Kaseya®

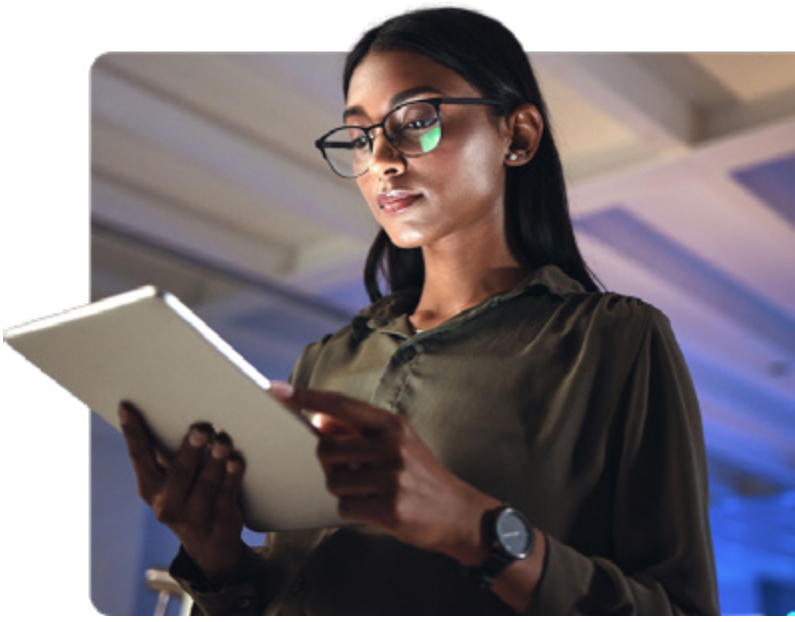
BUYER'S GUIDE

How to choose the right endpoint management solution

Table of contents

Introduction

Every business runs on endpoints. Laptops, desktops, servers and network devices must stay healthy and secure so people can do their work from anywhere. Teams need a single place to see what is happening, fix issues fast and automate routine tasks. This guide explains what to look for in an endpoint management platform and how to compare vendors with confidence.



How to read this guide

This guide is designed to help you make a confident decision without wasting time on noise. Each section builds on the last, so you can move from understanding the essentials to running a structured evaluation.

- **Scan the core capabilities** – Identify which features are must-haves for your business versus what's nice to have. Every environment is different, so knowing your priorities upfront saves time later.
- **Use the buying checklist** – Keep it handy during vendor demos and free trials. It gives you a clear, side-by-side way to compare solutions and ensure nothing important is missed.
- **Follow the evaluation plan** – A step-by-step approach that shortens the decision cycle, keeps your team aligned and helps avoid second-guessing.

By the end, you'll have a clear picture of what matters most to your business and the tools to choose the right endpoint management solution with confidence.

What modern endpoint management means

A modern endpoint management platform gives you centralized control with strong automation. It brings the key tools together so technicians can work from one console rather than juggling multiple windows. Look for simple workflows, fast ramp for new users and reliable operation at scale.

Key capabilities to look for

Not every solution will be right for your business. An endpoint management platform with the following set of core capabilities will make daily operations smoother, reduce technician effort and scale with growth. Use these as your baseline when comparing options.

Ease of use and deployment

The tool helps technicians work more efficiently and is simple to implement. A good user experience reduces training time and burnout.

- Clean interface with easy navigation and quick drill down into asset details
- Customizable dashboard with status across devices and apps
- Fast setup with sensible defaults and help for common tasks
- Modern communication between agent and server using reliable APIs
- Multitenant scale for providers and simple separation for business units

Scalability

Growth should not force a platform switch. The system must handle large fleets on a single service.

- Support for thousands of endpoints per instance
- Elastic performance for remote workers and branch offices
- Role-based access that matches how your teams work

Discovery and inventory

You cannot manage what you cannot see. Discovery should be automatic on the network and through your directory. Inventory must stay current without manual effort.

- LAN and domain discovery with continuous sync to your directory
- Automatic agent deployment where allowed
- Rich hardware details, such as manufacturer, model, serial and memory
- Rich software details, such as operating system, application and license data

Automated patch and vulnerability management

Patching is one of the most valuable controls for risk reduction. Automation removes delay and human error.

- Central control of patching for operating systems, browsers and common apps
- Scheduled scans for missing updates with clear reporting
- Policy to handle maintenance windows and reboots
- Coverage for devices on network and remote
- Compliance reports that are easy to share with auditors or clients

Remote monitoring and management

Technicians should fix issues without disrupting users whenever possible and should have deep visibility when they need it.

- Secure remote access that works over low-bandwidth links
- Behind the scenes troubleshooting so users can keep working
- One-click switch to a full remote-control session when needed
- Admin level access without handling local credentials
- Script execution, registry edits and command line access from one place
- Alerting and auto-remediation driven by policies and events

Policy-based automation

Standardize management across groups of machines and let the system do the repetitive work.

- Policies for device groups, such as servers, user laptops or specialized roles
- Simple yet powerful scripting with a shared library you can reuse
- Run automation from the console, the service desk or the mobile app

Endpoint and network monitoring

See the whole environment in one place. A topology view helps you find root cause fast and reduces finger-pointing.

- Visualization of discovered devices, including SNMP devices
- Up/down status at a glance with quick access to asset details
- Zero-configuration monitoring for common network devices
- Create alarms, tickets, emails or scripts when an event occurs

Integration with IT documentation tool

Keep asset details and procedures in the same place where technicians work so they can resolve issues faster and with fewer steps.

- View documentation, passwords and related assets from inside the console
- Update asset information in real time
- Run automation from the documentation tool when appropriate

Integration with service desk

Technicians should be able to move from a ticket directly to the device without switching tools. This streamlines workflows and helps close tickets faster.

- Automatic sync of asset records between the endpoint platform and the service desk
- Jump from a ticket into remote management for the affected device
- Platform-generated tickets for detected issues to reduce manual triage
- Trigger automation from within the ticket to resolve known problems

Integration with AV, AM and backup and recovery

Security and resilience are strongest when your endpoint management platform works hand in hand with antivirus, anti-malware and backup tools. When these systems share status and actions, you gain a single view of protection across your IT ecosystem.

- Central visibility of endpoint security status for both local and remote users
- Deploy and manage security clients from the same console
- See backup alerts and status in one view for faster recovery decisions

Mobile application

Work does not pause when you leave your desk. A mobile app should support quick checks and urgent fixes.

- View asset information on your phone
- Run approved scripts from the app
- Work tickets in the same app with context from the device

Complete IT management platform

If you've ever juggled three different tools just to close one ticket, you know the pain of a fragmented stack. You start in the service desk, copy details into your endpoint tool and then log into a separate system to check backup status — all while the clock is ticking and the user is waiting. Multiply that by dozens of tickets a day, and it's no wonder IT teams feel stretched thin.

A complete endpoint solution changes that. You can click on a ticket and immediately see the device's history, current alerts and backup status in the same window. Need to reset a password or push a patch? You can do it right there without switching screens. Documentation stays linked to the device record, so you don't waste time digging through outdated notes.

The impact is immediate — fewer errors slipping through, and issues get resolved faster. MSPs see the payoff in stronger margins and satisfied clients, while internal IT teams gain back hours and can finally focus on projects that push the business ahead.

Endpoint management buyer's checklist

Use this list during vendor demos to make sure the solution includes the features you need.

Capabilities

- [ ] Easy-to-use interface and quick deployment
- [ ] Scales easily to handle your device count and growth
- [ ] Automatic discovery with detailed inventory
- [ ] Automated patching with compliance-ready reporting
- [ ] Secure remote access plus full remote control
- [ ] Policy-based automation with a reusable script library
- [ ] Monitoring with real-time alerts and quick actions
- [ ] Built-in integration with IT documentation
- [ ] Smooth integration with your service desk
- [ ] Integration with antivirus and security tools
- [ ] Integration with backup and recovery
- [ ] Mobile app for on-the-go management

Evaluation plan

A structured evaluation keeps the process fair and focused. Instead of relying on vendor promises, test real-use cases in your own environment and measure the results against what matters most to your team.

- [ ] Pick three use cases, such as patch rollout, new laptop setup and remote fix for a common issue
- [ ] Shortlist two or three vendors that meet the core capabilities
- [ ] Test the solution on a small group of devices that represent your environment
- [ ] Measure technician effort, patch success and ticket resolution time
- [ ] Review security and backup integrations and confirm the data flows you need
- [ ] Confirm reporting for leadership and for clients if you are an MSP
- [ ] Ask about roadmap, release cadence and customer support model
- [ ] Document total cost and any growth triggers so there are no surprises

Total cost and value reminders

When comparing vendors, look beyond the license fee. Factor in the hidden costs and the real value gained from efficiency, risk reduction and tool consolidation.

- [ ] License cost for the endpoint platform and any required add-ons
- [ ] Implementation and training effort
- [ ] Time saved per technician from automation and integrations
- [ ] Risk reduction from faster patching and consistent policy
- [ ] Cost avoided by consolidating overlapping tools

Where Kaseya VSA fits

Kaseya VSA is built to solve the exact challenges IT teams face every day — tool sprawl, repetitive tasks and the constant demand to do more with less. What sets it apart is how it brings the essentials together in one place. A 4-in-1 solution that combines remote control, patch and software management, endpoint monitoring and executive reporting into one easy-to-use platform.

This consolidation gives you better outcomes:

Greater efficiency

automate routine tasks and increase efficiency by up to 50%

Stronger security

manage and protect every endpoint without gaps between tools

Lower costs

replace overlapping licenses with one unified solution

Consistent results

ensure patches, tickets, and reports get handled the same way, every time

VSA gives IT teams something most tools don't: control. Control over endpoints, over workflows and over how time is spent. One console. One platform. All the essentials handled.

Making the right choice

Choosing an endpoint platform is a strategic move. Focus on usability, automation, security, integration and scale. Use the checklists and plan above to compare options and select a system that helps your team do more with less effort. When you are ready for a demo, add Kaseya VSA to your shortlist and test it against your top use cases.

Book a demo

kaseya.com