

Best Practices for Selecting an Endpoint Management Solution

Based on Real User Reviews of ManageEngine Desktop Central

2020



ABSTRACT

Endpoint management has grown more challenging and complex in recent years. IT managers feel pressure to be efficient in managing endpoints while keeping them secure and high-performing. What makes for an effective endpoint management solution in these circumstances? Best practices for selecting a solution include factors like enabling remote administration, managing mobile devices, and coordinating patch management. This paper examines such selection criteria, among others, based on real user reviews of ManageEngine Desktop Central published on IT Central Station.

CONTENTS

Page 1.	Introduction
Page 2.	The State of Endpoint Management
Page 3.	Best Practices for Selecting an Endpoint Management Solution
	Enable Remote Administration
	Streamline Software Deployment
	Coordinate Patch Management
	Know which Applications are Installed
	Manage Mobile Devices and USB Connectivity
	Image OS's and Applications
	Manage Configuration
	Establish a Security Baseline
Page 9.	Conclusion

INTRODUCTION

Network endpoints like laptops and smartphones provide tempting targets for malicious actors. As a result, IT managers and their counterparts in security face an increasingly challenging and complex endpoint management mandate. Endpoints are expected to perform well, be highly available, and extremely secure. And the management process itself should not cost too much.

Endpoint management solutions are adapting in step with evolving requirements. The best practices for selecting a solution now include factors like enabling remote administration, managing mobile devices, and coordinating patch management. This paper examines such selection criteria, among others, for endpoint management solutions. It is based on real user reviews of ManageEngine Desktop Central published on IT Central Station.

The State of Endpoint Management

Endpoint management has never been simple, but the difficulties involved in the process have grown significantly in recent years. One issue is the simple quantity and variety of endpoints. Today, nearly every information worker has a mobile device as well as a corporate-issued laptop. He or she may also have a tablet and personal mobile device used in business. With the advent of nearly universal work-from-home due to the COVID-19 pandemic, such consumer-grade endpoints have become ubiquitous.

As the endpoint attack surface area grows and devices become more richly-populated with applications, the cyber threat environment has become more dangerous. Many major data breaches in recent years have started with a hacker compromising an endpoint. Additionally,



the endpoint management responsibility tends to fall in between IT operations and security operations. An effective endpoint management tool will balance operational and security concerns while enabling the two groups to collaborate on their respective workloads.

Best Practices for Selecting an Endpoint Management Solution

What makes for a good endpoint management solution? Opinions vary widely, of course, depending on use cases and organizational contexts. However, as members of IT Central Station reveal in their reviews, a number of best practices can guide the endpoint management solution selection process. By pursuing these practices, IT and security managers can find a solution that works for their needs.



Enable Remote Administration

Remote administration has always been useful for endpoint management, but today it's totally non-negotiable. Few employees are even on the premises today to have their endpoints managed. Figure 1 depicts the range of endpoint management processes that IT departments need to oversee for both on-premises and remote endpoints. As a [Product Manager - Solution Architect](#) at iOCO, a tech services company with over 10,000 employees, explained, "DesktopCentral allows you to do desktop support without interrupting the user."

“

It's very valuable being able to fix a problem without stopping user productivity.

By using remote event viewer or remote CMD [Command Prompt], a desktop technician can do troubleshooting without the user knowing. This allows for a more professional and modern way of doing IT support.”

“One of my favorite features is a simple remote CMD,” said an [IT Manager](#) at The White Family

Companies, a transportation company with over 500 employees. He added, “This enables us to troubleshoot certain things without interfering with the user desktop session or needing to ask them to take remote control of the machine. It’s very valuable being able to fix a problem without stopping user productivity.” A [System Administrator](#) at Vodovod Osijek, a small public utility, similarly found the tool for remote support to be “great with the ability to use shortcuts and chat.”

Streamline Software Deployment

IT operations teams are responsible for deploying the latest versions of software onto users’ devices. This can be an active or passive experience for the user. The best solutions streamline the passive updates, but also make the active updating process as smooth as

possible for everyone involved. iOCO’s Product Manager remarked that ServiceDesk Plus “has created even further efficiencies by allowing the user to use the agent’s self-service portal to request software, create a workflow to have approvals in place, and let Desktop Central automatically deploy the software once it’s approved.”

A [Systems Administrator](#) at a manufacturing company with over 500 employees also found value in the Desktop Central Self Service Portal. His team uses the portal to push out applications and give end-users the option to install the application if they want it. And, the application

“
... all features together have become the Swiss Army Knife of desktop management. They all work hand in hand.

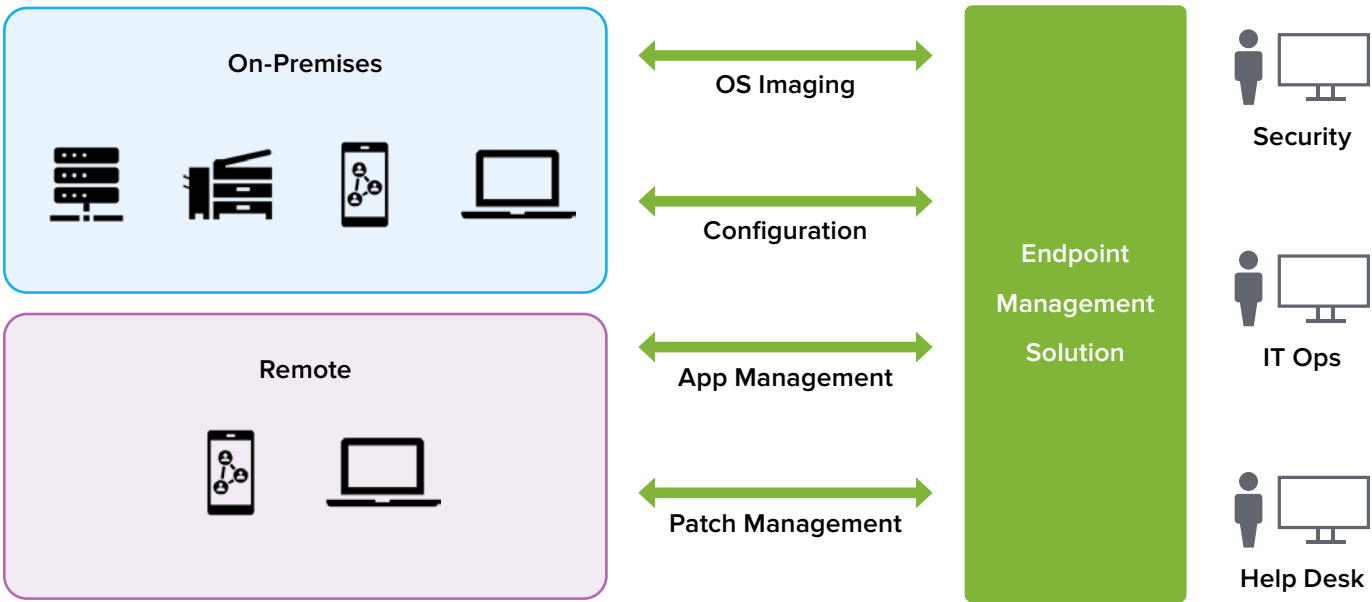


Figure 1 - The varying roles of an endpoint management solution

can be installed without administrative privileges, so the whole process takes less time from the company’s Help Desk or System Administrators.

“Software deployment saves an unbelievable amount of time installing an application on hundreds of computers,” said the White Family Companies’ IT Manager. He then shared, “Honestly, I have to say all features together have become the Swiss Army Knife of desktop management. They all work hand in hand.”

The System Administrator at Vodovod Osijek is responsible for 180 endpoints spread across several buildings. As he noted, “We have an Active Directory environment. It is hard to maintain updates, install software, and do support in such an environment. Desktop Central has given tools to maintain our environment with ease, deploy updates to machines. Deploy [sic] software is an easy to use tool for our needs.”

Coordinate Patch Management

IT Central Station members who manage endpoints all bear the burden of patch management. It’s a never-ending series of updates, most of which are required for maintaining a strong security posture. Patch management is time-consuming and disruptive. For these reasons, users look favorably upon endpoint management solutions that can help with coordination of patch management.

“The most valuable feature of this solution is the Patch Management,” said iOCO’s Product Manager. “With Desktop Central, we have

“**... patch management is an excellent tool because we deploy patches with ease and also decline patches.**”

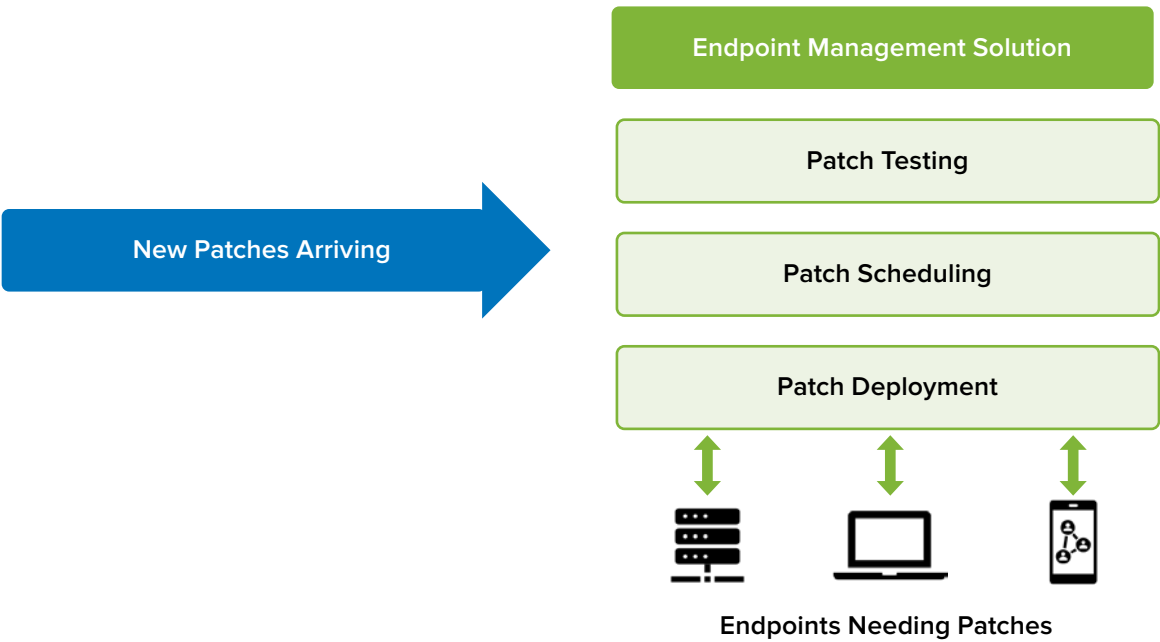


Figure 2 - The patch management workflow

been able to maintain patch compliance across our entire estate.” The System Administrator at Vodovod Osijek similarly found that “patch management is an excellent tool because we deploy patches with ease and also decline patches.” The latter point is significant. Not all patches are ready to go. They need testing, with their deployment scheduled for the right times of day and so forth. Figure 2 captures the essence of the patch management workflow.

“

It has enabled my team to quickly identify machines, who is using it, what applications are installed...

Other notable comments about the importance of patch management in endpoint management include:

- “The mundane process of patch management is now a breeze.” - IT Manager at The White Family Companies, Inc.
- “It has greatly simplified updating and patching within our systems.” - [Vice President Derivatives Ops IT](#) at a large financial services firm
- “It can do any kind of patch management. It is best at the general management of assets and reporting. For example, we can use it for virtually anything having to do with security on endpoints. Say we have maybe 4,000-plus devices that we have to monitor and upgrade the OSS (Operations Support Systems) and apply patching. This can all be handled with Desktop Central from a central location. That is what makes it a very good option.” Systems Administrator at a manufacturing company with over 500 employees

Know which Applications are Installed

Lack of awareness about applications installed on endpoints creates security risk exposure along with potential operational difficulties. IT and security managers need to know what software their device users are running. Endpoint management solutions should ideally provide this information on demand. This is what an [IT Projects Manager](#) at a small energy/utilities company found with Desktop Central. He said, “ManageEngine has improved my organization because right now we can actually monitor and find out which software products are installed on each desktop. We can then figure out which ones have to get patched and so forth.”

“It has enabled my team to quickly identify machines, who is using it, what applications are installed, and a huge set of tools to solve most problems,” remarked the White Family Companies’ IT Manager. “It has become a single pane of glass for a majority of client support and administration.” According to the [CISO & Head of IT Strategy](#), Architecture, Operations & Infrastructure at Lumber Liquidators, a retailer with over 1,000 employees, the most valuable feature of Desktop Central was its ability to ensure that the inventory of hardware and software is accurate.

Manage Mobile Devices and USB Connectivity

IT managers want to know that their endpoint management solutions can deal with the many varied challenges inherent in staying on top of smartphones and the like. This was the case for the White Family Companies’ [IT Manager](#), who shared that Desktop Central’s mobile device management eliminated the problem of

lost or missing iPads or iCloud-locked tablets and phones. The financial firm's [Vice President Derivatives Ops IT](#) also acknowledged the capabilities of Desktop Central's dedicated mobile device management module, which he referred to as part of "the complete gamut of offerings." He added, "It has got asset management, service management, and asset classification."

USB connectivity, a cause of risk exposure, is another area where best practices suggest having an endpoint management with tight control capabilities. Indeed, USB devices and unlocked USB ports can be serious threat vectors for malware and ransomware attacks. In this context, iOCO's [Product Manager](#) valued the fact that his endpoint management solution could perform basic tasks like setting up USB locks on specific departments in as little as three minutes.

Image OS's and Applications

IT Central Station members emphasized the importance of an endpoint management solution's operating system (OS) and application imaging features. IT ops and security depend on having up-to-date OS's installed. The OS imaging process also needs to be efficient. The workload has typically been labor-intensive in the past.

As the White Family Companies' [IT Manager](#) explained, "OS imaging and deployment has significantly reduced the amount of time and resources needed to deploy a large set of new computers, or even just reimagine a problematic PC because of malware or other problem that would take much longer to troubleshoot." iOCO's [Product Manager](#) also found time savings for OS imaging with his new solution. He said, "We have used the image capture and deployability to do remote deployment of OS in remote areas where previously we would have to send out a person."

Manage Configuration

Given the security and operational trouble a misconfigured endpoint can cause, IT managers want endpoint management solutions that can easily keep up with device configuration. As the [System Administrator](#) at Vodovod Osijek explained, "Since deploying Desktop Central, our endpoints are all updated. We use configuration management to deploy shortcuts to our users' desktops with ease. Also, we use configuration management to map logical hard drives to our users. We have an overview of all our endpoints and their configurations." The result? He revealed that "our users are very happy with how much ease IT can solve their problems."

“

Vulnerabilities are identified and remediated rapidly, and devices are able to be rapidly imaged.

"These devices and this software can be reliably configured in alignment with standards," said Lumber Liquidators' [CISO & Head of IT Strategy](#). For his team, Desktop Central "ensures that the configuration of this hardware and software is in alignment with organizational policies and procedures. Vulnerabilities are identified and remediated rapidly, and devices are able to be rapidly imaged."

Establish a Security Baseline

Endpoints are a huge target for hackers. They contain sensitive data and provide a point of entry into the network for malicious actors and malware. Thus, the more secure the endpoint—and the more clearly security managers can see the security status of endpoints—the better the organization's security baseline will be.

Lumber Liquidators' [CISO & Head of IT Strategy](#) is in touch with this fact. He relies on Desktop Central to sustainably and rapidly build secure devices. The financial firm's [Vice President Derivatives Ops IT](#) similarly depends on Desktop Central to push upgrades to endpoints and manage them securely.

“

Things like enforcing a baseline security compliance become more important every year and now with WFH, the system needs to easily cater for it.

“Standardizing security policies is almost impossible without an application to assist,” revealed iOCO's [Product Manager - Solution](#)

[Architect](#). In particular, as he noted, “Things like enforcing a baseline security compliance become more important every year and now with WFH, the system needs to easily cater for it. To add to the problems of managing a large environment we have to look after mobile devices too.” For context, his organization has 12,000 employees on 80 domains in more than 20 countries around Africa and the world.

They use Desktop Central to run scripts that enable BitLocker across departments because it passes the encryption key back to the security tab within the Desktop Central portal. As he shared, “This really saves a lot of time and extra expense on third-party tools. We have also locked down all systems for specific applications like BitTorrent and disabled automatic updates also in under three minutes.”

CONCLUSION

Organizations that are not using effective endpoint management methods and tools need to focus on this serious area of IT and security risk. Endpoints are the front line of cyber defense in a threat landscape that is not getting any less frightening. To cope, IT and security managers prefer endpoint management solutions that enable remote administration. They need sophisticated mobile device management and efficient patch management. As IT Central Station members explained, the best endpoint management solutions go even further, offering control over configuration, OS imaging, and a security baseline. Endpoints will undoubtedly continue to evolve, especially in this time of increased remote work. Their management solutions appear to be on track to keep up. By following best practices, their users can be certain of making the right solution choice.

ABOUT IT CENTRAL STATION

User reviews, candid discussions, and more for enterprise technology professionals.

The Internet has completely changed the way we make buying decisions. We now use ratings and review sites to see what other real users think before we buy electronics, book a hotel, visit a doctor or choose a restaurant. But in the world of enterprise technology, most of the information online and in your inbox comes from vendors. What you really want is objective information from other users. IT Central Station provides technology professionals with a community platform to share information about enterprise solutions.

IT Central Station is committed to offering user-contributed information that is valuable, objective, and relevant. We validate all reviewers with a triple authentication process, and protect your privacy by providing an environment where you can post anonymously and freely express your views. As a result, the community becomes a valuable resource, ensuring you get access to the right information and connect to the right people, whenever you need it.

www.itcentralstation.com

IT Central Station does not endorse or recommend any products or services. The views and opinions of reviewers quoted in this document, IT Central Station websites, and IT Central Station materials do not reflect the opinions of IT Central Station.

ABOUT MANAGEENGINE

ManageEngine is the enterprise IT management division of Zoho Corporation. Established and emerging enterprises - including 9 of every 10 Fortune 100 organizations - rely on ManageEngine's real-time IT management tools to ensure optimal performance of their IT infrastructure, including networks, servers, applications, desktops and more. ManageEngine has offices worldwide, including the United States, the Netherlands, India, UAE, Mexico, Singapore, Japan, China and Australia, as well as 200+ global partners to help organizations tightly align their business and IT.

ManageEngine Desktop Central is a unified endpoint management solution that helps in managing thousands of servers, desktops, and mobile devices from a central location. It automates the complete desktop and mobile device management life cycle, ranging from a simple system configuration to complex software deployment. Used by more than 8,000 customers around the globe, Desktop Central helps businesses cut costs on IT infrastructure, achieve operational efficiency, improve productivity, and combat network vulnerabilities. For more information, please visit www.manageengine.com

We're proud of this whitepaper and of the people who worked on it. Some of the people who helped bring this book to the market include the following:

Author: IT Central Station Team

ManageEngine Evangelist: Giridhara Raam