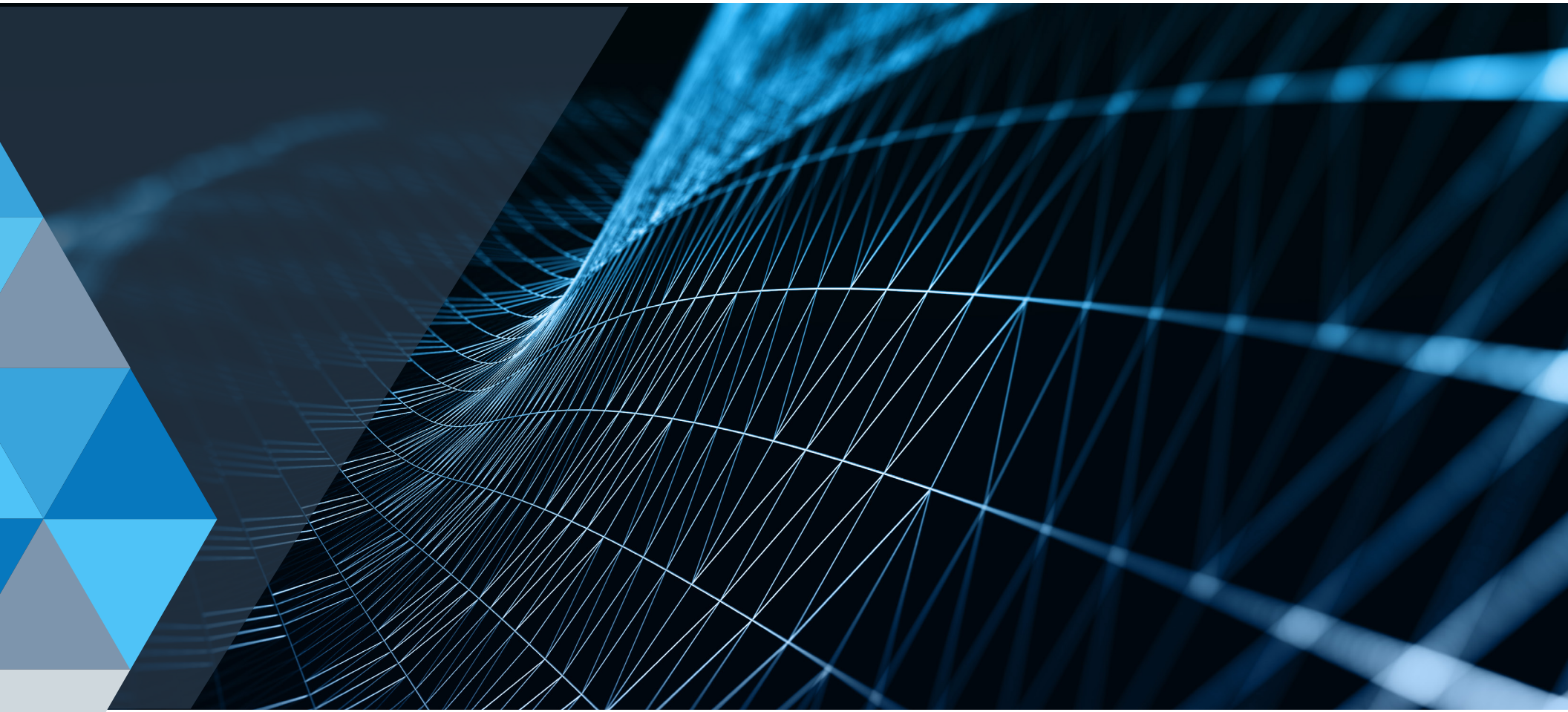
EBOOK

MODERN ENDPOINT MANAGEMENT

SOLUTION BUYER'S GUIDE



Contents

Click on any section below to jump directly to its respective page.

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.

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

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. The Kaseya 2019 State of IT Operations Survey Report showed that about half of the respondents reported managing 100 to 500 devices per technician.[1] Managing the growing number of endpoints in today's highly dynamic IT environments is a challenge. The best endpoint management tools 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.

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 solutions must offer seamless workflow integrations with all the other key IT management functions that allow the IT team to maintain a reliable and secure IT infrastructure.

Features to Look for in an Endpoint Management Solution

☑ *Ease of Use and Deployment*

Using an endpoint management tool that is unintuitive and hard to use can be a major challenge for your IT team. After all, a robust endpoint management tool is the foundation of successful IT management. If it isn't easy to use, it can lead to frustration, burnout and employee turnover. Not only that, it causes a serious loss in productivity.

Consider questions like these before purchasing an endpoint management 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)?

Today's IT environments are complex. Your endpoint management 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 and 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

Several enterprise-class endpoint management tools 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 tool 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 midsize 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 relatively low or no cost to help you get the tool up and running within a very short period, usually a few weeks.

Scalability

As your organization grows, so do the number of endpoints in your network. To manage this ever-expanding ecosystem of endpoints along with the ensuing network complexity, IT teams require an endpoint management tool that is highly scalable and can meet all your business needs today as well as 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 midsize businesses a lot of room for growth without worrying about overextending their endpoint management solution.

Scalability features to look for include:

- Modern UI communication approach
- Efficient endpoint agent-to-server communication using REST APIs
- Multi-tenant scalability

Discovery and Inventory

The endpoint management tool should discover all endpoints on the IT network and automatically deploy an agent to each endpoint. Two approaches to discovery are helpful – Network (LAN) Based and Domain Discovery. The latter approach allows the endpoint management tool to automatically discover Active Directory (AD) domains and stay in sync with all domain changes.

The discovery function should collect comprehensive IT asset information for the device, including both hardware and software data. This 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.

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 2018 survey by the Ponemon Institute, about 81 percent of respondents revealed that their companies did not have enough staff to patch fast enough to prevent a data breach.[2]

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.[3] Look for an endpoint management 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 third-party applications
- Automated, scheduled scanning of devices for missing patches
- Vulnerability management and reporting
- Patching of both on-network and off-network devices (especially important for work from home users)
- Patch compliance reporting to ensure adherence to company policies

See Software Vulnerabilities Affecting Your IT Environment—Security Risk

Robust Remote Monitoring and Management

Many organizations have their endpoints located in multiple locations. Additionally, in the current environment, with many people working from home, it's critical to be able to access and manage these remote, off-network devices.

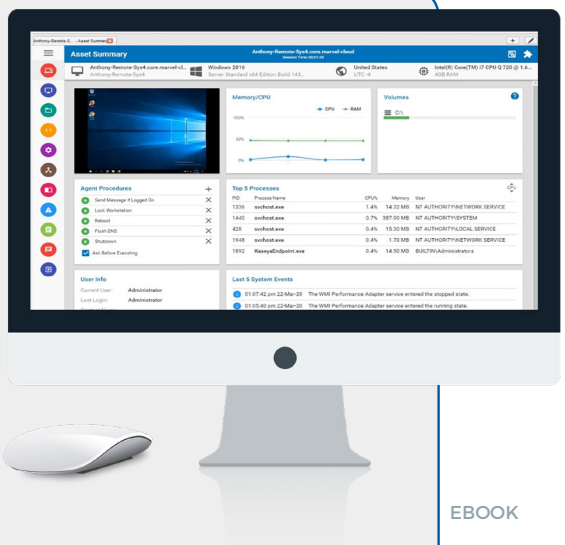
Remote management allows IT teams to easily access endpoints, wherever they are located, to troubleshoot issues and keep systems running 24/7, thereby minimizing downtime.

An endpoint management tool with robust remote monitoring and management (RMM) capabilities saves travel time and expenses and increases the overall productivity of IT technicians. 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 (agent procedures).

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 directly access the console on the endpoint
- 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 and more

Get Detailed IT Asset Information in the Remote Management Function



Policy-based 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 — the sky is the limit. An agent installed on the endpoint executes these scripts to automate tasks.

You can automate common IT processes such as software deployment, software patching, routine server maintenance and much more. Auto-remediate IT incidents to reduce the load on helpdesk reps. Automation guided by policy enables IT technicians to standardize management of different categories of machines. For example, you can define the processes needed to manage all your SQL servers.

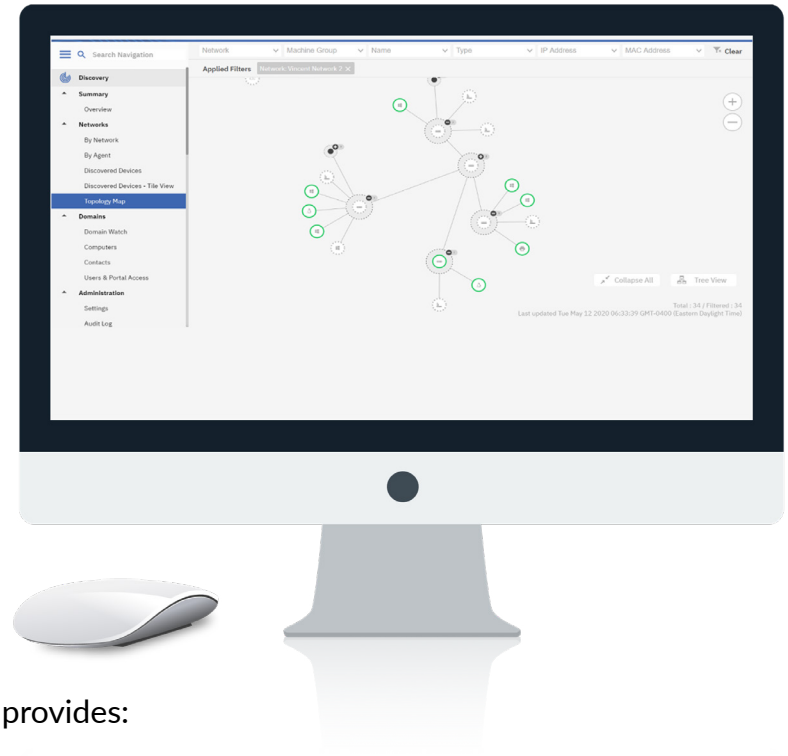
Automation features to look for include:

- Policies that can be applied to individual machines or to logical groups of endpoints to drive standardization of IT processes
- Modern, easy-to-use, yet powerful scripting editor
- A library of crowdsourced automation scripts, reports and other assets to easily get started on IT automation
- Ability to execute automation scripts from anywhere — endpoint management tool on your desktop, mobile app, service desk tool and IT documentation tool

Endpoint and Network Monitoring

A key requirement to quickly finding and fixing the root cause of an IT incident is gaining visibility of the entire IT network. Look for an endpoint management solution that provides you with 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) devices.

Your endpoint management solution should also be able to natively monitor both agent-based endpoints (servers, workstations) and SNMP 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.



Network Topology Map in the Endpoint Management Solution

Select an endpoint management 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 quickly identify potential problem sources, 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

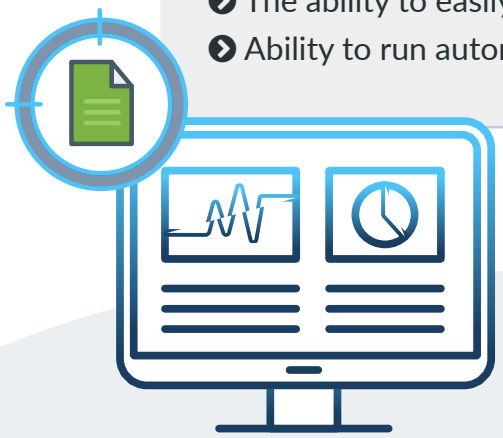
Integration With IT Documentation and Configuration Management Tools

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 percent of their time looking for information.[4] 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 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
- 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 tool 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 tool with a service desk solution include:

- Automatic synchronization of asset information between the endpoint management solution and the service desk solution
- Faster resolution of tickets 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

☑ *Integration With AV/AM and BDR for Enhanced Security From a Single Pane of Glass*

a. Integration with antivirus/antimalware (AV/AM) tools

Your endpoint management tool must provide layered protection by integrating with antivirus and antimalware solutions. The AV/AM solution should prevent malware attacks, secure users when sending and receiving emails, block spyware installation and warn users when browsing malicious websites.

The AV/AM solution may also provide integrated endpoint detection and response (EDR), which helps detects suspicious activity and malware and keeps the network safe by containing the threat to an endpoint in case of an incident.

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/AM clients from the endpoint management tool

b. Integration with backup and disaster recovery solutions

Going hand-in-hand with AV/AM and patch management is backup and disaster recovery (BDR). An endpoint management solution should provide workflow integration with BDR 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 tool.

Mobile Application

Productivity is critically important for businesses today. The more efficient your technicians are in managing your IT infrastructure, troubleshooting endpoints and resolving tickets, the greater your ability to do more with a leaner workforce. Look for an endpoint management solution that allows your IT team to access its key features and functions via a mobile app for efficient endpoint monitoring and management on the go.

Features to look for in the endpoint management mobile app include:

- Access to IT asset information in the palm of your hand
- Ability to execute automation scripts from within the mobile app for powerful automation on the go
- Integration with the service desk solution in the same mobile app

Complete IT Management Platform

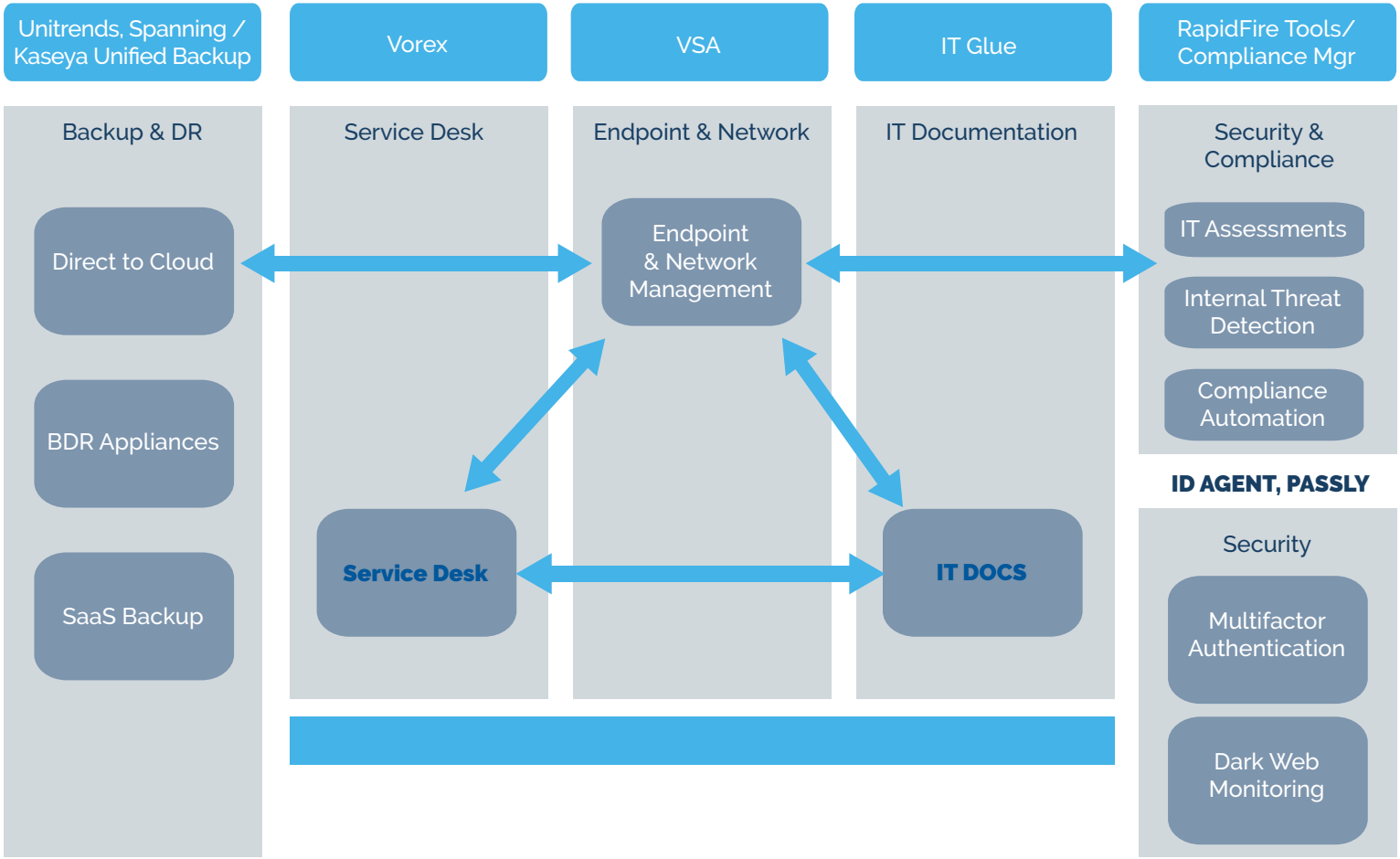
Most IT teams lose a major chunk of their time navigating a patchwork of non-integrated solutions, retrieving passwords, looking up information and orienting between multiple user interfaces. Look for a unified platform that allows you to efficiently manage your IT environment while reducing operational costs. Such a platform combines the powerful capabilities of endpoint monitoring and management with an array of other critical IT solutions to allow efficient endpoint management from a single pane of glass and frees up time for 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:

- Service desk
- Identity and access management
- Backup and disaster recovery
- O365 backup
- IT documentation

THE ULTIMATE IT MANAGEMENT SOLUTION for YOUR UNIQUE NEEDS

Kaseya VSA is our endpoint management solution that is the foundation of our IT Complete suite of products. Kaseya VSA meets all the above requirements and more. It offers seamless workflow integrations with the service desk (Vorex), IT documentation (IT Glue), backup and disaster recovery (Kaseya Unified Backup), and compliance (Kaseya Compliance Manager) solutions that make up IT Complete. Additionally, Kaseya VSA is integrated with leading AV/AM tools, such as Bitdefender, Webroot and Kaspersky, to allow management of endpoint security from the VSA UI.

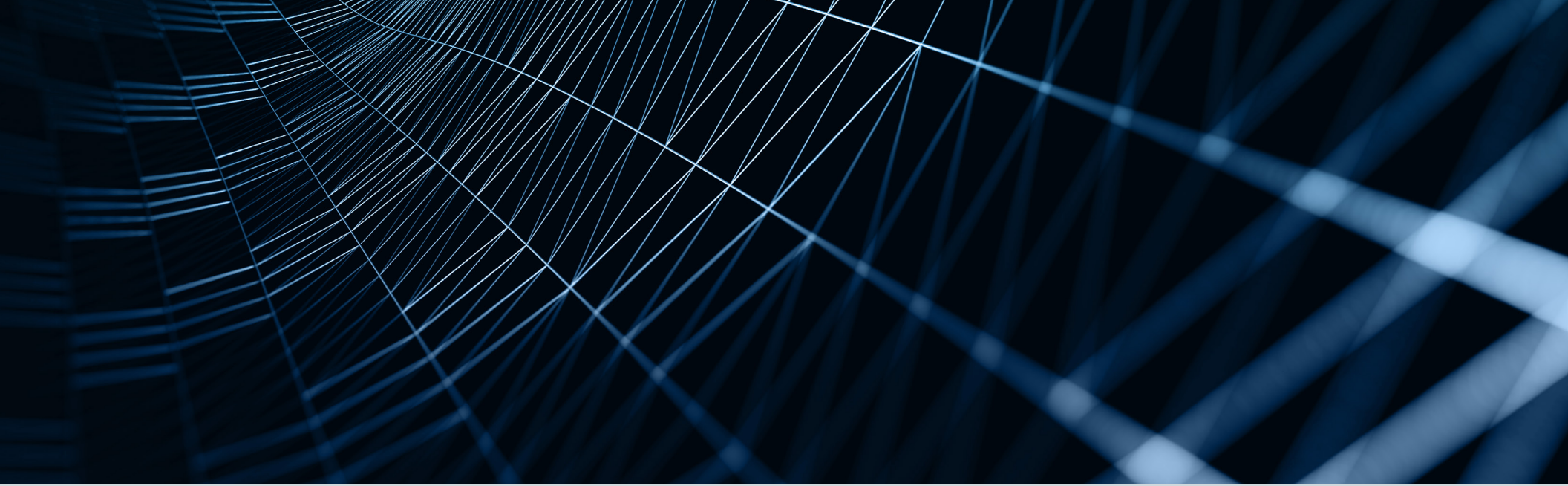


CONCLUSION

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

REQUEST A DEMO OF KASEYA VSA

OR START A FREE 14-DAY TRIAL TODAY!



References:

1. 2019 State of IT Operations Survey Report, Kaseya
2. Today's State of Vulnerability Response: Patch Work Demands Attention, Ponemon Institute
3. Ibid
4. 2019 Global MSP Benchmark Report, IT Glue
5. 2019 State of IT Operations Survey Report, Kaseya

About Kaseya

Kaseya® is the leading provider of complete IT infrastructure management solutions for managed service providers (MSPs) and internal IT organizations. Through its open platform and customer-centric approach, Kaseya delivers best in breed technologies that allow organizations to efficiently manage, secure, automate and backup IT. Kaseya IT Complete is the most comprehensive, integrated IT management platform comprised of industry leading solutions from Kaseya, Unitrends, Rapidfire Tools, Spanning Cloud Apps, IT Glue and ID Agent. The platform empowers businesses to: command all of IT centrally; easily manage remote and distributed environments; simplify backup and disaster recovery; safeguard against cybersecurity attacks; effectively manage compliance and network assets; streamline IT documentation; and automate across IT management functions. Headquartered in Dublin, Ireland, Kaseya is privately held with a presence in over 20 countries. To learn more, visit www.kaseya.com.

12282020