Intune – Modern Endpoint Proof of Concept Alignment

Service Information Document (Customer-Facing)

1. Offer Overview

The **ProArch Intune – Modern Endpoint Proof of Concept (PoC)** helps organizations evaluate Microsoft Intune as a secure, cloud-native endpoint management platform before committing to a full production rollout. The engagement provides a structured, low-risk way to validate modern device management, security controls, and operational readiness across a limited set of endpoints.

This service translates Microsoft best practices for modern endpoint management into a practical pilot that demonstrates how devices can be securely enrolled, configured, protected, and managed using Microsoft Intune, Conditional Access, and Windows Autopilot. The engagement produces documented validation results and clear next-step guidance that enable confident decisions about scaling modern endpoint management.

1.1 What "Modern Endpoint" Means in This Offer

- Endpoint management is cloud-first and policy-driven using Microsoft Intune
- Security and compliance are enforced through Conditional Access and device compliance policies
- Device provisioning is automated using Windows Autopilot
- Application deployment and configuration are centrally managed
- Visibility into device inventory, posture, and compliance is established early

2. Who Is This Offer For?

This offer is designed for organizations looking to modernize endpoint management, reduce reliance on legacy tools, and improve security across Windows and macOS devices. It is ideal for teams that want to validate Intune's capabilities in their own environment before scaling adoption.

The Proof of Concept supports organizations at various stages of modernization, including hybrid and cloud-first environments.

2.1 Common Scenarios

- Evaluating Microsoft Intune as a replacement for legacy endpoint management tools
- Preparing for broader endpoint modernization or Windows 11 initiatives
- Improving device security, compliance, and Conditional Access enforcement
- Reducing operational overhead associated with device provisioning and application delivery
- Establishing a foundation for Zero Trust endpoint access

---

3. Engagement Structure (Proof of Concept)

The engagement is delivered as a structured Proof of Concept. Final scope, duration, and deliverables are defined in the Statement of Work (SOW) and tailored to customer objectives.

3.1 Discovery & Planning

Discovery activities establish a clear understanding of business goals, endpoint challenges, and success criteria.

- Review of the current endpoint management approach
- Identification of target devices and user scenarios
- Definition of Proof of Concept success criteria
- Planning for enrollment, security policies, and testing activities

3.2 Intune Configuration & Deployment

The Proof of Concept validates core Intune capabilities using a limited number of devices.

- Device enrollment for Windows and macOS endpoints
- Configuration of security baselines and device compliance policies
- Conditional Access and MFA validation
- Application deployment using supported Intune methods
- Windows Autopilot configuration for new device provisioning scenarios

3.3 Testing & Validation

Configured policies and workflows are tested to confirm expected outcomes.

- Secure device onboarding and access enforcement
- Application deployment and policy behavior validation
- Device compliance reporting and visibility review

---

4. Deliverables & Customer Outputs

Deliverables vary by scope but are designed to provide clear, actionable outcomes that support informed decision-making and next-step planning.

4.1 Proof of Concept Deliverables (Examples)

- Configured Intune tenant settings and policies (PoC scope)
- Enrolled and managed pilot devices
- Application deployment validation results
- Windows Autopilot configuration and testing outcomes
- Device compliance and security validation
- Summary of findings, risks, and recommendations

4.2 Executive Readout

A structured executive-level summary provides an overview of results, key findings, and recommended next steps for broader adoption of Intune.

---

5. Scope Boundaries

5.1 In Scope (Defined by SOW)

- Intune Proof of Concept configuration and validation
- Limited device enrollment and testing
- Policy, security, and compliance evaluation
- Documentation and recommendations

5.2 Out of Scope (Common Examples)

- Full production rollout or mass device migration

- Ongoing endpoint operations or managed services
- Mobile (iOS/Android) device management unless explicitly included
- Custom application development or remediation

---

6. Customer Responsibilities & Prerequisites

Successful delivery requires active customer participation.

- Assign a primary technical and business point of contact
- Provide access to Microsoft 365 and Intune environments
- Supply pilot devices and application information
- Participate in discovery, testing, and review sessions

---

7. Delivery Responsibilities

ProArch will:

- Provide qualified endpoint and security specialists
- Conduct structured discovery and Proof of Concept activities
- Configure and validate Intune capabilities within scope
- Document findings and provide actionable recommendations

---

8. Microsoft Platform & Best Practice Alignment

This service aligns with Microsoft guidance and best practices for modern endpoint management and Zero Trust security principles.

- Microsoft Intune
- Windows Autopilot
- Microsoft Entra ID
- Conditional Access and device compliance

---

9. Optional Next Steps

Following the Proof of Concept, organizations may choose to proceed with:

- Full Intune rollout and endpoint modernization
- Windows 11 upgrade initiatives
- Security hardening and policy expansion
- Ongoing endpoint optimization or managed services