A NON-TECHNICAL GUIDE FOR EXECUTIVES

The Modern Endpoint Blueprint

Six practices that let your people work securely from anywhere, on any device, without your IT team touching the hardware — using the Microsoft 365 licenses you already own.

LUMEPLEX
INTELLIGENT IT CONSULTING

Lumeplex · Intelligent IT Consulting
lumeplex.com · 2026 edition

EXECUTIVE SUMMARY

Your devices are the new perimeter. Most companies still manage them like it's 2012.

Laptops, phones and tablets are where your data lives, where your people work and where most breaches begin. Yet a surprising number of growing businesses still run them with a golden image, a VPN, a password and a technician who "comes by the desk". This guide describes a better operating model, in plain language, and shows how to get there in stages.

6
connected practices that make up the Blueprint

0
additional licenses most Microsoft 365 Business Premium or E3 customers need to buy

90 days
a realistic window to move the first three practices from "partial" to "done"

The Blueprint is not a product. Microsoft Intune, Entra ID and Defender are the tools most businesses use to implement it, but the value comes from the design decisions, the rollout discipline and the follow-through. Each of the six practices below answers one business question: *how do we make sure the right person, on a healthy device, can reach the right data, with as little friction and as little IT labor as possible?*

What's inside

How to use this guide. Read pages 3–7 in fifteen minutes. Then hand page 8 to whoever runs your IT — internal or outsourced — and ask them to score each practice honestly. The conversation that follows is the point.

CONTEXT

Why endpoint management changed

For twenty years the corporate PC lived inside a fence. It was built in the office from an image, it joined a domain, it received updates from a server down the hall, and it was trusted because it was on the network. Security meant keeping bad things out of the building.

Three things broke that model. **Work left the building.** Hybrid and remote work made the office network just one place among many, and the least common one for a growing share of staff. **Data left the hard drive.** Email, files and chat moved into Microsoft 365, where they can be searched, shared and leaked from any device. **Attackers stopped hacking in and started logging in.** The typical incident now begins with a stolen or phished password and a device nobody was watching, not with a firewall breach.

The response from Microsoft and the rest of the industry has been a different operating model, usually called *modern management* or *cloud-native endpoint management*. Its core idea is simple: **manage the device from the cloud, verify every access request, and keep the data where it can be protected.** Devices are enrolled over the internet, policies arrive from the cloud, updates arrive from the cloud, and access to company data depends on the health of the device and the identity of the user rather than on which network they happen to be sitting on.

For a large enterprise this is a multi-year program with a dedicated team. For a business with 50 to 1,000 people it is far more approachable, for one reason: **you almost certainly already own the tools.** Microsoft 365 Business Premium, E3 and E5 all include Intune, Entra ID (with Conditional Access), Defender and OneDrive. The gap is rarely technology. It is design, sequencing and follow-through.

That is what the Blueprint is for: six practices you can assess, fund and complete in a sensible order. Each delivers a benefit on its own; together they change how IT feels to your people and how exposed your business is.

Question	Legacy answer	Modern answer
How does a new laptop get set up?	IT images it in the office, then ships it or hands it over	The supplier ships it to the employee; it configures itself on first sign-in
How do updates arrive?	From a server, when the device is on the office network or VPN	From the cloud, anywhere, with deadlines the user can't defer forever
Where does the data live?	On the hard drive, on file servers, in mailbox archives	In OneDrive, SharePoint and Teams — searchable, labeled, backed up

How do people sign in?	Username and password, MFA prompt if you're lucky	Face, fingerprint or PIN on a trusted device — nothing to phish
Who can reach company data?	Anyone on the network, or with a VPN and a password	Verified users on healthy, compliant devices — checked at every request
How does support work?	Someone comes by the desk, or you wait for a callback	Self-service first, remote assistance second, a defined SLA for the rest

THE SIX PRACTICES

Practices 1 and 2: control access, keep devices current

1 Zero Trust access

Every request to reach company data is checked on three things: who the user is, whether their device is healthy and managed, and what they're trying to reach. A device that's missing patches or has an active threat simply doesn't get into SharePoint until it's fixed. In Microsoft terms this is Conditional Access in Entra ID, fed by Intune compliance and Defender risk signals.

What it replaces
The VPN as a security boundary; "if you're on the network you're trusted".

Cost of getting it wrong
A stolen password is enough. Most business-email-compromise and ransomware cases start exactly here.

What "done" looks like
No VPN needed for Microsoft 365. Unmanaged or non-compliant devices are blocked or limited automatically. Exceptions are documented, not accidental.

What you already own
Entra ID P1 (in Business Premium and E3) covers Conditional Access; P2 (E5) adds risk-based policies.

2 Over-the-air updates

Operating systems and applications are updated from the cloud on a schedule you set, with rings (pilot, early, broad) and deadlines. The device that hasn't been in the office for four months is as current as the one on the CEO's desk. Windows Autopatch and Intune update rings handle Windows; Intune and Apple Business Manager handle macOS, iOS and iPadOS; Android Enterprise handles Android.

What it replaces
WSUS and Configuration Manager update servers that only reach devices on the corporate network; "please connect to VPN to receive updates" emails.

Cost of getting it wrong
Remote staff become the least-patched and most-exposed people in the company. Compliance reports you can't trust.

What "done" looks like
A dashboard showing patch compliance you'd be comfortable putting in front of an auditor. Third-party apps (browsers, Zoom, Adobe) patched, not just Windows.

What you already own
Intune and Autopatch are included in Business Premium, E3 and E5. Third-party patching may need a small add-on or a partner tool.

A note on order. Practices 1 and 2 depend on each other. Conditional Access can only require a healthy device if updates are actually reaching devices, and update deadlines only bite if non-compliant devices lose access. Plan them together.

THE SIX PRACTICES

Practices 3 and 4: protect the data, retire the password

3 Cloud data

Company data lives in OneDrive, SharePoint and Teams rather than on hard drives and ageing file servers. The practical work is redirecting Desktop and Documents into OneDrive (Known Folder Move), setting sensible sharing defaults, and applying sensitivity labels through Microsoft Purview to the categories that matter — contracts, client records, financials.

What it replaces
Local files, USB drives, personal cloud accounts and the file server nobody wants to touch.

Cost of getting it wrong
A lost laptop is an incident, not an inconvenience. Departing employees walk out with data. Copilot and search surface files that were never meant to be found.

What "done" looks like
A replacement device is productive within an hour, files already there. Sharing outside the company is deliberate and visible. Labels are applied to the handful of categories that carry real risk.

What you already own
OneDrive and SharePoint in every plan; Purview Information Protection in Business Premium (basic) and E5 (advanced).

4 Passwordless sign-in

People sign in with a face, a fingerprint or a PIN that is tied to a specific trusted device, using Windows Hello for Business, passkeys in Microsoft Authenticator, or FIDO2 security keys. There is no shared secret to phish and nothing to reuse across sites. Push-notification MFA — "approve this sign-in?" — is a stepping stone, not a destination; attackers now routinely defeat it by wearing users down.

What it replaces
Passwords, password rotation policies, and MFA prompts that people approve without reading.

Cost of getting it wrong
Credential phishing keeps working. Help-desk time goes to password resets. Executives get "MFA fatigue" attacks aimed squarely at them.

What "done" looks like
Phishing-resistant sign-in is the default for everyone, not a special setup for the IT team. Password-reset tickets drop sharply. A phished password on its own gets an attacker nothing.

What you already own
Windows Hello for Business, Authenticator passkeys and FIDO2 support are in Entra ID at every tier. Hardware keys are an optional purchase for high-risk roles.

Why 3 comes before 4. Passwordless is far easier to roll out once devices are managed and data is in the cloud, because the trusted device becomes the credential. Organizations that try to go passwordless on unmanaged laptops end up with exceptions everywhere.

Practices 5 and 6: stop touching devices, modernize support

5 Zero-touch provisioning

A new laptop ships from the supplier straight to the employee and becomes a fully configured, compliant company device on first sign-in. Nobody in IT unboxes it. Windows Autopilot, Apple Business Manager and Android Enterprise all register the device to your tenant at the factory or reseller; Intune applies your policies, apps and settings when the user signs in. The same mechanism turns a departing employee's laptop into a clean device for the next hire with a remote wipe.

What it replaces
Golden images, imaging benches, a box of laptops in the IT closet, and a technician's afternoon for every new starter.

Cost of getting it wrong
Onboarding takes days. Remote hires wait for a device to be built and shipped twice. Every device is slightly different because a human set it up.

What "done" looks like
Onboarding a remote hire means shipping a box. Devices are identical because policy built them. Your supplier registers devices to your tenant before they ship.

What you already own
Autopilot, Apple Business Manager and Android Enterprise are free with Intune. Business-class devices support it out of the box.

6 Modern remote support

The practice most often forgotten. If the first five are in place but people still wait two days for someone to "come by the desk", the experience hasn't modernized. Modern support is self-service first (Company Portal for approved apps, self-service password and PIN reset), remote assistance second (Intune Remote Help, with user consent and an audit trail), and human help with a defined response time when it's really needed.

What it replaces
Desk-side visits, ad-hoc screen-sharing tools, and a support model that assumes everyone is in the building.

Cost of getting it wrong
Remote staff feel like second-class employees. Simple problems consume expensive engineering time. Nobody knows how long a real issue will take to be picked up.

What "done" looks like
Routine requests are self-served. Remote assistance works on any managed device anywhere. Response and resolution targets are written down and reported on.

What you already own
Company Portal and self-service reset are included. Remote Help is a small per-user add-on or part of the Intune Suite.

> **For a growing business** this does not mean a 24/7 operations center. It means business-hours support with clear commitments, delivered by people who know your environment — internal, outsourced or a mix.

SEQUENCING THE JOURNEY

A three-phase roadmap that doesn't disrupt the business

You do not need to do all six practices at once, and you shouldn't. The order below is the one we use with most clients because each phase makes the next one cheaper and safer.

Phase 1 — Foundations (weeks 1–6)

Goal: know what you have, and get every device managed and current. Inventory devices, users and applications. Enroll existing devices in Intune (most can be enrolled in place, without wiping). Switch on update rings with a pilot group first. Move Desktop and Documents into OneDrive. Turn on the security defaults that cost nothing: MFA for everyone, legacy authentication blocked, admin accounts separated from daily accounts.

Practices advanced: 2 (updates), 3 (cloud data), groundwork for 1.

Phase 2 — Trust (weeks 6–12)

Goal: make device health and identity the gate to company data. Define compliance policies (encryption on, patches current, Defender running). Introduce Conditional Access in report-only mode, review the impact, then enforce for pilot groups and finally everyone. Roll out Windows Hello for Business and Authenticator passkeys, starting with the people attackers target first: finance, executives, IT.

Practices advanced: 1 (Zero Trust access), 4 (passwordless).

Phase 3 — Automation (weeks 12–20)

Goal: stop touching devices and make support predictable. Configure Autopilot and Apple Business Manager with your supplier so new devices arrive pre-registered. Publish a Company Portal catalogue of approved apps. Enable Remote Help. Write down and communicate support hours and response targets. Retire the imaging bench.

Practices advanced: 5 (zero-touch), 6 (modern support).

Phase	Business risk during the phase	How we keep it low
Foundations	Devices enrolled with the wrong policy; update reboots at bad times	Pilot groups; report-only first; deadlines with generous grace periods; change windows agreed with the business
Trust	People locked out of email by a Conditional Access rule	Report-only mode for two weeks; break-glass accounts; staged enforcement; a named person on call for the first days
Automation	A new starter's device fails to provision on day one	Test every device model end to end before go-live; keep one manual fallback for the first month

> **What this costs in people's time.** For a 100–300 person organization, Phase 1 and 2 typically need one experienced engineer part-time for three months plus a few hours a week from whoever owns IT internally. The most common reason projects stall is not budget; it is that nobody owns the decisions. Assign an owner before you start.

SELF-ASSESSMENT

Where do you stand today?

Score each practice honestly: **Not started**, **Partial** (switched on for some people or some devices, or on but never reviewed), or **Done** (enforced for everyone, documented, and reported on). Most organizations we meet have two or three practices at "Partial" — usually the ones that were turned on during a Microsoft 365 migration and never revisited.

Practice	The test	Score
1. Zero Trust access	Could someone with a stolen password, on their own laptop, open your SharePoint right now?	☐ Not started ☐ Partial ☐ Done
2. Over-the-air updates	Can you show, today, what percentage of laptops have this month's patches — including the ones that haven't been in the office?	☐ Not started ☐ Partial ☐ Done
3. Cloud data	If a laptop were stolen tonight, would anything on it be lost or exposed?	☐ Not started ☐ Partial ☐ Done
4. Passwordless sign-in	Do your executives and finance team sign in with something that cannot be phished?	☐ Not started ☐ Partial ☐ Done
5. Zero-touch provisioning	Does anyone in IT unbox a new laptop before the employee does?	☐ Not started ☐ Partial ☐ Done

6. Modern remote support	Is your response time for a locked-out remote employee written down anywhere?	☐ Not started ☐ Partial ☐ Done

Questions to ask your IT team or provider

- ☐ Which of our Microsoft 365 licenses include Intune, Conditional Access and Defender — and which of those are we actually using?
- ☐ How many of our devices are enrolled in management today? How many are we not sure about?
- ☐ What happens, step by step, when a new remote employee starts? How many people touch the laptop?
- ☐ If a user's password were phished tomorrow, what would stop the attacker?
- ☐ When did we last review our Conditional Access and compliance policies? Who owns them?
- ☐ What is our target response time for a support request, and did we meet it last month?

> **A useful rule of thumb.** If the answer to any question is "it depends who set it up", that practice is at Partial, however good the technology underneath it is.

ABOUT LUMEPLEX

Enterprise-grade Microsoft expertise, built for growing businesses

Lumeplex is a Microsoft-focused IT consultancy based in Dallas, Texas. Our team spent more than a decade designing and running endpoint, identity and security environments for large, regulated organizations in healthcare, legal and financial services — much of it alongside some of the country's largest IT service providers. We bring the same architecture-led, phased approach to businesses that can't afford to get technology wrong but don't need a big consultancy to get it right.

How we can help with the Blueprint

Modern Endpoint Assessment. A scored review of all six practices against your environment, with a prioritized roadmap and licensing check. Delivered remotely in two to three weeks.

Intune Deployment & Migration. Design, build, pilot and hand-over for Windows, macOS, iOS and Android — including migrations from Configuration Manager and other management tools.

Managed Services. Ongoing Intune, Microsoft 365 and security management with business-hours support and defined response SLAs, so the practices stay "Done" after the project ends.

Every engagement includes documentation and knowledge transfer, so your team owns the environment — not us.

Book a scoping session at lumeplex.com/contact