

Endpoint Protection Readiness Checklist

17 checks for every laptop, phone, tablet, and server that touches your business data.

How to use it: mark where your business stands today on each statement. **In Place** = established and consistently followed. **In Progress** = some groundwork done, gaps remain. **Not Yet** = not addressed. **N/A** = doesn't apply. Items marked ★ are critical: they're the device gaps attackers exploit first and cyber insurers ask about, so they can't be marked N/A.

STATEMENT	IN PLACE (2)	IN PROGRESS (1)	NOT YET (0)	N/A
1. Device Coverage & Visibility				
★ You have a complete, current inventory of every computer, phone, tablet, and server that accesses company data.	☐	☐	☐	—
Every company device, including Macs, iPads, and phones, is enrolled in central management, not just Windows computers.	☐	☐	☐	☐
Personal devices must meet baseline protections (a passcode, encryption, and a way to remove company data) before they can access company email or files.	☐	☐	☐	☐
Every managed device is monitored, so one that goes offline, falls behind on updates, or loses protection gets noticed.	☐	☐	☐	☐
2. Threat Protection & Response				
★ Every computer and server runs protection that detects threats in real time, not signature-based antivirus alone.	☐	☐	☐	—
★ Someone can respond to a threat at any hour, including isolating an infected device or disabling a compromised account.	☐	☐	☐	—
Security alerts are reviewed by a person, not just logged and left in a dashboard.	☐	☐	☐	☐
3. Patching & Configuration				
★ Security updates are applied at least monthly, on a defined schedule, instead of being left to each employee.	☐	☐	☐	—
Devices that miss updates are tracked and followed up on, not assumed to be current.	☐	☐	☐	☐
Operating systems that no longer receive security updates have been replaced or isolated.	☐	☐	☐	☐
Everyday users work without local administrator rights on their devices.	☐	☐	☐	☐
4. Data Protection & Lost Devices				
★ Full-disk encryption is enforced on every laptop and mobile device.	☐	☐	☐	—
★ Any lost or stolen device can be remotely locked or wiped as soon as the loss is reported.	☐	☐	☐	—
Every device requires a passcode or password and locks automatically when left idle.	☐	☐	☐	☐
5. Device Lifecycle & Evidence				
New devices are enrolled, encrypted, and protected before anyone uses them for work.	☐	☐	☐	☐
★ When an employee leaves, their access is shut off and their company devices are recovered or wiped the same day.	☐	☐	☐	—
You could show a cyber insurer documentation of device coverage, patching, and encryption today.	☐	☐	☐	☐

Score Your Results

1. Add up your points (In Place = 2, In Progress = 1, Not Yet = 0): _____
2. Multiply the number of statements you didn't mark N/A by 2: _____
3. Divide step 1 by step 2 and multiply by 100 for your score: _____ %

80%+

Strong Endpoint Protection

Your devices appear to have the core controls in place. The next step is keeping it that way as devices and staff change, and being able to prove it when an insurer or client asks. CelereTech can help you document it.

60-79%

Real Gaps Worth Closing

You have meaningful protections in place, but the gaps here are the ones attackers and cyber insurers look for first. Closing them now costs far less than dealing with them after a lost laptop or an incident.

0-59%

High Endpoint Exposure

Several baseline device protections are missing. These are the gaps ransomware and account takeovers most often exploit, and the ones cyber insurers ask about. CelereTech can help you close them quickly, starting with the most critical.

Any ★ item marked **Not Yet** deserves attention first, no matter how high your total score is. Each one is a specific gap that turns a lost laptop, a stolen password, or a missed update into an incident.

What Good Looks Like

A strong endpoint program covers every device type, not just Windows computers: Macs, iPads, iPhones, Android phones, and servers. Devices are patched at least monthly on a schedule, encrypted, able to be locked or wiped the moment one goes missing, and watched closely enough that a threat at 2 a.m. gets a response before morning. When someone leaves, their access ends the same day.

Score It Online and Get Your Results by Email

Take this checklist online for an instant score and a prioritized plan from CelereTech:

celere.tech.com/endpoint-protection-readiness-checklist

Learn what each item means and how managed endpoint protection works:

celere.tech.com/services/cybersecurity/guides/managed-endpoint-protection

Talk to us: (847) 658-4800 · [Get a free IT assessment](#)