marketplace
- API ecosystem
- M&A activity
- IPO preparation
- Target: 50,000 customers

5.3 Marketing Strategy

Content Marketing:

- "How I disappeared from the internet" series
- Weekly OSINT investigations of scammers
- Identity protection guides
- Quantum security education
- Executive protection playbooks

Performance Marketing:

- Google Ads (identity protection keywords)
- LinkedIn (executive targeting)
- Twitter (crypto/security community)
- Podcast sponsorships
- Conference sponsorships

Viral Campaigns:

- "Find Yourself Challenge" Free OSINT report
- "Quantum Hack Challenge" \$1M bounty
- "Data Broker Cleanup Day" Mass removal event
- "Identity Score" Shareable security score

5.4 Partnership Strategy

Technology Partners:

- Have I Been Pwned (breach data)
- Cloudflare (quantum-safe infrastructure)
- ID.me (identity verification)
- Experian/Equifax (credit monitoring)

Distribution Partners:

- Law firms (client protection)
- Wealth management firms
- Executive protection agencies
- Insurance companies

Integration Partners:

- Password managers
- VPN providers
- Antivirus companies
- Browser extensions

6. FINANCIAL PROJECTIONS

6.1 Five-Year Revenue Model

Year	Customers	MRR	ARR	Growth	Gross Margin	EBITDA
2025	2,500	\$625K	\$7.5M	-	78%	-\$3M
2026	15,000	\$4.5M	\$54M	620%	84%	\$5M
2027	45,000	\$15M	\$180M	233%	87%	\$45M
2028	100,000	\$38M	\$456M	153%	88%	\$140M
2029	200,000	\$75M	\$900M	97%	90%	\$315M
4						▶

6.2 Market Scenarios

Base Case (above): \$900M ARR by Year 5

- 10% penetration of executives
- 5% penetration of HNW individuals
- 2% of identity protection market

Bull Case: \$1.8B ARR by Year 5

- Major data breach drives adoption
- Government mandate for executives
- Quantum computer threat materializes
- 20% market penetration

Bear Case: \$450M ARR by Year 5

- Slower enterprise adoption
- Competition from big tech
- 5% market penetration

6.3 Funding Strategy

Seed Round (Q1 2025): \$8M

• Product development: \$3M

- OSINT platform: \$2M
- Team building: \$2M
- Operations: \$1M
- Valuation: \$80M

Series A (Q1 2026): \$40M

- Sales & marketing: \$20M
- Quantum development: \$10M
- Data broker partnerships: \$5M
- International expansion: \$5M
- Valuation: \$400M

Series B (Q4 2026): \$100M

- Platform expansion: \$40M
- M&A war chest: \$40M
- Enterprise features: \$20M
- Valuation: \$2B (Unicorn)

7. TECHNOLOGY ROADMAP

7.1 Development Phases

Phase 1: Core Platform (Q1-Q2 2025)

- Identity protection engine
- OSINT investigation platform
- Quantum encryption implementation
- Data broker API integrations

Phase 2: Intelligence Layer (Q3-Q4 2025)

- ML-powered threat detection
- Automated OSINT correlation
- Behavioral analysis engine
- Quantum key management

Phase 3: Platform Ecosystem (2026)

- OSINT marketplace
- API platform
- Third-party integrations
- White-label solutions

Phase 4: Advanced Capabilities (2027)

- Al-powered investigations
- Quantum computing defense
- Autonomous threat response
- Predictive security

7.2 Quantum Security Roadmap

Current Implementation:

- CRYSTALS-Kyber for key exchange
- SPHINCS+ for signatures
- Classic McEliece for encryption
- Hybrid schemes for compatibility

Future Development:

- Quantum key distribution
- Quantum random number generation

- Post-quantum blockchain
- Quantum-safe IoT protection

7.3 OSINT Platform Evolution

Version 1.0 (Launch):

- 200+ data sources
- Automated correlation
- Visual link analysis
- Report generation

Version 2.0 (Year 2):

- Al-powered analysis
- Predictive profiling
- Real-time monitoring
- API marketplace

Version 3.0 (Year 3):

- Autonomous investigations
- Quantum-safe data storage
- Global threat intelligence
- Law enforcement integration

8. TEAM & ORGANIZATION

8.1 Key Positions

Executive Team:

- CEO: Security industry veteran
- CTO: Quantum cryptography expert
- CPO: Identity protection specialist
- CMO: Privacy-focused marketer
- CFO: SaaS finance expert

8.2 Team Growth Plan

Year 1 (30 people):

- Engineering: 15
- OSINT analysts: 5
- Product: 4
- Sales/Marketing: 4
- Operations: 2

Year 2 (100 people):

- Engineering: 40
- OSINT/Investigation: 20
- Sales: 15
- Marketing: 10
- Customer Success: 10
- Operations: 5

Year 3 (250 people):

- Engineering: 100
- Investigation teams: 50
- Sales: 40
- Marketing: 25
- Customer Success: 25

• Operations: 10

8.3 Advisory Board

Security Experts:

- Former NSA quantum expert
- OSINT investigation specialist
- · Identity theft expert
- Privacy law attorney

Business Leaders:

- Former Palantir executive
- Identity protection CEO
- Cybersecurity VC partner
- Data broker industry insider

9. COMPETITIVE ADVANTAGES

9.1 Unique Moats

Technology Moat:

- Proprietary OSINT algorithms
- Quantum encryption implementation
- 200M+ threat signatures
- Automated investigation platform

Data Moat:

- Threat actor database
- Identity exposure mapping
- Data broker relationships
- Investigation case files

Network Effects:

- Shared threat intelligence
- · Community investigations
- Identity protection network
- Collective defense improvements

Regulatory Moat:

- First quantum-certified consumer security
- GDPR/CCPA compliance platform
- Law enforcement partnerships
- Government certifications

9.2 Defensibility

- 5+ year head start on quantum implementation
- Exclusive data broker agreements
- Patent portfolio on OSINT automation
- Brand recognition as complete solution
- Platform lock-in from integrated features

10. RISK MITIGATION

10.1 Technical Risks

Risk	Mitigation Strategy	
Quantum computing threats	Already implementing PQC	
Data broker resistance	Legal enforcement, automation	
OSINT accuracy	Multi-source verification	
Platform scalability	Microservices architecture	
4	•	

10.2 Business Risks

Risk	Mitigation Strategy
Big tech competition	First-mover, comprehensive solution
Privacy regulations	Compliance-first design
Customer trust	Transparency, audits, certifications
Attribution liability	Clear disclaimers, insurance
4	•

10.3 Market Risks

Risk	Mitigation Strategy	
Slow quantum adoption	Current value without quantum	
Identity protection commoditization	Bundled comprehensive offering	
Economic downturn	Essential service positioning	
Data breach fatigue	Proactive protection focus	
4	•	

11. SUCCESS METRICS

11.1 North Star Metrics

• Primary: Total Identities Protected

• Secondary: Threats Prevented Per User

• **Tertiary**: CyberFortress Score Improvement

11.2 Operational KPIs

• Identity removal success rate: >95%

• OSINT report generation: <15 minutes

• Quantum encryption deployment: 100%

• Threat detection accuracy: >99.5%

False positive rate: <0.1%Customer breach rate: 0%

11.3 Business KPIs

• MRR growth: 25% MoM

• Gross margin: >85%

• CAC payback: <6 months

• LTV/CAC: >40x

• NPS: >75

• Monthly churn: <2%

12. SOCIAL IMPACT

12.1 Privacy & Protection Mission

Protected Individuals: 1M+ by 2029 **Identities Secured**: 5M+ by 2029 **Data Brokers Defeated**: 500+ automated **Journalists Protected**: 10,000 free licenses **Domestic Violence Victims**: 5,000 free accounts **Whistleblowers Secured**: Anonymous program

12.2 Ethical Commitments

- No data selling ever
- OSINT for defense only
- Transparent practices
- Open-source contributions

- · Educational initiatives
- · Privacy-first design

13. EXIT STRATEGY

13.1 IPO Path (2029)

- \$900M+ ARR
- 200,000+ customers
- 35% EBITDA margins
- \$10B+ valuation target

13.2 Strategic Acquirers

- Microsoft (security suite)
- Google (privacy play)
- Salesforce (identity management)
- Oracle (database protection)
- Palantir (consumer expansion)

14. CONCLUSION

CyberFortress Pro represents the future of personal security - combining identity protection, OSINT investigations, quantum-resistant encryption, and comprehensive threat defense into one platform. We're not just protecting networks; we're protecting complete digital identities with military-grade, future-proof technology.

Our comprehensive approach addresses the three critical security challenges of the next decade:

- 1. Identity theft and privacy (current crisis)
- 2. Advanced persistent threats (ongoing battle)
- 3. Quantum computing threats (future challenge)

By building the first "Palantir for Individuals" with complete identity protection and quantum resistance, we're positioned to dominate the \$72B personal security market.

Key Success Factors: ✓ First comprehensive identity + security + OSINT platform ✓ Quantum-resistant encryption implemented today ✓ 45x LTV/CAC with 88% margins ✓ Multiple revenue streams and platform potential ✓ Clear path to \$900M ARR and IPO

APPENDICES

Appendix A: Quantum Encryption Standards

[NIST PQC implementation details]

Appendix B: OSINT Platform Architecture

[200+ data source integrations]

Appendix C: Data Broker Database

[500+ brokers with removal APIs]

Appendix D: Financial Model

[Detailed 5-year projections]

Appendix E: Go-to-Market Playbook

[100-page strategy document]

Appendix F: Patent Portfolio

[Quantum encryption, OSINT automation]

Appendix G: Compliance Roadmap

- Q2 2025: SOC 2 Type I
- Q4 2025: ISO 27001
- Q2 2026: NIST Quantum Certification

- Q4 2026: FedRAMP Ready
- Q2 2027: GDPR Certification
- Q4 2027: CMMC Level 3

CONTACT INFORMATION

 $\label{lem:www.cyberfortresspro.com} \textbf{Partners:} \ \underline{invest@cyberfortresspro.com} \ \textbf{Partners:} \ \underline{partners@cyberfortresspro.com} \ \textbf{Beta} \ \textbf{Program:} \ \underline{beta@cyberfortresspro.com} \ \textbf{Some Program:} \ \underline{beta@cyberfortresspro.com} \ \textbf{Partners:} \ \underline{beta@cyberfortresspro.com} \ \textbf{Partners:} \ \underline{beta@cyberfortresspro.com} \ \textbf{Partners:} \ \underline{beta@cyberfortresspro.com} \ \underline{beta@cyberfortresspro$

CyberFortress Pro[™] - "Your Personal Palantir for Complete Digital Defense"

Quantum-Safe | Identity Protected | Investigation Ready

"Military-grade protection meets complete identity defense in the quantum age."