SpiderOak

SERVICES

TEARA: Tactical Edge Assured Resilient Architecture

Mission continuity and success at the tactical edge starts with cyber resilient architecture. New platforms must be built to withstand evolving, advanced cyber threats from day one.

SpiderOak's Tactical Edge Assured Resilient Architecture (TEARA) applies zero trust and secure-by-design principles from the ground up, embedding access control, segmentation, and defense-in-depth directly into a system architecture design "DNA."

Whether designing space vehicles, UAVs, ground station systems, or tactical networks, TEARA prepares platforms to operate securely in contested, disconnected, degraded, intermittent, and low-bandwidth (DDIL) environments, while enabling asynchronous operations across highly distributed systems where cyber resilience is non-negotiable.

Scan to Get Started

What TEARA Delivers

- **Threat-Informed System Design:** Engineering resilient platforms with built-in containment, telemetry, and adaptive access controls from the start
- **Zero Trust Design Blueprinting:** Architecting systems with zero trust principles that assume compromise and limit lateral movement by enforcing strict access controls
- **Policy Enforcement Planning:** Developing enforcement mechanisms at key control points of network and application layers
- **Secure Component Integration Strategy:** Evaluating and aligning hardware, firmware, and operating system choices for security, interoperability, and long-term maintainability
- **Mission-driven Prioritization:** Prioritizing protection of critical functions, payloads, or data flows through differentiated controls and resilience strategies aligned to operational objectives.

services@spideroak.com

@spideroak

Why TEARA

Sophisticated adversaries do not wait for approved retrofits - they target systems no matter their position in the design, development, or deployment lifecycle. Without architectural defenses and secure-by-design principles embedded early, adversaries can gain access and persist undetected even as security improvements are introduced over time. Further, systems deployed without strong trust boundaries or access controls become mission liabilities. TEARA shifts the security conversation from remediation to proactive design for systems, including between systems or families of systems. By embedding enhanced cyber resilience principles from day one, SpiderOak helps teams build systems that can better withstand compromise, operate reliably in DDIL conditions, and maintain operational effectiveness under mission pressure.

Who SpiderOak Supports

SpiderOak's TEARA service supports commercial and defense system development teams designing the next generation of secure, resilient platforms:

- Tactical edge systems such as satellites, UAVs, ground infrastructure, edge compute nodes, specialized payloads and ISR platforms operating in DDIL and contested environments
- Sensitive platforms across space, air, and critical infrastructure requiring asynchronous, distributed operations, including integration into mission assurance monitoring platforms (i.e., SIEM or mission/payload dashboards)
- Mission-critical systems that demand embedded zero trust, secure-by-design principles, and architectural resilience from the outset

Key Benefits

- Prepares tactical edge systems for contested, DDIL environments with secure-by-design architectures following zero trust principles
- Minimizes costly redesigns and downstream integration complexity by building in security from day one through a layered approach
- Aligns with ZTA principles to support future mandates and cyber resilience

Compliance & Framework Alignment

TEARA is designed to utilize and align with the intent of mission-relevant frameworks, including:

- NIST SP 800-207: Zero Trust Architecture
- DoD Zero Trust Reference Architecture
- Secure-by-Design and Secure Software Development Lifecycle principles (NIST SP-800-218 Secure Software Development Framework)
- MITRE's Cyber Resiliency Engineering, ATT&CK, and EMB3D Frameworks

Get Started with TEARA

Effective security implementation strategy must be foundational to tactical edge system architectures, not a "phased in" post-deployment approach, as advanced adversaries actively develop capabilities to disrupt the continuity of critical missions. TEARA helps teams embed resilience from day one by aligning new architecture designs with threat-informed modeling, zero trust principles, and real-world operational constraints. Raise the bar for cyber resilience with TEARA for a system architecture designed to withstand sophisticated adversarial threats and support mission assurance.

Scan to Get Started

The TEARA Process

TEARA offers a structured yet flexible approach to designing secure, resilient architecture. Each engagement is tailored to your platform's design maturity, mission needs, and operational constraints, guiding architectural decisions and embedding long-term security from day one.

1. ### Mission Alignment

   Clarify mission priorities, operational assumptions, and risk tolerance to inform architectural tradeoffs and design scope.

2. ### System Architecture & Trust Modeling

   Map components, data flows, and control boundaries to establish trust zones and identify security-critical design surfaces.

3. ### Threat-informed Design Evaluation

   Model attacker behaviors, evaluate exposure paths, and identify design-level gaps that impact mission resilience.

4. ### Zero Trust Strategy Development

   Define access control enforcement, segmentation logic, and observability strategies aligned with Zero Trust principles and DDIL constraints.

5. ### Component & Supply Chain Assessment

   Review hardware, firmware, and third-party tools for sourcing integrity, lifecycle supportability, and compliance risks.

6. ### Resilient Architecture Guidance

   Deliver mission-aligned architecture design plans, Zero Trust–aligned blueprints, and advisory artifacts to drive secure platform development through the full lifecycle.