

Threadfin's Microsoft Intune QuickStart



Customer: Summit Re
Industry: Financial Services
Locations: 3

Employees: 200
Duration: 3 weeks
Delivery Model: Fixed fee

EXECUTIVE SUMMARY

Summit Re, a 200-person reinsurance brokerage headquartered in Chicago with 2 satellite offices, needed to modernize its endpoint management to support a hybrid workforce and improve security.

Their IT team managed a mix of Windows laptops, mobile devices and a few macOS systems using a patchwork of local policies, basic MDM tied to Exchange Online and manual application installs.

Threadfin was engaged to deliver a Microsoft Intune QuickStart—establishing a secure, scalable foundation for endpoint management, improving compliance and enabling zero-touch provisioning for new devices.

CURRENT COMPUTE ENVIRONMENT

Device mix:

- 150 Windows 10/11 laptops & desktops
- 20 macOS devices
- 25 iOS/iPadOS mobile endpoints
- 10 Android tablets

Identity platform:

- Entra ID (Azure AD) hybrid join enabled for Windows endpoints

Existing management tools:

- No centralized management for mobile devices
- Local GPOs for Windows security policies
- Manual application deployment

Security stack:

- Microsoft Defender for Endpoint licensed but not deployed to all endpoints
- BitLocker encryption not consistently applied

EXECUTION SUMMARY

Over the course of 3 weeks, Threadfin:

- Verified hybrid Entra ID join status across Windows endpoints
- Configured Intune tenant settings and baseline policies
- Established mobile application management for iOS and Android
- Created and applied compliance and security baselines for Windows devices
- Onboarded Windows endpoints into Microsoft Defender for Endpoint
- Configured Windows Autopilot for zero-touch deployment and validated workflows with 2 pilot devices
- Packaged and deployed core business applications
- Delivered runbooks and conducted live training sessions with Summit Re's IT staff

CASE STUDY | QUICKSTART

Threadfin's Microsoft Intune QuickStart

SCOPE OF WORK

Threadfin's Intune QuickStart for Summit Re included:

Licensing & setup configuration:

- Audit & validate Intune & Entra ID licensing
- Configure Azure AD Connect for hybrid join

Device policies:

- Configure 1 iOS & 1 Android MAM policy
- Create 2 Windows 10/11 configuration profiles

Compliance & security:

- Create 1 Windows compliance policy
- Establish MFA conditional access policy
- Configure Microsoft Defender for Endpoint onboarding
- Configure Intune for Windows updates

Application deployment:

- Deploy Microsoft 365 Apps for Enterprise, Google Chrome & Adobe Acrobat Reader via Intune/Autopilot
- Provide proof-of-concept deployment

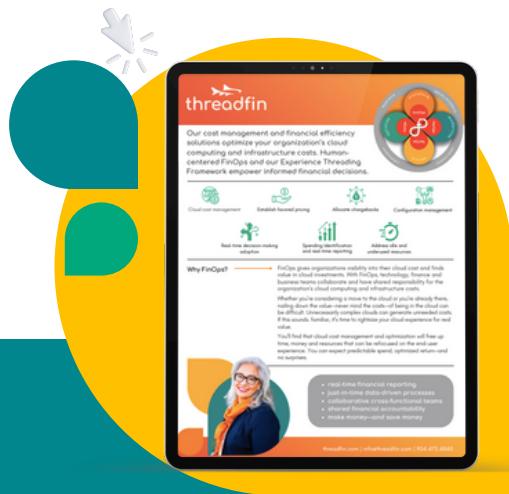
Windows Autopilot:

- Configure zero-touch deployment
- Test Autopilot with 2 devices
- Create runbooks for Autopilot workflows & software deployment processes

Knowledge transfer:

- Provide 8 hours of dedicated knowledge transfer & admin training

[Click here to learn more.](#)



POSSIBLE NEXT STEPS (OUTSIDE SCOPE)

During the QuickStart, opportunities for further improvement were identified:

- Expand Defender for Endpoint onboarding to macOS & mobile devices
- Migrate existing GPOs into Intune configuration profiles for centralized policy management
- Implement additional conditional access policies for location & risk-based controls
- Establish ongoing configuration drift monitoring using Microsoft Graph or M365DSC
- Transition to a full Intune modernization, including multi-platform app packaging & advanced reporting

COMPREHENSIVE ENGAGEMENT SUMMARY

The Intune QuickStart provided Summit Re with a secure, well-structured Intune environment ready to manage Windows, mobile and macOS devices. The engagement delivered:

- Centralized policy enforcement for core platforms
- Improved security through MFA, compliance baselines and Defender onboarding
- A functional zero-touch deployment workflow with Autopilot
- Packaged and deployed core productivity applications
 - Knowledge transfer & documentation for ongoing management

Summit Re now operates from a unified endpoint management foundation that is scalable, secure, and aligned with Microsoft best practices—ready to expand as the organization's needs grow.