CO-MANAGED IT / OCTOBER 2026

Monthly IT report

Professional services firm · Two offices in Québec

Three more workstations met the patch target in October. One laptop stopped reporting, and one new account still needs a sign-in safeguard.

October 1–31 · Québec time

Issued November 2, 2026

Month-end coverage

44 / 48

Workstations meeting the patch target

September: 41 of 48

47 / 48

Workstations reporting endpoint protection

One laptop last seen October 19

51 / 52

User accounts covered by MFA policy

Includes all 3 administrator accounts

DECISION REQUESTED

Approve the service portal update by November 4.

A retry could create the same service request twice. The fix passed staging tests. The operations director can approve the November 5 release window or defer to the next window.

What deserves attention

Identity	One enabled, non-admin account was outside the policy requiring multifactor authentication (MFA). Client IT owns the correction, due November 3.
Recovery	On October 22, a sampled file was restored and its contents matched the reference copy. Recovery time for the whole service remains untested.

Scope of this example

DITC handles workstation patching and reviews endpoint alerts during agreed hours. Client IT owns identity policy and backups. This example also includes one authorized restore check and a separately scoped application change.

CONTROL EVIDENCE · OCTOBER 2026

What we verified

The workstation, identity and backup counts below describe different populations. The offline laptop remains in the workstation denominator.

Month-end snapshot · October 31, 23:59 Québec time

CONTROL AND RESULT	EVIDENCE AND INTERPRETATION
OS security patches 44 / 48 at target	NinjaOne month-end inventory and patch records. A device qualifies with a scan in the last 24 hours and no approved OS security update outstanding for more than 14 days. Two awaited a restart, one update was deferred for compatibility, and one laptop had stale data. September used the same 48 devices.
Endpoint visibility 47 / 48 reporting	CrowdStrike sensor check-ins within 24 hours of cutoff, reconciled to the inventory. The laptop last seen October 19 is the same patch unknown above. Its current protection status could not be verified.
Identity protection 51 / 52 covered	Effective Microsoft Entra ID sign-in policies checked against enabled human accounts, including three admins. One new standard user was omitted. Guest and service identities are outside this count. The measure tracks policy coverage, not the number of sign-in prompts.
File recovery 1 / 1 sampled file	October 22 restore record. A file from the client-managed repository was restored to an isolated location. Its checksum matched the reference. This test covers that file only.

SECURITY REVIEW

6 detections reviewed

Four matched approved administration, one matched a verified updater and one potentially unwanted application was quarantined. For the last alert, DITC checked the quarantine record and follow-up scan. No repeat appeared in the available telemetry through October 31.

No incident was confirmed in the six reviewed detections. Visibility on the offline laptop ended October 19.

SERVICE DESK

3 requests carried forward

4	16	17	3
Open Oct 1	New	Closed	Open Oct 31

Counts are unique service requests. Endpoint detections are tracked separately.

ACTION REGISTER · OCTOBER 2026

Decisions and follow-up

Client IT retains change authority. The owners below are accountable for the next step and for recording evidence before closing each item.

OWNER AND DUE DATE	NEXT STEP AND CLOSURE EVIDENCE
NOV 03 **Client IT lead**	**Apply MFA policy to the new user** Confirm enrollment with the user, apply the policy and record a successful sign-in that satisfies MFA.
NOV 04 **Client site lead**	**Locate the offline laptop** Confirm custody and return it online for fresh endpoint and patch scans. If it cannot be located, escalate to the client security lead that day and keep the item open.
NOV 04 · 15:00 **Client operations director**	**Approve or defer the portal release** Record the decision for November 5, 18:30–19:00 Québec time. If deferred, keep the current version and have support check for duplicate requests until the next window.
NOV 06 **DITC endpoint lead**	**Clear three known patch exceptions** Coordinate the two restarts. Test the deferred update with the application owner, then patch in the agreed window. Close each item on a fresh qualifying scan.

APPLICATION CHANGE · SEPARATE PROJECT

Service portal / duplicate submissions

Observed	When a confirmation was delayed, a second submission could create a second ticket. Support had to reconcile the pair manually.
Tested in staging	Version 1.8.3 passed all 12 checks, including concurrent retries producing one ticket, distinct requests remaining separate, and older tickets still opening. Production was on 1.8.2 at cutoff.
Production acceptance	After approval, the DITC application lead deploys, verifies one ticket per test request and reviews errors for 30 minutes. If the check fails, revert to 1.8.2 and reconcile affected tickets before retrying.