Introducing a third platform, such as the new MacBook Neo, may multiply complexity, staffing demand, and support overhead

We quantify the IT labor and total cost of ownership (TCO) of supporting existing Windows and Chromebook deployments in K-12 districts, and measure the incremental burden of introducing a third device platform

Highlights of this report

Introducing macOS devices to a large K-12 district's Windows and Chromebook fleet **can increase total cost of ownership by $1.72M over three years***

Adding MacBook Neo devices to a Dell Pro Education 11 laptop and Dell Chromebook 14 fleet **can increase fleet-wide security and network policy deployment time by 54%** and **double the time required for fleet-wide app updates**, with both increases driven by the need to duplicate work across platforms*

Adopting a new platform can cost large K-12 districts an estimated **1,546 additional IT hours** over three years, in device management alone.*

A Principled Technologies report: Hands-on testing. Real-world results.

**The model reflects a large K-12 district with a fleet of 46,000 devices: 42,000 Dell Chromebooks deployed to students and 4,000 Dell Pro Education laptops supporting teachers and staff. Over a three-year period, the district will migrate 23,000 of those devices to MacBook Neo, working toward a mixed-platform environment by the end of the transition.*

Table of contents

Highlights of this report 1

Executive summary 3

Key outcomes 4

What we evaluated 5

- 1. Top-line IT effort differential across three platforms 5
- 2. Three-year cost delta: modeled against a representative district fleet 5

The IT burden: What it actually takes to manage three platforms 6

- Onboarding MacBook Neo devices 6
- Security policy deployment 8
- Application management 10
- Ongoing maintenance 11

From minutes to money: Translating task time into annual IT cost 14

MacBook Neo friction points that affect end-users daily 15

The hidden budget line that changes the conversation 16

- Cost model assumptions 16
- Fleet-level three-year total cost comparison 16

Physical suitability for K-12 environments 17

- Durability 17
- Warranty and repairability 17
- Key takeaways 21

Summary 22

Appendix A: MacBook Neo methodology 25

Appendix B: Dell Pro Education 11 methodology 31

Appendix C: Chromebook 14 methodology 36

Appendix D: Configuration table 39

Appendix E: K-12 endpoint cost model summary 41

Executive summary

Education procurement moves fast, and it can be challenging to make a buying decision given the wide range of factors necessary to consider in a K-12 environment. By the time a new platform crosses IT's desk, they're facing a different set of challenges: the operational reality of the systems they need to support.

For districts running Windows PCs and Chromebooks, introducing a third platform like the Apple MacBook Neo has the potential to multiply complexity, staffing demand, and support overhead. Our research and hands-on testing indicate that every procurement team already supporting Windows and ChromeOS should weigh these ramifications before signing up to support a third platform:

- **Admin capacity:** Adding a third operating system, like macOS, can strain IT workloads that are likely already at capacity. Retraining pulls admins away from pressing priorities and compounds the burden rather than spreading it.
- **Staff familiarity:** Your IT team has likely invested significant time developing, testing, auditing, and documenting workflows inside Intune and Google Admin consoles. Integrating macOS into these workflows may require new tooling, and without it, your team risks compliance and safety gaps.
- **End-user disruption:** Students, teachers, and office staff know Chromebooks and Windows PCs. Swapping student Chromebooks for MacBook Neo devices requires a macOS learning curve for everyone new to the OS, including teachers troubleshooting on the fly, that has the potential to drive help desk volume. The hardware can compound the problem: the MacBook Neo ships with 8GB of unified memory and no upgrade path.[1] While 8GB exceeds the 4GB configuration common in some school Chromebook deployments, the comparison has limits. Chromebooks offload most processing to the cloud, while the MacBook Neo may be running some workloads locally. Students or teachers running heavier workloads or keeping multiple tabs open simultaneously may encounter performance lag, depending on how they're using the device.[2]
- **Additional licensing and support costs:** Every platform you add brings its own cost structure. macOS deployments typically require AppleCare+ for Schools to cover repairs and hardware support, unless your team handles repairs internally or absorbs costs case by case. Mobile device management (MDM) licensing is a separate consideration: depending on your existing infrastructure, adding macOS devices many require additional per-device licensing or a new platform entirely. Because the MacBook Neo accesses Google services through a browser rather than native apps, your existing endpoint security, identity management, or content-filtering tools may not provide coverage, forcing you to procure new ones. These costs recur annually and scale with device count.

Key outcomes

- In testing commissioned by Dell Technologies, Principled Technologies proved that large K-12 school districts running mature Intune- and Google Admin-managed environments could face compounding operational challenges if they introduce macOS as a third platform.
- For a large district with 46,000 Dell Chromebooks and Dell Pro Education laptops supporting students, teachers, and staff, transitioning 23,000 of those devices to MacBook Neo devices over three years could add $1.72M to total cost of ownership, driven primarily by device acquisition, licensing, support, and management overhead.
- Introducing macOS to an existing Windows and ChromeOS deployment would increase fleet-wide security and network policy deployment time by 54% and double the time required for fleet-wide app updates, both a direct result of the need for duplicate work across platforms.
- Managing a third OS could consume an estimated 1,546 additional IT hours over three years in setup effort and ongoing maintenance.

What we evaluated

The decision to add a new platform to a K-12 environment is about much more than the devices themselves. Each new OS you add to your environment expands your operational footprint: additional or even different MDM licensing, software compatibility testing, added staffing demands, and possible retraining cycles. This report quantifies what those decisions cost in IT labor hours and total cost of ownership.

1. Top-line IT effort differential across three platforms

Intune works for small and large MacBook Neo deployments, but managing Windows and macOS devices side by side has the potential to increase IT workload, split app management across two systems, and force help desk retraining. Add Chromebooks you're managing via Google Admin, as many school districts do, and you're juggling three separate workflows. For larger or student-facing Windows fleets, pairing Intune and Microsoft Defender for Endpoint extends content filtering and web protection to macOS.[3] Districts willing to go deeper might consider Jamf, a macOS-native MDM that provides content filtering through Jamf Safe Internet, Apple Classroom integration, and end-of-year wipe and re-enrollment through its Return Service feature.[4] Jamf integrates with Intune, so districts have the option to retain their Microsoft Identity Infrastructure while managing macOS devices through a platform built for it.[5] But it still adds another workflow and a new console. Jamf is purpose-built for Apple devices only and cannot manage Windows or ChromeOS endpoints on its own, meaning districts with mixed device fleets must maintain Intune and Google Admin regardless to cover those platforms.[6,7] In contrast, Intune can manage macOS devices directly.[8]

The licensing costs and management overhead we describe are not hypothetical. They compound across a fleet as devices turn over. This report models a phased transition: shifting approximately one-sixth of the fleet to MacBook Neo devices each year over three years, and tracing what that shift would mean in practice.

Our hands-on testing, which included device setup and ongoing maintenance tasks assumes a baseline environment where students use Dell Chromebooks and teachers and staff use Dell Pro Education laptops. We measured the additional IT effort expended when introducing MacBook Neo devices to either fleet by comparing management tasks across Dell Pro Education laptop and MacBook Neo fleets in an Intune-managed environment, alongside a Dell Chromebook 14 fleet in a Chrome-managed environment.

2. Three-year cost delta: modeled against a representative district fleet

IT salaries, device procurement and support costs, and MDM licensing costs become budget reality when applied to a real fleet at real labor rates. We built the cost model in this report in two stages. The first stage establishes a time baseline: how long does it take IT staff to perform common management tasks for a Dell Pro Education laptop, a Chromebook, and a MacBook Neo? The second stage applies that baseline to a representative district fleet, comparing two scenarios over a three-year horizon:

- **Current two-platform environment:** new Dell Chromebooks for incoming students and Dell Pro Education laptops for eligible staff, supported within an existing Windows and Chrome management infrastructure
- **Three-platform option:** the same student and staff devices, with MacBook Neo devices added as an option, and the management, licensing, and support costs that introduction carries

We used the following large K-12 school district population and cost window in the first scenario:

- 42,000 student Dell Chromebooks
- 4,000 teacher/staff Dell Pro Education laptops
- Three-year cost horizon

K–12 staffing is already stretched

In education, the typical IT support ratio is between 1:300 and 1:1,000 devices.[9] Every incremental hour of per-device management burden displaces something else: a repair backlog, a deployment cycle, a classroom support call. Platform complexity is not an abstract risk. It is a measurable tax on a team that may be already fully spent.

Plus, with class sizes that often include 20 to 30 students per room,[10] every minute a teacher spends helping a student navigate an inconsistent interface or dealing with an issue on their own device is a minute not spent on instruction.

The second scenario adds the MacBook Neo devices to both the student and teacher/staff fleets, staggering the implementation over three years and ending with 50 percent MacBook Neo devices.

The IT burden: What it actually takes to manage three platforms

IT admins build their management infrastructure to fit the needs of their school district's devices, which means that any newly introduced devices that don't fit the existing support structure can cause trouble. Administrators need to reconfigure, retool, and integrate additional management solutions into their workflows.

Help desk volume often spikes at deployment and again each semester as new students encounter the fleet. Onboarding hours, IT orientation time, and macOS-fluent support staff rarely appear in a device proposal, but those costs can surface quickly in the first quarter.

The following sections document the IT work required to introduce MacBook Neo devices alongside existing Chromebooks and Windows devices. We performed and timed each task as a real-world team would do it, noting any portal dependencies or configuration requirements that add friction. Where applicable, tasks could be accelerated using PowerShell or other scripting tools -- those approaches could meaningfully reduce admin time but are not reflected in our timings or cost calculations.

Those measurements feed directly into our cost model. We multiply task times by frequency across the fleet over three years, then convert the result to a standard IT labor rate. Districts that want to apply their own labor rates or fleet numbers can find the raw time and step counts in the science behind the report.

Onboarding MacBook Neo devices

In a Windows and ChromeOS district, IT can largely automate device onboarding. Autopilot handles Windows end to end with no administrator interaction. ChromeOS needs only Google Admin credentials at the login screen.

macOS adds a bit of friction upfront. IT must synchronize devices between Apple Business Manager (ABM) and Intune before zero-touch provisioning is available to end-users. Once that sync is complete, the end user enrolls using IT-provided credentials. Apple also requires end users to opt in for Location Services at first boot, a prompt no policy can suppress, and enforces a hard boundary between what an MDM can control silently and what requires user action.[11,12]

For districts running all three platforms, macOS becomes a parallel workflow, with separate tooling and platform constraints that differ from the devices you already manage. To show what that looks like in practice, we walked through zero-touch enrollment on all three platforms, covering enrollment verification, compliance confirmation, and device naming and asset tagging. While most of our hands-on testing targets the entire fleet, the numbers below reflect one device, not a full fleet rollout.

From a single-user perspective, adding a macOS device to a fleet is roughly on par with adding a Windows device—but more work than adding a Chromebook.

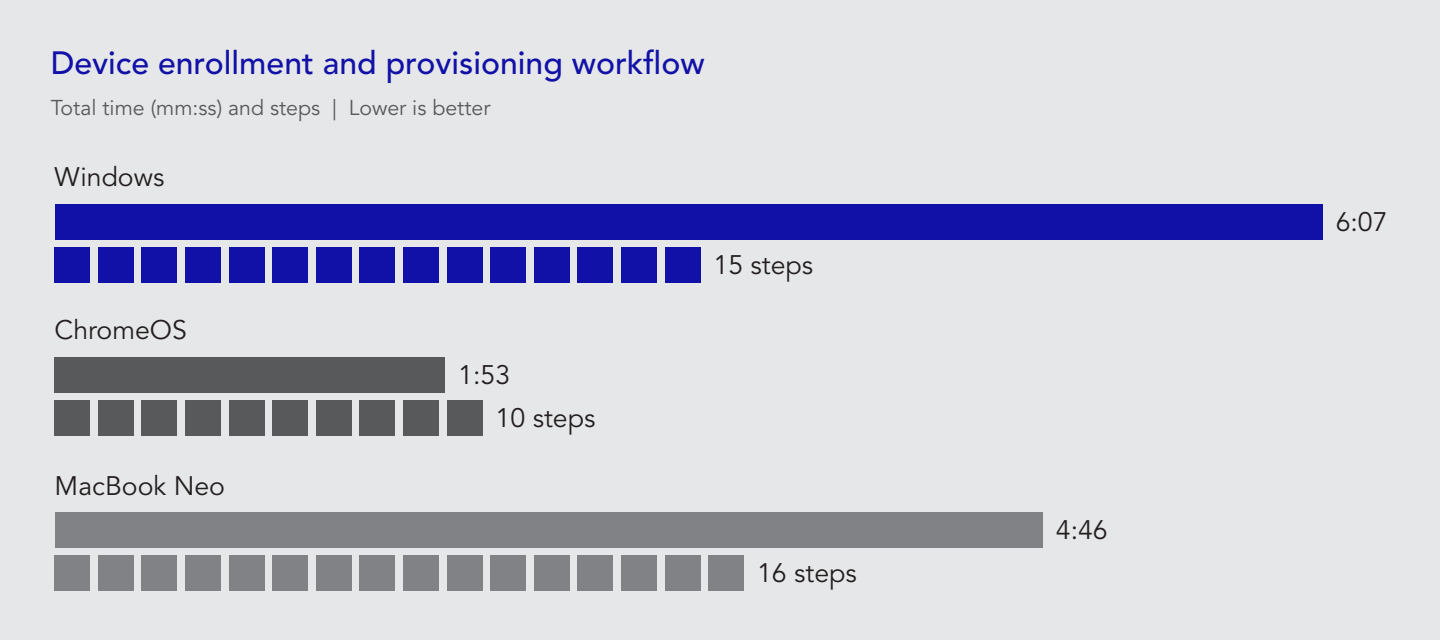

Figure 1: Total time and steps to complete zero-touch enrollment, verify enrollment status and compliance, and apply a device naming convention and asset tag on a single system. Source: PT.

APNs certificate handling

To send commands to Apple devices, MDM solutions like Intune and Jamf require an Apple Push Notification service (APNs) certificate. APNs certificate renewal is an annual administrative task for any district running Apple devices. The process itself is straightforward, but the consequences of mishandling it are more significant than the equivalent task on Windows or Chrome OS. For context: Windows environments renew certificates through Active Directory or a PKI infrastructure, where expiration affects services but rarely triggers forced re-enrollment of endpoints. Chrome OS device enrollment is tied to a Google Workspace domain, not a certificate with a hard expiration, so there is no equivalent annual renewal risk.

APNs work differently. Apple provides a 30-day renewal window before expiration and a 30-day grace period after, during which an administrator can renew the certificate using the original Apple ID credentials. If this happens, existing enrolled devices will accept the updated certificate without re-enrollment, and the fleet experiences no disruption.[13] The risk emerges in two scenarios: An administrator misses both windows entirely or attempts renewal with different Apple ID credentials. Either triggers forced re-enrollment across every macOS device under that certificate.[14] At fleet scale, that translates to IT labor, devices temporarily out of managed state, and a gap in policy enforcement and security posture until each device is re-enrolled and reconfigured. This means a small oversight from a busy administrator can turn into a catastrophe.

Windows and Chrome OS have operational risks of their own, but neither carries a single annual credential dependency where one mistake can force a full fleet re-enrollment. For districts adding macOS as a third platform, this is a process that warrants a dedicated owner, calendar reminders, and documented credentials, not a task that floats in a shared inbox.

Security policy deployment

In many K-12 environments, security policy deployment is a recurring workflow, not a one-time event. Back-to-school configuration cycles, OS updates, and evolving cybersecurity guidance from organizations like K12 SIX and CISA can drive multiple rounds of policy updates throughout the year.

To measure the administrative burden that adding macOS imposes for essential security efforts, we captured the time and steps required to complete a security and network policy deployment with two tasks: deploying a screen-lock policy and pushing a Wi-Fi configuration profile fleet-wide.

Adding macOS to an existing fleet increased fleet-wide security and network policy deployment time by 54% and added 15 steps to the workflow each time you execute this task.

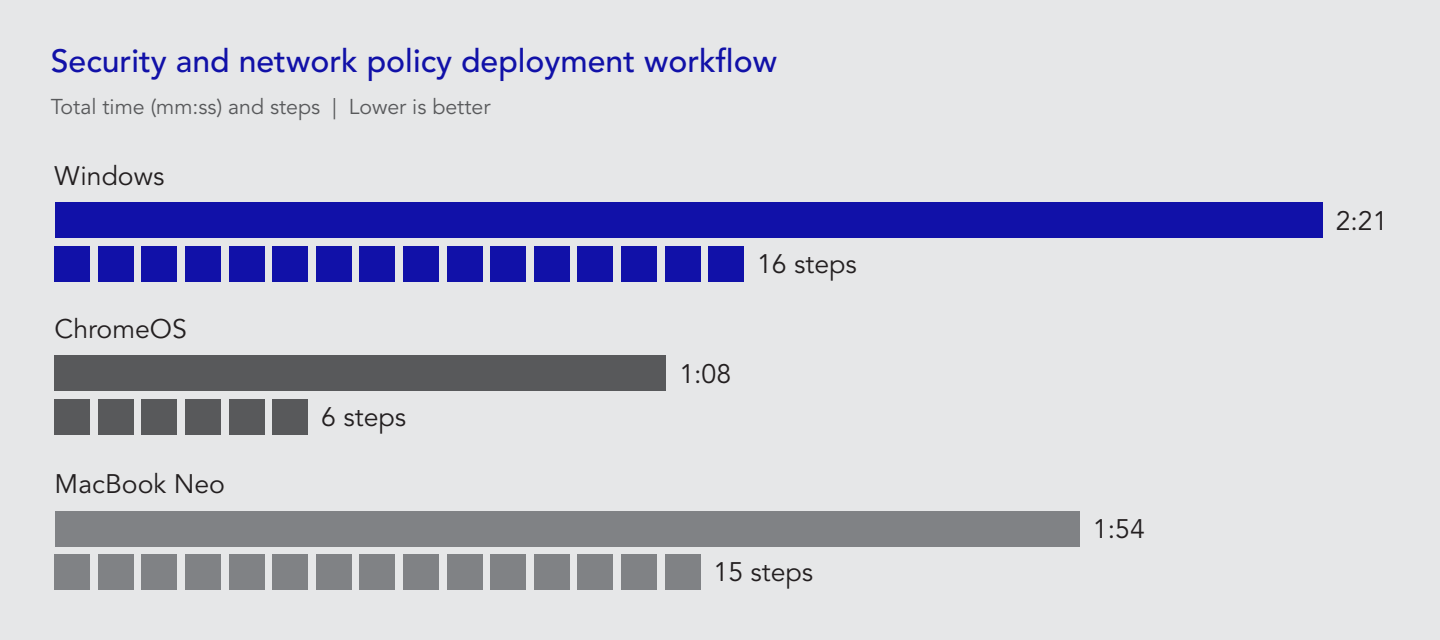

Figure 2: Total time and steps to deploy a screen-lock policy and push a Wi-Fi configuration profile fleet-wide. Source: PT.

But what about data protection? In a Windows and ChromeOS district, IT staff only enable **disk encryption** on Windows devices. ChromeOS encrypts by default and can't be disabled, so administrators simply verify compliance in Google Admin rather than configuring anything. Ensuring data is protected on macOS devices adds another task that lands squarely in IT's court. While this task is usually a once-and-done activity, doubling the effort is a micro-frustration added to the larger load.

macOS security control gap

There is a documented security control gap between macOS devices and Windows or ChromeOS devices. The macOS built-in firewall does not monitor, filter, or block outgoing connections; outgoing traffic is unrestricted at the OS level.[15] This means IT cannot prevent unauthorized VPN applications from bypassing content filtering and security controls enforced on the network.[16] This is directly relevant to Children's Internet Protection Act (CIPA) compliance, which depends on endpoints being unable to circumvent filtering.[17] Windows and ChromeOS devices do not share this gap. Intune can enforce a default-deny outbound firewall posture on Windows, blocking unauthorized VPN clients at the OS level.[18] And administrators can configure the Google Admin Console to block all ChromeOS apps and extensions except those on an admin-managed allowlist, preventing VPN apps from being installed at all.[19,20] On Windows and ChromeOS, endpoint-level circumvention can be technically prevented; on macOS it cannot.

Adding macOS to an existing fleet doubled the effort for a fleet-wide disk encryption task that only needs to be done once.

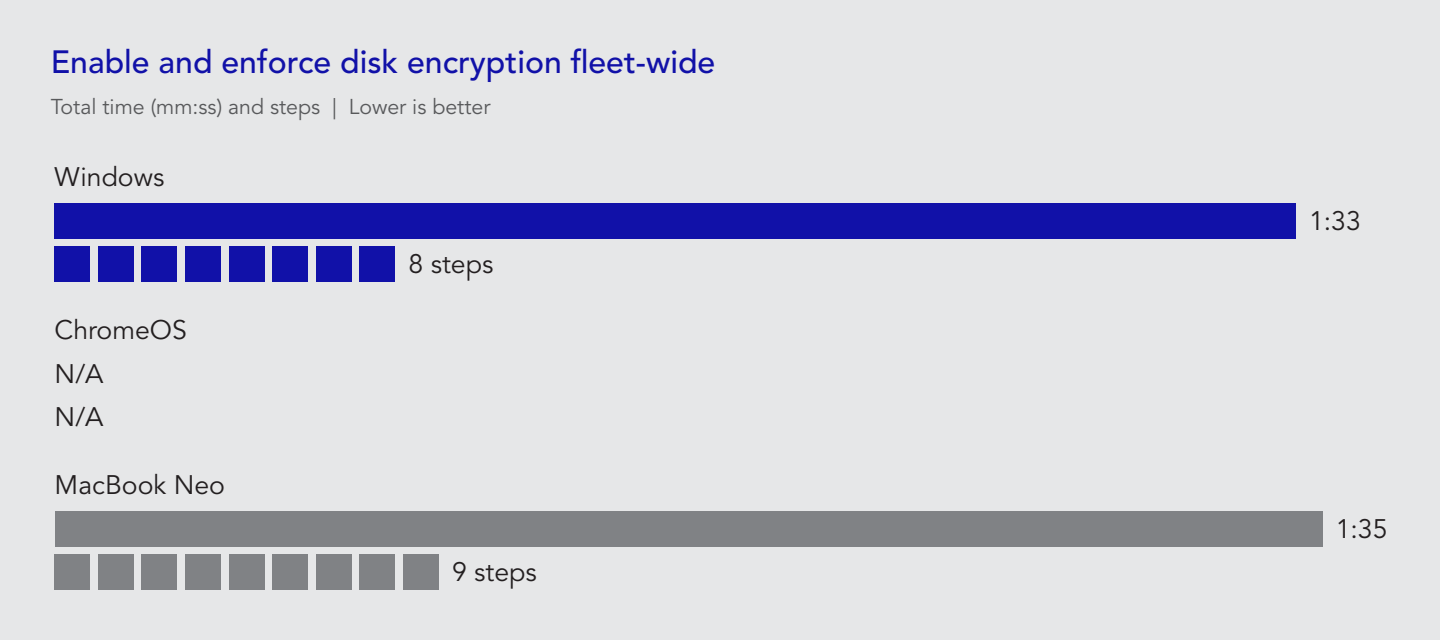

Figure 3: Total time and steps to enable and enforce disk encryption fleet wide. Source: PT.

Multiplied across several policy deployment events per year, per-task security-based time differences can compound into real annual staffing costs.

Browser or app policy configuration

In a district with both Windows PCs and Chromebooks, IT staff manage browser and app policy through two separate GUI-driven consoles. If your district has been using these platforms for many years, your teams are likely familiar with both of them. Windows policy runs through Intune, where the team imports a Chrome ADMX template once and controls all subsequent changes through a searchable settings interface. ChromeOS policy runs through the Google Admin console, with the Chrome Enterprise connector syncing device data into Intune for visibility and limited remote actions.

It's a very different process with macOS for third-party application configuration. Where Windows and ChromeOS policy changes flow through structured GUI interfaces, configuring many macOS applications requires an administrator to manually author a PLIST file, a structured XML format where policies, toggles, and string values require hand-written syntax. Then, they need to upload that file to the MDM and scope it to the correct device group, with no built-in validation step to catch syntax errors before deployment. And for every third-party application your district needs to control on macOS, that process repeats from scratch. Even well-documented vendors like Microsoft and Google require administrators to customize and convert sample files before deployment.[21,22]

In practice, K-12 district IT administrators tend to revisit browser and app policy configurations before the start of the year. However, they may also make mid-year security or compliance adjustments and address issues surfaced by help desk volume.

Application management

Application management runs throughout the school year, triggered by new tool adoptions, security removals, vendor update releases, and annual software refresh cycles. It is also one of the highest-frequency IT workflows: app updates follow regular patch cycles, emergency removals can surface at any time, and updates alone can account for a significant share of annual IT labor. That frequency makes per-task time differences more consequential than in lower-cadence workflows like enrollment or security policy deployment.

To measure the added burden of a third OS, we completed four common tasks across all three platforms, combining silent app deployment and remote app removal into a single fleet-wide workflow. App updates apply only to Windows and macOS; ChromeOS manages this automatically.

Onboarding macOS into a Windows-first Intune environment created a parallel management burden, doubling application management overhead in Intune.

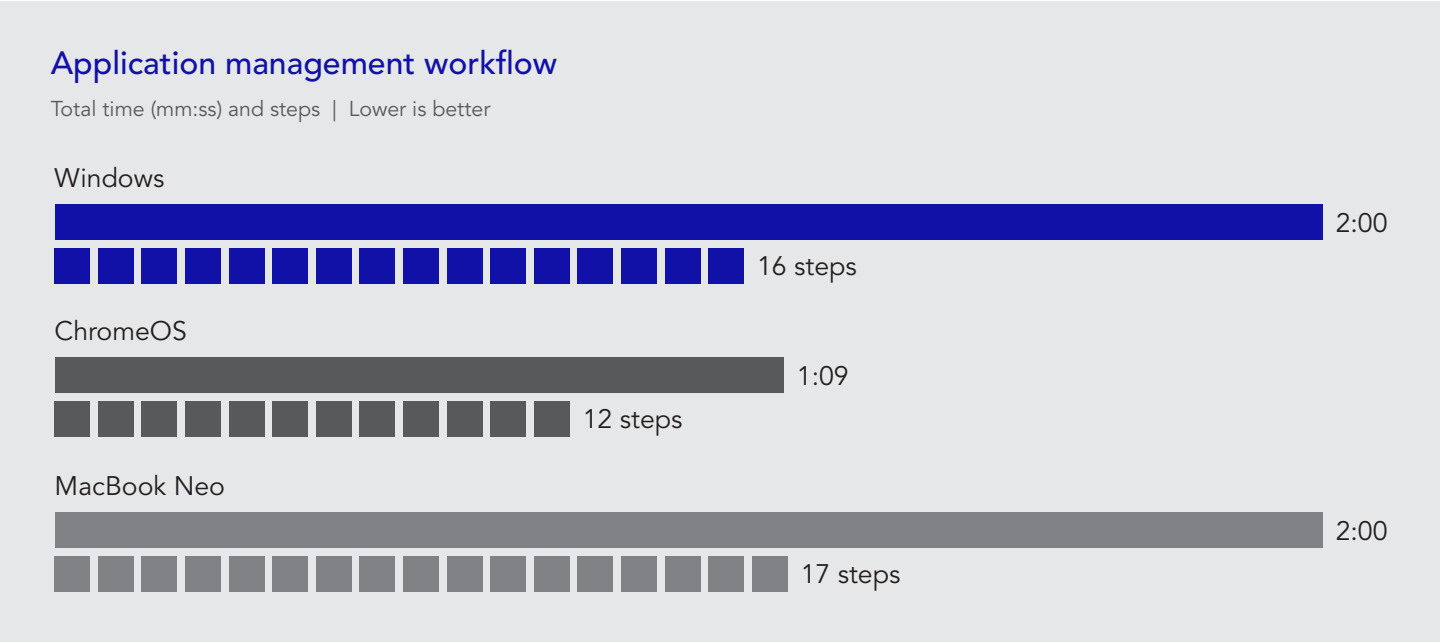

Figure 4: Total time and steps to silently deploy a required app and remotely remove a deployed app to all devices. Source: PT.

Adding macOS doubled the time for fleet-wide app updates due to work duplication.

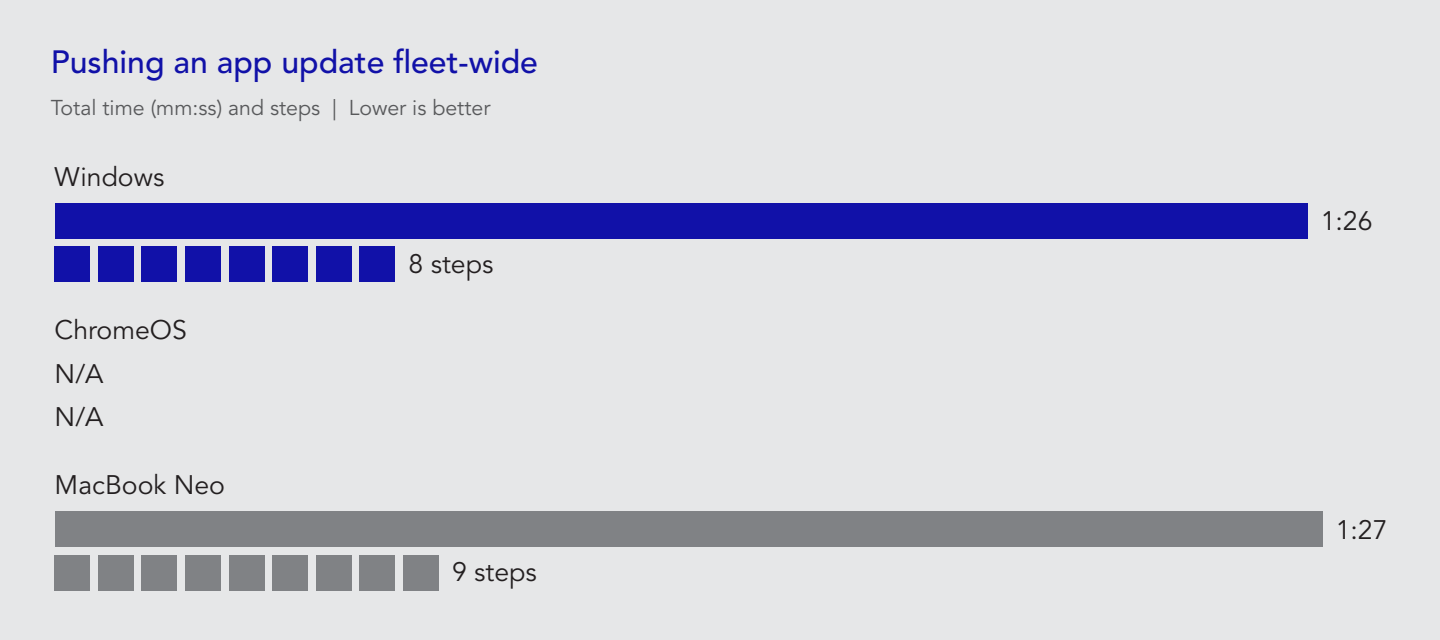

Figure 5: Total time and steps to push an app update fleet wide. Source: PT.

Ongoing maintenance

Ongoing maintenance represents the highest-frequency category in this report and the most direct driver of cumulative IT labor cost. Tasks range from weekly OS compliance checks to annual end-of-year device refreshes. To measure the burden each platform imposes, we captured time and steps for six representative tasks across Intune and Google Admin:

- **Initiating an OS update push** to a defined device group and confirming deployment began
- **Checking OS update compliance status** across the fleet
- **Remotely locking a device** for ChromeOS and macOS (note that remote lock is unavailable for Windows laptops[23])
- **Remotely wiping a device** and confirming re-enrollment
- **Completing an end-of-year device refresh** by wiping, re-enrolling, and reassigning a device to a new user
- **Generating a device compliance report** scoped to the teacher and staff segment

macOS took almost as long to initiate an OS update push as Windows and ChromeOS combined.

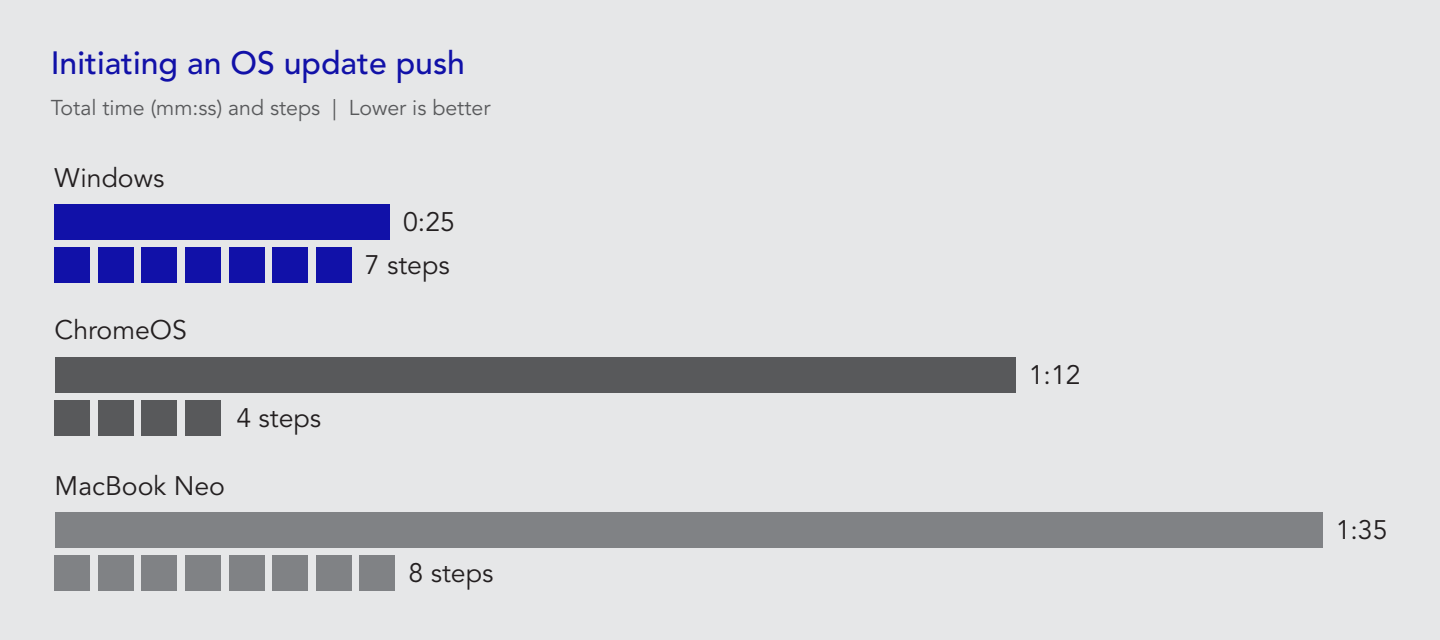

Figure 6: Time and steps to initiate an OS update push. Source: PT

Administrators completed the same Intune-based compliance check twice: once for Windows, once for macOS.

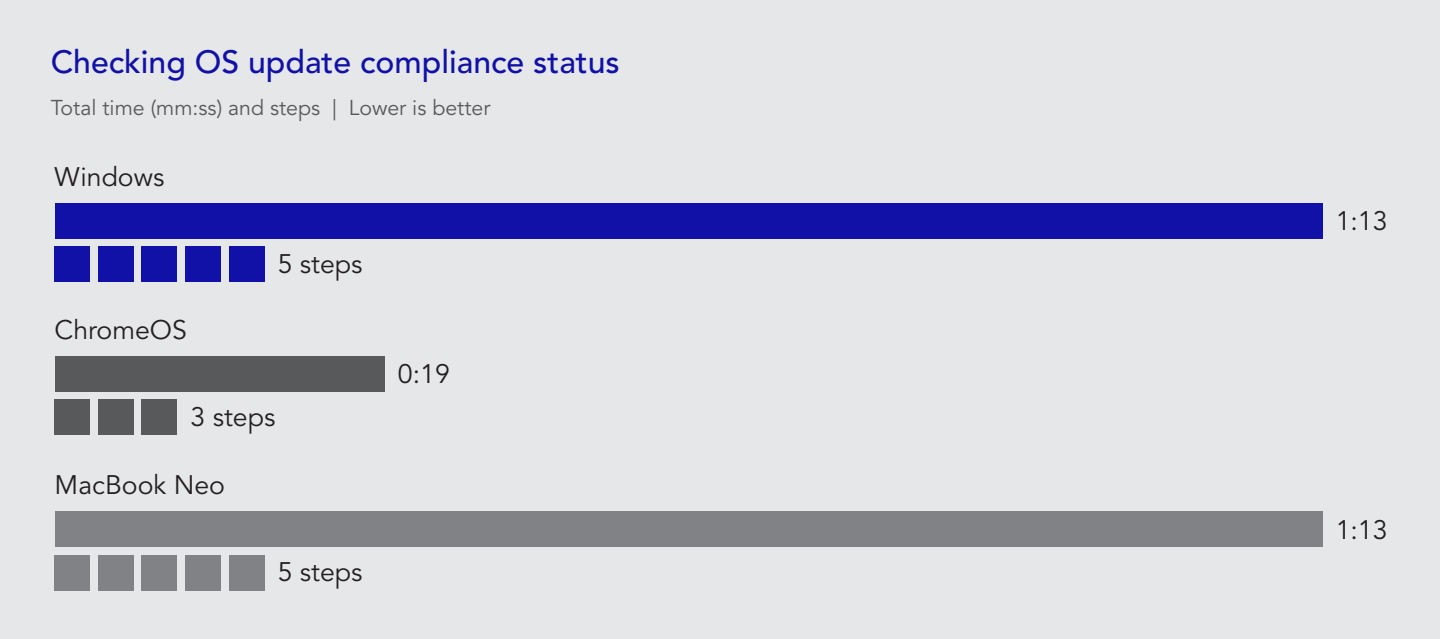

Figure 7: Time and steps to check OS update compliance status. Source: PT

macOS supported remote lock, but took slightly more effort than ChromeOS.

Figure 8: Time and steps to remotely lock a device. Source: PT

macOS required over a minute of post-wipe/device refresh reactivation time.

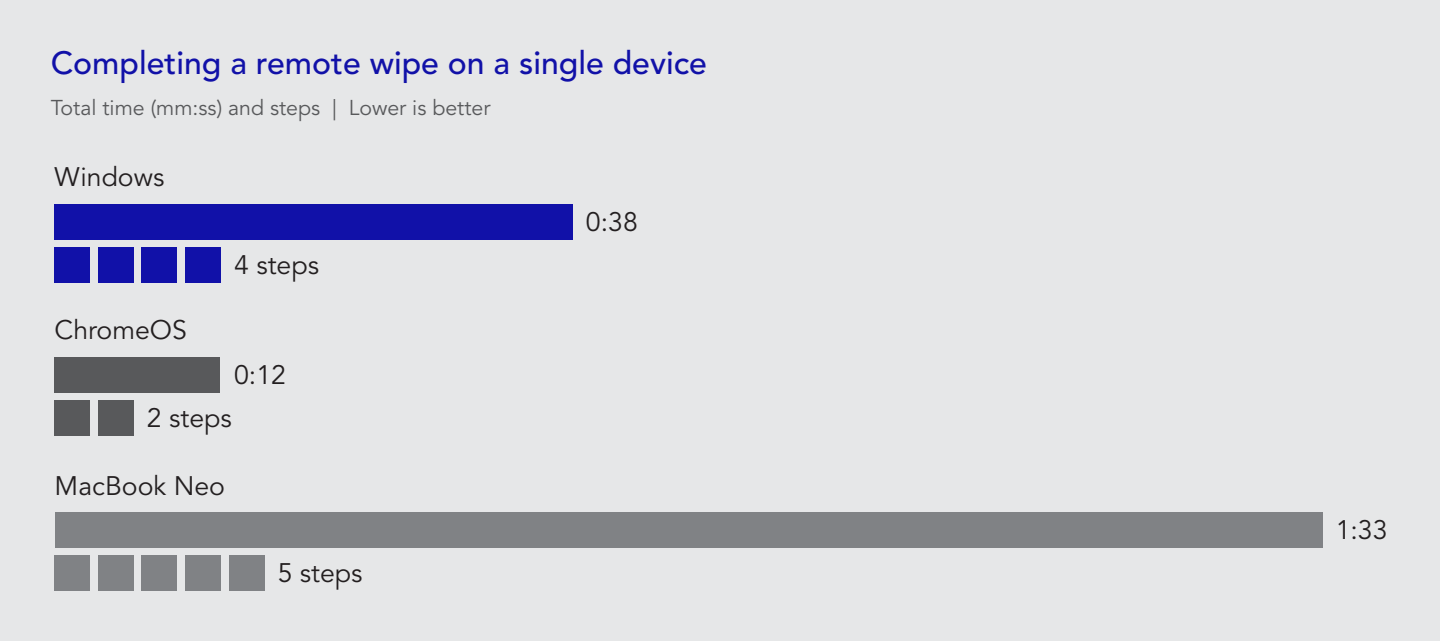

Figure 9: Time and steps to remote wipe a single device. Source: PT

Completing an end-of-year refresh on a fleet of devices: According to Microsoft, IT admins can perform bulk wipes on up to 100 Intune-managed devices at the same time.[24] However, while we were able to perform this action on the Windows device under test, we were unable to replicate it on the MacBook Neo. By contrast, ChromeOS wipe time does not increase as device count scales. You can see our results and extrapolations in the science behind the report.

Adding macOS to the report generation workflow doubled the effort in Intune.

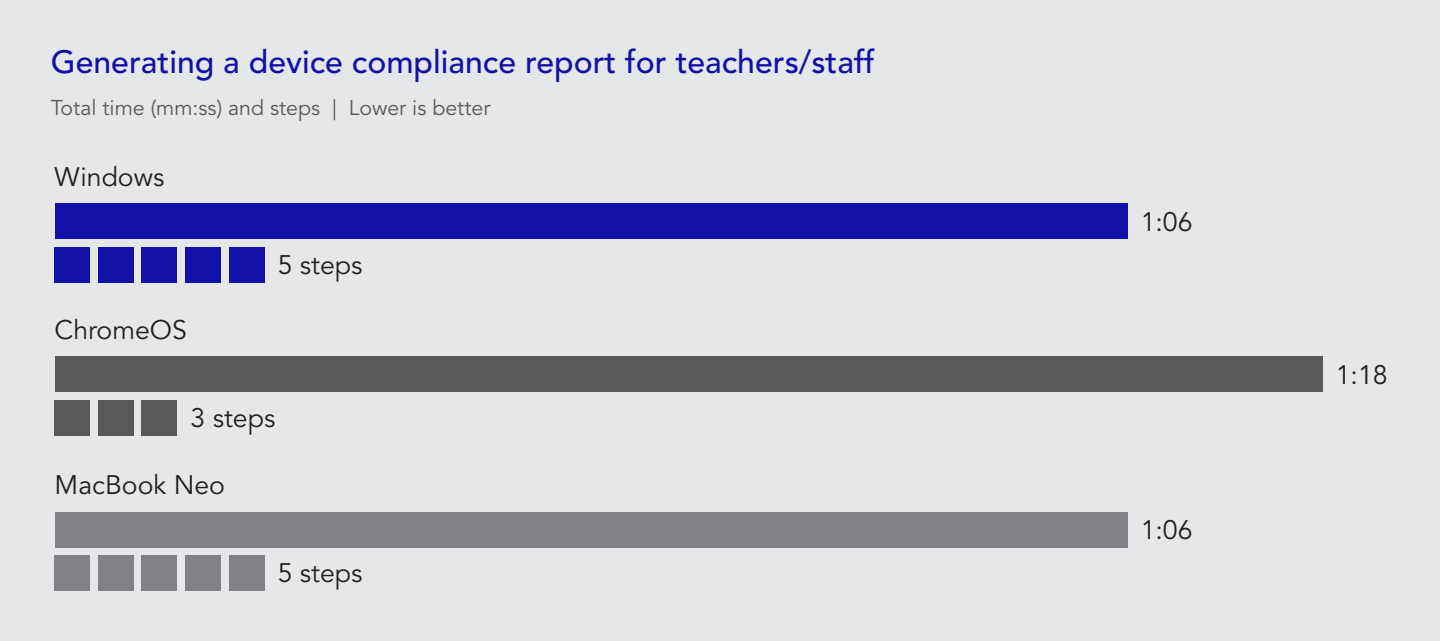

Figure 10: Total time and steps to generate a device compliance report for teachers/staff. Source: PT.

From minutes to money: Translating task time into annual IT cost

These figures reflect IT labor costs for managing the district modeled throughout this report. The two-platform (Windows + ChromeOS) environment assumes the district is supporting 42,000 Dell Chromebooks and 4,000 Dell Pro Education laptops. The three-platform (Windows + ChromeOS + macOS) environment transitions half of the devices to macOS over three years: 21,000 student MacBook Neo devices and 2,000 teacher/staff MacBook Neo devices, resulting in a fleet of 21,000 Dell Chromebooks, 2,000 Dell Pro Education laptops, and 23,000 MacBook Neo devices.

To calculate costs in our model, we assumed an hourly rate of $50.00 for a computer tech.[25] We applied the time it took us to complete each management task in the previous section against our estimated annual frequency of each task to produce total IT hours and costs for both scenarios. Results scale with fleet size and feed directly into the cost model in "The hidden budget line that changes the conversation" later in this report.

Table 1: Total IT labor hours and costs of managing a fleet consisting of 42,000 Chromebooks and 4,000 Dell Pro Education laptops compared to a fleet consisting of 21,000 Chromebooks, 2,000 Dell Pro Education laptops, and 23,000 MacBook Neo devices. Source: PT.

	Windows + ChromeOS	Windows + ChromeOS +macOS	Difference
Three-year IT hours	491.95	2,038.42	+1,546.47
Three-year cost at $50 per hour	$24,597.50	$101,921.15	+$77,323.65

For a full time and cost breakdown by task and frequency, see the K-12 endpoint cost model summary in Appendix E.

MacBook Neo friction points that affect end-users daily

If you make the choice to switch your personal device to one with a new-to-you operating system, you'll likely encounter both things you enjoy about the new OS and frustrations with it. When you make the change for a whole fleet of devices in a K-12 environment, however, the impact is bigger. For school systems that currently use Chromebooks and Windows machines, adding the MacBook Neo as a third platform can create significant friction.

1. **Instead of an M-series chip, the MacBook Neo runs full macOS on an iPhone chip (A18 Pro) with 8 GB of unified memory and no upgrade path.**[26] Unlike Chromebooks and many Dell Education devices, which offload most processing to the cloud, the MacBook Neo handles more locally on hardware that you can't expand.[27,28,29]
2. **Full workflow relearning can hit students harder than staff.** Students cycle through multiple classrooms and contexts daily. Students accustomed to school Chromebooks may have to adapt to a new OS while simultaneously hunting for familiar features and shortcuts, pulling focus away from instruction time. Unlike staff who can practice on their own schedule, some students aren't able to take their devices home. This means that some students encounter the unfamiliar device under time pressure and in assessed environments, where tech issues can affect their morale and their grades.
3. **The 8GB RAM ceiling may present challenges for students and teachers.** A student juggling a research tab, Google Doc, video assignment, LMS, and background music can exhaust available memory before the period ends, triggering compression and swap that slows the device mid-assignment.[30] It can be tricky for teachers, too, who run Google Meet or Zoom for parent conferences alongside curriculum tabs, gradebooks, and media players simultaneously. That workload alone can saturate available memory, triggering macOS swap and compression that slows the device mid-conference. The other devices we tested have upgrade paths to more than 8 GB of RAM, but the MacBook Neo has RAM soldered to the board and no upgrade path, meaning there is no opportunity to increase RAM.[31]
4. **You may need extra dongles or hubs.** The MacBook Neo ships with USB-C ports only. If a teacher or student needs to connect projectors, displays, USB drives, printers, or card readers to their laptops directly, that means the classroom also requires a dongle or USB-C hub. That accessory requirement would add between $10 and $60 per device or per classroom. In contrast, the Dell Windows and ChromeOS devices we tested include both USB-A and USB-C ports, so students and teachers can plug in peripherals directly, with no adapters required.

The hidden budget line that changes the conversation

Time measurements become actionable when they carry a dollar figure. This section builds a transparent cost model, giving district finance and IT leadership a clear view of the budget impact of introducing the new MacBook Neo into a large fleet.

Cost model assumptions

These calculations model a large K-12 district currently running a two-platform environment consisting of 42,000 Dell Chromebook 14 student devices and 4,000 Dell Pro Education 11 laptops. The district replaces a third of its fleet each year. The three-platform scenario introduces MacBook Neo devices into the same Intune- and Google Admin-managed environment, with half of each eligible cohort migrating to Apple devices over three years.

Fleet-level three-year total cost comparison

Table 2 includes device, support, spares, planning, training, and IT labor costs scaled to the district fleet and projected across a three-year horizon. Every line item belongs in the same budget conversation as device acquisition cost, including the ones that rarely appear in vendor proposals.

Table 2: Estimated three-year TCO, including unit cost acquisition and management costs, for a large district managing 42,000 Dell Chromebooks and 4,000 Dell Pro Education laptops compared to a three-platform environment where half of the devices for teacher/staff and students have been transitioned to MacBook Neo devices. Source: PT.

Cost category	Two-platform Dell only option	Three-platform Dell + Apple option
Devices + support (three-year per-unit cost × fleet)		
Staff: Dell Pro Education (4,000 / 2,000 fleet)	$3,614,240.00	$1,807,120.00
Staff: Apple MacBook Neo (0 / 2,000 fleet)	-	$1,793,940.00
Students: Dell Chromebook (42,000 / 21,000 fleet)	$26,352,060.00	$13,176,030.00
Students: Apple MacBook Neo (0 / 21,000 fleet)	-	$13,041,000.00
Spares (device + support cost only)		
Dell Pro Education spares (200 / 100 devices)	$121,918.00	$60,959.00
Dell Chromebook spares (2,100 / 1,050 devices)	$1,206,303.00	$603,151.50
Apple MacBook Neo spares (3,450 devices)	-	$2,080,350.00
Platform migration costs		
Solution planning	$7,500.00	$27,500.00
IT staff training	$0	$43,654.00
IT admin labor (device management)	$24,597.50	$101,921.15
Teacher training for a third platform	$0	$320,000.00
Three-year total	$31,326,618.50	$33,055,625.65
Savings with two-platform solution	**$1,729,007.15 5.5% less than three-platform**	-

For a full breakdown, see the K-12 endpoint cost model summary in Appendix E.

Physical suitability for K-12 environments

Physical durability and repair are additional cost considerations. For durability, we scoured manufacturer specifications and trusted sources to estimate how each device will hold up in school district conditions.

Durability

Dell Pro Education and Chromebook devices are engineered for tough school days. Each passes 17 MIL-STD-810H military-grade tests covering desk falls, micro-drops, vibrations, humidity, temperature extremes, and rough treatment before reaching market.[32] Reinforced design details, including rubberized edges, spill-resistant keyboards, and 180-degree lay-flat hinges rated for thousands of open/close cycles, back up the spec with physical durability features.[33]

Apple MacBook Neo is a consumer MacBook that, according to John Temus, Apple's senior vice president of Hardware Engineering, "delivers the magic of the Mac at a breakthrough price."[34] We could find no military-standard claim for the MacBook Neo or any consumer MacBook. Apple emphasizes recycled materials rather than ruggedization specs.[35]

Warranty and repairability

When districts buy devices, repairability and warranty coverage determine how long these devices last and how much it costs to keep them running. The ideal device is easy and inexpensive to repair, so it can stay in service longer.

Dell builds its **Pro Education and Chromebooks** with that in mind. They have shared parts across models, customer-replaceable batteries with tool-less access, and up to five years of warranty coverage. Meanwhile, the Apple **MacBook Neo** is the most repairable Mac in 14 years, earning a 6/10 iFixit repairability score, with modular USB-C ports, screw-mounted battery, and no parts-pairing restrictions.[36] That said, you can't upgrade RAM and storage after purchase, repairs require a specialty driver some shops don't stock, and wiping a device without signing out first can trigger Activation Lock and leave it unusable.[37]

Table 3: Serviceability and support comparison across three K-12 device platforms.

Dell Pro Education	Dell Chromebook	MacBook Neo
Warranty and support		
Up to 5 years ProSupport available; optional 24/7 monitoring & managed IT[38]	**Up to 5 years** ProSupport and Managed IT Services available[39]	**Up to 4 years** AppleCare+ for Schools offers 3- and 4-year plans; no 5-year path[40,41] There may also be a per-incident fee ($49-$149)
Battery access		
Tool-less and customer-replaceable Bottom door (CS) panel; customer-replaceable[42]	**Customer-replaceable** Parts sold directly via Dell Parts store[43]	**Screw-mounted** 18 screws on tray (vs. adhesive in prior models); improves over previous gen but not tool-less[44]
Parts strategy		
Shared parts Common components across models; reduces spare stock cost[45]	**Shared parts** Same portfolio strategy; service manual published Feb 2026[46]	**Model-specific** No cross-model shared parts program; parts available via Apple Self Repair

Dell Pro Education	Dell Chromebook	MacBook Neo
RAM / Storage		
Varies by configuration Check specific model spec sheet	**Varies by configuration** Check specific model spec sheet	**Soldered — not upgradeable** 8GB RAM; 256GB or 512GB SSD fixed at manufacture[47]
Keyboard repair		
Not independently documented	*Not independently documented*	**Complex** Touch ID model: 41 screws + adhesive tape Base 256 GB model (most common education purchase): 45 screws[48,49]
Activation Lock / MDM		
No equivalent risk Standard enterprise MDM; no device-level lock-out on resale	**No equivalent risk**	**Unresolved risk** Devices tied to iCloud accounts; unreleased locks render working units unsalvageable[50]
Documentation		
Service Manual + Setup/Spec Guide available[51]	Service Manual, Setup/Spec Guide, Statement of Volatility — all updated Feb 2026[52]	Apple repair manual available day one of launch[53]

If you're not able to repair the MacBook Neo yourself and it requires repair under warranty, the device has to go through Apple: to an Apple Store, an authorized repair shop, or the Apple mail-in depot.[54,55] While there is no official information on turnaround times, three to five business days is a general jumping-off point.[56]

Budgeting for spare inventory and end-of-life devices

Every fleet needs spares. We did not test the durability of any of these systems, but kids are rough on devices, and devices of all kinds break. When they break, a district needs spares on hand so students keep learning and teachers keep teaching. For this exercise, we budgeted 15 percent of spares across the board, regardless of platform, based on LocknCharge's guidance, "[K-12 school] districts should maintain spare inventory equal to at least 10%–15% of the whole fleet."[57]

How a district fills that 15 percent will differ depending on the platform, and this is where spare planning intersects with end-of-life (EOL) strategy. With 1-to-1 computing now the norm in most districts, each year brings a wave of retiring PCs and Chromebooks, and as Education Week notes, it falls to districts to recycle, repurpose, or dispose of devices that have reached the end of their useable lives.[58] Each of these paths carries costs for planning, prepping, and distributing the hardware, sometimes offset by modest resale or buy-back revenue. Our model proposes a different path for a portion of these retiring systems: repurpose them as spares that can temporarily swap in when newer devices break down during the school day

This repurposing strategy directly shapes our spare-inventory costs. For the pre-existing Dell Windows and ChromeOS fleets, we assume districts purchase 5 percent of spares as new devices and pull the remaining 10 percent from units retired after three years of service. In the three-platform scenario, however, the Apple fleet offers no retired devices to draw from, because the MacBook Neo would be a new platform for the district. Any district adding it must purchase the full 15 percent as new devices, and that difference drives the spare-inventory cost gap in our totals.

Repurposing retired devices as spares is not entirely free. Depending on a district's alternate plans for those machines, it might forfeit a few dollars in resale value, or it might save the staff costs of boxing and donating them. Each district's mileage will vary. Because of this flux, and to keep our model universal, we leave these EOL costs and offsets out of our totals.

Districts that want to handle repairs in house have to qualify for the Apple Self-Servicing Account program, which requires a minimum of 1,000 Apple devices, certified technicians, dedicated workspace, and a line of credit tied into Apple's service system.[59,60] Many districts won't meet that bar, but those that try to navigate AppleCare claims without it face real financial risk: One documented case saw a district incur $32,000 in unexpected charges from submission errors alone.[61]

The Dell service model is structurally different. ProSupport Plus provides next-business-day onsite repair after remote diagnosis, meaning a technician arrives at the school rather than the device leaving it.[62] The Dell Education portfolio is designed with shared components across models, and Dell sells customer-replaceable parts, including batteries, directly through the Dell Parts store, enabling districts to maintain an on-site spare parts depot.[63,64]

Dell's K-12 pricing stack

Pricing methodology

For the per-device cost model earlier in this report, we used single-device education pricing for both Apple and Dell. Apple pricing comes from Apple's published institutional price list (5-pack); Dell pricing comes from a direct quote Dell provided to us. Dell also provided a separate bulk scenario quote at the 5,000-unit tier, which we present in Table 4.

Comprehensive Hardware Support (CHS)

Dell offers K-12 districts an alternative to ProSupport Plus: Comprehensive Hardware Support (CHS), a prepaid repair plan available exclusively to U.S. K-12 schools. This plan provides:

- **Fleet-based tiers.** Pricing scales at 200, 2,000, and 5,000 or more covered devices.
- **Pooled incident bank.** A district prepays for a bank of repair incidents sized at 5, 10, or 15 percent of its Dell fleet. Any device can draw from the pool; unused incidents are forfeited at term end.
- **Coverage scope.** Cracked screens, spills, broken hinges, non-cosmetic wear, and battery replacement, layered on top of a separately purchased 3-year Dell Education Basic hardware warranty.
- **Repair logistics.** Depot-based only; 7 to 12 business day turnaround via mail-in.[66,67]

Dell bulk buy scenario: 5,000-unit quote

Table 4 below shows what a district deploying 5,000 devices pays per device under Dell's bulk pricing, with CHS at the 5 percent incident pool and a 3-year Education Basic warranty. The single-device column (device + ProSupport Plus with Accidental Damage Protection) is the figure used in the main cost model for direct comparison.

Table 4: Dell bulk pricing vs. single-device pricing, per device (3-year, hardware + support). Single-device pricing sourced from Dell's direct quote to Principled Technologies. Bulk pricing sourced from Dell's 5,000-unit scenario quote dated June 11, 2026.

Configuration	Single device + ProSupport Plus	Bulk device (5K)	+ Basic warranty (3-yr)	+ CHS 5% pool (3-yr)	Bulk all-in	Per-device savings
Dell Pro Education 11 2-in-1 (Intel N150 CPU, 4GB RAM, 128GB UFS storage)	$609.59	$404.24	$43.12	$35.68	$483.04	**$126.55**
Dell Chromebook 14 (Intel N150 CPU, 8GB RAM, 64GB eMMC storage)	$574.43	$410.72	$49.97	$30.60	$491.29	**$83.14**

Districts that purchase 5,000 or more devices and pair them with the Basic warranty and a 5 percent CHS pool could save over **$126 per PC** and over **$83 per Chromebook** against single-device ProSupport Plus pricing. Those expecting higher damage can scale the incident pool to 10 or 15 percent and still keep the bulk device discount.

Key takeaways

1. **macOS duplicates work your team already does for Windows.** Intune supports macOS alongside Windows, but almost every management task, from pushing updates to wiping devices, requires a separate run through Intune for macOS. That duplication added 54 percent to fleet-wide security and network policy deployment time and doubled the time required for fleet-wide app updates in our testing.
2. **Browser and app policy on macOS requires hand-written configuration files.** Windows and ChromeOS handle this through searchable GUI consoles. macOS requires manually authored PLIST files for third-party applications, with no built-in validation step to catch errors before deployment.
3. **APNs certificate mishandling can force a full fleet re-enrollment.** IT must renew the Apple push notification certificate annually with the same Apple ID credentials. Missing the renewal window or using different credentials triggers forced re-enrollment across every macOS device under that certificate, a risk Windows and ChromeOS do not carry.
4. **Many districts may not qualify to repair MacBook Neo devices in house.** Apple Self-Servicing Accounts requires a minimum of 1,000 Apple devices, certified technicians, dedicated workspace, and a line of credit. Districts that submit AppleCare claims without meeting that threshold face real financial exposure: one documented case resulted in $32,000 in unexpected charges from submission errors alone.
5. **Depot repair means devices leave the building for up to 14 days.** For a 500-device fleet, that turnaround requires keeping roughly 75 spare units on hand to maintain daily coverage, at a 15 percent spare ratio vs. 5 percent for Dell. Dell offers 24/7 service and Dell ProSupport Plus sends a technician to the school instead, keeping devices in the building and the spare pool smaller.
6. **Platform complexity is a staffing cost.** Three-platform device management adds an estimated 1,546 IT hours over three years, translating to $77,323 in labor costs for the district we modeled in this report. Every one of those hours displaces something else: a repair, a deployment, a classroom support call. That cost doesn't appear on a device spec sheet, but it shows up in the budget and compounds as the fleet grows.
7. **The 8GB RAM ceiling has the potential to be a classroom problem, not just a spec footnote.** The MacBook Neo ships with 8 GB of unified memory soldered to the board, with no upgrade path. A student running a browser, LMS, video assignment, and document simultaneously can exhaust available memory before the period ends. Unlike the MacBook Neo, Dell Pro Education and Chromebook configurations are available with higher memory options for demanding workloads.
8. **The MacBook Neo carries no military-grade durability rating.** According to Dell, Dell Pro Education and Chromebook pass 17 MIL-STD-810H tests covering drops, vibration, humidity, and temperature extremes. Apple makes no equivalent claim for the MacBook Neo.

Summary

The data tells a clear story: adding the MacBook Neo to a Windows and ChromeOS district is not a device decision. It is a platform decision, and it carries a platform's worth of overhead.

Nearly every task we measured took longer when macOS entered the picture. Policy changes that take minutes on Windows or ChromeOS add time on macOS, every cycle. End-of-year device refreshes that complete in seconds on Windows and ChromeOS could require over a minute more on macOS due to post-wipe reactivation. App updates, a recurring IT workload, add steps on macOS every single time.

Individually, the differences look small. Across a large fleet, repeated over three years, they add up to real cost: **1,546 additional IT hours worth an estimated $77.3K in IT labor costs** for the school system we modeled in our report. And every hour spent authoring configuration files, managing Apple's service requirements, or chasing depot repairs is an hour not spent keeping the rest of the fleet running.

The total cost difference is larger. For the large K-12 district (46,000 Chromebook and Windows laptops) we modeled, transitioning half the fleet (23,000 devices) to macOS can **increase the total cost of ownership by $1.72M over three years**. This figure accounts for devices, support, MDM tools, Microsoft Office for teachers and staff, Google Workspace for students, staff training, and ongoing management costs.

The districts most likely to feel that cost are the ones least equipped to absorb it. Small IT teams, tight repair budgets, and high device-to-staff ratios are the norm in K-12, not the exception. Adding a third platform does not spread the workload, it stacks on top of it.

1. Apple, "MacBook Neo," accessed May 18, 2026, https://www.apple.com/macbook-neo/specs/.
2. Dominic Reigns, "Average RAM Usage on ChromeOS Statistics 2026," accessed May 18, 2026, https://www.aboutchromebooks.com/average-ram-usage-on-chromeos-statistics/.
3. Microsoft Intune, "Blocking URLs and Websites on Managed macOS devices with Intune (Help Needed)," accessed May 21, 2026, https://techcommunity.microsoft.com/discussions/microsoft-intune/blocking-urls-and-websites-on-managed-macos-devices-with-intune-help-needed/4026561.
4. Jamf, "Jamf for K-12. Secure learning with Apple," accessed May 18, 2026, https://www.jamf.com/solutions/jamf-for-k-12/.
5. Jamf, "Jamf for K-12. Secure learning with Apple," accessed May 18, 2026, https://www.jamf.com/solutions/jamf-for-k-12/.
6. Jamf, "Windows Modern Device Management," accessed June 11, 2026, https://trusted.jamf.com/docs/win-modern-device-management.
7. Jamf, "Endpoint security with Chrome Enterprise and Jamf," accessed June 11, 2026, https://www.jamf.com/blog/chrome-enterprise-jamf-endpoint-security/.
8. Microsoft Learn, "Deployment guide: Manage macOS devices in Microsoft Intune," accessed June 11, 2026, https://learn.microsoft.com/en-us/intune/fundamentals/platform-guide-macos.
9. Microsoft, "Integrate Jamf Pro with Microsoft Intune to report device compliance to Microsoft Entra ID," accessed May 18, 2026, https://learn.microsoft.com/en-us/intune/device-security/compliance/jamf-entra-id.
10. Workwize, "IT Staffing Ratios: 2026 Updated Guide," accessed May 8, 2026, https://www.goworkwize.com/blog/it-staffing-ratios.
11. National Center for Education Statistics, "Average public school class size: Average class size in public K-12 schools, by school level, class type, and state: 2020-21," accessed May 12, 2026, https://nces.ed.gov/surveys/ntps/estable/table/ntps/ntps2021_sflt07_t1s.
12. PhillyPhoto, "Location Services can't be managed?" accessed May 13, 2026, https://community.jamf.com/general-discussions-2/location-services-can-t-be-managed-22497.
13. Iru Team, "Guide for Apple IT: Device Enrollment," accessed May 13, 2026, https://www.iru.com/blog/guide-for-apple-it-device-enrollment-uamdm-tcc-and-device-supervision.
14. Devicie, "Frequently Asked Apple Push Certificate (APN) Questions," accessed May 18, 2026, https://help.devicie.com/kb/frequently-asked-apple-push-certificate-apn-questions.
15. Apple, "Mac User Guide," accessed June 9, 2026, https://support.apple.com/guide/mac-help/block-connections-to-your-mac-with-a-firewall-mh34041/mac.

16. Microsoft Intune, "Firewall policy settings for endpoint security in Intune," accessed June 9, 2026, https://learn.microsoft.com/en-us/intune/device-configuration/endpoint-security/ref-firewall-settings.
17. Federal Communications Commission, "Children's Internet Protection Act (CIPA)," accessed June 9, 2026, https://www.fcc.gov/consumers/guides/childrens-internet-protection-act.
18. Microsoft, "Intune endpoint security firewall settings," Microsoft Learn, accessed June 10, 2026, https://learn.microsoft.com/en-us/intune/intune-service/protect/endpoint-security-firewall-profile-settings.
19. Google, "Allow or block apps and extensions," Chrome Enterprise and Education Help, accessed June 10, 2026, https://support.google.com/chrome/a/answer/6177431.
20. Google, "Allow or block access to websites," Chrome Enterprise and Education Help, accessed June 10, 2026, https://support.google.com/chrome/a/answer/7532419.
21. Devicie, "Frequently Asked Apple Push Certificate (APN) Questions," accessed May 18, 2026, https://help.devicie.com/kb/frequently-asked-apple-push-certificate-apn-questions.
22. Microsoft Learn, "Microsoft Build 2026," accessed May 22, 2026, https://learn.microsoft.com/en-us/microsoft-365-apps/mac/deploy-preferences-for-office-for-mac.
23. Chrome Enterprise and Education Help, "Chrome Browser quick start (Mac)," accessed May 22, 2026, https://support.google.com/chrome/a/answer/9020077.
24. Microsoft, "Microsoft Build 2026," accessed May 29, 2026, https://learn.microsoft.com/en-us/intune/device-management/actions/?tabs=macos.
25. Glassdoor, "How much does a Computer Tech School District make?" accessed May 29, 2026, https://www.glassdoor.com/Salaries/computer-tech-school-district-salary-SRCH_KO0,29.htm.
26. Microsoft Learn, "Microsoft Build 2026," accessed May 21, 2026, https://learn.microsoft.com/en-us/intune/device-management/actions/remote-lock?pivots=macos.
27. Apple, "MacBook Neo," accessed May 20, 2026, https://www.apple.com/macbook-neo/specs/.
28. Dell Technologies, "Chromebooks," accessed May 22, 2026, https://www.dell.com/en-us/shop/2-in-1-laptops/sf/chromebook-laptops.
29. Dell Technologies/World, "The Right Device for Every K-12 Role," accessed May 22, 2026, https://www.dell.com/en-us/blog/the-right-device-for-every-k-12-role/.
30. Apple, "MacBook Neo, " accessed May 22, 2026, https://www.apple.com/macbook-neo/.
31. Dominic Reigns, "Average RAM Usage on ChromeOS Statistics 2026," accessed May 18, 2026, https://www.aboutchromebooks.com/average-ram-usage-on-chromeos-statistics/.
32. Apple, "MacBook Neo," accessed May 18, 2026, https://www.apple.com/macbook-neo/specs/.
33. Dell Technologies/World. "Innovative Technology for Inspired Learning," accessed May 14, 2026, https://www.dell.com/en-us/lp/dt/industry-k12-ed-student-and-educator-computing.
34. Dell Technologies, "From Classrooms to Careers: Dell simplifies Learning with Purpose-Built Educations PC and Future-Ready Programs," accessed May 14, 2026, https://investors.delltechnologies.com/news-releases/news-release-details/classrooms-careers-dell-simplifies-learning-purpose-built.
35. Apple Newsroom, "Say hello to MacBook Neo," accessed May 14, 2026, https://www.apple.com/ne/newsroom/2026/03/say-hello-to-macbook-neo/.
36. Apple, "MacBook Neo Product Environmental Report," accessed May 14, 2026, https://www.apple.com/environment/pdf/products/notebooks/MacBook_Neo_PER_Mar2026.pdf.
37. iFixit, "MacBook Neo Is the Most Repairable MacBook in 14 Years," accessed May 14, 2026, https://www.ifixit.com/News/116152/macbook-neo-is-the-most-repairable-macbook-in-14-years.
38. iFixit, "MacBook Neo Is the Most Repairable MacBook in 14 Years," accessed May 14, 2026, https://www.ifixit.com/News/116152/macbook-neo-is-the-most-repairable-macbook-in-14-years.
39. Dell Technologies, "From Classrooms to Careers: Dell simplifies Learning with Purpose-Built Educations PC and Future-Ready Programs," accessed May 14, 2026, https://investors.delltechnologies.com/news-releases/news-release-details/classrooms-careers-dell-simplifies-learning-purpose-built.
40. Dell Technologies, "Meet the Dell Education PC Portfolio," accessed May 14, 2026, https://www.dell.com/en-us/blog/empowering-the-classroom-meet-the-dell-education-pc-portfolio/.
41. Apple, "AppleCare+ for Schools (ipads) AppleCare+ for Schools (Mac)," accessed May 29, 2026, https://www.apple.com/legal/sales-support/applecare/education/applecareplusus.html.
42. Apple, "Apple education Price List (Apple Products) 4-1-2026," accessed May 21, 2026, https://www.apple.com/education/pricelists/pdfs/Apple_US_Education_Institution_Price_List.pdf.
43. Dell Technologies, "New dell Pro Education AA Laptop or 2-in-1," accessed May 14, 2026, https://www.dell.com/en-us/shop/dell-laptops/dell-pro-education-11-laptop-or-2-in-1/spd/dell-pro-pe11260-education-2-in-1-laptop/xcto_pe11260_usx-?redirectTo=SOC.
44. Dell Parts store, "Chromebook battery selector – General Chromebook upgrades," accessed May 14, 2026, https://claude.ai/chat/808535e4-ecd2-4fb6-a178-1eb94cd-4dc81.
45. iFixit T, "MacBook Neo Is the Most Repairable MacBook in 14 Years," accessed May 14, 2026, https://www.ifixit.com/News/116152/macbook-neo-is-the-most-repairable-macbook-in-14-years.
46. Dell Technologies, "Meet the Dell Education PC Portfolio," accessed May 14, 2026, https://www.dell.com/en-us/blog/empowering-the-classroom-meet-the-dell-education-pc-portfolio/.
47. Dell Technologies, "Dell Chromebook 14 CC14260," accessed May 14, 2026, https://www.dell.com/support/product-details/en-us/product/chromebook-cc14260-laptop/resources/manuals.

48. iFixit, "MacBook Neo Is the Most Repairable MacBook in 14 Years," accessed May 14, 2026, https://www.ifixit.com/News/116152/macbook-neo-is-the-most-repairable-macbook-in-14-years.

49. iFixit, "MacBook Neo Is the Most Repairable MacBook in 14 Years," accessed May 14, 2026, https://www.ifixit.com/News/116152/macbook-neo-is-the-most-repairable-macbook-in-14-years.

50. Note: 41-screw count applies to Touch ID keyboard (ANSI/ISO). Base 256 GB education model uses keyboard without Touch ID: 45 screws. Source: Apple service manual.

51. iFixit, "MacBook Neo Is the Most Repairable MacBook in 14 Years," accessed May 14, 2026, https://www.ifixit.com/News/116152/macbook-neo-is-the-most-repairable-macbook-in-14-years.

52. Dell Technologies, "Innovative Technology for Inspired Learning," accessed May 14, 2026, https://www.dell.com/en-uk/lp/dt/industry-k12-ed-student-and-educator-computing.

53. Dell Technologies, "Dell Chromebook 14 CC14260," accessed May 14, 2026, https://www.dell.com/support/product-details/en-us/product/chromebook-cc14260-laptop/resources/manuals.

54. Apple, "MacBook Neo Repair Manual," accessed May 14, 2026, https://support.apple.com/en-us/126520.

55. Apple, "Apple Service and Repair," accessed May 14, 2026, https://support.apple.com/repair.

56. Apple, "Apple Service and Repair for Mac Laptops," accessed May 14, 2026, https://support.apple.com/mac-laptops/repair?services=service.

57. Apple Community, "Apple repair policy – turnaround time," accessed May 21, 2026, https://discussions.apple.com/thread/252657229?sortBy=rank.

58. Caitlynn Peetz Stephens, "What Districts Can Do With All Those Old Chromebooks," accessed June 11, 2026, https://www.edweek.org/technology/what-districts-can-do-with-all-those-old-chromebooks/2024/07.

59. Jennifer Lichtie, "K-12 Mobile Device Repair: Best Practices to Maximize Learning," accessed May 14, 2026, https://www.locknchargе.com/blog/mobile-device-repair-in-schools.

60. Self-Servicing Account Program," accessed May 14, 2025, https://support.apple.com/self-servicing-account-program.

61. Apple, "Apple Self-Servicing Account Program Manual," accessed May 14, 2026, https://go.boarddocs.com/pa/21cccs/Board.nsf/files/BST6RB162831/$file/Apple%20-%20Self%20Service.pdf.

62. Mac Solutions Plus, "Repairs and Managed Service for Buffalo Schools and Apple Devices," accessed May 14, 2026, https://www.macsolutionsplus.com/repairs-and-managed-service-for-education/.

63. Connection, "Dell 3-Year ProSupport Plus Next Business Day On-site," accessed May 14, 2026, https://www.connection.com/product/dell-3-year-prosupport-plus-next-business-day-on-site/812-9861/34338907.

64. Dell Technologies, "Meet the Dell Education PC Portfolio," accessed May 14, 2026, https://www.dell.com/en-us/blog/empowering-the-classroom-meet-the-dell-education-pc-portfolio/.

65. Dell, "Dell ProSupport Service Description," accessed May 14, 2026, https://www.cvsa1.com/app/uploads/2024/05/Warranty-Dell-Pro-Support.pdf.

66. Dell Technologies, "Dell Service Description: Comprehensive Hardware Support for the United States K-12 Education Market," accessed June 11, 2026, https://i.dell.com/sites/csdocuments/Legal_Docs/en/us/comprehensive-hardware-support-for-k12-education-sd-en.pdf.

67. Dell Technologies, "Comprehensive Hardware Support for the US K12 Education Market," accessed June 11, 2026, https://www.dell.com/support/kbdoc/en-us/000123179/comprehensive-hardware-support-for-the-us-k12-education-market.

The science behind the report

In this section, we list our complete results and describe the solutions on which we tested and our test methodologies.

We concluded our hands-on testing on May 20, 2026. During testing, we determined the appropriate hardware and software configurations and applied updates as they became available. The results in this report reflect configurations that we finalized on May 15, 2026 or earlier. Unavoidably, these configurations may not represent the latest versions available when this report appears.

Appendix A: MacBook Neo methodology

Overview

We completed all of the Apple® MacBook® Neo testing in Intune.

Configuring Intune

After creating a Microsoft Office 365 Business account and a Microsoft Azure account, we completed the following tasks and configured our Microsoft Intune environment to allow for Windows Autopilot deployments.

Adding the Intune Plan 1 and Entra Suite licenses

1. Using the admin account, log into Azure.
2. Under Azure services, select Entra ID.
3. Navigate to License.
4. Under Manage, select All products, and click +Try/Buy.
5. Select the free trial Intune Plan 1 Trial license.
6. Complete steps 1 through 4 again, select the free trial Entra Suite Trial license, and click Activate.

Adding Intune and configuring the MDM scope

1. Within the left Entra ID menu, select Entra ID, and click Mobility (MDM and MAM).
2. Click +Add application.
3. Select Microsoft Intune, and click Add.
4. Click Microsoft Intune.
5. On the Configure page, configure the following, and click Save:
   - MDM user scope: All
   - MAM user scope: All

Adding users

1. From the Azure portal, under Azure Services, select Entra ID.
2. In the left pane under Manage, select Users.
3. Click + New user, and click Create new user.
4. In the first block, enter a username, and after @ in the block, choose the proper domain name from the dropdown menu.
5. For Name, enter the desired name as required, and select your Password options. If you choose Auto-generate Password, check Show Password.
6. Copy the password to the clipboard, store it somewhere safe, and click Create.

Managing licensing on the target users

1. Under Users, select the recently created user.
2. In the left pane, under Manage select Licenses, click +Assignments, select both Entra Suite and Intune Plan 1, and click Save.

Creating Autopilot deployment profiles

1. Navigate to the Microsoft Intune Admin Center endpoint.microsoft.com.
2. Navigate to Devices > Windows > Windows enrollment > Deployment Profiles.
3. Select Create profile > Windows PC. Fill in the required information, and click Next.
   - Enter a name for the profile.
   - Leave Convert all targeted devices to Autopilot on No, and click Next.
   - Leave defaults, changing only Allow pre-provisioned deployment to Yes, and Apply device name template to Yes.
   - For the naming profile, enter `System-%RAND:6%`
4. Click Add groups, select desired group, and click Select.
5. Click Next.
6. Click Create.

Configuring Intune for Apple Business Manager integration

Creating the Apple MDM Push Certificate

1. Within Intune, select Devices > Enrollment, and click the Apple tab.
2. Click Apple MDM Push Certificate.
3. Check the I agree box.
4. To download your CSR, click the link. When prompted, save the file as IntuneCSR, and click Save.
5. To create your MDM push Certificate, click the link.
6. In the newly open tab, log in with your Apple ID credentials for managing ABM.
7. Click Create a Certificate.
8. Check the I have read and agree to these terms and conditions box, and click Accept.
9. Click the Choose File button, select the IntuneCSR file you just downloaded, and click Upload.
10. To save the new push certificate, click Download.
11. Accept the default name MDM_Microsoft Corporation_Certificate, and click Save.
12. Go back to the Intune portal. Within the Configure MDM Push Certificate, enter the Apple ID you used to create your certificate.
13. To browse for the .PEM file you just created, click the folder icon, select it, and click Open.
14. Click Upload. Intune will present a notification that the push certificate has been created. You can view the certificate information at the top of the panel, including the Active status indication. In the upper right of the panel, click X.

Creating the Enrollment Program Token

1. Within the Apple tab, in Intune, select Devices > Enrollment, and click Enrollment program tokens.
2. Click Create.
3. Check the I Agree box, and click the link for Download your public key.
4. To download the IntuneKey to your local system, click Save.
5. Switch over to the Apple Business Manager tab in your browser. If necessary, log in.
6. Click on your user name at the bottom left of the page, and select Preferences.
7. Beside Device Management Services, click Add.
8. For Service Info, provide a name for the MDM you're connecting. Under Service settings, click the Upload Certificate link and browse to the location where you saved the IntuneKey.pem file, select it, and click Open.
9. Click Save.
10. At the top of the page, click Download.
11. Save the token to your local system.
12. Switch over to the Intune tab in your browser.
13. Enter the Apple ID you used to log into Apple Business Manager when you created the token.
14. To browse for the token file you just downloaded, click the folder, and click Next.
15. Click Create.

Creating an Enrollment Profile

1. Within the Apple tab in Intune, select Devices > Enrollment, and click Enrollment program tokens.
2. Click the Intune token.
3. Under Manage, select Profiles, and click Create profile >macOS.
4. Provide a name for the profile, and click Next.
5. Use the User affinity pull-down menu, and select Enroll with User Affinity.
6. Use the Authentication method pull-down menu, and select Setup Assistant with modern authentication.
7. For Await final configuration, accept the default Yes.

8. Use the Locked enrollment pull-down menu, and select Yes.
9. Click Next.
10. Provide a department name and department phone number.
11. To hide all the screens that would appear in setup assistant, click Toggle All, and click Next.
12. Use the Create a local admin account pull-down menu, and select Yes.
13. Use the Create a local primary account pull-down menu, and select Yes.
14. Set the account type to Standard, select Yes for Prefill account info, and click Next.
15. Click Create.
16. Once the profile has been created, click the Set default profile icon in the profiles section.
17. Use the macOS Enrollment profile pull-down menu, select the profile you just created, and click OK.

Configuring a macOS configuration policy in Intune

Creating a macOS group in Intune

1. Within the left menu in Intune, click Groups.
2. Click New Group.
3. Name the group MacBook Neos, and change the Membership type to Dynamic Device.
4. Under Owners, click the link, select an administrative account as the owner, and click Select.
5. Under Dynamic device members, click Add a Dynamic Query. Click the Property pull-down menu, and select deviceOSType. Click the Operator pull-down menu, and select equals. Under Value, enter macMDM in the input box. To see the Rule Syntax and enable the Save button, press tab twice, and click Save.
6. Click Create.

Creating a macOS policy in Intune

1. Within the left menu in Intune, select Devices.
2. Click Configuration, and select Create >New Policy.
3. Use the Select platform pull-down menu, and choose macOS. Use the Profile type pull-down menu, and select Templates. From the list, select Software updates, and click Create.
4. Provide a name for the policy, and click Next.
5. Using the pull-down menus, adjust the settings for Critical updates, Firmware updates, and Configuration file updates to Download and Install. Using the schedule type pull-down menu, select Update during scheduled time, choose the check updates target time window, and click Next.
6. Under included groups, click Add groups, check the MacBook Neos box, click Select, and click Next.
7. Click Create.

Performing device enrollment and provisioning

Synchronizing Intune and Apple Business Manager

1. Log into Apple Business Manager.
2. Select Devices.
3. Locate and select the newly registered device. To quickly locate our target device, we used Neo as a filter.
4. In the upper-right corner of the far-right panel, click the ellipses, and select Assign Device Management.
5. Select your Intune instance for MDM, and click OK.
6. Log into Intune.
7. Within the Apple tab in Intune, select Devices > macOS devices > Enrollment, and select Enrollment program tokens > {token name} > Manage > Devices > Sync. The manual sync will take about 15 minutes.
8. Once the sync has completed, power on the MacBook.

Performing zero-touch enrollment of a new MacBook Neo device (performed by end user)

1. Power on the MacBook Neo.
2. From the menu, select a Wi-Fi network, and click Restart.
3. Select United States, and click Continue.
4. Click Continue.
5. Click Not Now.
6. Select Wi-Fi, and click Continue.
7. Enter the password, and click Join.
8. Click Enroll.
9. Enter the credentials provided by your IT organization, and click Next. When prompted, enter the password, and click Connect.
10. At Create a Mac Account, re-enter the password provided by your IT organization, and click Continue.
11. Using current location, toggle the Set time zone automatically, click Turn On Location Services, and click Continue.

Verifying enrollment and compliance

1. Within the left menu in Intune, click Devices, and click All devices. The device's screen shows compliance and device state (managed).

Applying device naming convention and asset tag

1. Within Intune, click Devices, and select All devices.
2. Click the system you want to edit.
3. In the Properties tab, click Edit.
4. Change the device name to the asset tag or naming convention you want to apply, and click Save.

Performing security policy deployment

Deploying a new security policy

1. Within Intune, click Endpoint Security.
2. Under Manage, select Firewall, and click Create policy.
3. Use the Platform pull-down menu, and select macOS. Use the Profile pull-down menu, select macOS Firewall, and click Create.
4. Provide a name for the policy, and click Next.
5. Toggle Enable Firewall to True. Use the Allow Signed pull-down menu, and select True. Use the Allowed Signed App pull-down menu, and select True. Add a BundleID by clicking +Edit instance. Toggle Allowed to True, enter the Bundle ID (such as com.google.Chrome), and click Next.
6. Under Scope tags, click Next.
7. Under Included Groups, click Add groups, select the group or groups you want to add, click Select, and click Next.
8. Review the information, and click Create.

Deploying a Wi-Fi configuration profile

1. Within Intune, click Devices. Under Manage Devices, select Configuration.
2. On the policies tab, select Create >New Policy.
3. In the right panel, select macOS for the platform, and select Templates for profile type. Under template name, select Wi-Fi, and click Create.
4. Provide a name for the Wi-Fi profile, and click Next.
5. For Deployment Channel, select Device Channel.
6. For Wi-Fi type, select Basic.
7. Enter the SSID for the Wi-Fi network, and leave the defaults disabled.
8. For Security type, select WPA/WPA2-Personal, and enter the Pre-shared key (password) for the target Wi-Fi network.
9. Click Next.
10. Under Included Groups, click Add groups, select the group or groups you want to add, click Select, and click Next.
11. Review the information, and click Create.

Enabling and enforcing fleet-wide disk encryption

1. Within Intune, click Devices, and click the macOS panel.
2. Click Configuration, and select Create > New Policy. Under Profile type, select Settings Catalog, and click Create.
3. Provide a name for the profile, and click Next.
4. Click Add Settings, expand Full Disk Encryption, click FileVault, and check the boxes beside Enable, Defer, Force Enable in Setup Assistant, Show Recovery Key, and Use Recovery Key.
5. Expand FileVault Recovery Key Escrow, and select Location.
6. In the main panel:
    a. Set the location as /var/db/FileVaultPRK.dat.
    b. Set Use recovery key to Enabled.
    c. Set Show recovery key to Enabled.
    d. Set Force Enable in Setup Assistant to True.
    e. Set Defer Force at User Log in Max Bypass Attempts to 0.
    f. Set Defer to Enabled.
    g. Set Enable to On, and click Next.
7. Under Scope tags, click Next.
8. Under Included Groups, click Add groups, select the group or groups you want to add, click Select, and click Next.
9. Review the information, and click Create.

Performing application management

Deploying a required app silently to all devices

1. Within Intune, click Apps.
2. Click the macOS panel.
3. Click Create.
4. Select Line-of-business app, and click Select.
5. Click select app package file, browse to the .PKG file you want to deploy, click Open, and click OK.
6. Provide a publisher for the app, and toggle Install as managed to Yes. Remove all files except the one application you want to manage, and click Next.
7. Under Assignments, locate the Required section, and click Add group.
8. Choose the target group, click Select, and click Next.
9. Review, and click Create. The application will automatically deploy to all targets in the group.

Removing a deployed app remotely

1. Within Intune, click Apps.
2. Click the macOS panel.
3. Click the app you want to remove.
4. Under Manage, click Properties, scroll down to Assignments, and click Edit.
5. Click the ellipses, and select Delete from the target group.
6. Under Uninstall, click Add Group.
7. Select the uninstallation target group, and click Select.
8. Click Review, and click Save. The application will be removed the next time the system checks in.

Updating a deployed app across the fleet

1. Within Intune, click Apps.
2. Click the macOS panel.
3. Click Create.
4. Select Line-of-business app, and click Select.
5. Click select app package file, browse to the .PKG file you want to deploy, click Open, and click OK.
6. Provide a publisher for the app, toggle Install as managed to Yes, toggle Ignore App version to No, remove all files except the one application you want to manage, and click Next.
7. Under Assignments, locate the Required section, and click Add group.
8. Choose the target group for the application, click Select, and click Next.
9. Review, and click Create. The application will be automatically deployed to all targets in the group.

Pushing a driver or firmware update fleet-wide

1. Within Intune, click Devices. Under By platform, click macOS.
2. Click Configuration, and select Create >New Policy. Under Profile type, select Settings Catalog, and click Create.
3. Name the profile `Update to 26.5 - DDM` and click Next.
4. Click Add Settings, expand the Declarative Device Management (DDM) category, select Software Update, and click Select all these settings and notifications. In the upper right of the Settings Picker panel, click X.
5. Complete the information for Software Update. (For the details URL, we used https://developer.apple.com/documentation/macos-release-notes. For Target Build Version, we used 25F71.) Enter a target date and time, enter the Target OS Version (we used 26.5), and click Next.
6. In Scope tags, click Next.
7. For assignment, under Included groups, click Add groups, check the Mac Endpoints box, click Select, and click Next.
8. Click Create, click Review, and click Save.

Performing ongoing maintenance

Pushing an OS update to all devices

1. Within Intune, click Devices. Under By platform, click macOS.
2. Click Configuration, and select Create >New Policy. Under Profile type, select Settings Catalog, and click Create.
3. Name the profile `MacOS DDM` and click Next.
4. Click Add Settings, expand the Declarative Device Management (DDM) category, select Software Update, and click Select all these settings and notifications. In the upper right of the Settings Picker panel, click X.
5. Complete the information for Software Update. (For the details URL, we used https://developer.apple.com/documentation/macos-release-notes. For Target Build Version, we used 25F71.) Enter a target date and time, enter the Target OS Version (we used 26.5), and click Next.
6. In Scope tags, click Next.
7. For assignment, under Included groups, click Add groups, check the Mac Endpoints box, click Select, and click Next.
8. Click Create.

Checking OS update compliance status across the fleet

1. Within the left menu in Intune, click Reports.
2. Under Reports, expand device management, and click Apple updates.
3. Click the reports tab, and select Apple software update report.
4. Click Generate report.
5. To download the results into a .CSV file, click Export.

Remotely locking a device

1. Within the left menu in Intune, click Devices, and select All devices.
2. Click the target macOS device.
3. Use the Secure pull-down menu, and select Remote Lock.
4. Click Remote lock device. The generated PIN listed beside the Remote Lock Action can be used to restore access to the system.

Remotely wiping a device and confirming re-enrollment

1. Within the left menu in Intune, click Devices, and select All devices.
2. Click the target macOS device.
3. Use the Remove data pull-down menu, and select Wipe.
4. Check the I Understand box, and click Wipe. In the far upper right menu, provide a recovery PIN, and click Wipe. The device is already connected through Apple Business Manager, and upon reactivation (when connected to a Wi-Fi network) will automatically be available for re-enrollment.
5. When the system finishes rebooting, to reactivate the MacBook Neo, select a wireless network or connect a cable.

Generating a device compliance report for teacher/staff

1. Within the left menu in Intune, click Reports.
2. Under Reports, click Device Compliance.
3. Click Reports, and select Device compliance.
4. Use the OS pull-down menu, select only macOS, and click Generate Report.
5. To download the results into a .CSV file, click Export.

Appendix B: Dell Pro Education 11 methodology

Overview

We performed all of our Dell™ Pro Education11 laptop testing in Intune.

Configuring Intune

Creating Autopilot deployment profiles

1. Navigate to the Microsoft Intune Admin Center endpoint.microsoft.com.
2. Navigate to Devices > Windows > Windows enrollment > Deployment Profiles.
3. Select Create profile > Windows PC. Fill in the required information, and click Next.
   - Enter a name for the profile.
   - Leave Convert all targeted devices to Autopilot on No, and click Next.
   - Leave most defaults, except:
     - Change Allow pre-provisioned deployment to Yes.
     - Change Apply device name template to Yes.
     - For the naming profile, enter `System-%RAND:6%`
4. Click Add groups, select desired group, and click Select.
5. Click Next.
6. Click Create.

Performing device enrollment and provisioning

Performing zero-Touch enrollment of a new Windows 11 device (performed by end user)

1. Press the power button on the laptop. Wait for the boot menu and Windows loading screens to complete.
2. Select United States as the country, and click Yes.
3. Accept the US keyboard, and click Yes.
4. When prompted for a second keyboard layout, click Skip.
5. Select a wireless network to connect with, click Connect, and click Next.
6. Wait for Checking for updates to complete, then accept the terms of the license agreement.
7. When prompted to name the device, click Skip for now.
8. On the Let's set things up for your work or school screen, enter the username for the user created above.
9. Enter the user password.
10. Using the authenticator application, confirm the user's log in.
11. When prompted to choose privacy settings, scroll to the bottom, and click Accept.
12. On the Windows Hello facial recognition screen, click Skip for now.
13. Click OK.
14. On the Set up a Pin screen, enter a PIN, confirm the PIN, and click OK.

Verifying enrollment and compliance

1. Within the left Intune menu, click Devices, and click All devices. The device's screen shows compliance and device state (managed).

Applying device naming convention and asset tag

Naming convention is applied automatically via the Autopilot enrollment profile.

Performing security policy deployment

Deploying a new security policy

1. Within Intune, click Endpoint Security.
2. Under Manage, select Firewall, and click Create policy.
3. Use the pull-down menu under platform, and select Windows. To select Windows Firewall, use the pull-down under Profile, and click Create.
4. Provide a name for the policy, and click Next.
5. Use the pull-down beside Enable Domain Network Firewall, and select False. Use the pull-down beside Enable Private Network Firewall, select False, and click Next.
6. Under Scope tags, click Next.
7. Under Included Groups, click Search by group name, select the group or groups you want to add, and click Next.
8. Review the information, and click Create.

Deploying a Wi-Fi configuration profile

1. Within Intune, click Devices. Under Manage Devices, select Configuration.
2. On the policies tab, click Create > New Policy.
3. On the right panel, select Windows 10 and later for the platform, and select Templates for profile type. Under template name, select Wi-Fi, and click Create.
4. Provide a name for the Wi-Fi profile, and click Next:
5. For Deployment Channel, select Device Channel.
6. For Wi-Fi type, select Basic.
7. Enter the SSID for the Wi-Fi network, and leave the defaults disabled.
8. For Security type, select WPA/WPA2-Personal, and enter the Pre-shared key (password) for the target Wi-Fi network.
9. Click Next
10. Under Included Groups, click Add groups, select the group or groups you want to add, click Select, and click Next.
11. User the pull-down menu for rule, and select Assign profile if. Use the pull-down menu for property, and select OS edition. Click the pull-down menu under value, and select all the editions you want to include for the profile. Click Next.
12. Review the information, and click Create.

Enabling and enforcing fleet-wide disk encryption

1. Within Intune, click Devices, and click the Windows panel.
2. Click Configuration, and click Create >New Policy. Under platform, select Windows 10 and later. Under Profile type, select Settings Catalog, and click Create.
3. Provide a name for the profile, and click Next.
4. Click Add Settings, expand BitLocker, and click Select all these settings.
5. In the main panel, set Configure Recovery Password Rotation to Refresh on for Entra ID-joined and hybrid-joined devices, toggle Require Device Encryption to Enabled, and click Next.
6. Under Scope tags, click Next.
7. Under Included Groups, click Add groups, select the group or groups you want to add, click Select, and click Next.
8. Review the information, and click Create.

Configuring BIOS/firmware security policy fleet-wide

1. Within Intune, click Devices, and click the Windows panel.
2. Click Configuration, and click Create >New Policy. Under platform, select Windows 10 and later. Under Profile type, select Templates, select Device Firmware Configuration Interface, and click Create.
3. Provide a name for the profile, and click Next.
4. Expand UEFI access, and in the pull-down menu, select None.
5. Expand Security Settings, and use the pull-down menu to set CPU and IO virtualization to Enabled.
6. Expand Boot Options, and use the pull-down menu to set Boot from external media and Boot from network adapters to Disabled.
7. Click Next.
8. Under Scope tags, click Next.
9. Under Included Groups, click Add groups, select the group or groups you want to add, click Select, and click Next.
10. For rules, use the pull-down menu, and select Assign profile if.
11. For property, use the pull-down menu, and select OS edition.
12. Click the pull-down menu under value, select all the editions you want to include for the profile, and click Next.
13. Review the information.
14. Click Create.

Performing application management

Deploying a required app silently to all devices

Obtaining the software

Steps for this sub-section are not included in time or steps calculations.

1. Open a browser and, in the search bar, enter https://dl.google.com/chrome/install/GoogleChromeStandaloneEnterprise64.msi.
2. Open the downloads folder.
3. Copy the downloaded file (GoogleChromeStandaloneEnterprise64.msi) into a folder by itself.

Creating the app and uploading the package

1. Within the left Intune menu, click Apps.
2. In the Apps panel, click Windows, and click Create.
3. To select Line-of-business app, use the pull-down menu, and click Select.
4. To browse to the .MSI file you wish to upload, click Select app package file, click the folder icon, select the file, click Open, and click OK.
5. In the App Information section, add the publisher's name (the software vendor), and click Next.
6. In the Assignments section, under the Required heading, click Add group.
7. Check the box of the device group(s) for which this package is required, click Select, and click Next.
8. Review the information, and click Create.

Removing a deployed app remotely

1. Within Intune, click Apps.
2. Click the Windows panel.
3. Click the app you want to remove.
4. Under Manage click Properties, scroll to Assignments, and click Edit.
5. To remove the target group, click the ellipses, and select delete.
6. Under Uninstall, click Add Group.
7. Select the uninstallation target group, and click Select.
8. Click Review and Save. The application will be gone the next time the system checks in.

Updating a deployed app across the fleet

1. Within Intune, click Apps.
2. Click the Windows panel, and click Create.
3. Select Line-of-business app, and click Select.
4. Click select app package file, browse to the .MSI file you want to deploy, click Open, and click OK.
5. Provide a publisher for the app, and click Next.
6. Under Assignments, locate the Required section, and click Add group.
7. Choose the target group for the application, click Select, and click Next.
8. Review, and click Create. The application will automatically deploy to all targets in the group.

Pushing a driver or firmware update fleet-wide

This procedure assumes you have downloaded the device driver in .exe format.

Converting the software

1. Open the Microsoft-Win32-Content-Prep-Tool-master application folder downloaded from GitHub.
2. Double-click IntuneWinAppUtil. If prompted, click Run.
3. Enter the following information into the text-based prompts:
    a. Provide the path directory for the executable you want to convert, and press Enter. NOTE: This directory should contain ONLY the file you want to convert.
    b. Provide the name of the executable you want to convert, and press Enter.
    c. Provide the directory where you want to save the converted program, and press Enter.
    d. When prompted for catalog directory, press n, and press Enter.

Creating the app and uploading the package

1. Open a browser, and log into intune.microsoft.com.
2. In the left menu, click Apps.
3. In the Apps panel, click Windows, and click Create.
4. To select the type of app you want to deploy, use the pull-down menu, select Windows App (Win32), and click Select.
5. To browse to the converted file you wish to upload, click Select app package file, click the folder icon, select the file, click Open, and click OK.
6. In the App Information section, add the publisher's name (the software vendor), and click Next.
7. In the Program section, provide the install and uninstall commands (for installation this will be the name of the executable followed by /s for silent installation), and click Next.
8. In the Requirements section:
    a. Choose the radio button for Yes.
    b. Specify the systems the app can be installed on.
    c. Check the box for the appropriate architecture type - Install x64 and install on x86 for AMD and Intel® processor-based systems.
    d. To select the minimum operating system (we selected the earliest version of Windows 11)., use the pull-down menu, and click Next.
    e. To select manually configure detection rules:
    f. Use the pull-down menu in the Detection rules section, and click Add.
    g. To select File, use the pull-down menu.
    h. To search for application presence, provide the path and folder on the target systems, use the Detection method pull-down menu to select File or folder exists, and click OK.
9. Click Next.
10. In the Dependencies section, click Next.
11. In the Supersedence section, click Next.
12. In the Assignments section, under the Required heading, click Add group.
13. Check the box of the device group(s) for which this package is required, click Select, and click Next.
14. Review the information, and click Create.

Performing ongoing maintenance

Pushing an OS update to all devices

1. Within Intune, click Devices. Under By platform, click Windows.
2. Expand Manage Updates and click Windows Updates.
3. Click Feature Updates.
4. Click Create >Create feature update policy.
5. To select the correct version, use the pull-down menu, and name the profile `Windows 11 25H2`. Ensure the Make available to users as a required update option is selected, and the Make update available as soon as possible option is selected, and click Next.
6. Under Included groups, click Add groups, check the box for Dell Endpoints, click Select, and click Next.
7. Click Create.

Checking OS update compliance status across the fleet

1. Within the left menu in Intune, click Reports.
2. Under Reports, expand device management, and click Windows updates.
3. Click the reports tab, and select Windows 10 and later feature updates report.
4. Click Generate report.
5. To download the results into a .CSV file, click Export.

Remotely wiping a device and confirming re-enrollment

1. Within the left menu in Intune, click Devices, and select All devices.
2. Click the target Windows device.
3. For Remove data and select Wipe, use the pull-down menu.
4. Select Single wipe, check the I Understand… box, and click Wipe.

Bulk remotely wiping a fleet and confirming re-enrollment (end of year refresh)

1. Within the left menu in Intune, click Devices, and select All devices.
2. Click Bulk device actions.
3. To select which devices you want to remote wipe:
    a. Use the pull-down menu for OS, and select Windows.
    b. Use the pull-down menu for Device type,and select Physical devices.
    c. Use the pull-down menu for Device action, and select Wipe.
    d. Click Next.
4. Click Select devices to include.
5. Click each device you want to include (up to 100 devices), click Select, and click Next.
6. Click Create.

Generating a device compliance report for teacher/staff

1. Within the left menu in Intune, click Reports.
2. Under Reports, click Device Compliance.
3. Click Reports, and select Device compliance.
4. Use the pull-down menu for OS, select only Windows, and click Generate Report.
5. To download the results into a .CSV file, click Export.

Appendix C: Chromebook 14 methodology

Overview

Unless otherwise noted, we performed all of our Chromebook tests in Google Admin. We used Intune for visibility only.

Configuring Intune

Connecting Chrome Enterprise to Intune

1. Open a browser, and log into Intune.microsoft.com.
2. Navigate to Tenant Administration, and click Connectors and Tokens.
3. Expand Android and ChromeOS, and click Chrome Enterprise.
4. Click Connect.
5. Copy the ClientID.
6. Open a browser tab, and log into admin.google.com.
7. Navigate to Security, expand Access and data control, and click API controls.
8. Click Manage domain wide delegation.
9. Within API clients, click Add new.
10. Paste the ClientID you copied from your Intune instance, and navigate to the browser tab containing Intune.
11. Within Intune, copy the OAuth scope, and navigate to the browser tab containing Google Admin.
12. Paste the OAuth scope you copied from your Intune instance, and click Authorize.
13. Click the browser tab containing Intune. To activate the connector and authenticate, click Launch Google. Device synchronization will occur automatically between Google Admin and Microsoft Intune.

Performing device enrollment and provisioning

Performing zero-touch enrollment of a Chromebook device (performed by end user)

1. Press the Chromebook power button. Wait for the Welcome to your Chromebook screen, and on the Turn on screen reader pop-up, press Close.
2. Click Get Started.
3. Select a wireless network, enter the password, and click Next.
4. Click Done.
5. Log in with your provided credentials.
6. Click Accept and Continue.
7. Click Accept and Continue to sync your Chromebook.

Verifying enrollment and compliance

1. Within the left Google Admin menu, expand Devices > Chrome > Devices. Click the Dashboard tab, which contains enrollment and compliance views.

Applying device naming convention and asset tag

1. Within the left Google Admin menu, click Devices, and click the device you want to edit. In the custom fields, click Edit.
2. Enter the Asset ID. Click Save.

Performing security policy deployment

Deploying a new security policy

1. Within Google Admin, expand Devices > Chrome, and click Settings.
2. In User & browser settings, search for disabled system features, and click the Disabled System features link.
3. Select the apps you want to disable (such as Recorder, Camera, and Terminal), and click Save.

Deploying a Wi-Fi configuration profile

1. Within Google Admin, expand Devices, and click Networks.
2. Click Create Wi-Fi Network.
3. Check the box for Chromebooks (by device). Scroll down and provide a name and the SSID of the wi-fi network. Check the box for automatically connect. Use the pull-down menu for Security type, select WPA/WPA2/WPA3, provide the passphrase, and click Save.

Configuring BIOS/firmware security policy fleet-wide

1. Within Google Admin, expand Devices > Chrome, and click Settings.
2. Click the tab for Device Settings.
3. Search for TPM, and click the TPM firmware update link.
4. Set Configuration to Block users from performing TPM firmware update, and click Save.

Performing application management

Deploying a required app silently to all devices

1. Within Google Admin, expand Devices > Chrome, and click Apps & extensions.
2. Click the Users & browsers tab.
3. In the lower right of the screen, click the + icon, and select the source. (We added from the Google Play Store.)
4. Select the app you want to add (we selected Google Classroom), and click Select.
5. To grant permissions, click Accept.
6. Under the app's details, change the installation policy to Force install, pin to ChromeOS taskbar, and click OK.
7. In the upper right of the screen, click Save.

Removing a deployed app remotely

1. Within Google Admin, expand Devices >Chrome, and click Apps & extensions.
2. Click the Users & browsers tab.
3. Click the app you want to remove.
4. To delete the app and remove it from deployed systems, click the trashcan icon.
5. Under Manage, click Properties, scroll down to Assignments, click Edit, and remove the app..

Performing ongoing maintenance

Pushing an OS update to all devices

1. Within Google Admin, Expand Devices >Chrome, and click Settings.
2. Click the Device Settings tab.
3. Search for device update, and click Auto-update settings:
    a. For Allow devices to automatically update OS version, set to Allow updates.
    b. For Target version, use the pull-down menu to select a version or Use latest version.
    c. For Auto reboot after updates, select Allow Auto-reboots.
    d. Verify Rollout plan is set to Default (devices should update as soon as a new version is available).
4. Click Save.

Checking OS update compliance status across the fleet

1. Within Google Admin, expand Devices > Chrome > Reports, and click Versions.
2. To generate a. CSV file containing all the version information for ChromeOS devices, click Export.
3. In the Your tasks panel, click Download CSV to download the report to your local system.

Remotely locking a device with Google Admin

1. Within Google Admin, expand Devices > Chrome > Devices, and click the device you want to lock.
2. Click Disable.
3. Choose the disable with Lock Screen option, and click Disable.

Remotely locking a device with Intune

1. Within the left Intune menu, click Devices, and select All devices.
2. Click the target Chromebook device.
3. Click Lost mode.
4. Toggle Lost mode to Enable, and click OK.

Remotely wiping a device and confirming re-enrollment with Google Admin

1. Within Google Admin, expand Devices > Chrome > Devices, and check the box of the system(s) you want to wipe.
2. Select the Clear User Profiles option, check the I understand… box, and click Reset.

Remotely wiping a device (or fleet) and confirming re-enrollment with Intune (end of year refresh)

1. Within the left Intune menu, click Devices, and select All devices.
2. Click the target Chromebook device(s).
3. Click Wipe.
4. Select Factory Reset, check the I Understand… box, and click Wipe Device(s).

Generating a device compliance report for teacher/staff

1. In Google Admin, expand Reporting >Devices, and click ChromeOS & browser versions.
2. To generate a .CSV of the report, click Export.
3. To download the report to your local system, navigate to the Your tasks panel, and click Download CSV.

Appendix D: Configuration table

Table 5: Detailed information on the systems we tested.

System configuration information	Dell Pro Education 11 (PE11260)	Dell Chromebook 14	Apple MacBook Neo
Processor			
Vendor	Intel	Intel	Apple
Model number	N150	N250	Apple A18 Pro
Cache	2MB L2 6MB L3	6 MB L3	16 MB L2 24MB L3
Core frequency (GHz)	3.6	3.8	4.05 (performance) 2.42 (efficiency)
Number of cores	4 (efficiency)	4 (efficiency)	2 (performance) 4 (efficiency)
Memory			
Amount (GB)	8	8	8
Type	LPDDR5X	LPDDR5X	LPDDR5X
Speed (MHz)	4,800	4,800	8,533
Discrete graphics			
Vendor	Intel	Intel	Apple
Model number	Integrated Intel Graphics for Intel Processor N150	Integrated Intel Graphics for Intel Processor N250	Integrated Apple A18 Pro chip
Storage			
Amount (GB)	128	128	256
Type	M.2 UFS	UFS	Internal SSD (NAND soldered to motherboard)
Connectivity/expansion			
Wired internet	Generic USB Ethernet	Generic USB Ethernet	Generic USB Ethernet
Wireless internet	Intel Wi-Fi 6E AX211	Intel Wi-Fi 6E AX211	MediaTek Wi-Fi 6E
Bluetooth	5.3	5.3	6
USB	2 x USB-C (USB 3.2) 1 x USB-A (USB 3.2)	2 x USB-C (USB 3.2) 1 x USB-A (USB 3.2)	1 x USB-C (USB 3) 1 x USB-C (USB 2)
Display			
Size (in.)	11	14	13
Type	IPS	FHD+	IPS
Resolution	1,366x768	1,920x1,200	2,408x1,506
Operating system			
Vendor	Microsoft	Google	Apple
Name	Windows 11 Professional	ChromeOS	macOS Tahoe
Build number or version	26200.8328	147.0.7727.147	26.4.1

System configuration information	Dell Pro Education 11 (PE11260)	Dell Chromebook 14	Apple MacBook Neo
Dimensions (closed)			
Height (in.)	0.86	0.92	0.50
Width (in.)	11.96	13.20	11.71
Depth (in.)	8.19	9.29	8.12
Weight (lbs.)	3.44	3.79	2.70

Appendix E: K-12 endpoint cost model summary

Overview: Two platform vs. three-platform comparison

This summary compares two device-platform strategies for a large K-12 district with 4,000 faculty/staff PCs and 42,000 student PCs over a three-year refresh cycle. The two-platform model provides teachers and staff with Dell Pro Education PCs and students with Dell Chromebooks. The three-platform model has half of the teachers and half of the students on those same devices and moves the rest to Apple MacBook Neo devices.

The model estimates the following three-year costs for two- and three-platform strategies and compares the total cost for the strategies:

- Per-student or teacher/staff device cost – hardware and support; platform-specific management software, and either Microsoft 365 Education A3 or Google Workspace for Education Plus subscriptions. Some of software is via per user subscription but licenses a single device.
  - New Dell Pro Education PCs (teachers/staff)
  - New Apple MacBook Neo (teachers/staff: three-platform comparison only)
  - New Dell Chromebooks (students)
  - New Apple MacBook Neo (students: three-platform comparison only)
- Hardware spares
  - Dell Pro Education spares
  - Dell Chromebook spares
  - Apple MacBook Neo spares (three-platform comparison only)
- IT and training costs
  - Solution planning
  - Apple certification training for IT staff (three-platform comparison only)
  - IT admin time on setup and critical management tasks (3-year cost at $50 per hour)
  - Teacher training on Apple MacBook Neo (80 percent of staff × 2 hr × $50 per hour)

System information

This is a summary of the hardware configurations that we priced for this analysis and the US education institution pricing for the devices.

Table 6: A summary of system Information.

Attribute	Dell Pro Education 11 (2-in-1)	Dell Chromebook 14	Apple MacBook Neo
Model	Dell Pro Education 11 PE11260	Dell Chromebook 14 CC14260	Apple MacBook Neo
Processor	Intel Processor N150 (4 cores, up to 3.60 GHz, 6 W)	Intel Processor N150 (4 cores, up to 3.60 GHz, 6 W)	Apple A18 Pro (6-core CPU, 5-core GPU, 16-core Neural Engine)
Operating System	Windows 11 Pro	ChromeOS	macOS
Memory	4 GB LPDDR5, 4800 MT/s	8 GB LPDDR5, 4800 MT/s (onboard)	8 GB LPDDR5X, 8533 MHz
Storage	128 GB UFS	64 GB eMMC (onboard)	256 GB internal SSD
Display	11.6-inch, touch IPS, 1366 x 768	14-inch, non-touch FHD+ (1920 x 1200) TN, anti-glare	13-inch, non-touch IPS, 2408 x 1506
Battery	3-cell, 45 Wh	3-cell, 45 Wh	2-cell, 36.5 Wh
Support (3-year)	Dell ProSupport Plus, next-business-day on-site repair after remote diagnosis (Accidental Damage Protection included)	Dell ProSupport Plus, next-business-day on-site repair after remote diagnosis with 3-year Accidental Damage Protection	AppleCare+ for Schools 13-inch MacBook Neo, no service fee
Hardware + 3-yr support cost	$609.59[1]	$574.43[2]	$603.00[3]

Configuration

We compare three similarly priced devices. To match the price of the Apple MacBook Neo, we configured the two Dell devices we priced for the cost model differently than the devices we used as endpoints in our testing of the management tools (see Table 6). Those results would be unaffected by these changes to the endpoints: the Dell Pro Education 11 (2-in-1) device tested had 8 GB memory; the one for the cost model had 4 GB. The Dell Chromebook 14 device used in testing had an N250 processor and 128 GB storage, which is a configuration that is currently not available on the Dell US store; we substituted a configuration with an N150 processor and 64 GB storage for the cost analysis. The 3-year support plans for each platform include accidental damage protection and don't add a per-incident service fee.

Hardware and support cost

Prices reflect institutional pricing at time of testing. Apple prices are sourced from the Apple US Education Institution price list (single-unit equivalent for the five-unit bundle). Dell provided the institution pricing for the two devices we tested.

Cost summary

Overall assumptions

Devices

- Devices have a three-year lifecycle with one-third of the fleet refreshed each year at the end the three-year support plans purchased when the district acquired those systems. New purchases also include three-year support plans with accidental damage protection.
- Device prices, licenses, and IT staff costs hold flat across the three years of this model.
- The district will buy spare devices to replace devices needing repair. New spares are sized at 5 percent of the Dell PC and Chromebook fleets with the assumption that any additional spares can be pulled from the three-year old systems being replaced each year. Spares are at 15 percent for the all-new Apple MacBook Neo fleet—the higher Apple multiplier reflects depot repair turnaround versus Dell's next-business-day on-site service.
- Software licenses and subscriptions:
  - Teachers and staff use Microsoft Office apps in the cloud or on their devices to do their work. Students work with Google Workspace for Education apps.
  - District IT administrators use Microsoft Intune as the MDM to manage the Windows and macOS devices, and to provide visibility into the Google Admin console that it uses to manage the ChromeOS devices. They use Apple School Manager, a free web-based portal, to deploy the macOS devices.

Device management

- We used an IT staffing ratio of 1:500 devices for staffing calculations.

Per-device cost summary

Three-year cost includes the one-time device-and-support charge plus three years of annual license fees per device or user. Apple devices use AppleCare+ for Schools (3-year) bundled into the hardware figure; the Dell PCs and Chromebooks bundle ProSupport Plus with Accidental Damage Protection.

Table 7: A summary of cost information.

Device option	Device + support (one-time)	Other one-time	Annual subscriptions	3-year total
Teachers/staff — Dell Pro Education 11	$609.59	$0.00	$97.99	$903.56
Teachers/staff — Apple MacBook Neo	$603.00	$0.00	$97.99	$896.97
Students — Dell Chromebook 14	$574.43	$35.00	$6.00	$627.43
Students — Apple MacBook Neo	$603.00	$0.00	$6.00	$621.00

Software for faculty and staff

The district provides two subscriptions for faculty and staff, totaling $97.99 per year.

- Microsoft 365 Education A3 subscriptions at $69.00 per year
  - These subscriptions provide the Windows 11 and the Microsoft Office 365 Education A3 software teachers need to do their work. It also provides Microsoft Enterprise Mobility and Security A3 that includes MDM software that IT uses to manage the devices Entra Basic, Entra ID P1, and Intune for Education. Intune for Education includes Microsoft Intune Plan 1, which is the MDM that IT uses to manage all the devices.
- Microsoft Entra Suite for Education Faculty subscription at $28.99 per year (faculty/staff pricing)
  - Microsoft Entra Suite for Education is an add-on to the Microsoft 365 Education A3 subscription that provides centralized identity management and integration with educational applications. IT can use it to reset passwords and assign permissions.

Annual subscriptions and one-time software purchases for students and their devices

The district provides per-device and per-user software for students and their devices:

- For students using Chromebooks, the district subscribes to Google Workspace for Education Plus at $6 per year, per user and provides a one-time ChromeOS Education Upgrade license, which is what IT needs to manage devices with Google Admin console, at $35 per device.
- Students on Apple MacBook Neo devices also use Google Workspace for Education Plus at $6 per year.
- IT manages student Apple MacBook Neo devices via Microsoft Intune Plan 1 (offered at no cost via the Microsoft 365 Education A3 student-use benefit) plus Apple School Manager (free).

Two-platform solution cost

The two-platform solution has teachers/staff on Dell Pro Education 11 and students on Dell Chromebook 14 devices. New spares are sized at 5 percent of each Dell fleet. IT could gather additional spares from among the retired systems. Additional costs cover annual roll-out planning including device and software acquisition, IT admin time on critical management tasks (detailed in the next section) and no IT and teacher training (because both groups are familiar with devices and procedures).

Table 8: Summary of the two-platform solution cost.

Line item	Devices	3-year cost per device	3-year total
New Dell Pro Education PCs (teachers/staff)	4,000	$903.56	$3,614,240.00
New Dell Chromebooks (students)	42,000	$627.43	$26,352,060.00
Dell Pro Education spares (5 percent)	200	$609.59	$121,918.00
Dell Chromebook spares (5 percent)	2,100	$574.43	$1,206,303.00
Additional costs			
Planning ($50 per hour × 3 yrs)	-	-	$7,500.00
IT staff training (none)	-	-	$0.00
IT admin time on critical management tasks	-	-	$24,597.50
Teacher training (none)	-	-	$0.00
Two-platform solution total			**$31,326,618.50**

Three-platform solution cost

For this scenario, half of the teachers/staff move to MacBook Neo devices and half remain on Dell Pro Education PCs; half of the students move to MacBook Neo devices and half remain on Dell Chromebooks. Apple spares are 15 percent of the combined Apple fleet versus 5 percent for the Dell fleets. Additional costs include the same Dell baseline planning costs from the two-platform model plus roll-out planning specific to Apple, IT certification on Apple device management, IT admin time on critical tasks across all three platforms, and teacher training on the MacBook Neo.

Table 9: Summary of the three-platform solution cost.

Line item	Devices	3-yr cost per device	3-yr total
New Dell Pro Education PCs (teachers/staff, 50 percent)	2,000	$903.56	$1,807,120.00
New Apple MacBook Neo (teachers/staff, 50 percent)	2,000	$896.97	$1,793,940.00
New Dell Chromebooks (students, 50 percent)	21,000	$627.43	$13,176,030.00
New Apple MacBook Neo (students, 50 percent)	21,000	$621.00	$13,041,000.00
Dell Pro Education spares (5 percent)	100	$609.59	$60,959.00
Dell Chromebook spares (5 percent)	1,050	$574.43	$603,151.50
Apple MacBook Neo spares (15 percent of combined Apple fleet)	3,450	$603.00	$2,080,350.00
Additional costs			
Planning — Dell baseline (50 hr/yr) + Apple Neo (400 hr) at $50/hr x3 yrs	-	-	$27,500.00
Apple certification training for IT staff ($949 per Apple FTE-equivalent)	-	-	$43,654.00
IT admin time on critical management tasks (3-yr value at $50/hr)	-	-	$101,921.15
Teacher training on Apple MacBook Neo (80 percent of staff × 2 hr × $50 per hour)	-	-	$320,000.00
Three-platform solution total			**$33,055,625.65**

Side-by-side comparison

Table 10: Summary of the two-platform solution and three-platform solution costs.

Solution	3-year total cost
Two-platform (Dell PC + Dell Chromebook)	$31,326,618.50
Three-platform (Dell PC + Dell Chromebook + Apple MacBook Neo)	$33,055,625.65
Two-platform savings vs. three-platform	$1,729,007.15
Savings as percentage of two-platform cost	5.52%

Management cost detail

This section breaks down the "IT admin time on critical management tasks" line in each cost summary. Time-per-task values are measured per-platform from MDM-console testing; frequencies reflect typical district operational cadence (monthly OS patching, quarterly enrollment audits, annual security policy reviews, etc.). The 3-year total seconds in each table multiplied by $50/hr labor cost produces the corresponding cost summary line item.

Two-platform (Windows 11 + ChromeOS) management task frequencies

Table 11: Summary of the two-platform management task frequencies. Time reported in seconds.

Management task	Windows device time	Windows device annual frequency	ChromeOS device time	ChromeOS device annual frequency	Total seconds over 3 years
Verify enrollment status and compliance	9	1,333.33	11	14,000	498,000
Apply device naming convention and asset tag (not supported on Windows 11)	n/a	0	13	14,000	546,000
Deploy a new security policy	69	6	28	6	1,746
Deploy a Wi-Fi configuration profile (fleet)	72	2	40	2	672
Enable and enforce disk encryption (not supported on Chromebook)	93	1	n/a	0	279
Configure BIOS/firmware security policy (fleet)	71	1	27	1	294
Deploy a required app silently to all devices	86	8	44	8	3,120
Remove a deployed app remotely	34	3	25	3	531
Update a deployed app across the fleet (enabled by default for Chromebook)	86	18	n/a	0	4,644
Push an OS update to all devices	25	12	72	12	3,492
Check OS update compliance status across the fleet	73	12	19	12	3,312
Remote lock a device (not supported on Windows 11)	n/a	0	13	210	8,190
Remote wipe a device and confirm re-enrollment	38	1,400	12	14,700	688,800
End-of-year device refresh (wipe, re-enroll, reassign)	148	20	12	1	8,916
Generate device compliance report (teacher/staff segment)	66	12	18	12	3,024
Total seconds over 3 years					**1,771,020**
Total hours over 3 years					**491.95**
3-year IT labor cost at $50 per hour					**$24,597.50**

Three-platform (Windows 11 + ChromeOS + macOS) management task frequencies

To keep the comparison readable, the three-platform table is collapsed to the 3-year seconds contributed by each platform per task (the source spreadsheet's per-platform time and year-by-year frequencies multiply out to these totals). Each platform's column is the time-per-task on that platform multiplied by the 3-year frequency for that platform; the rightmost column is the row total used in the cost summary.

Table 12: Summary of the three-platform management task frequencies. Time reported in seconds over three years.

Management task	macOS device time	Windows device time	ChromeOS device time	Total seconds over 3 years
Apple one-time setup/configuration for Intune	435	n/a	n/a	435
Verify enrollment status and compliance	207,000	18,000	231,000	456,000
Apply device naming convention and asset tag (not supported on Windows 11)	506,000	n/a	273,000	779,000
Deploy a new security policy	1,242	1,242	504	2,988
Deploy a Wi-Fi configuration profile (fleet)	270	432	240	942
Enable and enforce disk encryption (not supported on Chromebook)	285	279	n/a	564
Configure BIOS/firmware security policy (not supported on macOS)	n/a	213	81	294
Deploy a required app silently to all devices	2,040	2,064	1,056	5,160
Remove a deployed app remotely	315	306	225	846
Update a deployed app across the fleet (enabled by default for Chromebook)	4,698	4,644	n/a	9,342
Push an OS update to all devices	3,420	900	2,592	6,912
Check OS update compliance status across the fleet	2,628	2,628	684	5,940
Remote lock a device (not supported on Windows 11)	4,370	n/a	5,460	9,830
Remote wipe a device and confirm re-enrollment	1,497,333	106,387	352,800	1,956,519
End-of-year device refresh (wipe, re-enroll, reassign)	4,092,047	6,068	36	4,098,151
Generate device compliance report (teacher/staff segment)	2,376	2,376	648	5,400
Total seconds over 3 years				**7,338,322**
Total hours over 3 years				**2,038.42**
3-year IT labor cost at $50 per hour				**$101,921.15**

1. Dell provided a quote for hardware and 3-year support cost on 5/22/26.
2. Dell provided a quote for hardware and 3-year support cost on 5/22/26.
3. Apple, "Apple Education Price List (Apple Products) April 1, 2026," accessed May 16, 2026, https://www.apple.com/education/pricelists/pdfs/Apple_US_Education_Institution_Price_List.pdf.

Commissioned by

Dell Technologies

How we created this report

A PT team, which includes the contributors we've listed and others, created this report and performed the technical work behind it.

We used AI to develop the report outline and edit portions of the text.

Primary contributors

Tech: Craig B.

Writing: Ticia I.

Design: Laura K.

PM: Peter H.

Principled Technologies®