THE VALUE OF MANAGED ENDPOINT SERVICES

Delivering support to users anywhere, at any time, on any device.

CDW
PEOPLE WHO GET IT®

EXECUTIVE SUMMARY

In nearly every industry, it's almost impossible to imagine work getting done today without equipping employees with devices such as smartphones, tablets and laptops.

As these end-user devices have grown more numerous (and more powerful), organizations and their employees have come to rely on them for virtually all aspects of their business. Previously analog workflows are now faster and more efficient, and employees can work from anywhere at any time, completing once-cumbersome tasks with the help of collaboration software and business apps that have drastically improved productivity.

As enterprise device environments have grown, however, inefficiencies have inevitably crept in. Especially for large organizations, these inefficiencies can add up, with untold dollars being spent on underused devices and countless hours dedicated to unwieldy management processes. By optimizing their device environments, organizations can save money, enhance productivity and improve the end-user experience.

This is easier said than done. But a comprehensive lifecycle management engagement such as Managed Endpoint Anywhere can simplify device provisioning and management, allowing employees and IT staff to get back to business.

The Challenge of Meeting Users' Needs

Today, IT shops are able to place a truly astonishing level of processing power, connectivity and usability in employees' hands, in the form of smartphones, tablets and laptops.

And it's still not enough.

The problem is that, as the quality and power of devices increase, so do the expectations of end users. Today, the device needs of executives, sales staff and back-office workers are more demanding than ever (and still growing), and even well-organized, sophisticated IT shops may have trouble keeping up.

Of course, the proliferation of devices has brought huge benefits to many organizations.

- **More timely communication:** Previously disconnected traveling sales staff are able to keep in touch with their home offices, log sales before they even make it back to their hotel rooms and file expense reports from the road.

- **More direct access to data resources:** Workers are able to access practically any file they might need from home, rather than having to make a special trip back into the office over the weekend (or wait to go back in on Monday).

- **Remote work benefits:** Companies have increasingly embraced remote work, which not only improves employee satisfaction, but also lowers office space and utility costs, and gives organizations the option of hiring talented workers from across the country — or even the world — without relocation.

- **Remote work support:** During a serious crisis, many organizations are able to seamlessly switch to a mostly remote work model, largely using their existing devices and networks, thanks to the device and connectivity progress of the previous few years.

Overcoming Hurdles

Along with these benefits, though, come challenges for IT shops. For instance, many users want to be able to use multiple devices

for the same work. This not only requires organizations to procure and manage more devices than before, but it also places pressure on them to produce a consistent experience across device types for users. Users demand constant connectivity and the ability to collaborate in real time with their colleagues around the world. On top of everything, users want access to the latest devices, and many want the ability to choose their own device.

Survey data shows that device management continues to be an area of significant struggle for many organizations. In a recent IDG survey, nearly all IT decision-makers (94 percent) said that the quality of digital interactions between people, business processes and technologies has a direct impact on workforce productivity. However, 30 percent of respondents admitted that their environments weren't fully optimized to create the most productive end-user experience, and 44 percent said that their organizations do not measure the quality of the user experience.

The challenges of modern device environments, though, extend far beyond heightened user expectations. Many organizations struggle with fundamentals such as deploying and configuring devices, supporting and maintaining endpoints, providing security and retiring devices at end of life.

While these may be relatively basic tasks for a small organization supporting only a few device types, these functions can quickly become unwieldy and complex in environments with hundreds or thousands of employees using a wide array of smartphones, tablets and laptops. It's even common for companies to struggle with simply financing timely refreshes of their device environments.

The irony is that, for most organizations, device configuration and management is not an effective use of IT staffers' valuable time anyway. It's true that organizations can have a positive impact on their bottom lines by empowering employees to be as productive as possible with the right mix of apps and devices.

However, it is also true that device environments can feel like a distraction for IT professionals, whose time is often better

$66 BILLION

Global spending on Device as a Service forecast for 2023[1]

invested in strategic projects than on replacing broken phone screens or configuring laptops for employees. When IT shops are overburdened by complex device environments, they lack the time they need to work on IT initiatives that create value for the business. This ultimately leads to an increase in costs and waste.

To strike a balance between the competing priorities of users' pressing needs and IT staffer bandwidth, many organizations have turned toward a managed engagement, such as CDW's Managed Endpoint Anywhere. It gives organizations the opportunity to offload IT support tasks, allowing IT staff to tackle mission-critical initiatives.

Additionally, some customers want a comprehensive solution that gives them the ability to maintain a three-year device refresh cycle, ensuring users have the most current device capabilities. In these cases, customers should consider a Device as a Service (DaaS) subscription model.

While DaaS was once primarily considered a mere financing method for smartphones, tablets and laptops, when coupled with device support, it has now become an end-to-end device delivery and management model that provides customers with a single price for both the device and its support.

Four Pillars of Managed Endpoint Anywhere

Many organizations have taken a reactive, one-size-fits-all approach to their end-user device environments. Often, a large enterprise will roll out just a handful of device types to thousands of employees across dozens of job roles, without giving a great deal of thought to how those users' needs differ.

Sales staff, accountants, executives and human resources employees may all be given the same laptops, for instance — with the IT department either preloading the devices all with the same applications, or else requiring employees to wait as their devices are configured.

Then, device environments are rarely revisited until it is time for a refresh, a process that often gets bumped a year or two beyond the originally planned time frame (stretching budgets, but also forcing users to work with outdated devices). And management and support tasks are typically put off until a major equipment failure takes place, forcing IT to delay other projects and unnecessarily leaving employees without the devices they need to be productive.

This approach to deploying and managing devices is backward, and it leads to inefficiencies that pop up throughout the device lifecycle. However, most organizations lack the time, capacity or internal expertise to implement device programs that truly emphasize employee productivity. Managed Endpoint Anywhere takes these burdens out of organizations' hands, providing end-to-end, subscription-based services that help enterprises to optimize every component of their device lifecycles.

Specifically, Managed Endpoint Anywhere focuses on four pillars: identity management, asset management, streamlined deployment and proactive support.

Developing Personas

Identifying different user types (or personas) within an organization is a critical step to improving the health of the digital workspace. By catering to the specific needs of user groups such as road warriors, back-office workers, warehouse employees and call center agents, companies can get the right devices to the right users and avoid waste.

Here are three tips for developing personas:

1. Emphasize business benefits: A one-size-fits-all approach to device deployment no longer works. By taking the time to determine the real needs of each user group, an organization can dial back the functionality for some users and reinvest that money in the user types that need additional device capabilities.

2. Don't forget about apps: What applications are actively being used by your end users? Are you paying for licenses that are not being used? In order to eliminate waste in your environment, it is important to know what applications are used by each persona group.

3. Refine over time: Device personas shouldn't be static. Using data analytics, organizations can constantly fine-tune their personas, leading to further cost reductions and productivity improvements.

Identity Management

Getting the right devices and the right apps into the right users' hands should be a simple objective at this point, but it's an area where many organizations continue to struggle. That's because this is more complex than it appears upon examination. To get this crucial step right, organizations must first identify core personas throughout the enterprise, simplify access to data and apps and unify management across all devices.

That's where identity management comes in.

Identity and access management (IAM) typically focuses on security and authentication solutions that help organizations keep their data and systems secure. While those solutions certainly play a pivotal role in any device environment, the term "identity management" can also refer to tasks earlier in the lifecycle, by defining the applications, access and functionality required for each user type.

By taking a careful approach to this foundational component of device management, organizations can ensure they're not providing end users with too little (or too much) in the way of computing power, apps and other resources. Finding the "Goldilocks" spot for each user is a critical step in ensuring that all employees have what they need to be productive, without encouraging wasteful spending.

For instance, proper identity management can prevent scenarios where organizations are provisioning expensive, powerful laptops to employees who never take them home (or, conversely, scenarios where knowledge workers are accessing

files and sending long emails from their phones at night because they weren't given a work laptop).

Getting identity management right can boost employee satisfaction as well — a key benefit at a time when half or more of the workforce is made up of younger workers who prioritize access to technology. This, itself, can lead to additional productivity benefits; according to Gallup, organizations with higher employee engagement see a 17 percent bump in employee productivity.

Asset Management

Asset management initiatives that are proactive, effective and ongoing can have a huge impact on an organization's overall productivity and can reduce waste in dramatic ways. For instance, imagine that a company has 1,200 licenses for a software program such as Adobe Acrobat, but a Managed Endpoint Anywhere team discovers that most users who have

25%

The estimated cost savings organizations can see from moving to a DaaS model[2]

access to the program aren't using it. By requiring employees to request access to the application (instead of pushing it out to them automatically), a company can make much more efficient use of its software assets.

These types of efficiency gains extend to devices as well. A Managed Endpoint Anywhere team can see, for example, when a device has gone unused for weeks. In a disorganized environment, employees might leave the company and then simply leave their smartphones sitting unused in their desk drawers — with their former employer continuing to pay not only the device cost, but also the cost of a monthly data plan. By identifying these scenarios, a Managed Endpoint Anywhere team can recover these devices and redeploy them effectively.

Streamlined Deployment

Deploying devices is a surprisingly complex process in many organizations. Typically, companies will procure smartphones, tablets and laptops, and then these devices will go to the IT team to be configured for each individual employee. This is an inefficient, multitouch deployment process with significant user downtime.

However, when device teams complete configurations based on a user's predetermined credentials, the process of deployment becomes more automated. This process improves accuracy and saves time for both device teams and employees. Workers get immediate access to the main applications they need to do their jobs, and as a result, employees are not only more satisfied, they're also vastly more productive.

Proactive Support

In most device environments, service desks get calls only when something goes wrong. By this point, machines aren't functioning properly, and time is being lost. With continuous monitoring, organizations can solve problems before users even know anything is wrong — leading to increased uptime and a much higher level of user satisfaction.

For example, if an organization that operates a customer engagement center sees its network capacity drop to 50 percent, it likely will reduce revenue. Often, the problem will persist for hours, or even days, before anyone elevates the issue to someone who can diagnose and solve it. The automation within CDW's Managed Endpoint Anywhere eliminates these delays. For instance, an organization might set a baseline expectation of 75 percent network health, and then monitoring tools will proactively send a ticket to the IT team if performance falls below that threshold.

Ultimately, proactive support improves productivity for end users while also simplifying support tasks for IT staffers. That's a win–win.

How Managed Endpoint Anywhere Improves Security

Cybersecurity is a major concern for organizations with dispersed device environments. Here are five ways that a Managed Endpoint Anywhere engagement can give organizations a security boost.

1. Better device tracking: When devices aren't being monitored, organizations have no way of knowing whether they're safe. Managed Endpoint Anywhere ensures that every device in an organization is accounted for.

2. Improved insight: With more insight into how devices are being used, organizations can eliminate security vulnerabilities, preventing scenarios where outdated hardware or unauthorized software puts the company at risk.

3. More time for mission–critical tasks: According to IDC, 63 percent of IT decision–makers say they could devote more time to IT projects such as security if they spent less time on device management.

4. Centralization: Managing cybersecurity for dozens of different device types can be daunting. Centralized management breaks down silos and creates a much more unified security environment.

5. Lifecycle management: Managed Endpoint Anywhere retires devices for organizations, so executives and IT shops never need worry that sensitive data is sitting on a laptop in a landfill or a second–hand shop.

The Details on Managed Endpoint Anywhere

Most organizations simply lack the capacity to effectively deliver identity management, asset management, streamlined deployment and proactive support on their own. Even businesses with effective, strategic IT staffs will inevitably become overwhelmed as their attention is pulled in multiple directions. As other pressing IT issues pop up, device management will fall by the wayside, and device refreshes will become delayed — resulting in the sort of sprawling and inefficient environments that organizations hope to avoid.

To help take pressure off of internal IT shops, and to help organizations derive as much value from their device environments as possible, CDW created Managed Endpoint Anywhere. This ongoing engagement not only delivers devices for a monthly fee, but also provides the ongoing management and support necessary to keep employees as happy and productive as possible.

Managed Endpoint Anywhere includes:

Management and strategy: The average worker today has roughly 2.5 devices, and that number is expected to increase to 5 or 6 devices in the coming years. With such a rapidly expanding device landscape, management and strategy are essential.
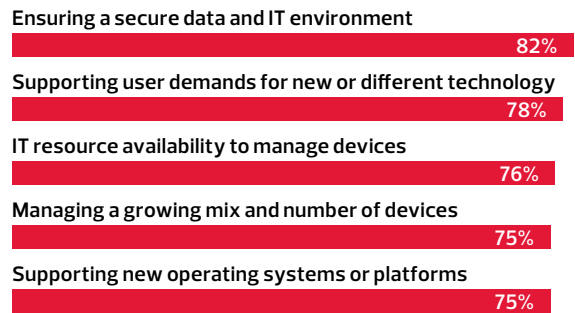
Improvement Needed

Research suggests that the very people currently running device environments acknowledge that they need help. According to survey data from IDC, large portions of IT professionals say that improvements are needed to the way their organizations currently provision, manage and support employee devices.

- **62 percent** of IT professionals say their organizations need "some" or "significant" improvement in the way they handle device deployments. Meanwhile, **68 percent** say the same about their organizations' device optimization efforts, **60 percent** say their organizations need to improve device maintenance, and **55 percent** see the need for improvements in device disposal.

- **50 percent** of IT professionals say they spend too much time procuring and managing devices.

- The top draw of DaaS is a reduced workload for IT, with **40 percent** of IT professionals citing it as a "major benefit." **30 percent** cite lower device procurement costs, and **28 percent** mention a more predictable cost model.

- **65 percent** of IT professionals believe that a DaaS engagement would have a positive impact on their organizations' device management.

Source: IDC, "How Device as a Service Could Revolutionize Lifecycle Management," April 2018

Top Device Challenges

Significant portions of IT decision-makers say the following components of their device programs are "somewhat challenging" or a "major challenge."[2]

Ensuring a secure data and IT environment
82%

Supporting user demands for new or different technology
78%

IT resource availability to manage devices
76%

Managing a growing mix and number of devices
75%

Supporting new operating systems or platforms
75%

Managed Endpoint Anywhere helps companies ensure their devices are delivering value to the business, rather than simply adding cost and management hurdles.

Initiation: For many organizations, simply getting the right devices into employees' hands is a struggle. The device onboarding process requires companies to coordinate with multiple vendors, negotiate prices, procure and configure devices, roll out apps and set up employees with their personal data. In Managed Endpoint Anywhere, CDW works with customers to define a unique workflow for order management, enrollment and configuration, deployment and data transfer. This allows IT staffers to stay focused on value-added initiatives, while getting employees up and running on their new devices faster.

Workplace support and management: This is an area where organizations chronically underestimate the amount of time and effort required to get things right, and the level of complexity that can arise after just a few missteps. CDW offers not only hardware and software support, but also device management, warranty support, app management and user identity and access.

Predictive analytics and monitoring: To optimize performance and cost over time, organizations must constantly monitor their environments and track data points that help them to make predictions about breakage and evolving needs. To this end, Managed Endpoint Anywhere proactively monitors device health checks based on 10 performance criteria.

The benefits of proactive monitoring are numerous, but here are a few examples of how analytics can deliver direct cost savings to your organization:

- **Recoup unused licenses.** By tracking who is using which applications and how they're using them, CDW's Managed Endpoint Anywhere team can help organizations to right-size their device and application environments. This can also reduce renewal costs and ensure compliance in anticipation of software audits.

- **Automate repairs based on device performance.** By identifying issues before users experience significant impact, organizations can significantly reduce downtime for end users.
- **Recommend changes to boost productivity.** Ongoing monitoring and analytics can identify trends and operational insights that may reduce the number of future issues and improve inventory control.

End of lifecycle: Many organizations have seldom-visited closets or storage rooms that effectively serve as device graveyards. Much like consumers, companies struggle to find eco-friendly ways of disposing of old devices that will not put their sensitive data at risk, and so they often simply hold onto the devices, creating clutter and never really solving the challenges that come with the end of a device lifecycle. Managed Endpoint Anywhere provides device disposition, data management and reuse or recycling of devices.

Getting Started

Especially for large enterprises with thousands of users, the prospect of transitioning the entire organization to a lifecycle support model can be incredibly daunting. Instead, CDW offers a 60-day proof-of-concept engagement for Managed Endpoint Anywhere. During the proof-of-concept period, between 250 and 500 users try out the support model, with CDW providing configuration services, telemetry, white-glove deployment, hardware triage and warranty services.

This gives organizations a low-risk way to assess Managed Endpoint Anywhere in their real-world environments, putting the engagement up against their day-to-day management challenges. At the end of the proof-of-concept period, business and IT leaders will have a comprehensive understanding of how Managed Endpoint Anywhere can help them solve their business problems.

CDW: We Get Endpoints

CDW has an experienced staff of end-user computing experts to help organizations optimize their device deployment and management strategies. Because CDW offers vendor-neutral suggestions about devices, IT decision-makers can be confident that they are getting unbiased advice about best-in-class product offerings that are the best fit for their environment.

Services from CDW include:

QuickStart Assessment: CDW's solution architects evaluate end-user experience in several areas, including device, app and data access, networking, security and support. After analyzing the results of this assessment, experts deliver recommendations to optimize the device environment.

Roadmap Workshop: This workshop includes an analysis of factors that affect end-user experiences, in-depth roundtables, evaluation of readiness for hardware upgrades and virtualization and an analysis of the potential return on computing investments using real end-user data.

CDW Amplified™ Services

CDW Amplified™ Workspace services employ a comprehensive approach that enables employees to work from anywhere, on any device.

DESIGN Platforms
Our design and planning workshops help you align your business goals and needs to create an outcome-based unified communications strategy based on end-user satisfaction.

ORCHESTRATE Connectivity
Our certified experts help you create an implementation plan, deploy your fully configured solutions and help ensure adoption success among employees.

MANAGE Collaboration
Our certified experts provide 24/7/365 support and routinely track, measure and optimize your digital workspace solutions to help you exceed business goals.

Sponsors

Learn more about how CDW can help you bring together the benefits of a comprehensive endpoint management solution in a DaaS consumption model to lower costs and increase flexibility.