

USE CASE

Secure Over-the-Air iOS & iPadOS Updates for Air-Gapped Networks

Enabling timely, secure OTA software updates for iPhones & iPads in closed environments

Summary

Challenge

Air-gapped networks block iOS & iPadOS software updates, risking security and increasing costs.

Solution

XD Tyton enables secure over-the-air software iOS & iPadOS updates in classified or otherwise closed environments.

Outcome

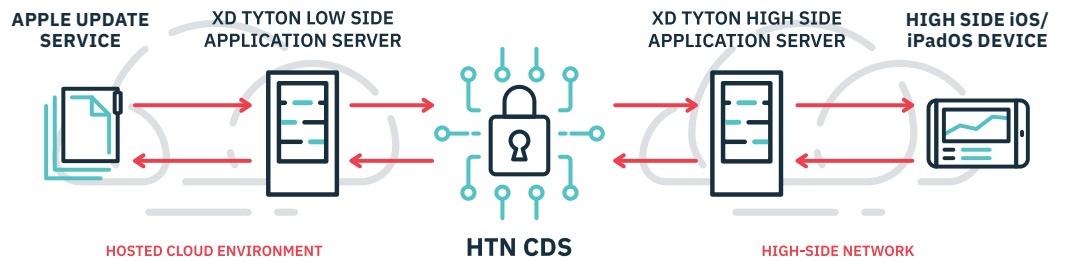
Extended device lifecycle, automated patching, cost reduction, operational continuity, and compliance.

Challenge: iPhones & iPads in Closed Environments Miss Critical Security Updates

Currently, air-gapped networks prevent iPhone® & iPad® devices running iOS® & iPadOS® from connecting to the Internet to receive critical, recurring Over-the-Air (OTA) software updates. This connectivity gap forces agencies to frequently destroy and replace functioning devices or rely on non-compliant, labor-intensive manual workarounds to maintain software currency. These inefficiencies degrade security postures, dramatically increase hardware procurement costs, and leave mission-critical mobile assets vulnerable to unpatched exploits and rapid obsolescence.

XD Tyton™: The First Secure Gateway to Enable iOS & iPadOS Updates in Closed Environments

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 address this challenge by securely routing and filtering update requests from closed environments to the Internet where software updates live through a specialized protocol adapter. This innovative approach enables automated, compliant over-the-air iOS & iPadOS updates, even within isolated, high-risk environments where traditional connectivity is not an option for the first time ever. By bridging this gap, XD Tyton eliminates the need for manual workarounds or device replacements and ensures that critical security patches and software updates are delivered so agencies can maintain operational readiness and data integrity. This solution not only reduces costs but also enhances mission efficiency by keeping devices secure and up-to-date in real time.



OWL XD TYTON ARCHITECTURE

Results/Outcomes

- **Extended Device Lifecycle:** Eliminates the costly requirement to destroy and replace devices due to update inability.
- **Automated Security Patching:** Ensures devices receive critical security updates immediately without manual administrative intervention.
- **Significant Cost Reduction:** Lowers total cost of ownership by maximizing the operational lifespan of deployed hardware.
- **Operational Continuity:** Maintains mission readiness by preventing device unauthorized status or software expiration.
- **Strict Compliance:** Adheres to U.S. Government Raise the Bar requirements for secure data transfer in high-threat networks.
- **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 or otherwise closed 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.

