SpiderOak

SERVICES

FORTEXS: Fortifying Existing Systems

Fielded tactical edge systems continue to serve mission-critical roles, even as the threat landscape has evolved beyond their original security assumptions – often without modern protections like zero trust or secure-by-design principles.

FORTEXS is SpiderOak's zero trust and cyber resilience upgrade pathway for existing platforms.

Modernizing deployed architectures is achieved by layering in access controls, containment mechanisms, and policy-driven telemetry monitoring without requiring a full system redesign.

Whether supporting communication networks, space vehicles, or UAV swarms operating in DDIL environments, FORTEXS enables a transformation into more cyber-resilient tactical edge systems.

Scan to Get Started

What FORTEXS Delivers

- **Architecture Assessment & Trust Boundary Mapping:** Identifying trust violations, exposure points, and segmentation gaps in current system designs or fielded configurations
- **Zero Trust Strategy & Implementation:** Designing and integrating overlay mechanisms to introduce authentication, authorization, and control without requiring full system redesign
- **Adversary-Resilient System Defense:** Enhance mission assurance by aligning security improvements with attacker behaviors, inherited architectural risk, and system-critical functionality
- **Legacy Integration Strategy:** Bridging existing components with modern access controls, policy, and telemetry tooling while preserving core operational functionality
- **Cyber-Informed Resilience Engineering:** Strengthen critical system functions through segmentation, fallback control paths, and autonomous response strategies to withstand, recover from, and adapt to cyber compromise in contested or degraded environments

services@spideroak.com

@spideroak

Why FORTEXS

Tactical edge systems that lack modern cyber defenses are increasingly vulnerable to disruption, degradation, and adversarial exploitation. Particularly in disconnected, degraded, intermittent, and low-bandwidth (DDIL) environments. FORTEXS helps close that gap by bringing zero trust principles, assured communications, and cyber resilience to existing platforms. The result is a hardened system capable of sustaining operations at the tactical edge, maintaining mission continuity, and resisting compromise in the most contested environments.

Who SpiderOak Supports

SpiderOak's FORTEXS service offering supports commercial and defense organizations working to modernize and secure fielded systems:

- Programs operating and sustaining tactical edge platforms such as UAVs, space vehicles, specialized payloads, communication networks, and ground infrastructure
- Integrators and engineering teams retrofitting modern cyber defenses into mission-critical systems while preserving original mission functionality
- Teams advancing legacy systems toward increased cyber resilience in contested environments, secure redeployment, or adversary-informed red team evaluation

Key Benefits

- Embeds modern cyber defenses with playbook strategies into legacy systems without requiring full system redesign
- Preserves original mission functionality while strengthening resilience in DDIL environments
- Introduces policy-driven access control and telemetry to secure both internal and external-facing system interfaces
- Supports secure redeployment and aligns with emerging zero trust architecture mandates

Compliance & Framework Alignment

FORTEXS is an engineering-driven upgrade path that utilizes and aligns with the intent of key cyber resilience frameworks. SpiderOak's definitive security architectural approach reinforces real-world principles defined under:

- NIST 800-207: Zero Trust Architecture
- DoD Zero Trust Reference Architecture
- MITRE's Cyber Resiliency Engineering, ATT&CK, and EMB3D Frameworks

Get Started with FORTEXS

Modernizing existing systems to defend against today's advanced cyber threat landscape does not require a full redesign, but rather a robust architectural enhancement strategy. FORTEXS strengthens fielded platforms by integrating zero trust principles, reinforcing critical control paths, and enhancing cyber resilience in contested, degraded, and denied environments. Whether preparing for redeployment or mitigating known risks, SpiderOak's FORTEXS engineering-driven upgrade pathway delivers fortified defenses tailored to the reality of your platform's operational environment.

Scan to Get Started

The FORTEXS Process

FORTEXS helps security and platform teams identify architectural risks and apply zero trust principles to fielded systems, without disrupting mission operations or creating unmanageable redesign overhead. Each engagement follows a flexible, structured process designed to evaluate deployed systems in context and deliver actionable resilience guidance.

1. ### Mission Alignment

   Clarify mission priorities, deployment realities, and risk thresholds through stakeholder interviews and operational analysis.

2. ### Architecture Intake & Trust Assessment

   Map current trust boundaries, access paths, and platform constraints to baseline architectural assumptions and inherited exposures.

3. ### Threat-Informed Architecture Review

   Model realistic adversary pathways, identify resilience gaps, and recommend retrofit opportunities tailored to system realities.

4. ### Zero Trust Integration Strategy

   Design enforceable access, segmentation, and logging strategies compatible with constrained or disconnected systems.

5. ### Secure Component Evaluation

   Assess firmware, OS, and third-party component integrity, lifecycle risks, and compliance with sourcing and provenance expectations.

6. ### Resilient Architecture Refinement Guidance

   Deliver mission-aligned architecture refinement guidance and roadmap-ready outputs to support resilient system sustainment and modernization.