Kaseya®

EBOOK

A COMPREHENSIVE GUIDE TO **BRING YOUR OWN DEVICE (BYOD)**

A LOOK AT BYOD POLICIES, SECURITY RISKS, BENEFITS AND BEST PRACTICES

BYOD stands for bring your own device, a practice in which employees use their own devices rather than those provided by the company to do their work. BYOD adoption has been fueled by factors such as the easy availability of mobile devices, fast cellular network connectivity and hybrid work environments.

The BYOD trend has been ongoing for many years and accelerated during the COVID-19 pandemic as more employees work remotely and prefer to use their own devices. The pandemic has taught us that remote or hybrid work environments do not reduce productivity, but instead can boost it. Seeing this play out, many companies are adopting the BYOD culture where employees can work using their own devices. In this way, companies can onboard new employees and clients quickly, streamline blended or distributed work environments, and enhance employee satisfaction and productivity by giving them the freedom to choose their own device.

With remote work set to become a permanent and a prominent feature of the work culture, companies must develop policies regarding the safe and secure use of personal devices at work.

This comprehensive ebook will help you understand how BYOD may benefit your employees and company, and what policies, guideline, and practices you should be mindful of to build a secure and productive BYOD program.

What Does BYOD Mean?

The BYOD and enterprise mobility market was valued at $54.69 billion in 2019 and is expected to reach $165.25 billion by 2027, growing at a CAGR of 15.99% from 2020 to 2027. BYOD is the most common acronym associated with personal devices at work but, you might also hear other terms like bring your own technology (BYOT), bring your own phone (BYOP) or bring your own computer (BYOPC).

A BYOD policy saves businesses money because they don't have to pay for costly hardware. Additionally, allowing staff to use their own devices ensures employee comfort and satisfaction. The convenience of using a single device means employees do not have to carry and manage multiple devices simultaneously. This avoids the friction and stress that comes with switching between devices.

In an organization, BYOD policies outline the rules and regulations regarding the use of personal devices like laptops, smartphones and tablets by employees to conduct business. A BYOD practice can be beneficial for the organization, but it can pose significant security risks if left unmanaged. As employees will be accessing their organization's private network, communication channels, storage, applications and systems via their own devices, even a simple security lapse can result in the company falling victim to a cyberattack.

The question arises, how can companies establish effective BYOD policies that are resilient against threats yet not intrusive. Tactical questions arise as well, like how can you to delete official data in the case of loss or theft of a device? Questions like these have become even more pertinent given the COVID-19 pandemic and the increasing frequency of cyberattacks across industries. In an environment where hybrid work environment is becoming the norm, BYOD policies need re-examining.

But first, here's the lowdown on BYOD essentials.

How Popular Is BYOD?

The Enterprise Mobility Management exceeded $3.5 billion in 2019 and is estimated to grow by over 15% CAGR between 2020 and 2026, according to Global Markets Insight.

In recent years, BYOD practices have grown in popularity, and the COVID-19 pandemic, which forced professionals around the world to work remotely, further drove this growth. Other global trends fueling the growth of BYOD is the availability of high-speed mobile internet and the rapid rollout of 5G throughout the world. Furthermore, an increasing number of smartphone users in many countries also aid the culture of BYOD.

Why Do Companies Use BYOD?

In 2004, VoIP provider BroadVoice introduced a way for businesses to route calls to their personal devices, and the term BYOD caught on. But it was Intel that brought the term to a wider audience in 2009. The company was among the first to draft and implement a BYOD policy after noticing employees connecting their own devices to the corporate network. BYOD adoption has increased since then, as has the need for related policies. Several companies are now looking into offering employees the option to use their own devices at work and implementing a BYOD policy.

Benefits include:

Higher Productivity

Employees are comfortable using their personal devices due to practice and want to keep using them at work. As a result, they can do their jobs more efficiently and effectively. Moreover, the personal devices that employees purchase are often superior to the ones provided by the company. Organizations benefit from employees producing better quality output as well as work faster using their own top-end devices and tools. Employees also tend to upgrade their devices quicker than their respective employer.

Increased Employee Responsiveness

According to a Deloitte report, more than one-third of smartphone owners worldwide check their phones within five minutes of waking up. In our daily lives, we are highly dependent on our personal devices. Our productivity on personal devices is enhanced by our familiarity with the UI compared with a new device. Because employees are accustomed to their personal devices, allowing them to continue using these devices at work improves their feeling of comfort and satisfaction. It's also easier for employees to work with a single device than with multiple devices, especially if their work requires them to travel, as it makes work more convenient.

Lower Shadow IT Risks

It is predicted that by 2030, nine out of every 10 people aged six and above will be digitally active. In a world where smartphones and tablets are ubiquitous and virtually an extension of our lives, it is inevitable for employees to use their personal devices for work even if a BYOD policy is not in place.

The term shadow IT refers to information technology projects that are managed outside of and without the knowledge of a company's internal IT team. It can be a pool of applications and devices that employees use for work without prior approval from IT. This could also include checking the office email or using the common communication channel outside of the secure business environment. Companies must accept that employees will use their personal devices for work and thus set guidelines for their use. This will ensure better security while giving employees a choice in their work style.

Cost Savings

The price of a mobile device can range from $200 to well over $1,000. It can add up to a large number when multiple employees need new devices. There is constant pressure on companies to lower IT costs because it entails heavy investments and can take a big chunk out of the budget, especially of small and medium-sized companies that must spend every dollar wisely. BYOD policies can help companies drastically reduce their IT costs while ensuring employees can choose and use their own devices of superior quality. Due to bulk purchases, companies often get a good deal on consumer tech. Partnering with brands can help them offer their employees a more affordable option to own the gadgets they want. All parties benefit from the deal. It's a win-win situation for everyone.

Connected Remote Workforce

Since employees will always need to visit clients or travel, remote work is inevitable, not to mention many companies are adopting hybrid work arrangements even as the pandemic winds down. Without a BYOD policy, on-desk and remote workforce might communicate in a way that poses potential security risks. On the other hand, a stringent policy will help establish the necessary security protocols for personal devices.

Improved IT Management

In addition to helping companies tame their IT investments, BYOD policies enhance device management. The use of personal devices for work is a given. Businesses can reduce the number of devices they need to manage by eliminating the requirement to use different devices for work and personal purposes. By setting guidelines for device requirements and establishing clear policies, they can further reduce this number. Having fewer devices to manage allows companies to further reduce costs and improve security for each device while improving their IT efficiency.

Support for Cloud Adoption

Market research firm Mordor Intelligence expects the cloud migration market to reach $448.34 billion by 2026, up from $119.13 billion in 2020, a CAGR of almost 29%. Due to the COVID-19 pandemic, cloud adoption has surged among small and midsize businesses. Allowing BYOD policies enables your company to integrate more mobile devices into its IT infrastructure that are best suited for cloud computing. With this, employees can access critical business applications from anywhere and at any time.

Retention of Top Talent

It is inconvenient for employees to carry multiple devices that have work applications installed. Furthermore, switching between personal and work devices consumes precious productivity time. This makes work tedious, and companies risk losing some of their best talent to competitors who permit personal devices at work.

What Is an Example of BYOD?

Some professionals may benefit more from BYOD policies than others. Let's look at managed service providers (MSPs). MSPs use multiple tools to manage their own IT infrastructure and that of their clients. They use these tools to automate many of the routine tasks, so they can focus on the critical ones. The ability to use these tools even on the move gives these professionals the freedom to perform their tasks no matter where they are. A secured mobile device could let them take care of an urgent service ticket for a client while they are in the middle of a meeting with another client.

Having strong BYOD policies allows MSPs to streamline their business and reduce costs. Imagine an MSP employee visiting a client and having to carry multiple devices like a personal mobile, a work mobile and a laptop. It is sure to affect the employee's performance if he or she must travel with a heavy load. With a BYOD policy in place, the employee needs only one device to manage everything.

BYOD policies also allow employees to strike a balance between their personal and professional lives. As the MSP industry moves toward a mobile-first philosophy, adding a BYOD policy at work will support this shift and ensure that the security of devices is upheld.

Pros and Cons of BYOD

There will always be positives and negatives to any new work practice you adopt. By addressing this weakness, the usefulness of the program increases, and the risks are outweighed. A BYOD policy has proven beneficial for many roles that involve travel, remote work or customer contact. On the other hand, the naysayers have always emphasized the security risks associated with BYOD. Employees accessing company networks with personal devices increases cybersecurity threats by giving hackers an easy way to breach the system. However, companies have begun fixing security loopholes that occur when BYOD is practiced because they recognize it's a pain point. Let's examine both the pros and cons of allowing BYOD at the office in this section.

Advantages of BYOD Practice

BYOD not only reduces hardware costs for the company, but also encourages employees to take care of their own devices. Additionally, it gives employees greater mobility, which improves their satisfaction and productivity. Overall, it has a positive effect on the company's environment and bottom line.

The advantages are as follows:

Better Quality Work Due to Familiarity With the Device

Whether we choose an Android, iOS or Windows operating system or customize the layout of the apps and user interface, we go to great lengths to customize our devices. So, if we get to use personal devices for work, we feel more comfortable and in control of the device. As a result, our productivity increase since the device is specifically tailored to our skill level, and we know the best way to use its features.

Flexibility

Flexibility is often cited as an important quality in a business. Businesses that are flexible can adapt to economic, technological and consumer changes easily and thus perform well consistently. A BYOD policy allows for greater flexibility in the workplace. With flexibility to work anywhere and anytime, employees gain more productive hours while also striking a better work-life balance.

Financial Saving

Earlier we noted that companies can save a great deal of money with BYOD. Consumer tech brands often provide devices at a discounted rate to companies. Employers can extend this discount to their employees so that they can buy a device at a lower price and use it for work and personal purposes.

Latest Gadgets and Higher Turnaround Time

Generally, employees upgrade their devices more frequently than a company would. With the latest device, employees get upgraded features, faster speed and improved functionality, which speeds up work. As a result, companies generate more revenue because workers are more productive.

Disadvantages of BYOD Practice

It is important to implement BYOD policies carefully. To ensure that BYOD policies offer more benefits than risks, companies must follow a strategic planning process and implement security measures. BYOD has demonstrated the good side but let's discuss areas of concern.

Security

Bringing your own device to work poses a significant security risk. We know that cybersecurity is no longer a question of "if" but "when." A company's network becomes more vulnerable with every new device it adds. By allowing your employees to bring their own devices to work, you're essentially trusting them to keep the device secure.

It is important for BYOD policy to include strict security guidelines to minimize the risk. It is imperative that companies have some access to their employees' devices ensure that security protocols are followed and implemented. Companies can remotely control and access their employees' devices to keep antivirus and antimalware running and deploy updates in a timely manner. It can, however, create a feeling of distrust between the employer and the employees since the latter doesn't know how much control the employer has over their phone.

Employee Privacy

Currently, cybersecurity and data privacy are dominating headlines across the world. In recent years, companies are increasingly under fire for violating privacy regulations. In the wake of increased privacy concerns, employees may object to companies watching over their personal devices that they use for work. For BYOD policies to work, companies must carefully balance privacy and security. To do so, companies can use enterprise mobility management (EMM) and mobile device management (MDM) tools that allow them to manage the security of their employees' devices without intruding on their security.

Lack of Standardization

Another challenge of BYOD is lack of standardization. In collaboration and teamwork, using different tools and devices for the same task can bog down the process. It is possible for files on one person's device to not work on another person's device due to differences in operating systems and applications. The purpose of BYOD policies is to bring about uniformity in the workplace so that collaboration does not suffer. Tools and software for critical work can be recommended so that files and information can be shared more easily.

Device Repair

It is the responsibility of the company to repair and fix devices that it issues. But BYOD can create confusion regarding who pays for device repair and maintenance and in what proportion, slowing productivity. While employees might expect employers to bear some of the cost of repair since they use the phone for official purposes, employers might assume employees will bear the cost as the BYOD policy is implemented to give employers more flexibility. Before allowing BYOD at work, both employees and companies should have a clear understanding of how to handle damage and maintain business continuity.

BYOD Security

The corporate world is still divided over adopting BYOD practices at work despite its many benefits. The biggest concern they have is security risks. This section will investigate the security concerns that come with BYOD practices and how they impact productivity, culture, and reputation of a company.

Data Theft

Global cybercrime costs will increase 15% per year over the next five years, reaching $10.5 trillion annually by 2025, according to Cybersecurity Ventures. Cybercriminals are constantly developing and employing sophisticated, modern methods of gaining access to secured business environments. Remote work has opened up a playground for cybercriminals and demonstrated that security risks increase when workers leave a secured company environment.

If updated security measures are not in place, BYOD devices become a hot target for hackers to exploit and gain access to a company's IT infrastructure and steal valuable information. Although the phone might be secured, employees may not exercise enough caution when using WIFI networks. Even if hackers cannot get into a phone, they can steal data-sensitive files while they are being transferred over an insecure network or internet connection. Both the employee and the employer should proceed with extreme caution when implementing BYOD practices.

Malware Infiltration

Many of the biggest cyberattacks are successful due to employees falling victim to phishing emails that once clicked on download crippling ransomware on a company's internal network. With BYOD practices, human error in cyberattacks increases exponentially. Every day, employees download multiple tools, files, and software on their devices. A slight carelessness can result in an employee downloading malware and putting sensitive company data at risk. It is important to set clear guidelines on phone usage and download activities so that the employees' personal usage does not impact company data.

Loss of Device

Company data is also at risk from device being lost or from stolen. BYOD policies outline strict password protocols, but if employees don't follow them, company data may fall into the wrong hands. Employees often store passwords on their devices without using secure apps. It could expose data across the organization to further exploitation.

Issues With Data Removal and Retrieval

In the event that an employee resigns, or the device gets damaged, stolen or lost, BYOD policies lay down the guidelines for managing data. In these cases, employees must wipe the company data from their phone so it cannot be exploited by them or an external entity. Even employees who have the best intentions can forget to take the necessary data protection and deletion steps, putting the data at risk of being misused or stolen.

Legal Cost

An organization's reputation and financial well-being will be affected if BYOD devices become compromised and information falls into the hands of threat actors. It may lead to a spate of lawsuits for damages if the data concerned is extremely sensitive or belongs to customers or business clients. In addition to irreparable reputational damage, this can set the company back by millions of dollars.

Weak Policies

Many companies lack a robust BYOD policy, even though they have a BYOD program. In the absence of strong policies, mistakes and slips are not held accountable and no one takes responsibility for them. Employees also do not have knowledge of data handling and security best practices in the absence of policies. Companies should establish robust BYOD guidelines and practices to minimize these risks.

What Are the Risks and Liabilities of BYOD?

It is possible that BYOD practices conflict with the company's compliance guidelines. Several sectors, like healthcare and finance, have strict guidelines in place around the management, access and distribution of confidential data and information. Compliance and security rules are easy to enforce on company-issued devices, but on personal devices it becomes difficult to keep track of how securely the data is stored and who else can access it.

With BYOD practices, the challenge goes beyond security to compliance. To ensure compliance with company policies, how many extra tools and software will an employee be willing to download on their personal devices and how much access are they willing to give the company through their devices without worrying about privacy? To ensure compliance, employees and employers need to be on the same page when it comes to these questions. A better compliance rate is achieved when there is more agreement between the two parties.

How Do You Make BYOD Secure?

However, while BYOD practices can increase the risk of security to company data, network and confidential information, there are many ways to secure the practice and make it also have more positives than negatives. Here are some tips to make your BYOD practice both secure and flexible:

Password Rules

Your first line of defense is a strong password. A weak password is as bad as having no password at all. First, make sure your employees use strong passwords for their devices as part of your BYOD program. Also include critical software and applications in the rule. Employers can prevent unauthorized access to company databases and networks by password locking all work-related applications. Clearly define the password strength requirements because "Password123" will not help keep anybody safe.

Security Solutions

Invest in the latest antimalware and antivirus solutions to protect your employees' devices from common cybersecurity threats. Business continuity is ensured when these tools mitigate a variety of threats and prevent viruses from encrypting or stopping work.

Prohibited Websites and Applications

BYOD policies work best when employers and employees commit to doing their part. Viruses and malware are more likely to be downloaded on a device when an employee accesses unsafe or suspicious websites. It is important to establish clear guidelines regarding the types of applications, files and websites that are to be avoided because they pose a security risk. It is also crucial to set clear guidelines regarding social media usage, since it can also be used as an entry point of attack.

Principle of Least Privilege

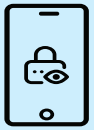
Every day companies gather more and more information, tools, and software. Employees need access to only parts of the database that are relevant to their work. Therefore, companies can enhance safety precautions by enforcing the principle of least privilege on BYOD devices. A company's entire IT infrastructure is less likely to be infected because of malware or ransomware when employees have only the required tools or datasets at their disposal. A data breach will result in less damage if this practice is implemented.

Backup

In addition to security concerns, lost or stolen devices can pose problems for businesses if the data is not backed up. Having to repeat work slows productivity and can be frustrating for the employee. If employees bring their own devices to work, companies should make sure they follow a strict backup procedure and regularly take backups. It would ensure business continuity even in the event that a device gets stolen, lost or damaged.

Security Training

The companies that train their employees in cybersecurity best practices identify more security breaches and have fewer incidents. According to a Webroot survey, respondents reported a reduction of 41% in phishing incidents and a 59% increase in the reporting of suspicious emails to IT teams after completing a security awareness training program.



Opting for Mobile Security Tools

Companies can keep their employees' devices secure without compromising their privacy by using mobile security tools. The strongest weapon in the IT department's arsenal is mobile security tool to ensure implementation of BYOD policies at work. IT departments can use these tools to monitor, manage and secure devices used by their employees at work. In addition, they can manage IOT devices that are increasingly being used at work.

Mobile Security Tools

Mobile Device Management (MDM)

BYOD at work led to the development of MDM tools. MDM tools can be used to remotely manage mobile devices in real-time as part of BYOD security policies. The tool can be used for activities such as device enrollment, patching security updates, location tracking, device provisioning, or even wiping data from a device in case it is lost or stolen.

Mobile Application Management (MAM)

MAM tools were developed in response to employees' demands for security and privacy when using their own devices at work. In contrast to MDM tools, these MAM tools are solely focused on specific applications rather than the entire device Therefore, it offers better privacy on devices. An enterprise app store is created using an MAM solutions, and only the apps within the store are monitored and updated remotely.

Mobile Information Management (MIC) Tool

MIC and mobile content management (MCM) are extensions of MAM. Most organizations have a centralized repository through which employees can access and share files and documents easily. It is home to valuable company data. The MIC and MCM tools protect this repository on mobile devices that employees use as part of the BYOD policy. Hence, the balance between privacy and security can be improved in the company.

Enterprise Mobility Management (EMM) Tool

EMM tools are designed to meet the increasing complex security requirements of companies and employee BYOD demands. It integrates into the network directory service and offers policy compliance, application customization and data security benefits. An EMM tool offers the functionality of MDM and MAM tools combined with features like containerization. The containerization process separates personal information from work data on the same device. As a result, IT departments are clearly able to monitor and access only that content that ties into the work segment.

Unified Endpoint Management (UEM) Tools

UEM is the latest and the smartest tool in the category of remote monitoring and management. Using this tool, companies can manage a variety of endpoints including laptops, mobile devices, tablets, PCs, printers and IoT devices. A UEM tool can be quickly deployed and scaled as more and more devices are deployed each day. In addition to mitigating cyber threats remotely, they can also contain a leak before it spreads throughout your entire network.

Using Kaseya VSA you can automate many endpoint management tasks and see the status of all endpoints in one place.

Containerization

IT teams can balance enterprise requirements with user requests for enhanced privacy by utilizing containerization technology on mobile devices. Using containerization, IT can create separate, encrypted, policy-enforced "containers" within a personal device, delivering emails, browser apps, and data to only those containers. It is possible for IT to wipe the containers without disturbing personal assets if a device is lost or stolen. Therefore, if users choose to leave their devices unprotected, only their personal data is at risk.

Communication with containers can be conducted over a secure encrypted channel, eliminating the need for VPNs and other inbound network connections between devices and the enterprise. As only the secure containers connect to the enterprise network, the network is shielded from probes, attacks, malware and compromised devices.

Implementing a BYOD Policy

To manage and govern BYOD devices within the network, you must establish a BYOD policy. BYOD policy should clearly define objectives, scope, procedures, protocols, and contingency plans so that all parties involved are informed of what to do when certain scenarios arise.

It is important to discuss these policies thoroughly and to write them in clear language before rolling them out. The BYOD policy should be designed with people from various teams, like HR and IT, on board so that multiple perspectives are obtained. Consider the opinion of employees, as well. The policy will be comprehensive and have no loose ends as a result.

Furthermore, it's important to ensure that employees follow company policies. Make sure everything stays on track by checking in with employees regularly and reminding them to follow policy rules.

What Should a BYOD Policy Include?

The use and evolution of technology are in constant flux. Once a policy is in place, you should revisit it periodically to make changes and keep it current. Elements of an effective BYOD policy are as follows.

Device Usage Protocols

Employees who bring their own devices to work should install antivirus and antimalware tools on the devices, as well as a UEM solution. To ensure the security of company data, employees should only take backups of their data using authorized company cloud-backup applications and should only do this through the secure company network. In addition, any updates to computer software or hardware should only be made after securing approval from IT.

Reimbursement Policy

Employees are reimbursed for certain expenses, such as internet bills or device repairs, by their employers. There should be a simple and clear reimbursement process for BYOD. Some companies even provide a stipend for this purpose. A clear explanation of reimbursement and cost details should be provided so employees know that if the expenses exceed the set limits, the company is not responsible for it.

Remote Wiping of Data

When an employee's personal device used for work is lost or stolen, a remote wipe procedure will help organizations clean all the sensitive data from that device. The company's policy should state that it will not be held accountable for personal data loss in these scenarios. In addition, it should state how quickly a remote wipe should be executed in the event that a device is lost or stolen.

End of employment

When an employee leaves the company, the best way to ensure data safety is to have the internal IT team inspect it. Ensure that this step is spelled out in the BYOD policy and make sure IT removes all business information before an employee takes leave.

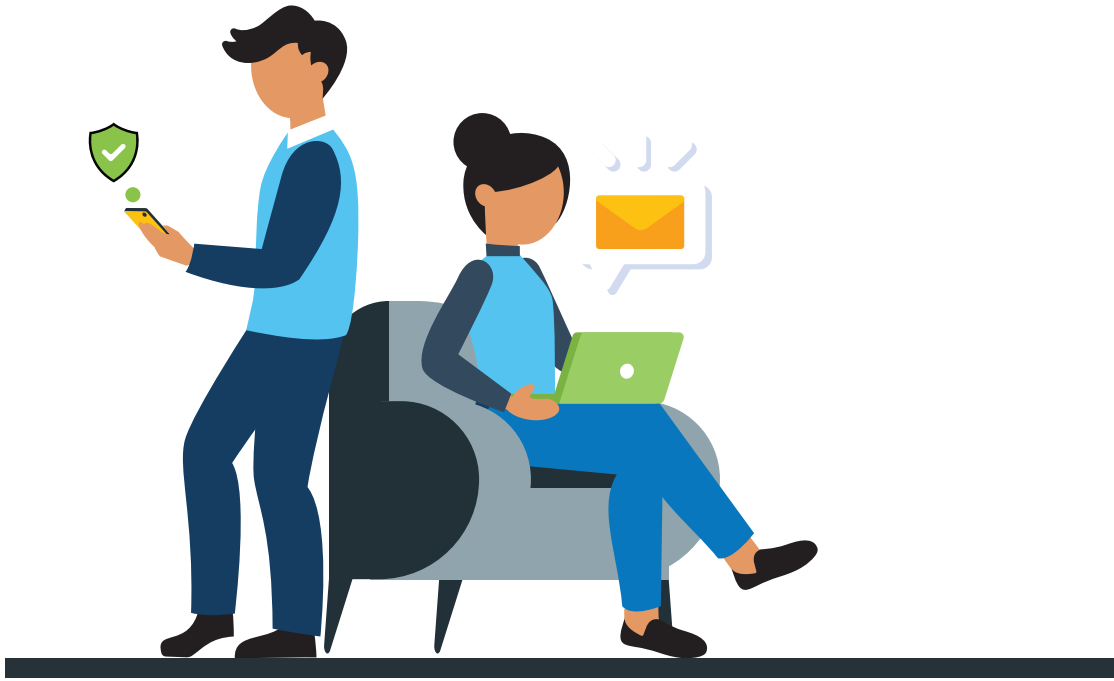
Policy violation

Even if policies are well written, employees may forget or become careless about implementing them. As a result, it is important to put rules in place around policy violations to protect company data.

Secure BYOD Management with Kaseya

Kaseya's EMM tool combines the capabilities of BYOD, MDM and MAM tools into one. To provide comprehensive device security, Kaseya EMM integrates with Kaseya VSA IT management solution. Secure BYOD management, robust app management, and ease-of-use allow you to achieve maximum administrative efficiency. The UI is stream-lined to facilitate quick user onboarding.

Kaseya VSA is also integrated with Cortado MDM to give MSPs and internal IT teams a simple and effective mobile device management system to their clients and users. Get started with secure BYOD today.



Learn more about VSA

About Kaseya

Kaseya is the leading provider of complete IT management solutions for managed service providers (MSPs) and midsized enterprises. Through its open platform and customer-centric approach, Kaseya delivers best in breed technologies that allow organizations to efficiently manage and secure IT. Offered both on-premise and in the cloud, Kaseya solutions empower businesses to command all of IT centrally, easily manage remote and distributed environments, and automate across IT management functions. Kaseya solutions manage over 10 million endpoints worldwide.Headquartered in Dublin, Ireland, Kaseya is privately held with a presence in over 20 countries. To learn more, visit www.kaseya.com.

09082021