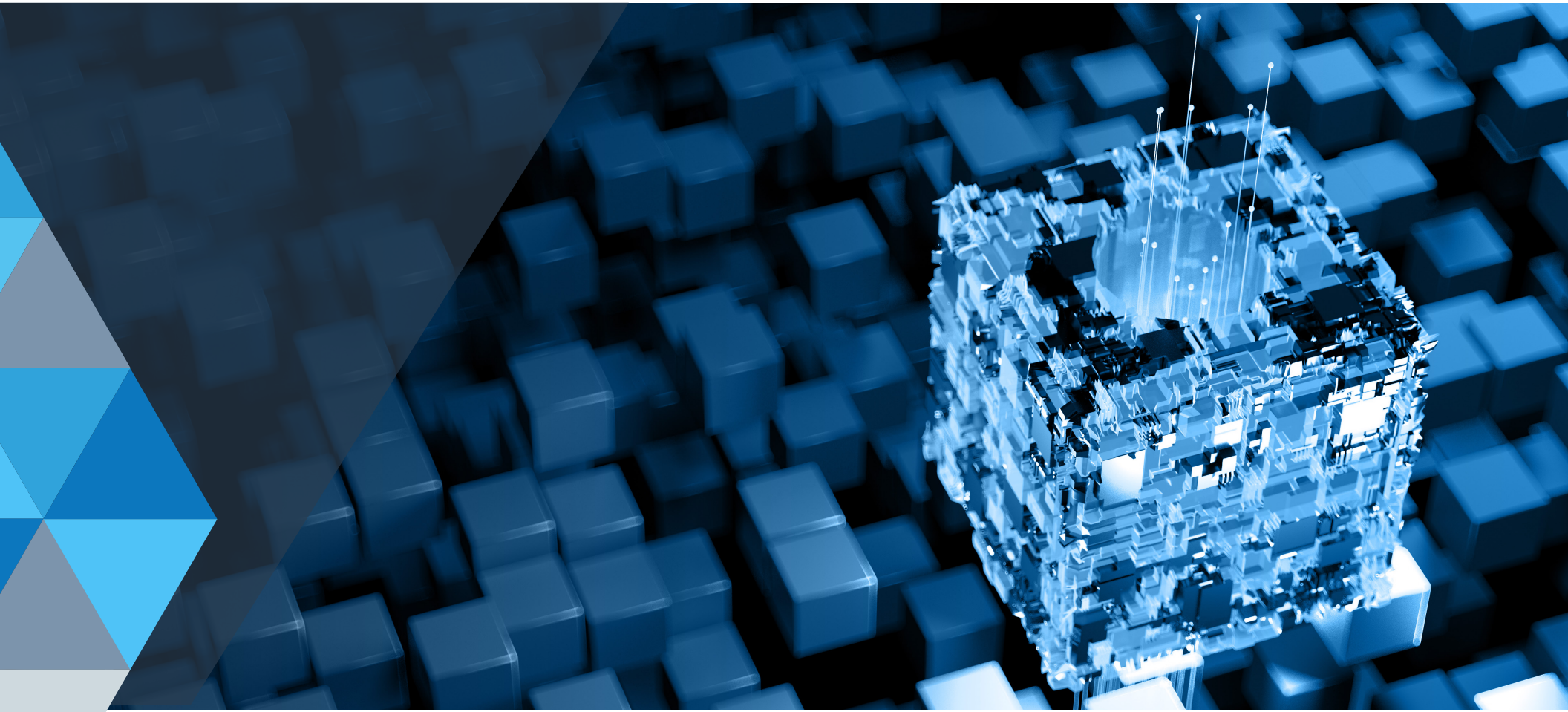
EBOOK

# TOP 10 REQUIREMENTS FOR MODERN ENDPOINT MANAGEMENT TOOLS



## Introduction

The success of your business depends on having a reliable IT infrastructure that allows your workforce to work efficiently and get the job done. They require endpoint devices which include laptops, desktops, servers, and network devices that are "always on," meaning that the IT team must maintain system uptime. The business also requires a high level of IT security to prevent downtime and other costs associated with cyberattacks.

Endpoint management solutions are continually 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 does the number of endpoints. The Kaseya 2019 State of IT Operations Survey Report showed that about half of the respondents reported managing one hundred to five hundred devices per technician.[1]

Managing the growing number of endpoints in today's highly dynamic IT environments is a challenge. Endpoint tools should be simplifying IT professional's job, not make it difficult by having poor integrations between tools and cumbersome 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 ensure endpoint security. In addition, modern endpoint management solutions must offer *seamless workflow integrations to all the other key IT management functions* that allow the IT team to maintain a reliable, secure IT infrastructure.

# 10 MUST-HAVE REQUIREMENTS FOR MODERN ENDPOINT MANAGEMENT TOOL

## 1: *Ease of use*

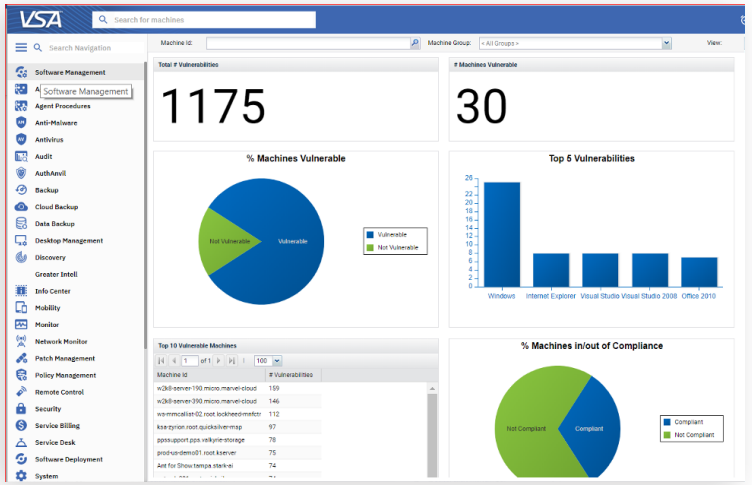
Nothing can be more daunting to the IT team than using an endpoint management tool that is unintuitive and hard to use. The endpoint management tool is where the team lives and breathes. If it's not easy to use, it can lead to frustration, burnout, and employee turnover. In today's tight job market, where finding qualified IT technicians is harder than ever, it pays to have the right tools in place.

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 must not suffer the same level of complexity your IT environment does. Look for a solution that provides an intuitive user interface, enabling IT technicians to ramp up quickly and work efficiently on an ongoing basis like:

- 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: find what you're looking for with the least amount of mouse clicks
- A quick drill down into the details of assets and endpoint agents




Modern Endpoint Management UI

## 2: *Ease of deployment*

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 through this process. Even then, there are no guarantees the system will work the way you expect it to. This involves considerable cost and poses 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. Usually, the vendor will provide basic implementation services for relatively low or no cost to help get it up and running in a very short period —a few days, not a few months.

## 3: *Scalability*

As your organization grows, so does your number of endpoints. Your IT environment may become more diverse, with a range of devices running various operating systems: Windows, Linux, MacOS. To manage this ever-expanding ecosystem of endpoints accompanied with the complexity, IT teams require an endpoint management tool that is highly scalable and can meet all your business needs today and in the future.

A Software as a Service (SaaS) endpoint management solution should be able to support upwards of **50,000 endpoints on a single instance.** This gives midsize businesses and Managed Service Providers (MSPs) a lot of room for growth without worrying about over-extending their endpoint management solution.

Scalability features to look for:

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

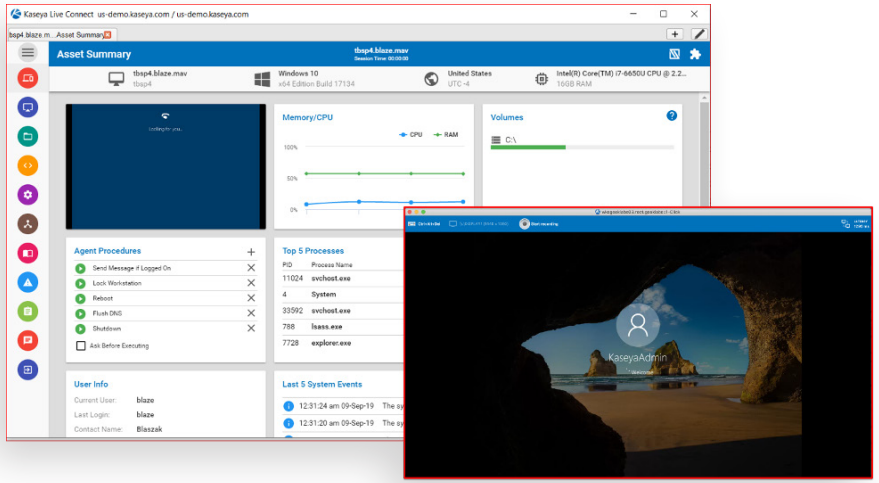
## 4: *Reliable patch management*

Patching systems 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 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 upon 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 indicates that an average of 12 days is lost coordinating across teams before a patch is applied.[3] Look for a centralized endpoint management solution that automates patching and keeps your business secure.

Features to look for:

- Automated patch management from a single, centralized console
- Patching of both operating systems 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
- Patch compliance reporting to ensure adherence to company policies




View of asset information in a remote management solution

## 5: *Robust remote management*

Many organizations have their endpoints located in multiple locations and ensuring all endpoints are up and running is essential for smooth IT operations. Remote management allows IT teams to easily access endpoints from a central location to troubleshoot issues and keep systems running 24/7, wherever they are located, minimizing downtime. An endpoint management tool with robust remote monitoring and management (RMM) capabilities saves travel time and expenses and increases overall productivity of IT technicians.

Remote management features to look for:

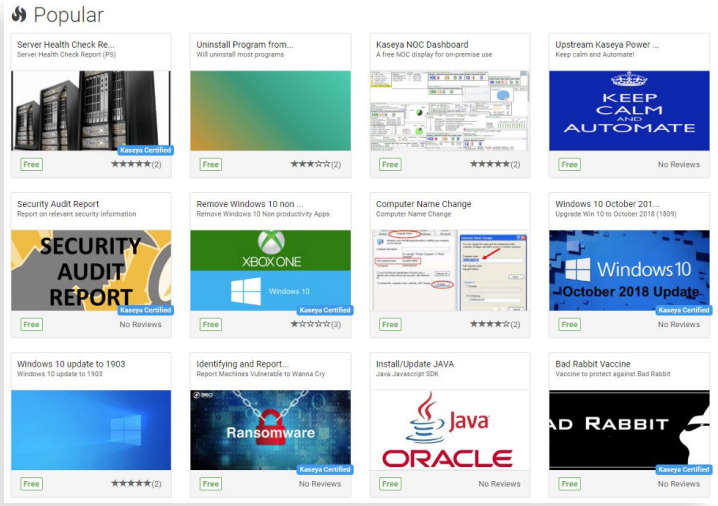
- Manage devices regardless of location, even over high latency networks
- Securely and reliably access endpoints with role-based and policy-based control
- Get secure, admin level access without having to know or manage login credentials
- Access endpoints and troubleshoot issues without disrupting end-users

## 6: 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. Automate common IT processes such as software deployment, patching, routine server maintenance, backup, and much more. Auto-remediate IT incidents to reduce the load on helpdesk reps.

*Automation Exchange*



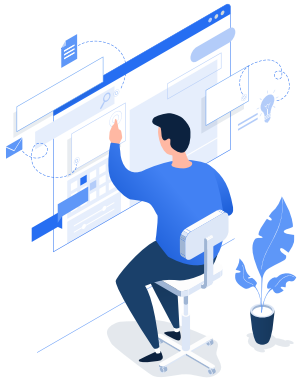

Automation guided by policy enables IT technicians to standardize management of different categories of machines. For example, you can define the processes needed to manage all your SQL Servers.

Automation features to look for:

- 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 crowd-sourced automation scripts, reports and other assets to easily get started on IT automation

## 7: *Quick access to IT asset information and documentation*

IT documentation is often overlooked. IT teams spend so much time managing networks and endpoints and troubleshooting issues, rarely do they 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 by 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.



Features that indicate powerful IT documentation capabilities:

- Easy access to enhanced IT asset information, right in the endpoint management solution
- The ability to easily make updates to asset information in real time
- A structured documentation framework
- Relationship mapping that links related items together

## 8: *Integration with a service desk solution*

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, wherever you need it and save time and improve productivity.

Features that indicate seamless integration of endpoint management tool with a service desk solution:

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

*Learn more about integration of endpoint management and service desk solutions.*

## 9: *Built-in two-factor authentication*

Today's enterprises are at risk of attack from a growing number of sources both inside and outside the organization. Moreover, the sophistication of attacks has risen due to the advancement of technology. In this environment, the rudimentary authentication process of username and password can no longer protect a business.

Two-factor authentication (2FA) adds an extra layer of protection to keep IT environments secure. A 2FA process requires the use of a second factor along with username and password to access applications and data. This second factor could be a smartphone-based token that generates a one-time password, a push authentication on smartphone, a desktop soft token or a physical token such as a YubiKey.

Your endpoint management should provide a 2FA solution that improves your endpoint security.

*More about endpoint management and 2FA solution integration.*

## 10: *Integration with antivirus/anti-malware, backup and disaster recovery, and compliance solutions*

### a. Integration with antivirus/anti-malware (AV/AM) tools

Your endpoint management tool must provide layered protection by integrating with antivirus and anti-malware 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.

Features that indicate comprehensive endpoint security:

- Centralized visibility of the security status of endpoints whether on-premise or remote
- Real-time scanning of devices to protect against security threats
- Ability to customize security levels based on requirements

### 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 management of backups from a single pane of glass.

Features that indicate effective backup and recovery:

- Automated backup processes
- Automated testing for guaranteed recovery
- Scalable to meet business needs
- Cloud compatible backup appliances for long-term data retention

### c. Integration with compliance solutions

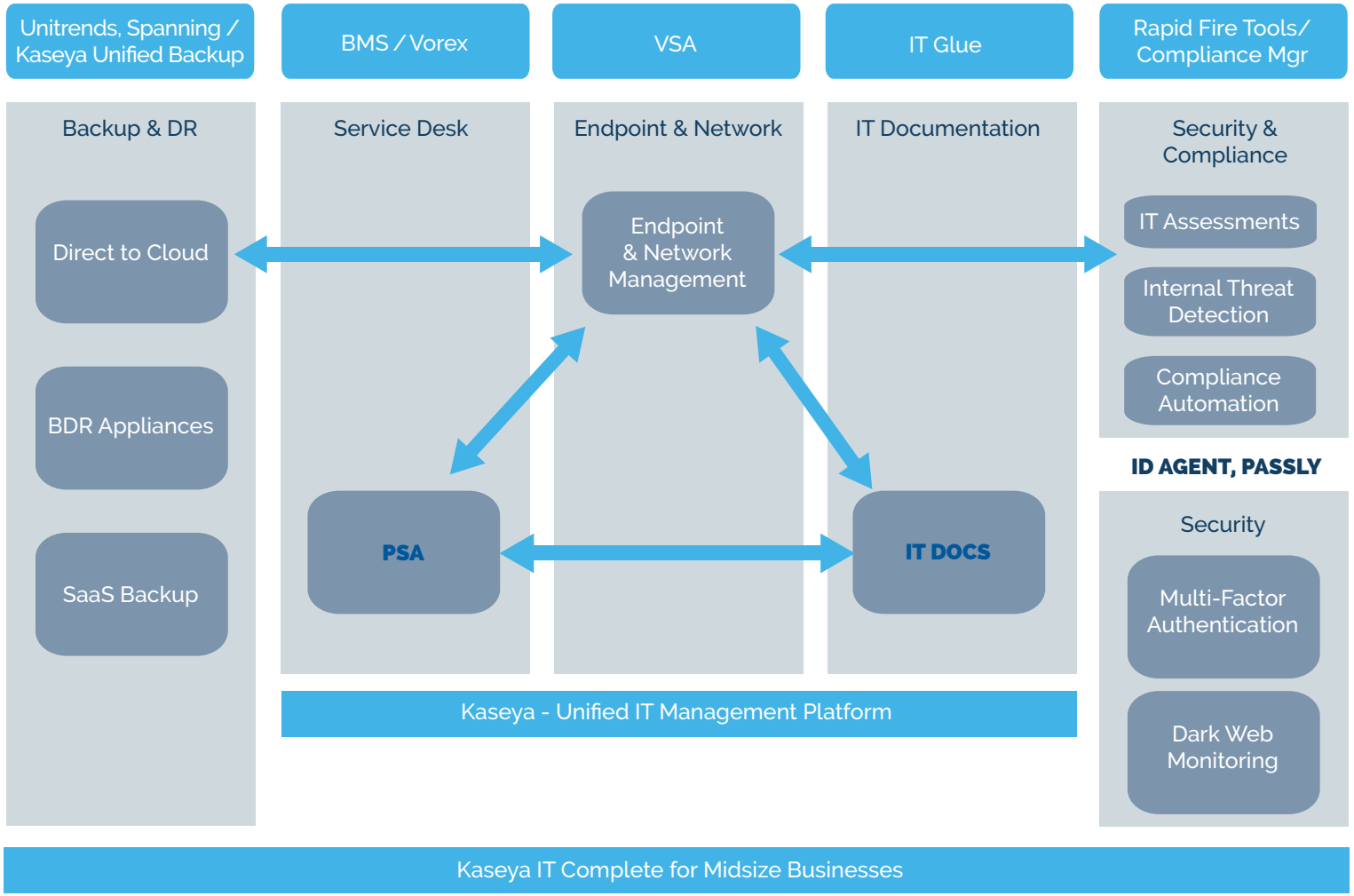
The importance of data privacy regulations has risen considerably over the past few years with HIPAA, PCI, and GDPR topping the list for most small and midsize businesses.[5] Organizations can be liable to pay fines and penalties in the case of non-compliance. An endpoint management tool that integrates with a compliance solution is a must-have requirement. It should enable you to document compliance from a single pane of glass and help reduce your organization's compliance risk.

Features that indicate powerful compliance capabilities:

- Automates compliance assessments and reporting processes to reduce manual effort
- Provides approved documentation that can be provided to auditors to demonstrate compliance
- Coverage for the most common regulations including GDPR, HIPAA, and PCI

## THE ULTIMATE IT MANAGEMENT SOLUTION FOR YOUR UNIQUE NEEDS

Kaseya IT Complete is a comprehensive suite of products that meets all the above requirements and more. **Kaseya VSA is our endpoint management solution that is the foundation of IT Complete.** VSA has seamless workflow integrations with the service desk, IT documentation, backup and disaster recovery (BDR), and compliance solutions that make up IT Complete.



## Conclusion

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

## To learn more, request a demo of Kaseya VSA.


**Sources**

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.




01242020