

CASE STUDY · NOVEMBER 2026

Beyond virtual desktops: a phased Microsoft cloud migration plan

An anonymized November 2026 SOW-based case study of planned AWS WorkSpaces retirement, Intune-managed laptops, cloud identity, and file and print modernization for an insurance organization.



Conceptual illustration only; not the customer's production environment.

Project snapshot

Detail	Documented scope
Customer	A multisite insurance organization; customer anonymized
Case study date	November 2026
Starting environment	Local laptops used to access AWS WorkSpaces, with AWS-hosted identity, file, print, and VPN infrastructure
Proposed destination	Entra-joined, Intune-managed laptops with Microsoft cloud identity, file collaboration, and printing
Status represented	Proposed discovery, remediation, migration, validation, and retirement; results are not verified

The case study is dated November 2026 as requested; the underlying SOW is dated September 2026. This is a planning account, not a completion report. Customer names, contacts, domains, office locations, exact environment counts, private security evidence, and commercial estimates have been omitted.

Executive summary

The supplied SOW described a hybrid environment in which employees used physical laptops primarily to reach AWS WorkSpaces. AWS-hosted domain controllers, file shares, print services, and office VPN connectivity supported the desktop estate. The document reported user-experience concerns and the overhead of managing both local and hosted endpoints.

Massive IT proposed a phased transition to locally operated Windows laptops joined to Microsoft Entra ID and managed through Intune. SharePoint, OneDrive, and Universal Print were the proposed destinations for collaboration and printing. Cloud-only identity and retirement of the AWS dependencies were later steps, conditional on validation and customer approval.

A sequencing decision: endpoints before files

The plan deliberately placed the full endpoint rollout before file-server migration. Users would move to managed local laptops while retaining temporary access to existing file services. Only after the endpoint waves were confirmed complete would shared data move to its new destination.

This dependency reduced simultaneous changes for users, but made file migration dependent on the customer's rollout capacity. The SOW's calendar and effort estimates are not presented as guaranteed delivery dates. Pauses, fallback options, and approval gates were planned safeguards, not proof that every future change would be automatically reversible.

Proposed workstreams

1. Discovery and immediate security review

Reconcile device inventories and enrollment status, catalog business applications, validate authentication dependencies, review licensing, and map site readiness. Application-vendor confirmation was required before assuming daily-use tools could operate without domain-joined endpoints.

The source documented identity and endpoint-security concerns requiring early attention. Planned work included encryption remediation, least-privilege administration, emergency-access planning, MFA and access-policy review, and investigation or escalation of suspicious account activity to the existing security provider. Private attack details are omitted, and the case study does not establish a confirmed compromise or completed remediation.

2. Establish cloud identity and endpoint management

Configure Intune compliance and security profiles, update rings, device groups, application deployment, and Autopilot provisioning. Produce a GPO-to-Intune mapping with documented decisions about policies retained, replaced, or retired.

Conditional Access and device requirements would be validated while retaining the customer's existing Duo MFA integration. Privilege-management and advanced identity features remained subject to appropriate licensing. The SOW recognized existing mobile application management policies; it did not propose a new MAM deployment, and the customer retained responsibility for its personal-device policy decision.

3. Add Microsoft security and information protection

Introduce scoped Defender and Purview capabilities alongside the existing security stack, not as a wholesale replacement. The primary endpoint and email security platforms, vulnerability management, SOC monitoring, and service-management arrangements were intended to remain in place.

Proposed work included endpoint and identity visibility, email policy review, cloud-app monitoring, sensitivity labels, and DLP initially reviewed in audit mode. Actual coexistence modes, supported SaaS connectors, licensing, telemetry, and enforcement behavior would need testing. Existing SOC responsibilities would not expand merely because supplementary Defender portal access was provided.

4. Pilot, train, and hand off endpoint waves

Massive IT would lead the controlled pilot, engineering, configuration, migration orchestration, and remote support through that pilot. The customer's IT team would perform physical device work throughout, including wiping laptops, Autopilot enrollment, and user handoff.

Following a successful pilot, the customer would independently execute the remaining site waves using Massive IT's runbook and hands-on training. Massive IT would maintain cadence calls and escalation coordination. Parallel waves were an option only where customer staffing and site readiness allowed.

Planned pilot criteria included successful business-application access, no unresolved critical migration issues, acceptable user feedback, and a usable support runbook. WorkSpaces would remain available as a temporary fallback; powering down desktops during rollout was distinct from final deletion.

5. Migrate files after endpoint readiness

Map shared drives, department ownership, permissions, classification, and stale content before designing SharePoint libraries and OneDrive destinations. Translate access groups and review sensitive-data sharing boundaries.

The SOW proposed initial bulk transfers followed by incremental cutover synchronization, source read-only periods, information-protection configuration, and staged user communications. File compatibility, permissions, data validation, storage requirements, and user acceptance would require confirmation rather than treating every file share as a simple cloud copy.

6. Modernize printing

Inventory printers, validate a reference Universal Print implementation, and extend supported connectors and permissions to appropriate offices. Intune provisioning and Entra groups would support printer access.

Connector hosts, printer compatibility, licensing, and production print behavior would need validation. The objective was to remove AWS print-server and VPN dependencies where confirmed; it was not an assurance that no local connector infrastructure would remain.

7. Retire dependencies only after approval

Validate sustained local-laptop usage, absence of legacy file access, production printing through the new path, and absence of application dependence on domain-controller authentication before retiring infrastructure. Obtain explicit customer sign-off at the pre-decommissionment gates.

The SOW proposed snapshots and retention-aware retirement of WorkSpaces and AWS servers, followed by removal of legacy synchronization, domain controllers, and relevant VPN paths. The precise cloud-only identity transition would need a supported, verified procedure; placing synchronization in staging mode or uninstalling a tool alone is not proof that directory objects have become cloud-managed.

Ownership and evidence gates

Area	Planned ownership or required evidence
Engineering and pilot	Massive IT leads design, configuration, pilot orchestration, documentation, and training
Physical devices and later waves	Customer IT performs device work and independently executes post-pilot rollout waves
File migration start	All endpoint waves confirmed migrated before shared-data cutover begins
Security continuity	Existing MFA and security providers retained; added capabilities validated for coexistence
Infrastructure retirement	Usage and dependency checks, retained recovery evidence, and explicit customer approvals
Closeout	Environment documentation, administrative runbooks, and phase sign-off records

Project status and takeaway

The source establishes an intended migration strategy and responsibility model, not completed endpoint waves, migrated files, retired AWS services, cost savings, or improved user satisfaction. Inventory and schedule assumptions would need reconciliation during discovery.

The planning lesson is to separate endpoint modernization from data cutover, prove application and identity dependencies before retirement, and make the customer's operational role explicit. A cloud-only destination is a design objective; it becomes an achieved outcome only after validated delivery and acceptance.