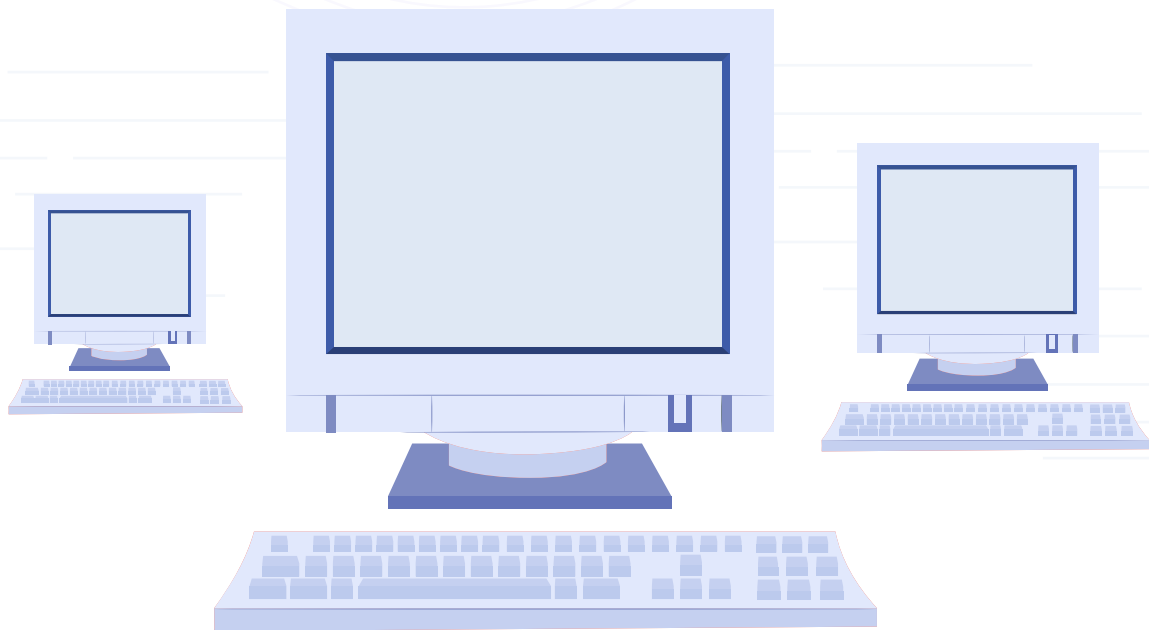


Stuck with legacy devices? Endpoint Central helps you modernize

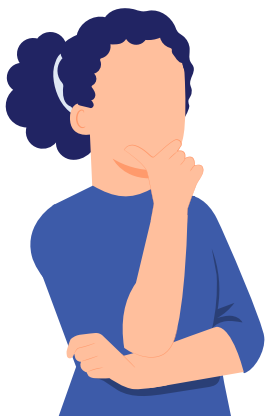




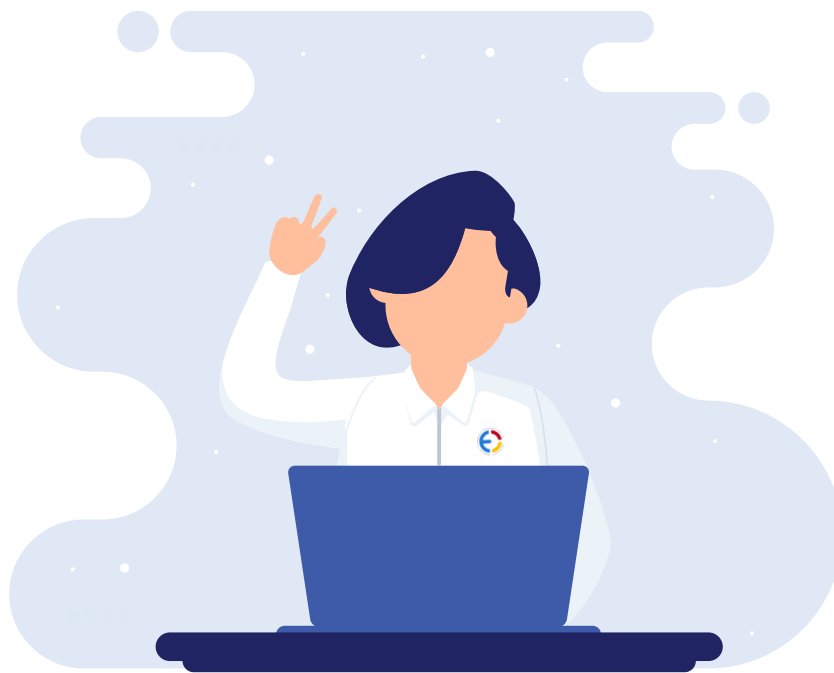
Introduction

Bill Gates once famously said, "Legacy is a stupid thing! I don't want a legacy." But enterprises do not see legacy devices that way. Business leaders often are risk averse and take the philosophy of "if it's not broken, don't fix it" to heart. For example, the massive disruption in flight operations during January 2023 was due to the **prolonged usage** of outdated hardware in the pilot alert system, despite a clarion call several years ago from experts and officials to replace it with sophisticated tools.

Even with IT leaders having the best intentions to modernize, they often prioritize cost saving and keep these upgrade or modernization decisions on the back burner. It's often a difficult choice between the up-front expense of upgrades and the growing necessity of those upgrades.



- ♦ As of April 2023, **3.78% of all Windows desktops** still run on Windows 7.
- ♦ CentOS continues to command a **market share of 8.1%** for all websites running on Linux distros, despite being discontinued in 2021.
- ♦ Microsoft has announced end of support for Windows 10 by 2025,



So, how does Endpoint Central come into the picture?

While each IT decision maker and CISO takes time to strategize for modernization, their enterprise needs a solution capable of managing a broad range of devices and OSs—especially the legacy ones. Endpoint Central helps your enterprise based on these two pillars.

01

Secure and manage legacy systems until you replace them: Endpoint Central offers vulnerability and threat management, patching for legacy OS and applications, asset management, user access control, admin privileges management, and much more.

02

Acting as a bridge to modernize legacy systems: Endpoint Central is compatible with legacy and modern devices. So you don't have to search for alternate UEM solutions when you upgrade your IT.

1

Understand the criticality of the legacy devices in your environment:

To truly understand the criticality of legacy devices in your day-to-day operations, you need both a granular and a bird's-eye view of your IT enterprise. Endpoint Central offers these by providing for:



Operating systems available in your IT: Know granular-level details about your endpoints operating on legacy OSs.

Age of the endpoints: Classify endpoints based on how long they have been in your enterprise.

Software details: Track the legacy software present in your network.

Warranty tracking: Know the warranty details of your endpoints.

Windows 11 compatibility: Scan your network for devices capable of upgrading from the legacy OS to Windows 11.

2

Legacy or modern, Endpoint Central supports your patches:

Did you know that, as of 2020, **75% of the global ATM network** runs on Windows 7? Besides simply dispensing money, ATMs are a part of a bank's Core Banking systems. Microsoft has also announced that it will end support for Windows 10 by 2025.



Did you also know that 68% of all the organizations that have suffered **ransomware** attacks didn't have an effective vulnerability and patch management process in place? This highlights the importance of patching and updating legacy OS and applications.

Using Endpoint Central, you can:

Patch legacy endpoint OSs and server OSs. If patch support ends for an OS, you can still patch the applications in those legacy systems.

Monitor high-risk software: Track the legacy software's expiration date along with the number of days left before expiration.

Quarantine the End-of-Life OS endpoints using Network Access Control.

3

Legacy devices could be the weakest link in your security chain: Strengthen them using security configurations



Security is the biggest reason why an enterprise should upgrade from legacy devices. According to [Morphisec](#), endpoints with legacy OSs are often part of the core operational backbone of an organization, and it is challenging to take them offline for an upgrade, especially in healthcare, finance, and manufacturing enterprises.

At ManageEngine, we understand how critical this issue is. Endpoint Central can help you:

Configure firewalls in legacy devices.

Monitor high-risk software: Track the legacy software's expiration date along with the number of days left before expiration.

Configure password policies, strengthening the security of legacy endpoints and preventing insider threats and brute-force attacks.

Prevent data leakage from USB devices by implementing a Zero Trust model. Create a list of verified peripheral devices for transferring data to and from your legacy endpoints.

Manage privileges with user account control: Revoke administrative rights to unintended users and enforce the principle of least privilege.

Ensure that end users do not ignore certificate errors, enable safe browsing, restrict unsecured plugins, disable automatic file downloads, and manage add-ons for Internet Explorer.

Harden [legacy OS security](#).

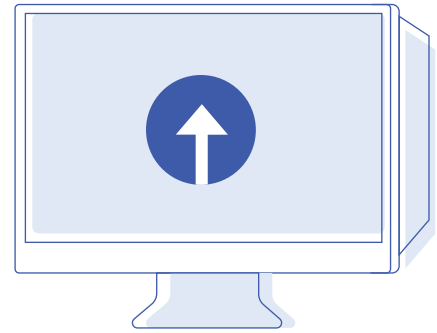
Allowlist and blocklist applications, and restrict user privileges to these applications in legacy endpoints.

Disable legacy protocols like Telnet, SMB, SNMP, and TFTP, which might make your IT more vulnerable to threats and provide hackers access to your network.

4

Seamlessly upgrade your legacy OS to a modern OS using Endpoint Central's OS Deployer

Now that the management and security of the legacy devices is taken care of, it is essential to migrate to a modern OS. Endpoint Central's OS imaging and deployment feature helps with:



Zero-touch deployment of the OS of your choice.

Hardware-independent deployment. Never worry about having multiple computer brands in your enterprise.

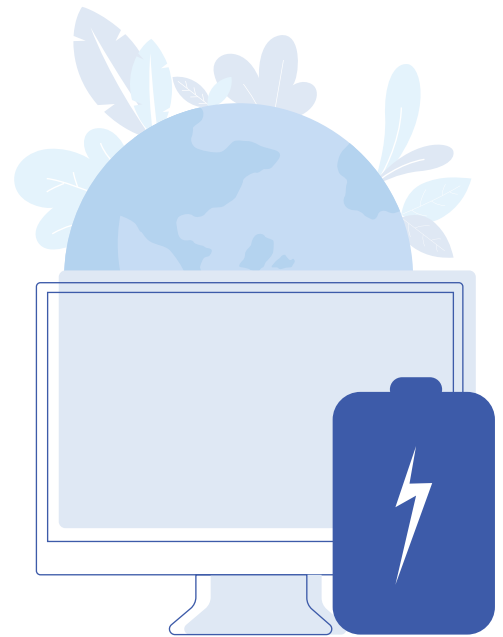
User profile migration. Cut down the time required to customize user profiles in new computers so that users can start being productive on day one of migration.

5

Conserve power while modernizing

Realizing the value of energy saving, both in terms of money and from the perspective of climate change, we have [written in depth](#) about how having configurable power management policies could save a lot of expenses for your enterprise.

If your organization uses legacy hardware like CRT monitors and bulky server machines, Endpoint Central helps you reduce costs by:



Adjusting the brightness of your display or turning it off when not in use.

Remote shutdowns.

Keeping the systems in sleep mode.

Turning off only the hard disk and more.

But what happens after you modernize? Will Endpoint Central help you manage and secure your modern devices?

Absolutely! Many of our competitors are focused on the next big thing in the market without realizing that bringing a change, such as **modernizing IT, is one of the biggest obstacles enterprises face.**

At ManageEngine, we've designed our **UEM solution** to alleviate this pain point and make the transition much smoother.

Endpoint Central can manage devices spanning from Windows 7 to Windows 11. It leverages both client and modern management capabilities. This broad support is intended to help the enterprises modernize in a phased, planned, and gradual manner.

Remember that **modernization is not a one-time activity.** Your enterprise will most likely deal with end of life for various endpoints and at various times.

Envisioned to serve enterprise IT nearly two decades ago, our **UEMS solution now manages over 20 million endpoints and serves 25,000 customers worldwide.** Ready to get started? Manage and secure endless endpoints for free for 30 days.

TRY OUT NOW