Kaseya 365
Endpoint

EBOOK

Endpoint management solution buyer's guide

Table of contents

Introduction **3**

Features to look for in an endpoint management and security solution **4**

Ease of use and deployment 4

Scalability 5

Discovery and inventory 6

Automated patch and vulnerability management 7

Robust remote monitoring and management 8

Intelligent IT automation 9

Endpoint and network monitoring 10

Integration with service desk 11

Integrated IT documentation tool 12

Unified antivirus and EDR for enhanced security 13

Unified backup from a single pane of glass 14

Complete IT management platform 15

The ultimate IT management solution for your unique needs **16**

Conclusion **17**

Introduction

IT teams, whether at an MSP or internal departments, have more on their plates than ever. They're responsible for keeping hundreds of endpoints connected, secure and running smoothly.

The scale of that challenge is clear in the numbers. The Kaseya 2025 MSP benchmark survey found that 32% of technicians now manage more than 750 endpoints. Meanwhile, the share handling between 251 and 500 endpoints has climbed from 17% in 2024 to 21%.[i]

Against this backdrop, relying on a patchwork of solutions is no longer viable. Fragmented systems slow down operations, create inefficiencies, prevent businesses from scaling and open dangerous security gaps.

This is why the need for modern endpoint management and security solutions has never been more important. It's not just about automating patching. It's about having centralized oversight, real-time control, automation that removes repetitive tasks and built-in security that doesn't slow teams down.

Just as importantly, it should connect seamlessly with the other tools IT teams use. The best platforms feel intuitive to use, streamline day-to-day work and continue to evolve as new challenges emerge.

The most effective platforms strike this balance.

32%

of technicians reported managing more than 750 endpoints

To manage endpoints effectively, internal IT teams require a centralized solution that can efficiently manage software updates across complex environments, provide real-time visibility and control of the IT environment, automate common IT processes and enhance endpoint security. In addition to this, modern endpoint management and security solutions must offer seamless workflow integrations with all the other key IT and security management functions.

Features to look for in an endpoint management and security solution

Ease of use and deployment

A robust solution is the foundation of successful IT management. If it isn't easy to use, it can lead to frustration, burnout, employee turnover and significantly reduced productivity.

Even enterprise-class endpoint management and security tools can be difficult to configure, often forcing businesses to spend heavily on consultants for deployment — yet professional help still doesn't guarantee the system will work as expected.

Consider questions like these before purchasing an endpoint management and security solution:

Can you easily view the status of all endpoints?

Can you configure devices quickly according to a standard corporate policy?

Is it easy to find the functions you're looking for in the application?

Does it have a modern user interface (UI) that delivers a good user experience (UX)?

Can you manage endpoints, patching, EDR, AV and backup from a single pane of glass?

Today's IT environments are complex. Your endpoint management and security solution should make your life easier, not harder. Look for a solution that provides an intuitive UI that enables your technicians to ramp up quickly and work efficiently on an ongoing basis.

Some important UI features to look for include:

A customizable dashboard view that enables complete visibility of all endpoints, applications, security alerts and backup status information in an easy-to-understand layout.

Easy navigation within the application so you can find what you're looking for with just a few clicks.

A quick drill-down into the details of assets and endpoint agents.

A single pane of glass experience for all essential endpoint management and security functions.

Scalability

As your organization or client base grows, the number of endpoints in your network increases. To manage this expanding ecosystem and the resulting network complexity, technicians need a scalable endpoint management and security solution that meets all the business needs both today and in the future.

A Software-as-a-Service (SaaS) endpoint management solution should be able to support tens of thousands of endpoints on a single instance. This gives MSPs and midsize businesses a lot of room for growth without worrying about overextending their endpoint management solution.

Look for a solution that is easy to configure and deploy in your environment. More often than not, the vendor will provide basic implementation services at a relatively low cost to help you get the tool up and running within a very short period, usually a few weeks.

Scalability features to look for include:

Robust granularity in filtering capability with saved views.

Efficient endpoint agent-to-server communication using REST APIs.

Multitenant scalability.

Unified endpoint management and user management in the same UI.

Powerful but easy automation to auto-remediate everyday tasks and tickets.

Discovery and inventory

The endpoint management tool should discover all endpoints on the IT network and automatically deploy an agent to each. Two approaches to discovery are helpful: Network (LAN)-based and Domain Discovery. The latter approach allows the endpoint management solution to automatically discover Active Directory (AD) domains and stay in sync with all domain changes. Best-in-class endpoint management and security solutions let you discover, manage and protect endpoints and users from one platform. If your team or clients use Microsoft 365, the solution should integrate with it seamlessly and make management simple.

The discovery function should collect comprehensive IT asset information for the device, including hardware, software and user data, which typically includes:

Hardware information:

- Manufacturer, model, serial number.
- Bus speed, chassis type.
- CPU/processor family, manufacturer, clock speed.
- Memory installed, max memory size and number of slots.

Software information:

- Operating system, version, edition.
- Application name, manufacturer, version, edition, license.
- Application directory path.

User information:

- Name, email, company.
- Groups, roles, software licenses.
- MFA status, risk level, last login.

Automated patch and vulnerability management

Timely patching keeps your and your clients' IT environments safe from attacks and ensures systems perform at their best. However, without automation, patching quickly becomes a slow, manual process that also increases security risks.

A study by Adaptiva and the Ponemon Institute found that 59% of IT teams take at least two weeks to start deploying a patch after it's released. From a cybersecurity perspective, two weeks is long enough for a threat actor to exploit a vulnerability and cause irreparable damage.[ii]

The research also revealed that 44% of patches are handled on an ad hoc basis, with no clear process or schedule. That means teams are reacting as issues come up instead of following a consistent patching strategy. This approach not only slows down the process but also increases the risk of errors and missed updates. Only 31% of organizations use automation.

An endpoint management and security tool with automated patching applies updates on time, closes security gaps fast and lightens the team's workload. Instead of repeating the same manual steps, your team can focus on strategic projects while staying confident that your systems are protected.

Features to look for include:

- Automated patch management from a centralized console.
- Patching of operating systems, browsers and all third-party applications.
- Automated, scheduled scanning of devices for missing patches.
- Risk-based patching and vulnerability management.
- Patching of both on-and off-network devices (especially important for work-from-home users).
- Patch compliance reporting to ensure adherence to company policies.

Robust remote monitoring and management

With a dispersed workforce, your team and clients may be spread across many locations. That makes it essential to access and manage remote, off-network devices.

Remote management makes this possible. It lets you reach endpoints from anywhere, resolve issues quickly and keep systems running 24/7 with minimal downtime.

A unified endpoint management and security solution with strong remote monitoring and management (RMM) capabilities helps you cut travel time and costs while boosting your IT team's productivity.

The right tool should also help you stay ahead of issues. It should monitor endpoint events in real time, quickly identify problems and speed up resolution. A complete solution will generate alerts, notify the IT team, create tickets and even automate fixes through scripts and workflows so incidents are handled faster and with less manual effort.

Remote management should give you the ability to:

- Manage devices regardless of location, even over high-latency networks.
- Securely and reliably access endpoints "behind the scenes" to allow users to continue working on their computers while the technician works on resolving a problem.
- Use remote control to access the console on the endpoint directly.
- Get secure, admin-level access without having to know or manage login credentials.
- Gain visibility into detailed asset information on the endpoint via the remote control function.
- Run scripts, edit Windows Registry Keys, run from the command line.
- One-click resolution of common user requests like password resets, account quarantine and adding software licenses.

Intelligent IT automation

A common issue for many MSPs and internal IT teams is that they don't have enough time in the day to get everything done. IT automation solves this problem. Automating IT tasks can save significant technician time and reduce IT operating costs. Automate almost any IT process with scripts, policies and workflows — the sky is the limit.

You can automate common IT processes such as software deployment, software patching, routine server maintenance and much more. You can also auto-remediate IT incidents to reduce the load on help desk reps. Automation guided by policy enables IT technicians to standardize the management of different categories of machines.

For example, you can define the processes needed to manage all your SQL servers. Automation in a best-in-class endpoint management and security solution can also tackle activities that cross the endpoint/user divide, such as automating user onboarding and offboarding.

Automation features to look for include:

Policies that can be applied to individual machines or to logical groups of endpoints to drive standardization of IT processes.

A modern, easy-to-use scripting editor that enables teams to customize workflows, streamline processes and handle complex tasks easily.

A library of crowdsourced automation scripts, reports and other assets to easily get started on IT automation.

Ability to execute automation scripts from anywhere, i.e. your endpoint management, IT documentation or service desk tool.

Endpoint and network monitoring

Visibility across the entire IT network is a key requirement for quickly identifying and resolving the root cause of an IT incident. Look for an endpoint management and security solution that provides complete visibility of your or your clients' IT environment through automated discovery and visualization of all endpoints.

Your endpoint management and security solution should also be able to natively monitor both agent-based endpoints (servers, workstations) and SNMP, VMs and iOS devices. This eliminates the need for a separate, standalone network monitoring tool. Ideally, your endpoint management should require no configuration to set up SNMP device monitoring.

Select an endpoint management and security solution that has a network topology map that provides:

Connectivity of all discovered endpoints on the network.

Asset status visibility — up/down status of each endpoint on the network.

Easy access to IT asset (endpoint) information.

Fast access to the remote endpoint management function from the topology map to enable your IT team to identify potential problem sources quickly, remediate IT incidents and maintain system uptime.

Monitor events on agent-installed and non-agent installed devices.

Be able to create an alarm, generate a ticket, run a script or send an email in case of an incident.

Easily monitor SNMP devices with zero configuration required.

Integrated IT documentation tool

IT documentation is a crucial yet often overlooked part of IT. With technicians focused on managing networks, endpoints and troubleshooting, documenting their work often slips to the bottom of the list. The outcome is lost efficiency and wasted time searching for information that should have been easy to find.

The Kaseya 2025 global IT trends and priorities survey reflects this shift in awareness. The percentage of respondents who felt it was important to be able to automation scripts directly from IT documentation tools doubled from 7% in 2024 to 13% in 2025.

An efficient endpoint management and security solution must have deep workflow integration with an IT documentation tool that maximizes technician efficiency by providing asset information at their fingertips.

Features that indicate powerful IT documentation integration include:

Easy access to enhanced IT asset information and IT documentation (including passwords, procedures, related assets and more) right within the endpoint management solution.

Ability to securely inject passwords during remote control without copying and pasting.

Ability to easily make updates to asset information in real time.

Ability to run automation scripts from within the IT documentation tool.

Integration with service desk

Integration of your endpoint management and security solution with a service desk tool enables seamless workflows, allowing speedy resolution of service tickets. Jump from the service ticket right into the remote management function of the endpoint management tool to troubleshoot an issue.

Need documentation and asset information to resolve tickets? Use an endpoint management tool that is integrated with both service desk and IT documentation tools. Access information whenever and wherever you need it to save time and improve productivity.

Features that indicate seamless integration of an endpoint management and security solution with a service desk tool include:

- Automatic synchronization of asset information between endpoint management and the service desk.
- Automatic generation of tickets by the endpoint management solution to reduce manual processes.
- Faster ticket resolution with easy access to remote endpoint management from the ticket.
- Ability to auto-remediate service tickets by running automation scripts from within the service desk tool.

Unified antivirus and EDR for enhanced security

Natively integrated antivirus (AV) and endpoint detection and response (EDR)

Your endpoint management and security solution must provide layered protection, extending beyond basic API-level integrations with antivirus and EDR solutions. Best-in-class solutions integrate antivirus and EDR at a level where these core security products look, feel and act as if they are a core component of the system.

The AV solution should prevent malware attacks, secure email communications, block spyware installations and warn users about malicious websites. The EDR must detect and respond to advanced threats that may go unnoticed by antivirus or traditional endpoint monitoring solutions. The *Kaseya 2025 global IT trends and priorities survey* of small and midsize businesses found that EDR is the rising star of cybersecurity investments. Its adoption jumped from 49% in 2024 to 65% in 2025, making it the most widely adopted IT management tool in this year's survey.

Choose a solution where endpoint management and EDR work together to auto-remediate incidents before they escalate into full ransomware attacks. Additionally, reporting on cybersecurity is no longer optional. Look for tools that provide high-value dashboards and out-of-the-box reporting capabilities.

Features that indicate comprehensive endpoint security include:

Centralized visibility of the security status of endpoints, both on-premises and remote.

The ability to deploy and manage AV/EDR clients from the endpoint management solution.

Auto-remediation of potential incidents by utilizing the automation capabilities of the endpoint management and security solution.

High-value dashboards and reports, using data from AV and EDR tools, available within the endpoint management and security solution.

Unified backup from a single pane of glass

Going hand-in-hand with AV/EDR and patch management is backup. An endpoint management and security solution should provide workflow integration with backup solutions to allow seamless management of backups from a single pane of glass. Alarms from the backup solution should be visible in the endpoint management and security solution.

Complete IT management platform

Most IT teams spend a significant amount of time navigating a patchwork of solutions, retrieving passwords, looking up information and switching between multiple user interfaces. To manage your IT environment more efficiently and reduce operational costs, seek a unified platform that combines powerful endpoint monitoring and management capabilities with other critical IT solutions in a single pane of glass. It frees up your technicians to focus on more strategic tasks.

Your endpoint management solution must integrate seamlessly with critical IT tools such as:

- Service desk
- Identity and access management
- Backup and disaster recovery
- Office 365 backup
- IT documentation

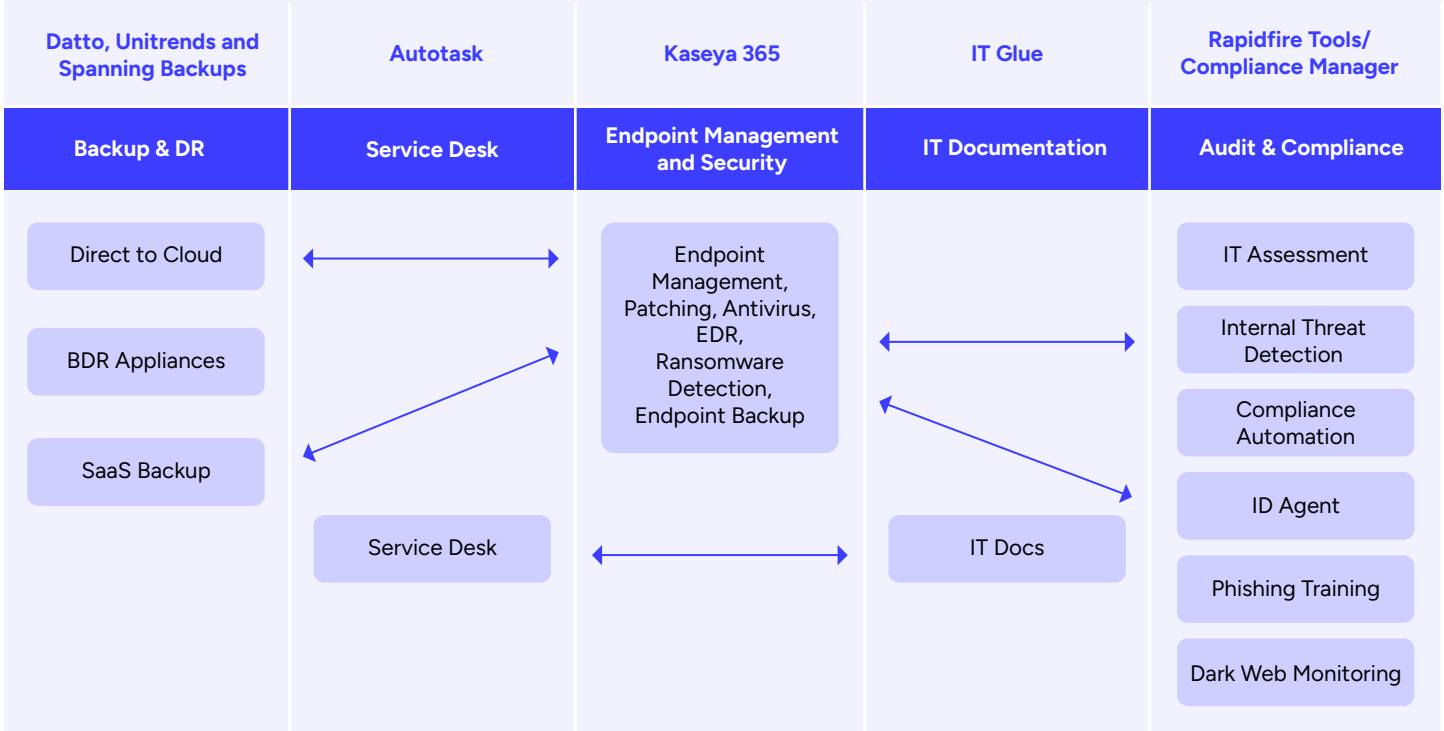
The ultimate IT management solution for your unique needs

Kaseya 365 Endpoint is everything you need to manage, secure, back up and automate your endpoints in a single subscription. Starting at as low as $2.80 per endpoint, it provides built-in access to tools that typically require separate licenses — saving IT teams time, reducing costs and cutting out the complexity of juggling disconnected systems.

What makes Kaseya 365 Endpoint such a time-saver is how everything works together out of the box. You're not switching between five different tools to handle routine tasks — patching, backups, antivirus monitoring — it's all right there, integrated seamlessly.

For IT professionals, that means fewer manual steps and less context switching. You're not chasing alerts in one platform while trying to deploy fixes in another. With Kaseya 365, your stack is streamlined, and your day runs smoother.

Kaseya gives you everything you need to run IT with confidence.
Start with Kaseya 365 Endpoint as your core foundation platform. From there, you can explore and add other Kaseya solutions — adding them as needed to strengthen your stack and services.



See how it all comes together

If you're looking to turn these insights into real-world impact — stronger security, smoother operations and better results — our eBook shows you how. **Be Stronger, More Secure and Profitable With Kaseya 365 Endpoint** offers a closer look at what an all-in-one approach can really do for your IT.

Show me how Kaseya 365 Endpoint works

Sources

i. The 2025 MSP Benchmark Survey Report

ii. The State of Patch Management in the Digital Workplace

©2025 Kaseya Limited. All rights reserved. Kaseya and the Kaseya logo are among the trademarkes or registered trademarks owned by or licensed to Kaseya Limited. All other markes are the property of their respective owners.