The Endpoint Operations Scorecard

Are you running your endpoints, or just deploying to them?

Most organizations have the tools to manage endpoints. Far fewer can say a change reaches every device and stays enforced. This scorecard measures that difference. It walks through the four areas where partial automation tends to hide risk and places your operation on the spectrum from deploying endpoints to running them. It takes about five minutes, and there is nothing to submit to see your result.

How to score

For each statement, mark Yes, Partly, or No. Score Yes as 2, Partly as 1, and No as 0. Total each section, then add the four section scores to your overall result.

Deploy **Stabilize** **Run**

Section 1. Patching and remediation

Running looks like: every required change reaches every device, and you can prove it.

Statement	Yes	Partly	No	Score
1. When a critical patch goes out, we can confirm it landed on every device, not just that the job completed.	☐	☐	☐	____
2. At any given time, we know how many endpoints are missing a required patch, and which ones.	☐	☐	☐	____
3. Failed installs, deferred reboots, and offline devices are caught and resolved without someone chasing them by hand.	☐	☐	☐	____
4. We can push an emergency change across the entire estate within hours and verify the coverage.	☐	☐	☐	____
5. End-of-life and unmanaged devices are accounted for, not missing from our patch reporting.	☐	☐	☐	____

Section subtotal ____ / 10

Section 2. Manual load and automation

Running looks like: automation handles the routine, and a defined process handles the exceptions.

Statement	Yes	Partly	No	Score
1. Routine endpoint work, including patching, configuration, and provisioning, runs without manual intervention.	☐	☐	☐	____
2. Exceptions and failures follow a defined path to resolution, instead of landing on whoever notices first.	☐	☐	☐	____
3. Our team spends less than ten hours a week on manual endpoint upkeep.	☐	☐	☐	____
4. When a key person is out, endpoint operations continue without a gap.	☐	☐	☐	____
5. Keeping the estate healthy does not depend on one person or on legacy knowledge.	☐	☐	☐	____

Section subtotal ____ / 10

Section 3. Visibility

Running looks like: one current view of the whole estate, not last-reported state stitched across tools.

Statement	Yes	Partly	No	Score
1. We have a single view of every endpoint, regardless of platform, location, or ownership.	☐	☐	☐	____
2. Our endpoint data reflects current state, not the last time a device checked in.	☐	☐	☐	____
3. We can see non-compliant, unmanaged, and unknown devices, not only the managed fleet.	☐	☐	☐	____
4. Remote and personal devices appear in the same view as corporate ones.	☐	☐	☐	____
5. We can tell whether the whole estate is in the state we intend without combining several tools by hand.	☐	☐	☐	____

Section subtotal ____ / 10

Section 4. Compliance

Running looks like: compliance is enforced continuously and provable on demand, not assembled at audit time.

Statement	Yes	Partly	No	Score
1. We can produce current evidence of compliance on demand, not only at audit time.	☐	☐	☐	____
2. Drift, such as a changed setting or a disabled control, is detected and corrected continuously.	☐	☐	☐	____
3. Policy exceptions are tracked and revisited, not granted once and forgotten.	☐	☐	☐	____
4. Our compliance posture is enforced automatically, rather than depending on manual checks.	☐	☐	☐	____
5. We could pass an audit today without a scramble to gather evidence.	☐	☐	☐	____

Section subtotal ____ / 10

Add your four subtotals = Total ____ / 40

How to read your score

Two numbers matter. Your total places you on the spectrum below. Your lowest section subtotal tells you where to start, because a single weak area, often visibility or compliance, usually drags the rest down with it. Fix the foundation before optimizing what already works.

0 to 15	16 to 31	32 to 40

0 to 15. You are deploying to your endpoints, not running them.

The tools are in place, but most of what keeps the estate healthy still depends on people noticing and stepping in. The danger is not that the work is hard. It is that your reporting looks healthier than your actual state, because the work that does not automate falls out of view. This is the most common starting point and the most exposed one, because the gaps stay invisible until something goes wrong.

Where to start: Resist the urge to automate more first. You cannot enforce what you cannot see, so begin by surfacing what is currently invisible: the failed patches, the unmanaged devices, the standing exceptions. Establish one source of truth for the whole estate, then automate against it. Visibility before automation is the order that holds.

16 to 31. You have automated the routine. The exceptions are where you are exposed.

The predictable work is automated and it runs well. The problem is everything that did not fit the pattern. This is partial automation, where the managed majority reports as healthy while failures, exceptions, and edge cases are handled by hand or not at all. It is the most dangerous place to plateau, because the day-to-day pain is gone but the risk is still sitting in the part you stopped watching.

Where to start: The next gain is not more automation of the easy work, it is closing the loop on the hard work. Give exceptions and failures a defined path to resolution so they are handled by process rather than by whoever happens to notice. Move your standard from the job ran to the change is verified on every device. That shift is the line between stabilize and run.

32 to 40. You are running your endpoints.

Routine work is automated, exceptions are handled by process, you have one current view of the whole estate, and you can enforce and verify a change everywhere it needs to land. Your reporting reflects reality rather than the last good news. This is a strong position. The work now is holding it as the estate grows, platforms shift, and the time between a vulnerability appearing and being exploited keeps shrinking.

Where to start: Protect the operating model as you scale. The common failure for run-state teams is sliding back toward partial automation when scope, tooling, or headcount changes faster than the operation adapts. Pressure-test enforceability on a schedule. Choose a change and confirm it can reach every device, including the exceptions, within hours.