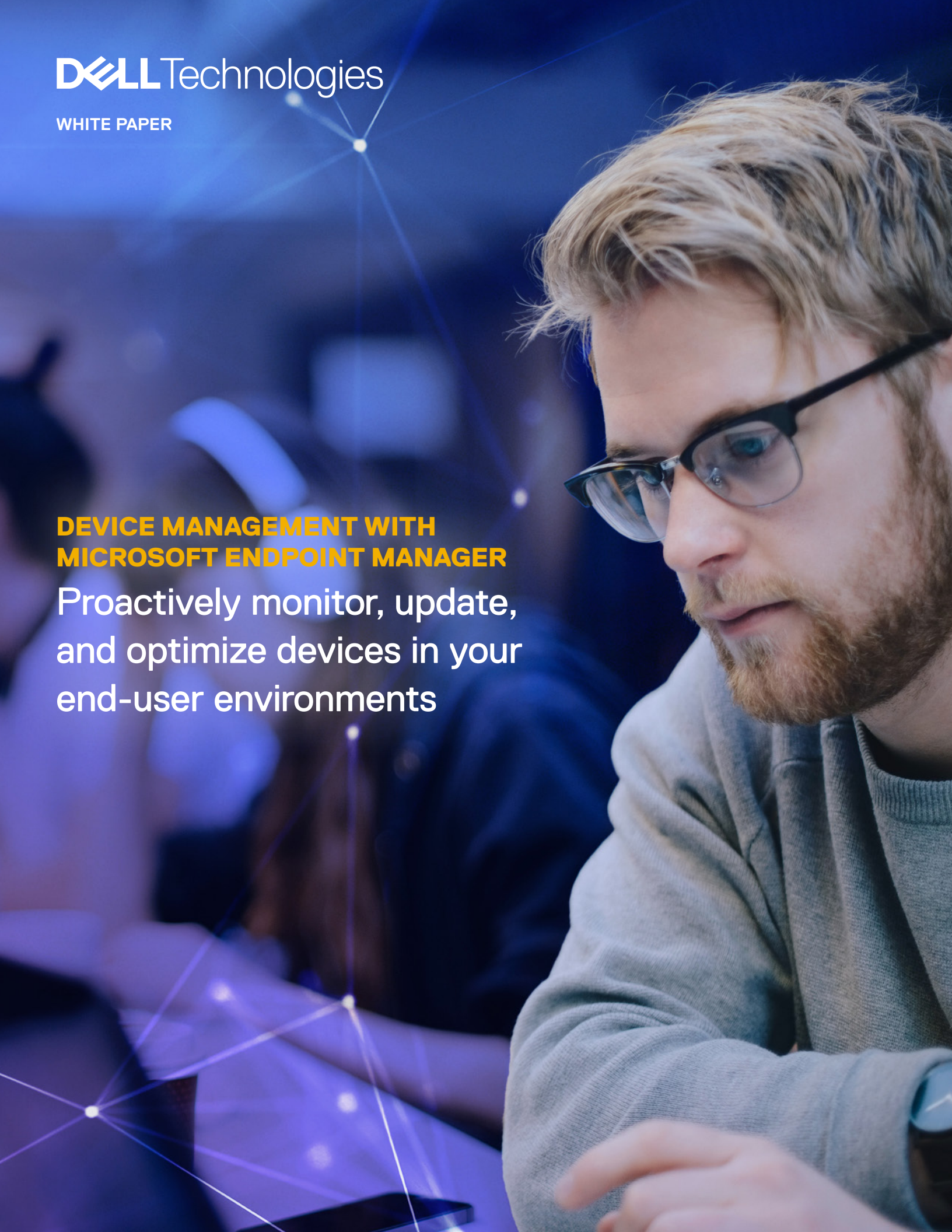
DELL Technologies

WHITE PAPER



DEVICE MANAGEMENT WITH MICROSOFT ENDPOINT MANAGER

Proactively monitor, update, and optimize devices in your end-user environments

While **40%** of businesses acknowledge that mobile devices are the biggest IT security threat to their organizations, **45%** knowingly sacrificed mobile device security in favor of productivity.

—Verizon Mobile Security Index[1]

EXECUTIVE SUMMARY

Digital transformation has taken a dramatic leap forward in the past couple years, especially in response to work-from-home requirements. Businesses in a short timespan have been forced to deploy new enabling technologies to ensure business continuity and workforce productivity. IT decision makers (ITDMs) have had to shift plans and priorities to accommodate quickly evolving workplace environments.

These digital transformation trends and shifts in how we work are not going away anytime soon. According to a recent McKinsey report, the workplace will continue to be borderless, ubiquitous, and continuous for the long-term.[2] IT in response will be tasked with providing users with the flexibility to maintain high-quality, productive work regardless of location or time of day. The number of end-user applications and devices will continue to grow rapidly, and user preferences will evolve with them.

Managing all of these details is becoming increasingly difficult for internal IT teams. Cybersecurity risks are escalating, and remote or mobile workforces exacerbate those risks. Devices used for business, regardless of their locations, must be kept up to date. IT departments need to meet all of these needs while providing seamless and consistent end-user experiences often with limited internal resources and restricted budgets.

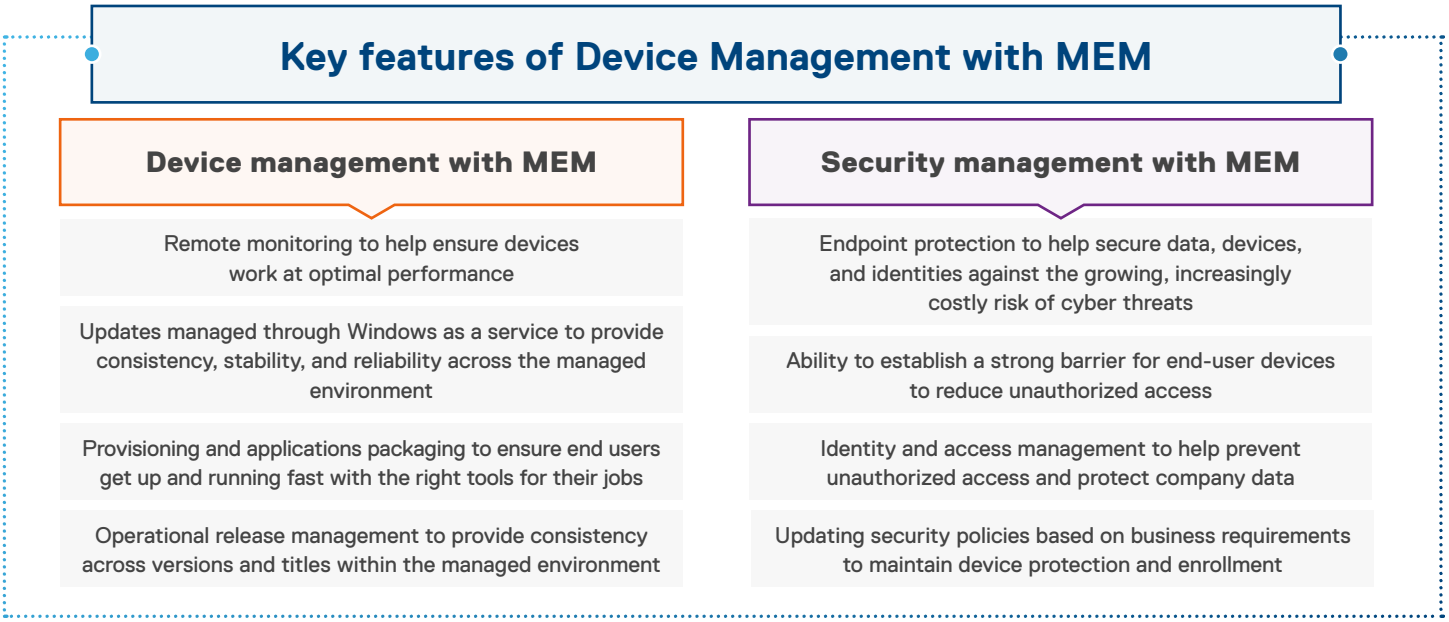
Many businesses are now turning to managed services to ease the burdens on their IT departments and free IT staff to focus on core business goals. A recent survey conducted by Forrester Research identified several key trends in the growth of managed services. The survey indicated that the global crisis in 2020 caused many IT priorities and plans to shift with nearly two-thirds of organizations opting to transition from a CAPEX to OPEX model.[3] The study also cited that over

Top Reasons **Why ITDMs Rely on IT Services Providers[3]**

90% of IT decision makers plan to maintain or increase their investments in IT services in the next 12 months to gain the specific technology, security, and resource expertise needed to minimize risk and meet their goals.[3]

As part of a broader managed services portfolio, Dell Device Management with Microsoft Endpoint Manager (MEM) provides modern device and security management that helps companies keep ahead of system health and performance issues. By proactively monitoring, updating, and optimizing the end-user environment and by applying a multi-layered approach to security management, Dell Technologies Services takes care of day-to-day device management requirements so that your team can focus on leveraging IT to innovate and enhance your business. End users benefit from reliable and secure applications and devices without overextending your internal IT department.

Figure 1. Key features of Device Management with MEM



DEVICE MANAGEMENT ON DEMAND

When making the decision to adopt an as-a-service model for device management, it's important to keep the following criteria in mind:

- Given the complexity of today's device ecosystems, device monitoring, updating, and optimizing the end-user environment must be proactive rather than reactive.
- Employees who work remotely require device support with cloud-based capabilities to maintain consistent, high-quality experiences that encourage productivity.
- A best practices, multilayer cybersecurity approach combined with leveraging the latest security solutions is needed to protect the business from today's sophisticated threats.
- A partner must have the right mix of skills, including expertise in device management, to keep pace with the latest industry standards, policies, releases, and protocols.

With all of these pieces in place, a device-management service should help businesses make optimal use of their technology investments as well as free key IT talent to focus on business innovation.

Modern security and device management using Intune through the cloud with Azure

Device Management with MEM provides proactive device and security management using Intune through the cloud with Azure. This comprehensive offering is designed to meet the critical needs of your distributed workforce, IT staff, and business.

Accelerate modernization of your device environment by relying on our proactive device monitoring, updating and optimization, and multi-layer approach to device security. These capabilities combine with our team of experts—who are continually trained as technology evolves—to deliver greater consistency, reliability, and stability across your managed environment. The need for IT to interact with end-user devices is lessened.

Regardless of where you are on your digital transformation journey, we cover both traditional legacy device management through System Center Configuration Manager (SCCM/ ConfigMgr) and modern mobile-device management (MDM). While SCCM requires specific on-premises equipment and infrastructure, modern Intune MDM-based management exists entirely in the cloud through Microsoft Azure. Over time, we can help transition your workloads from SCCM to Intune to enable you to capitalize on the benefits of Microsoft Azure (including Microsoft 365 where applicable) and move further into a mode of modern IT operations management.

Taking care of day-to-day device management

With Device Management with MEM, we deliver the following four critical features for proactively monitoring, updating, and optimizing your end-user environment:

1. **Remote monitoring** ensures timely updates and thorough monitoring to keep your devices working optimally. We monitor device health, performance, and application usage for all registered devices in your managed environment. Our comprehensive coverage includes both Dell and non-Dell systems running Windows 10, iOS, iPadOS, and Android, regardless of whether the devices are end-user owned, company issued, or desktop as a service, and we support devices both onsite and remote. Our processes comply with ITIL so that issues can be addressed in predictable ways

that support your business. We leverage Microsoft Desktop Analytics to monitor key functions and suggest proactive measures to increase system performance.

2. **Provisioning and application packaging** leverages cloud-based capabilities to streamline device updates and application availability as needed. We create and manage modern provisioning with Windows Autopilot and customize application packages from a library of the most commonly used Windows software titles, while up to five uncommon packaged applications may be added per year. As a result, your end users can get up and running quickly and have the right tools for their jobs.

   Additionally, MEM customers have entitlements to our client engineering team that make factory provisioning an easier process with Windows Autopilot.

3. **Windows as a service** eases your management burden. Feature updates are distributed with the biannual Windows 10 feature releases, while quality updates are applied monthly to address security and reliability. All updates are aligned with specific intervals in time for deployment from the initial feature release date. With these updates, you can ensure consistency, stability, and reliability of Windows devices across the managed environment.

4. **Operational release management** is our thorough process for testing and applying the right updates at the right time. We identify which operating-system and application patches are best suited for your particular environment and then subject them to rigorous tests, with changes bundled into a weekly update package, while urgent updates can be expedited. All software and configuration elements of an end-user device are included. This process drives consistency across versions and titles within the managed environment.

Taking care of critical security tasks

In addition to our focus on device management, Device Management with MEM leverages the security management features of Microsoft Defender and Advanced Threat Protection (ATP). We apply a multilayer approach to secure your company data, devices, and identities against the risk of cyberattacks.

With Microsoft Endpoint Manager, we can help you reduce unauthorized access by establishing a strong barrier for end-user devices. Our team can configure and manage USB devices and controlled folder access for applications to help prevent malicious activity and data loss. We can also help implement a Microsoft Zero Trust security model.

Identity and access management are another layer of protection offered through the service. We manage employee access to company resources, assisting you with security policy, SSPR, and configuration of multifactor authentication. Our team configures and deploys conditional access based on your policies and security priorities. Microsoft Endpoint Manager also enables secure enterprise wipe of all managed resources, including applications and profiles. Our team will fully utilize the security capabilities you are entitled to with Microsoft Endpoint Manager.

Device Management with MEM helps accelerate modernization and reduce IT touches on endpoints

- ✓ Shift workloads over time from SCCM to Intune
- ✓ Accelerate "out-of-the-box" deployments by enabling Autopilot for Dell Factory Provisioning
- ✓ Standardize environments on the latest Windows release
- ✓ Stay current with updates for applications, software, OS quality and features, BIOS, firmware, and device drivers
- ✓ Configure and optimize Microsoft Defender and Advanced Threat Protection (ATP)
- ✓ Extend management to BYOD mobile phones and tablets

Comprehensive Account Management

Device Management with MEM includes account management as a key function. Your designated team oversees account performance and ensures a positive customer experience for the life of the contract. Your Account Management Team includes an onboarding manager and an experience manager. Your onboarding manager will make sure that you can get up and running quickly by overseeing all phases of the process, facilitating needed changes in your IT department and communicating to end users about any new processes. The onboarding manager will ensure that you are ready to transition to production.

At that point, your experience manager will take over responsibility for your service contract. Your experience manager functions as your single source for accountability, communication, and governance for the life of the contract. A designated team will actively manage your customer experience, monitor your service for any issues in order to resolve them quickly, and provide billing, account, true-up, governance, and service-performance reporting.

Figure 2. Dell Technologies IT services industry recognition

Technology & Services Industry Association (TSIA) 2020 Awards

Hall of Fame Lifetime Achievement
Awarded for 30 or more STAR Awards

Best Practices in Field Services
Digital Repair

Innovation in Leveraging Analytics for Service Excellence
Predictive Case Intelligence

Innovation in Leveraging Customer Outcomes
Client Deployment Assessment

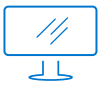
Innovation in XaaS Product Management
Subscription Services

GET STARTED WITH A TRUSTED PARTNER

Entrusting another company with device management is a major decision, especially when doing so directly affects end users. Dell Technologies has the knowledge and the experience to be an effective and valuable partner to your IT department and your business as a whole. We have decades of experience successfully delivering managed services for some of the world's largest organizations. And with more than 200 million assets supported, no one is better qualified to manage Dell devices. In 2020, we also won multiple awards from the Technology & Services Industry Association (TSIA), including awards for lifetime achievement, best practices in field services, and innovation in multiple service fields (Figure 2).

With Dell Technologies you gain the expertise, best practices, and support technologies to provide world-class device management that streamlines provisioning and updates, device monitoring, and endpoint protection.

To learn more about Dell Device Management with MEM services, contact your local Dell Technologies representative today.



Learn more about our Managed Workplace Services

Contact one of our experts

1. Verizon Mobile Security Index 2021. https://www.verizon.com/business/resources/reports/mobile-security-index/?CMP=OLA_SMB_NA_11111_NA_20210406_NA_M20210052_00001
2. McKinsey & Company Survey, October 5, 2020. https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever
3. "IT leaders leverage outside expertise to achieve business outcomes: A spotlight on IT Services Providers." A Forrester Consulting Thought Leadership Spotlight Commissioned By Dell Technologies, 2021

Dell **Managed Services** offers are available directly from Dell Technologies only.

DELL Technologies