EBOOK

Kaseya 365

MODERN ENDPOINT MANAGEMENT AND SECURITY SOLUTION BUYER'S GUIDE

Contents

Introduction 03

Features to look for in an endpoint management and security solution 04

- Ease of use and deployment 04
- Scalability 05
- Discovery and inventory 06
- Automated patch and vulnerability management 07
- Robust remote monitoring and management 08
- Intelligent IT automation 09
- Endpoint and network monitoring 10
- Integration with IT documentation and configuration management tools 11
- Integration with service desk 12
- Unified antivirus and EDR for enhanced security 13
- Unified backup from a single pane of glass 14
- Complete IT management platform 14

The ultimate IT management solution for your unique needs 15

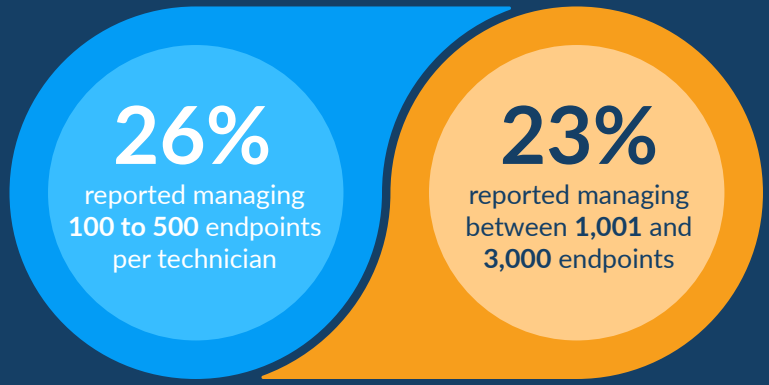
Conclusion 16

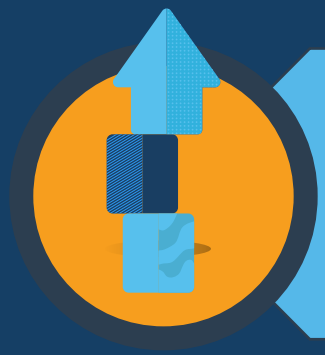
Introduction

The success of your business depends on having a reliable IT infrastructure that allows your employees to work efficiently and get the job done regardless of whether they are working from home or the office. They require endpoint devices, which include laptops, desktops, servers and network devices that are "always on," meaning the IT team must always maintain system uptime.

Another responsibility of IT is to enable business growth and transformation. As a business grows, so do the number of endpoints that must be managed. About 26% of respondents to the Kaseya 2024 MSP Benchmark Survey reported managing 100 to 500 endpoints per technician, while another 23% reported managing between 1,001 and 3,000 endpoints[i]. Managing the growing number of endpoints in today's highly dynamic IT environments is a challenge. The best endpoint management and security solutions make an IT professional's job easier with intuitive user interfaces, access to all core IT management functions from a single console and streamlined workflows.

Your business also requires a high level of IT security to prevent downtime and other costs associated with cyberattacks. The best endpoint management and security solutions are constantly evolving to keep up with the demands of IT teams to deliver on these requirements.





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 that allow the IT team to maintain a reliable and secure IT infrastructure.

Features to look for in an endpoint management and security solution

Some important features to look for when choosing an endpoint management and security solution are:

Ease of use and deployment

Using an unintuitive and difficult endpoint management and security solution can be a major challenge for your IT team. After all, 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.

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 IT 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.

Several enterprise-class endpoint management and security solutions on the market are notoriously difficult to configure and deploy in the customer's environment. They typically require businesses to hire a team of consultants to help them with the deployment process. Unfortunately, engaging professional help to deploy your endpoint management and security solution doesn't necessarily guarantee that the system will work the way you expect it to.

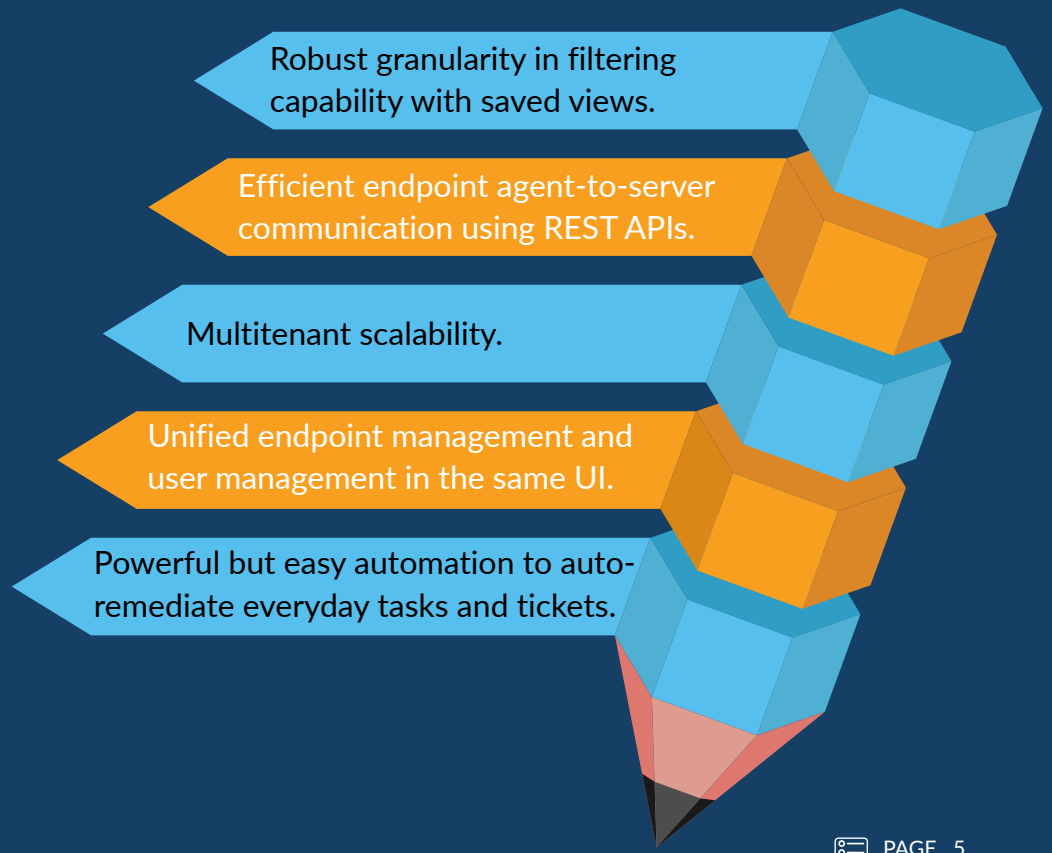
The deployment alone can be a major expense and pose a serious risk to midsized businesses that have smaller internal IT teams. Look for a solution that is easy to configure and deploy in your environment. More often than not, the vendor will provide basic implementation services at a relatively low cost to help you get the tool up and running within a very short period, usually a few weeks.

Scalability

As your organization grows, the number of endpoints in your network increases. To manage this expanding ecosystem and the resulting network complexity, IT teams 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 midsized businesses a lot of room for growth without worrying about overextending their endpoint management solution.

Scalability features to look for include:



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 integrate directly with Microsoft 365, allowing you to discover, manage and secure both endpoints and users from a single platform.

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

Hardware information such as:

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

User information such as:

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

Software information such as:

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

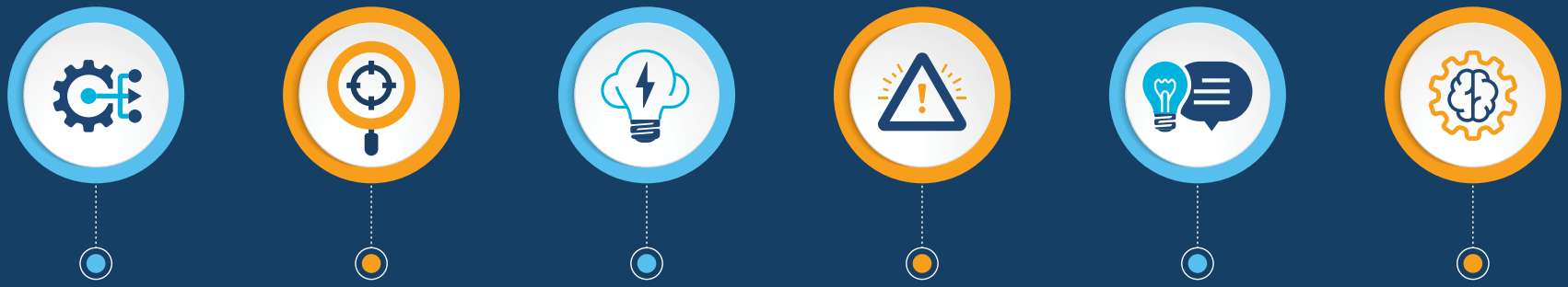
Automated patch and vulnerability management

Patching software in a timely manner is critical to keeping your IT environment secure from cyberattacks. However, patch management can be a labor-intensive process, especially for organizations with limited IT staff. In a survey by the Ponemon Institute, about 65% of respondents revealed that their companies did not have enough staff to patch fast enough to prevent a data breach[ii] .

The survey also pointed out that most organizations relied on manual processes to mitigate software vulnerabilities, which put them at risk. Ineffective patch management tools and manual processes can derail timely patching.

The Ponemon survey indicated that an average of 12 days are lost coordinating across teams before a patch is applied. Look for an endpoint management and security solution that automates patching and keeps your business secure.

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

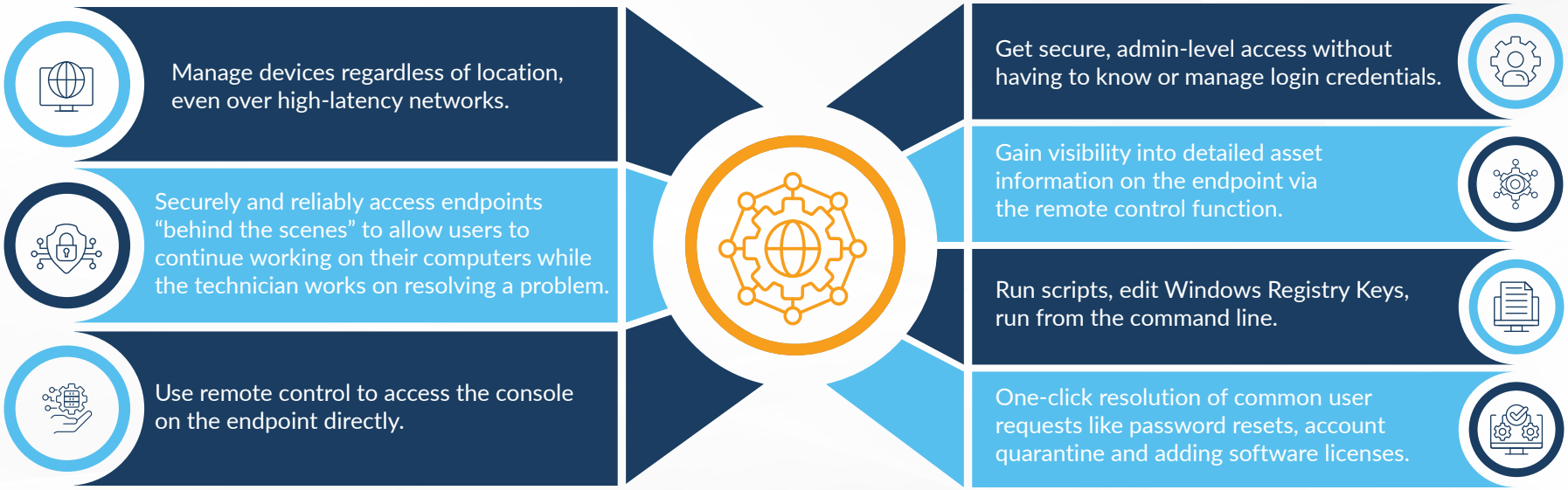
Robust remote monitoring and management

Many organizations have endpoints and users spread across multiple locations. In today's dispersed workforce environment, it's crucial to access and manage these remote, off-network devices.

Remote management enables IT teams to access endpoints easily, no matter where they are located, to troubleshoot issues and maintain system operations 24/7, thereby minimizing downtime.

A unified endpoint management and security solution with robust remote monitoring and management (RMM) capabilities saves travel time and expenses and increases IT teams' overall productivity. Your endpoint management tool should allow you to monitor endpoint events and conditions for faster identification and resolution of IT incidents. It should respond to alarms by generating alerts, sending notifications to the IT team, creating tickets and automating the remediation of IT incidents with the help of scripts and automated workflows.

Remote management should give you the ability to:

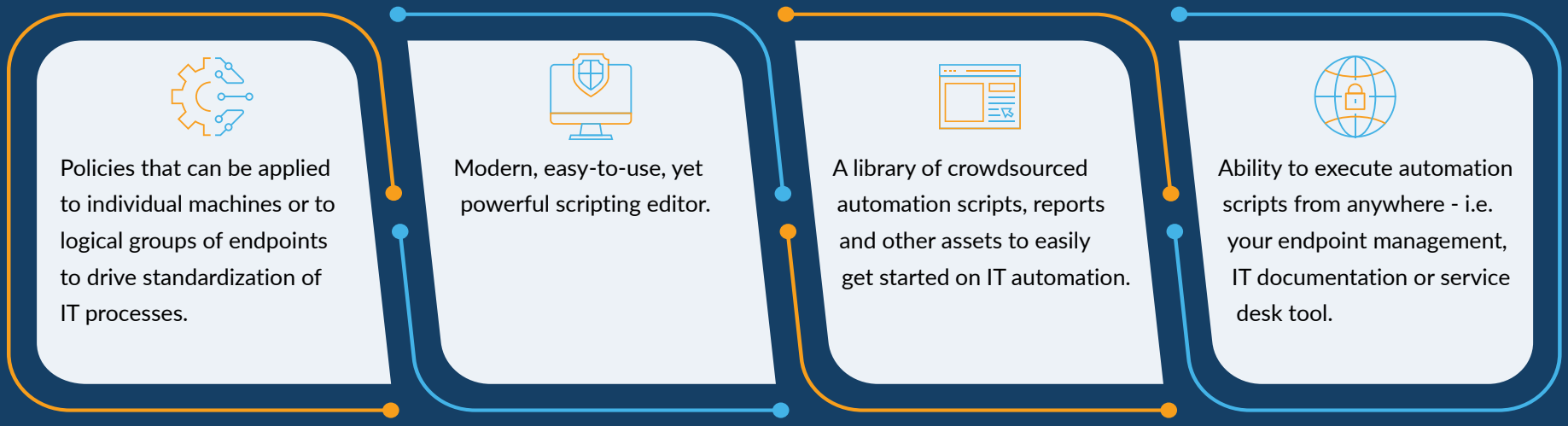


Intelligent IT automation

A common issue for many 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:



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 IT environment through automated discovery and visualization of all endpoints on your network — both agent -based and agentless (e.g., SNMP, VMs and iOS) devices.

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:

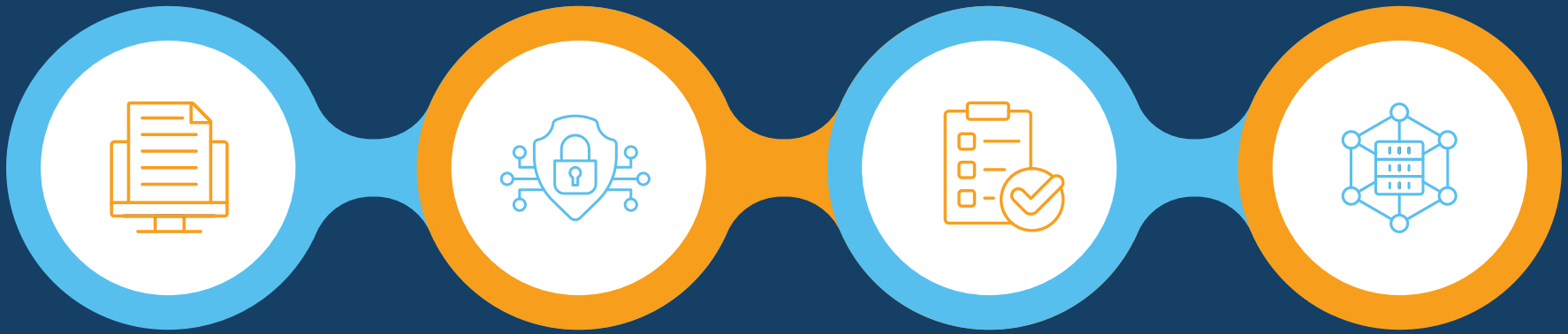
- Connectivity of all discovered endpoints on the network.
- Asset status visibility — up/down status of each endpoint on the network.
- Easy access to IT asset (endpoint) information.
- Fast access to the remote endpoint management function from the topology map to enable your IT team to identify potential 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.

Integration with IT documentation and configuration management tools

IT documentation is often overlooked. IT teams spend so much time managing networks and endpoints and troubleshooting issues that they rarely have time to document their work. Survey data from IT Glue shows that IT technicians spend up to 20% of their time looking for information[iii]. The time wasted due to this lack of access to IT documentation and asset information can be costly for your business.

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. It should enable IT teams to quickly access IT asset information and documentation as
and when they need it.

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.

The 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 solution 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 solution include:

Automatic synchronization of asset information between the endpoint management solution and the service desk solution.

Faster ticket resolution with easy access to remote endpoint management from the ticket.

Automatic generation of tickets by the endpoint management solution to reduce manual processes.

Ability to auto-remediate service tickets by running automation scripts from within the service desk tool.

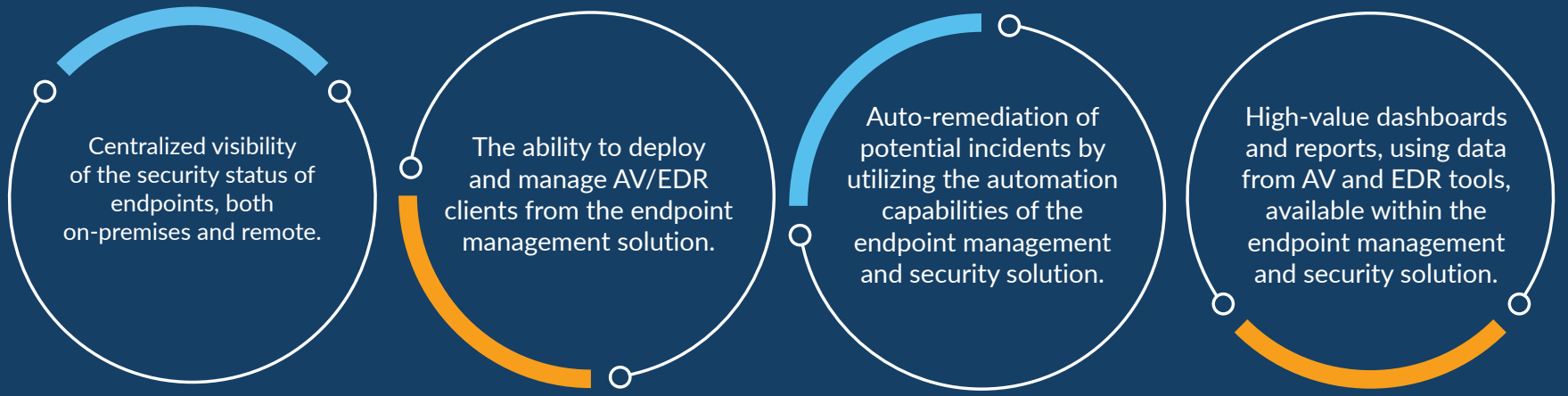
Unified antivirus and EDR for enhanced security

a. 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. 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:



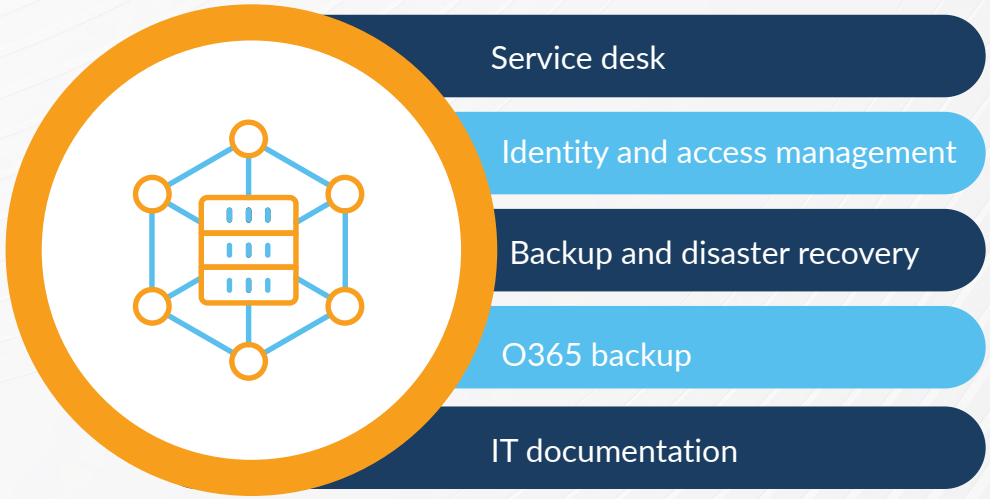
b. Unified backup from a single pane of glass

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 non-integrated 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.

The complete IT management solution must offer seamless integration of your endpoint management solution with critical IT tools such as:

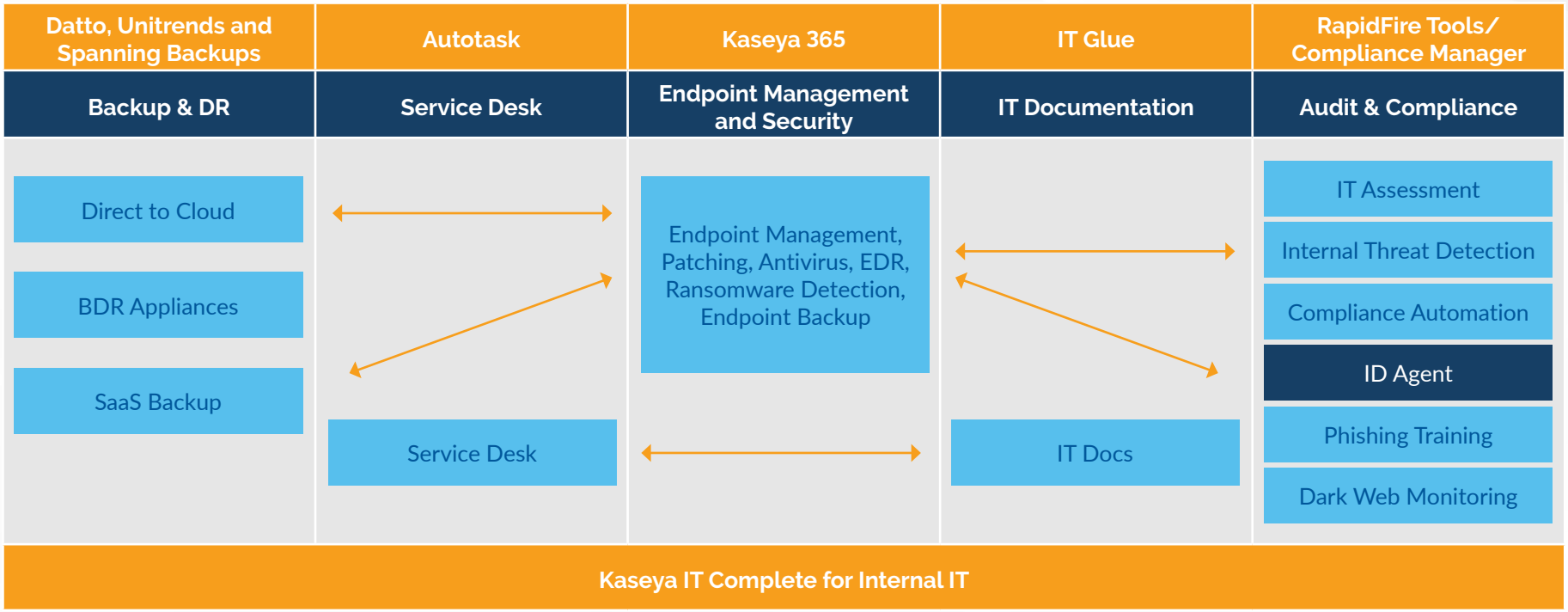


The ultimate IT management solution for your unique needs

Kaseya 365 is everything you need to manage, secure, backup and automate your endpoints in a single subscription. Starting at as low as $2.80 per endpoint, Kaseya 365 provides seamless access to functions in endpoint management, security and backup.

These solutions are joined under one subscription, effortlessly integrated, and live within the unified interface experience of IT Complete. It offers seamless workflow integrations with Autotask, IT documentation (IT Glue), backup and disaster recovery (Datto and Unitrends Backup) and compliance (Kaseya Compliance Manager) solutions that make up IT Complete.

As the core subscription of IT Complete, Kaseya 365 delivers the essential tools needed by every IT professional. The supporting power of IT Complete's 30+ additional modules and 1,300+ integrations allow for unlimited efficiency gains and cost savings.



Conclusion

With Kaseya 365, you can efficiently manage your entire IT infrastructure, keep all your systems and data secure and make your IT team's job easier, all while reducing your IT operating costs.

REQUEST A DEMO OF KASEYA 365

©2024 Kaseya Limited. All rights reserved. Kaseya and the Kaseya logo are among the trademarks or registered trademarks owned by or licensed to Kaseya Limited. All other marks are the property of their respective owners.

Sources

i. The 2024 MSP Benchmark Survey Report
ii. Cost and Consequences of Gaps in Vulnerability Response
iii. 2019 Global MSP Benchmark Report, IT Glue