

USE CASE

Mission-Ready Mobility on a Single Device

Enabling defense leaders to realize secure mobility in closed enclaves

Summary

Challenge

Reliance on multiple device types increases security risks, hardware costs, and delays decision-making across diverse, air-gapped environments.

Solution

XD Tyton delivers secure mobility in closed environments by replacing the current multi-device burden with a single, trusted device.

Outcome

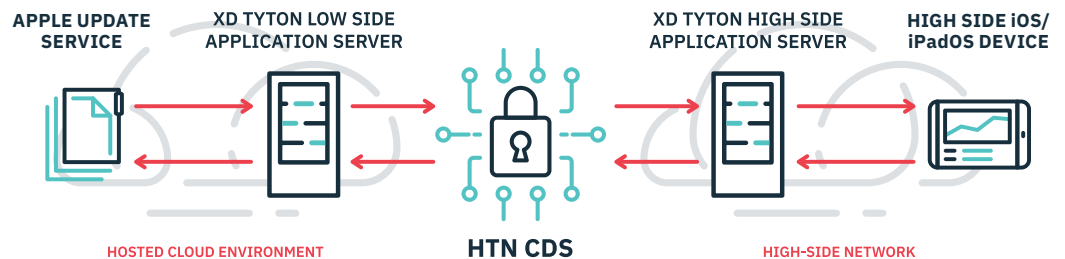
Accelerated decision-making, hardware reduction, enhanced user experience, secure workflows, and compliance with U.S. Government mandates.

The Burden of Multi-Device Management

Executives and practitioners working in air-gapped environments traditionally have had to manage multiple devices to maintain secure communications across networks. This means users may be juggling three or more government-issued device types, and their personal devices may be completely off-limits for work in closed environments. This approach complicates workflows, results in cumbersome device management, slows critical decision-making, and prevents personnel from leveraging iOS® and iPadOS® within air-gapped domains. The resulting hardware redundancy increases costs and disrupts coordinated command and response during mission-critical operations.

A Single Device for Secure Communications with XD Tyton™

Owl XD Tyton is a breakthrough solution that provides an approved secure gateway for iOS and iPadOS into air-gapped networks. XD Tyton is purpose-built to solve the executive need for secure, uninterrupted communications from any location—home, office, or classified environments. Designed specifically for users operating in classified or otherwise closed enclaves. XD Tyton replaces the current multi-device burden with a single, trusted device. Its secure protocol adapter bridges classified and unclassified networks, seamlessly integrating with High Threat Network (HTN) Cross Domain Solutions and Mobile Device Management (MDM) systems. This framework ensures U.S. Government Raise the Bar and Commercial Solutions for Classified (CSfC) compliance, eliminates device sprawl, and preserves a similar OS experience for decisive, secure communications anywhere.



OWL XD TYTON ARCHITECTURE

Results/Outcomes

- **Unified Device Usage:** Use one familiar iOS device for both unclassified and classified communications.
- **Accelerated Decision Making:** Connect securely from remote locations, reducing response times during critical events.
- **Reduced Hardware Costs:** Eliminate the need for purchasing and managing multiple devices per executive.
- **Enhanced User Experience:** Deliver the intuitive iOS interface users prefer without compromising security protocols.
- **Seamless Mobility:** Transition effortlessly between home, office, and field environments while maintaining secure connectivity.
- **Proven Compliance:** Meets U.S. Government CSfC and Raise the Bar requirements to ensure secure, approved communications.
- **Commercial-Grade Security at Scale:** Instead of relying on fragmented mobile platforms, XD Tyton leverages the same Apple servers and technology used by commercial customers, delivering constant software updates and the latest security protections from a leading mobile device provider



XD Tyton™: Revolutionizing Secure Mobility

Owl's XD Tyton™, the first secure gateway for iPhone® & iPad® in air-gapped networks, enables iOS and iPadOS devices to update securely within air-gapped environments by facilitating secure over-the-air (OTA) updates to keep iPhones and iPads protected, compliant, and mission-ready. When deployed alongside a compliant commercial High Threat Network (HTN) Cross Domain Solution (CDS), the integrated architecture meets the U.S. Government's Raise the Bar (RTB) and Commercial Solutions for Classified (CSfC) program requirements. XD Tyton can also integrate with Mobile Device Management (MDM) solutions for centralized device provisioning, policy enforcement, and streamlined management. XD Tyton, the first and only solution to secure closed and high risk networks, delivers connected and compliant mobility with iPhones and iPads performing critical missions spanning flight decks, field operations, and command centers.

iPhone, iPad, iOS, and iPadOS are trademarks of Apple Inc., registered in the U.S. and other countries. Owl Cyber Defense is not affiliated with or endorsed by Apple Inc.



Owl Cyber Defense Solutions, LLC, headquartered in Columbia, MD, leads the industry in data diode and cross-domain network cybersecurity solutions for faster, safer and smarter decision making. We create solutions tailored for high-risk sectors including the military, government and critical infrastructure. Our advanced technologies enable secure, near-instantaneous collaboration, bridging network barriers to protect critical missions. With a focus on scalability and interoperability, Owl ensures that organizations can maintain secure, reliable, and compliant communication channels against evolving cyber threats.

For more information on Owl, or to schedule a demo, visit www.owlcyberdefense.com.

