Kaseya

15 TIPS TO ELIMINATE IT INEFFICIENCY

Beware the Ides of March. Instead of suffering under the tyranny of inefficient workflows this year, let's use this day to eliminate IT inefficiency on all fronts.

From inefficient processes to outdated technology, a number of factors contribute to IT department sluggishness. However, there are several ways to overcome these challenges and build a lean, mean IT machine. According to a McKinsey report, modern technology can automate 45% of IT activities. Automation empowers small and midsize businesses (SMBs) with modest budgets to deliver value at a reduced cost. Beyond the bottom line, 76% of IT professionals reported increasing burnout, and automation can make a real impact on the lives of the people who manage business-critical functions.

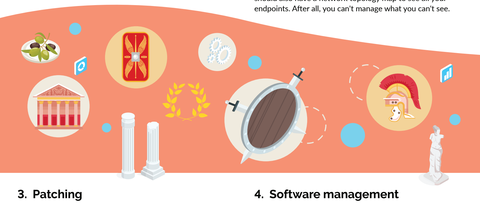
Here are 15 tips and tricks you can use right away to eliminate IT inefficiency and meet your targets so you can go back to loving your job again.

1. Onboarding new users

Automating the user onboarding process leads to increased efficiency, improved user experience and fewer manual errors. This approach gives new users proper access and security from the get-go, reducing the risks of a cyberattack or misconfigurations. Automating tasks like configuration hardening, permissions and enforcing two-factor authentication (2FA) streamlines the process, saving time and effort for both the new user and the technician.

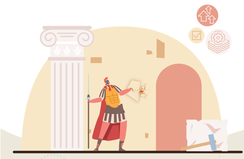
2. Discovery and inventory

Organizations can take advantage of deep, rich and continuous insights into their physical and virtual assets by automating endpoint discovery and inventory. A comprehensive understanding of the endpoint landscape, including hardware and software configurations, usage patterns and vulnerabilities, leads to improved decision-making and proactive risk management. Real-time tracking enables timely response to changes or threats and reveals hidden or misconfigured devices, reducing the risk of blind spots. You should also have a network topology map to see all your endpoints. After all, you can't manage what you can't see.



3. Patching

Automating patching keeps systems up to date and secure while helping organizations perform at their best. With **"fire and forget"** automated patching, organizations can effortlessly apply patches and update MacOS and Windows operating systems and third-party software, saving valuable time and resources. Technicians can minimize the potential for day-one disruptions by vetting patches to ensure they don't interfere with existing processes and procedures. With VSA's futuristic patching, you can even turn an endpoint on in the middle of the night, patch it and turn it off again.



4. Software management

Automation helps streamline the software deployment process for different end users based on policies. Software distribution can be customized and tailored to meet specific needs based on user groups, departments or machine locations. This results in a faster, more efficient and cost-effective process for managing software, freeing up valuable time and resources for other critical tasks.

5. Routine server maintenance

Automating routine server maintenance can improve reliability, reduce downtime and free up time for IT staff to focus on higher-priority tasks. It covers scheduled server downtime, "fire and forget" maintenance tasks that run automatically, scheduled reboots and automatic retries in case of failures. Automating server maintenance helps organizations ensure the health and performance of their servers and minimize disruptions.

6. VDI management

Automating VDI management simplifies the process by allowing users to set a Golden Image, changes made to which reflect in all clone images. Automating VDI patching ensures that all clone images are patched, keeping your virtual infrastructure up to date. Using VSA, you can easily deploy software and harden your VDI configuration with customizable policies.

7. Backup management

Automated backup management helps you stay on top of your data protection strategy, restoring your data in the event of a failure and providing detailed reporting so you can track the status of your backups. By deploying agents to your devices and endpoints, you can automate the backup process and schedule backup jobs at regular intervals.

8. Integrated documentation

Integrating documentation directly into your endpoint management solution means that you have quick and easy access to the information you need and when you need it. Access procedures, passwords and information related to an asset or organization in under THREE clicks, eliminating the need to search through stacks of papers and files.

9. IT reporting

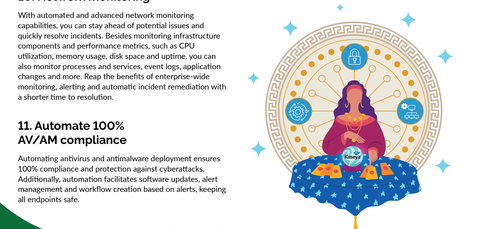
Automated IT reporting is indispensable for demonstrating the impact and success of IT initiatives. With automation, reports can be easily prepared and delivered to stakeholders, providing clear and concise information on the performance of various technological systems and processes. Pre-built templates reduce manual report creation, allowing technicians to save time and help drive better business outcomes.

10. Network monitoring

With automated and advanced network monitoring capabilities, you can stay ahead of potential issues and quickly resolve incidents. Besides monitoring infrastructure components and performance metrics, such as CPU utilization, memory usage, disk space and uptime, you can also monitor processes and services, event logs, application changes and more. Reap the benefits of enterprise-wide monitoring, alerting and automatic incident remediation with a shorter time to resolution.

11. Automate 100% AV/AM compliance

Automating antivirus and antimalware deployment ensures 100% compliance and protection against cyberattacks. Additionally, automation facilitates software updates, alert management and workflow creation based on alerts, keeping all endpoints safe.



12. Ransomware detection

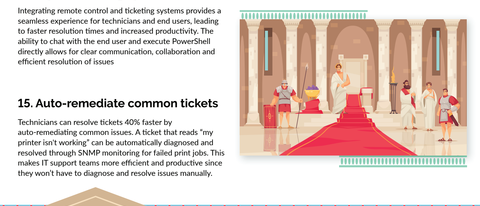
Automated ransomware detection technology can quickly and accurately identify the signs of a ransomware attack. Your RMM should detect signs of infection, such as the easy-to-detect elements like ransomware notes, encrypted and deleted files, and more complex behaviors like lateral movements in the network and privilege escalations. This real-time protection helps organizations stay one step ahead of the attackers, keeping their sensitive information and systems secure from harm.

13. Quarantine infected endpoints

After automated ransomware detection, the next step is automatically quarantining infected endpoints immediately by disconnecting them from the network. With the dwell time increasing to 30 days, automatically detecting and quarantining infected endpoints is a significant step toward combating ransomware effectively.

14. Launch remote control directly from your ticketing system

Integrating remote control and ticketing systems provides a seamless experience for technicians and end users, leading to faster resolution times and increased productivity. The ability to chat with the end user and execute PowerShell directly allows for clear communication, collaboration and efficient resolution of issues



15. Auto-remediate common tickets

Technicians can resolve tickets 40% faster by auto-remediating common issues. A ticket that reads "my printer isn't working" can be automatically diagnosed and resolved through SNMP monitoring for failed print jobs. This makes IT support teams more efficient and productive since they won't have to diagnose and resolve issues manually.

Follow these 15 steps to assassinate IT inefficiency, deliver best-in-class service to your end users, and get your nights and weekends back. If you find these tips outlandish or struggling to conceive how you would execute them in your current RMM, that's a sure-fire sign to upgrade your software. Get rid of your outdated, hard-to-use RMM and replace it with a best-in-class RMM like VSA that can empower you to improve efficiency, integrate with your current IT stack and protect your IT ecosystem.

Book your free trial now!