Modern device management: Transforming enterprise agility, trust and workforce productivity in the AI-driven economy

Discover how AI-powered modern device management, integrated with Microsoft ecosystem, can revolutionize your enterprise.

Enhance business resilience, boost operational agility and build digital trust with actionable insights that transform endpoint management into a strategic advantage, delivering measurable outcomes for enterprise success.

Executive summary

The digital workplace has reached an inflection point. Organizations are no longer simply reacting to change — they are proactively redesigning how work happens, where it happens and which technologies shape the employee experience. According to Microsoft Work Trend Index, 2023, “73% of employees want flexible remote work options to stay.” As hybrid work, AI integration and distributed operations become standard, the way enterprises manage endpoints must evolve from tactical IT configuration to strategic workforce enablement.

Modern device management is now a foundational capability for business resilience, operational agility and digital trust. IT leaders must ensure every endpoint — whether corporate-owned, employee-managed or AI-assisted — is secure, compliant, productive and intelligently governed. This requires a shift from legacy tools and siloed management models toward a unified, intelligent and proactive ecosystem.

This white paper examines the seismic shifts in workforce expectations, business risk posture, compliance obligations and sustainability mandates that are reshaping endpoint strategy. It unpacks Microsoft modern device management architecture offering tangible business outcomes such as — elevated user experience, strengthened security and data protection, regulatory alignment and AI governance at scale.

It presents a forward-looking blueprint tailored for CIOs, CTOs and technology executives who are driving enterprise transformation and provides a roadmap — one that has been successfully applied across multiple global transformation engagements led by partners such as NTT DATA, who have helped enterprises modernize their device infrastructure, reduce operating costs and deliver measurable outcomes.

The opportunity is clear: organizations that embed secure and adaptive device management into their digital DNA will outperform peers in agility, cost-efficiency, employee retention and regulatory preparedness. The challenge lies in bridging operational gaps with a phased roadmap that aligns infrastructure evolution with business ambition. This white paper provides that roadmap.

Introduction

The modern enterprise is undergoing a profound structural and behavioral transformation. Business operations are no longer confined to physical offices, fixed infrastructure or traditional working hours. The workforce has become dynamic, geographically distributed, digitally fluent and increasingly reliant on real-time access to data and services. At the same time, executive leadership teams face a volatile macroeconomic environment characterized by cybersecurity escalation, geopolitical uncertainty, evolving compliance mandates and intense pressure to achieve more with leaner resources.

This convergence of people, risk and technology has elevated the strategic relevance of device management to the highest levels of enterprise decision-making. Once viewed as a back-end IT task, device strategy is now directly tied to business resilience, risk mitigation, workforce performance and digital innovation.

Consider the implications: onboarding delays are no longer a simple IT issue — they represent lost productivity and a degraded employee experience. Outdated devices and inconsistent security patching expose the organization to operational and reputational risks. Lack of visibility into device compliance weakens the ability to scale AI responsibly or meet evolving ESG disclosure requirements.

In this new reality, IT leaders are not merely technology custodians — they are business enablers. Their mandate has expanded to include delivering secure, consistent and intelligent digital work environments that support hybrid work, accelerate innovation and embed trust at scale. This white paper explores how Microsoft modern device ecosystem — spanning Intune, Autopilot, Entra ID, Defender, Purview and Copilot — provides a robust foundation for building secure, scalable and AI-ready digital workplace environments.

Organizations partnering with experienced integrators like NTT DATA have already begun leveraging these environments to improve time-to-productivity, enforce AI governance and align device operations with business priorities.

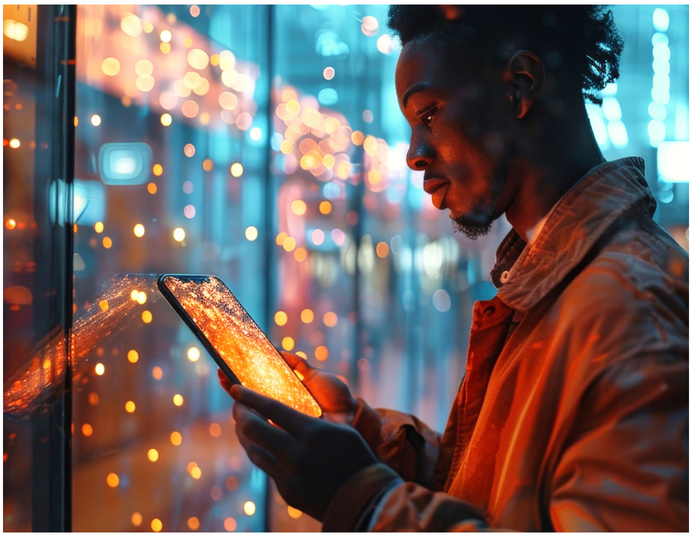
How the modern workforce is changing

The composition and expectations of the workforce have undergone a fundamental shift, driven by a confluence of technological disruption, demographic evolution and shifting workplace norms. Employees today operate in an extended digital fabric — working from home offices, shared co-working spaces, airports, client sites and industrial locations — with the expectation of seamless, secure and instantaneous access to business-critical applications and data. This ubiquity of work has rendered traditional perimeter-based IT models obsolete.

Simultaneously, the rise of generative AI has introduced new paradigms in productivity, knowledge access and human–machine collaboration. Tools like Microsoft 365 Copilot and Copilot in Intune are being integrated into the way people work. They help people make better decisions, automate tasks and increase productivity for themselves and their teams.

Generationally, Gen Z and Millennial employees — who now make up the majority of the workforce — expect digital experiences that mirror the consumer platforms they use daily. They seek autonomy, personalization and frictionless interactions. Frontline workers, on the other hand, require resilient and context-specific devices that support business-critical tasks without latency or failure. Senior leaders demand secure mobile collaboration to drive high-impact decision-making in real time.

This diversity of roles, needs and working styles challenges IT leaders to build a workplace infrastructure that is not only responsive and inclusive, but also aligned with emerging tools, security frameworks and business metrics. Modern device management, infused with AI-readiness and compliance-centric architecture, is now essential to supporting this evolution at scale.



Business challenges and the IT leadership mandate

Across industries, organizations are contending with a growing list of strategic and operational challenges. These include rising cybersecurity threats, escalating customer expectations, heightened regulatory scrutiny and the persistent demand to increase efficiency while navigating talent retention. The workplace is at the intersection of these disruptions.

Traditional endpoint management strategies, which center on static device controls, manual provisioning and fragmented tooling, cannot meet the demands of this new environment. They expose the business to operational risk, increase total cost of ownership and diminish employee trust and engagement.

In response, the role of IT leaders is rapidly expanding. CIOs and CTOs are no longer expected to simply ensure uptime — they are being asked to architect resilient, secure and intelligent digital workplaces that deliver business outcomes. This includes deploying scalable provisioning, maintaining real-time visibility into device compliance, enabling secure AI usage and creating high-quality digital employee experiences.

The mandate is clear: IT must now function as a strategic enabler of employee productivity, innovation and trust. Deploying modern workplace solutions that are secure by design, scalable by default and human-centric by outcome — provides the foundational infrastructure required to deliver.

Macro trends driving modern device management

Global enterprises are operating in a landscape marked by accelerated digital dependency, heightened security threats, rising workforce expectations and increased regulatory scrutiny. These macro forces are transforming the device management agenda from a tactical IT function to a strategic pillar of business performance. Seven key trends are redefining what IT leaders must anticipate, architect and operationalize in this new paradigm.

Institutionalization of hybrid work and location-agnostic access

According to the report, Gartner Future of Work Trends Post-COVID-19, 2022 — “Over 70% of knowledge workers now expect flexible work arrangements.” Hybrid work is no longer a response to disruption — it has become the default architecture of modern enterprise operations. Work is now fluid, borderless and asynchronous. Employees expect to access business-critical applications across multiple devices and locations without compromising security, speed or user experience. This shift has challenged CIOs to rethink traditional network perimeters and invest in platforms that deliver ubiquitous access with enterprise-grade security and governance.

Microsoft modern device management, when deployed through trusted partners such as NTT DATA, enables frictionless onboarding, centralized policy enforcement and real-time support for a geographically and functionally diverse workforce. Location-agnostic operations are now a competitive advantage — and require endpoints to be provisioned, secured and governed as dynamic extensions of the enterprise infrastructure.

Enterprise adoption of Zero Trust security framework

According to the study Gartner, Market Guide for Zero Trust Network Access, 2022 — “By 2025, 60% of organizations will embrace zero trust as a starting point for security.” Cybersecurity threats have grown in frequency, velocity and sophistication — rendering traditional perimeter-based defenses obsolete. In response, Zero Trust has emerged as the dominant security framework for enterprises navigating a distributed workforce and proliferating endpoints. This approach mandates that no user, device or network connection is trusted by default.

Microsoft MDM is central to Zero Trust framework — where every user, device and access request is verified continuously. This approach validates device posture, pushes compliance configurations and monitors deviations in real time, ensuring that access decisions are context-aware and dynamically enforced.

Integration of AI for increased productivity and cost benefits

AI is redefining the operating model of the enterprise. From generative AI assistants to intelligent automation, organizations are embedding AI in workflows, processes and platforms to drive scale, efficiency and competitive differentiation. According to Microsoft Copilot Early Access Report, 2023 — “Microsoft 365 Copilot has shown productivity improvements of up to 29% in task completion and writing quality.”

Microsoft Intune is transforming endpoint management and extending AI innovation for IT with the introduction of Security Copilot agents. Agents empower organizations to improve their security posture, boost productivity and simplify IT operations, while helping to address the constant pressure IT and security teams are under to manage complex endpoint environments and stay ahead of evolving threats.

Microsoft Randomized Controlled Trials for Security Copilot for IT Administrators, 2024 study found that “IT professionals using Security Copilot were 35% more accurate in completing tasks.” Now, Copilot in Intune is expanding its capabilities with Security Copilot agents. These agents bring powerful, adaptive automation to IT and security operations teams — streamlining critical tasks and enabling them to act faster and with greater confidence. The first of these agents in Intune is the Vulnerability Remediation Agent, launching in May 2025 in public preview. This marks a major advancement in endpoint management as it brings AI-powered automation to vulnerability remediation.

But AI adoption also introduces new requirements for device performance, data access, policy controls and governance. NTT DATA’s device management enablement ensures AI-readiness by provisioning compliant endpoints, securing privileged access to sensitive datasets and monitoring AI usage across employee roles and business functions. In doing so, it empowers productivity while preserving data integrity and governance oversight.

Expanding support for BYOD and device ecosystem diversity

Today’s workforce operates across a heterogeneous mix of endpoints — including corporate-owned devices, personal smartphones, tablets and industry-specific ruggedized tools. The rise of bring your own device (BYOD) and corporate-owned, personally enabled (COPE) models reflect an employee-first technology ethos. However, they introduce significant complexity in endpoint visibility, support and policy compliance.

Modern device management platforms such as Microsoft Intune deliver a seamless experience regardless of ownership or operating environment. NTT DATA provides organizations with the ability to support a fluid and diverse device landscape that is now essential to workforce satisfaction, productivity and security.

Alignment with sustainability and ESG objectives

According to NTT DATA ESG and IT Asset Study, 2022 — “Extending device life cycles by one year can reduce endpoint carbon footprint by up to 30%.” Sustainability is now a strategic business imperative — driven by investor pressure, consumer expectations and evolving global regulation. Enterprises are being held accountable for their carbon footprint, electronic waste and energy consumption across the value chain, including IT assets.

Modern device management contributes to ESG goals by enabling energy-efficient configurations, extending asset lifecycles through predictive maintenance and improving visibility into device utilization. These capabilities allow organizations to reduce e-waste, optimize refresh cycles and embed sustainability into their digital infrastructure strategy. NTT DATA’s global experience in aligning IT modernization with ESG commitments makes it a valuable partner in this space — accelerating impact through actionable insights and proven execution models.

Elevated focus on compliance and data governance

With global data protection regulations proliferating, compliance is no longer a legal formality — it is a board-level priority. According to the IDC Future of Trust Survey, 2023 — “More than 76% of global executives consider data governance critical to business strategy.” Enterprises must demonstrate accountability, transparency and control over how data is accessed, processed and stored across devices and cloud environments.

Modern device management, integrated with Microsoft Purview, strengthens data protection, prevents insider threats and provides forensic-level audit trails. This ensures that compliance is continuous, scalable and defensible — even in highly regulated industries and jurisdictions requiring industry compliance standards of HIPAA and GDPR.

Digital employee experience (DEX) as a core performance metric

According to Qualtrics X-Data and Gartner Workforce Trends, 2023 — “Companies that invest in DEX outperform peers by 22% in employee retention and 17% in productivity.” NTT DATA believes that employee experience has emerged as a measurable enterprise KPI — with direct ties to engagement, productivity and retention. In digital-first workplaces, the quality of a user’s interaction with their device often determines their perception of the organization itself.

Modern device management platforms enable organizations to track, benchmark and enhance DEX by reducing friction points, automating support and enabling personalization. When IT becomes invisible and empowering, the enterprise reaps the rewards of a highly engaged, high-performing workforce. This transforms IT from a support service to a contributor to employee success.

Closing the readiness gap

Despite widespread recognition of the need for modern device management, many enterprises remain reliant on outdated tools, siloed teams and reactive processes — none of which are sustainable in the era of hybrid work, AI acceleration and persistent cyber risk.

IT departments often face fragmented environments — managing multiple endpoint platforms with inconsistent policies and limited automation. This gap leaves businesses vulnerable — not just to security breaches, but to experiencing attrition, higher support costs, diminished user satisfaction, regulatory missteps and AI adoption without governance.

In organizations without automated and unified endpoint management, a simple onboarding process can take days, requiring manual setup and redundant approvals. Business apps are not delivered on time, security updates are applied inconsistently and IT lacks visibility into which devices are compliant. This friction fuels the rise of shadow IT — introducing unmonitored risk and reducing overall IT control. Without integrated analytics, IT leaders are unable to benchmark experience, predict failures or demonstrate business impact.

NTT DATA partnering with Microsoft has repeatedly helped organizations break through these limitations — enabling unified endpoint management, driving DEX benchmarking and reducing onboarding times by over 50% in some enterprise-scale deployments.

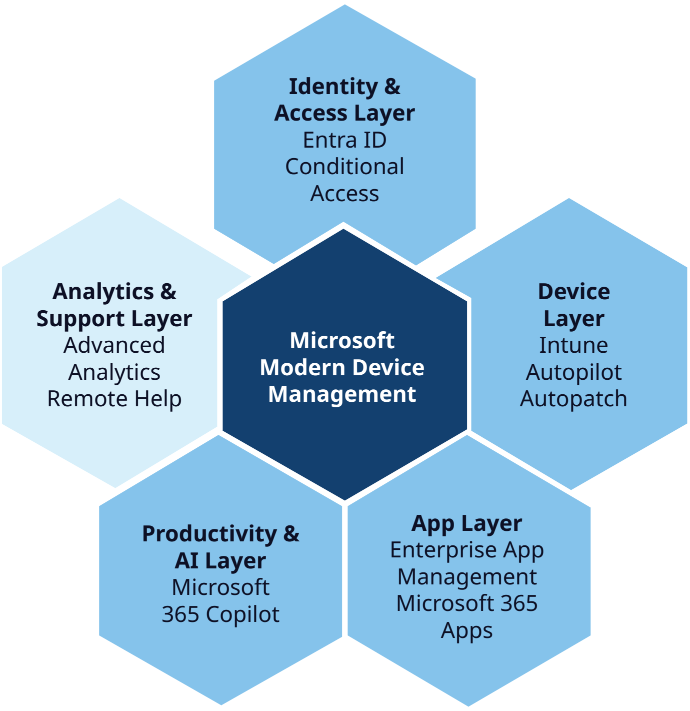
Case in point: NTT DATA collaborated with one of the world’s largest air carriers to facilitate a transformational shift toward a modernized digital workplace by deploying Microsoft device management solutions — including Intune and Autopilot. This initiative modernized and unified device and mobility services across more than 30,000 devices at 400 global locations. The result: a 24% reduction in service desk calls, driving measurable gains in employee satisfaction and operational efficiency. The engagement enabled the client to dynamically align IT operations with business priorities, such as managing seasonal peaks, supporting critical locations, and ensuring proactive maintenance.

Thus, closing the legacy gap demands more than a tool refresh. It requires a foundational redesign of how endpoints are deployed, governed, supported and measured across the employee lifecycle. It demands that IT leaders elevate device management to a board-level discipline — integrated with workforce strategy, risk posture, compliance architecture and the digital experience agenda.

The solution: Unlocking immediate business impact through Microsoft modern device management

Microsoft modern device management portfolio provides a consolidated, comprehensive, cloud-native foundation to address the dual imperatives of productivity and security. Anchored in the principles of Zero Trust, built for hybrid environments and aligned with business continuity principles, the solution stack brings together provisioning, management, protection, governance, productivity and automation under a unified operational model. This empowers IT leaders to shift from fragmented toolsets and reactive firefighting to proactive service delivery and strategic enablement.

With Microsoft Intune, Autopilot, Autopatch, Defender, Purview and 365 Copilot, enterprises can: automate onboarding at scale, apply configuration management, enforce dynamic security policies, enable responsible AI adoption and operationalize compliance — all while enhancing the digital experience of the workforce. The result is a more agile, secure and future-ready digital workplace.



Key capabilities include:

1. **Microsoft Entra ID** serves as the foundation for secure identity in a hybrid or cloud-native environment. It is often the first step in an organization's Zero Trust journey — enabling conditional access, policy-based controls and seamless user authentication across all devices and applications.

2. **Microsoft Intune** delivers centralized, cloud-based visibility and management across all endpoint devices — desktops, laptops, mobile devices and virtual environments, delivering business and productivity apps when it matters, ensuring consistent security posture with baselines, compliance enforcement, remote configuration and policy orchestration.

3. **Windows Autopilot** enables zero-touch provisioning, drastically reducing onboarding time while delivering a standardized user experience across roles and geographies – optimal for hybrid work scenarios.

4. **Microsoft Defender xDR** delivers advanced threat protection and real-time response, using AI-driven analytics to identify and neutralize threats at the device, email, apps and identity level.

5. **Microsoft 365 Copilot** infuses AI directly into the flow of work — amplifying employee productivity — while device management ensures secure and compliant access to the necessary data sources.

6. **Microsoft Purview** applies governance policies, protects data, secures company's sensitive resources from insider threats, prevents data exfiltration and supports regulatory standards and frameworks like HIPAA, GDPR and NIST AI RFM through built-in data classification and audit capabilities.

7. **Windows Autopatch** automates patch management, ensuring devices are always up-to-date without disrupting user productivity or requiring manual intervention — allowing IT teams to focus on strategic initiatives instead of routine maintenance.

Together, these solutions help IT leaders drive measurable outcomes: reduced support costs, improved security posture, faster onboarding and higher employee satisfaction. Microsoft platform approach reduces tool sprawl, simplifies compliance and aligns device management with broader digital transformation strategies.

NTT DATA's expertise in deploying Microsoft modern management stack across complex environments ensures that these benefits are realized quickly and at scale. From roadmap design to change management, it brings execution certainty to device modernization, realizing tangible business outcomes such as workforce productivity, cost optimization, business continuity, secure operations, regulatory alignment and AI readiness.

Implementation roadmap for IT leaders using the Microsoft maturity model

Implementing a modern device management strategy is not a single event — it is a journey that evolves through defined stages. Microsoft maturity model provides a structured framework that helps IT leaders assess their current state, identify capability gaps and plan an actionable path toward a fully integrated and optimized device management environment. Each phase delivers tangible value while building toward long-term resilience, security and workforce productivity — helping IT leaders evolve from device maintenance to digital enablement.

Stage 1: Traditional — fragmented operations, limited visibility and risk-prone

Most organizations begin with a legacy device management model characterized by siloed management tools, static controls and policies and manual provisioning. Devices often require on-premises presence to access corporate resources, and visibility into compliance or threat posture is fragmented at best. Security policies are inconsistent, user experience is unmeasured and onboarding is slow and labor-intensive.

Organizational reality: High support costs, long onboarding times, inconsistent security enforcement and poor user experience.

IT mandate: This stage focuses on understanding the existing device ecosystem, aligning with key stakeholders and creating the governance structures needed to support transformation. IT leaders must conduct a current-state assessment across device inventory, endpoint tools, security posture and compliance processes. The goal is to build a roadmap to prepare for centralized management — one that aligns technical upgrades with workforce needs and business objectives.

Stage 2: Advanced — Standardized, governed and managed but reactive operations

Organizations at this stage initiate their modernization journey. With assessment and governance architecture in place, organizations begin standardizing baseline endpoint policies, consolidating tools and activating core Microsoft device management solutions. Intune is deployed to provide centralized control, Autopilot is configured to support zero-touch provisioning and Defender is activated for threat response. Hybrid identity and conditional access policies govern user-device-access relationships.

Strategic moves:

- Foundation of organization’s cloud-native or Hybrid Identity with Microsoft Entra ID
- Centralize device management with Intune — deliver apps and configuration
- Launch zero-touch device provisioning with Windows Autopilot
- Enforce Zero Trust framework with Conditional Access
- Threat Protection and Response with Defender

Enterprise gains: Elevated employee experience across devices, improved operational control, stronger onboarding velocity, reduced attack surface, proactive threat mitigation, and early-stage cost optimization.

Stage 3: Optimal — Integrated, automated and analytics-driven

The optimal stage marks a decisive shift from policy compliance to proactive optimization. Device health telemetry, usage insights and security signals are fed into analytics engines that drive predictive action. Autopatch drives automated patch management and compliance. Microsoft Purview enables data protection and governance.

Capabilities deployed:

- Windows Autopatch for automated patch management
- Advanced Analytics with proactive device health telemetry and monitoring
- Classification and encryption of sensitive data, and DLP Policies with Microsoft Purview

Enterprise gains: Near-zero downtime, Secure data fabric, and audit-ready governance.

Stage 4: Strategic — Scalable, intelligent and business-aligned

At this stage, device management becomes fully embedded in the enterprise's business model and digital fabric. A Zero Trust framework is institutionalized across devices, identities, data, apps and networks. Microsoft 365 Copilot infuses productivity into employee workflow and AI governance ensures ethical usage of such productivity tools. Device controls are part of ESG reporting; DEX metrics influence HR and workforce planning. Endpoint strategies scale seamlessly across M&A, global hiring and new business models.

Capabilities deployed:

- Zero Trust framework
- Microsoft 365 Copilot
- AI Governance frameworks with Microsoft Purview

Organizational transformation:

- Device strategy aligns with business
- Endpoint metrics drive DEX and ESG reporting
- Zero Trust and AI-readiness become enterprise-wide norms

NTT DATA helps enterprises deploy and operationalize these capabilities using Microsoft maturity model providing a tested pathway for progressive improvement. By aligning strategy, tools and execution, IT leaders can evolve from managing devices to enabling resilient, secure and AI-powered digital workplaces that create tangible business value.

Stage	Operations	Device posture and operations	Governance and insights	Capabilities deployed	Business impact
Traditional	Fragmented	Manual provisioning, siloed tools and policies	No governance and basic inventory tracking	On-premises legacy tools	High-cost, low visibility and risk-prone
Advanced	Reactive	Zero-touch provisioning and automated employee onboarding, cloud/hybrid identity, faster app and config deployments, dynamic condition-based access, standardized policy control and threat protection and response	Compliance management and unified asset inventory	Entra ID, Intune, Autopilot, Conditional Access and Defender xDR	Elevated workforce productivity and stronger security – both leading to cost-optimization
Optimized	Proactive	Automated patching, data security and real-time AI-driven telemetry	Analytics and telemetry, risk scoring, audit-ready governance	Autopatch, Purview and Advanced Analytics	Enhanced employee experience and secure data fabric – leading to talent retention and near-zero downtime
Strategic	Intelligent, automated and AI-driven	AI-ready Zero Trust enabled self-healing devices	DEX metrics, ESG initiatives and AI governance	AI governance with Purview, Microsoft 365 Copilot and Zero Trust	Device management aligns with business strategies

Repositioning device management as a strategic lever for enterprise agility and trust

Modern device management has moved from the IT back office to the center of business strategy. In a world shaped by hybrid work, AI-driven productivity and growing cybersecurity threats, how companies manage devices directly affects employee performance, business costs, risk exposure and operational speed.

Microsoft device management platform enables IT leaders to shift from fragmented, reactive operations to secure, automated and intelligent endpoint management that is anchored in Zero Trust. It delivers faster onboarding, stronger security, smarter and compliant AI usage and consistent digital experiences — at scale.

These improvements are not just technical wins — they translate into real business outcomes. Lower support costs. Faster time to productivity. Higher workforce satisfaction. Better audit and compliance readiness. These are the metrics today's executives care about.

In today's enterprise landscape, digital dexterity is not just a technology initiative — it's a competitive differentiator. This white paper delivers a compelling blueprint for IT leaders navigating this complexity. It examines the evolving demands of the workforce, the macrotrends shaping endpoint strategy and the operational gaps that hinder business execution. Most importantly, it reveals how Microsoft modern device management ecosystem empowers organizations to transform endpoints from a legacy cost center into a dynamic engine for agility, trust and talent engagement.

NTT DATA and Microsoft share a common vision for delivering secure, location-agnostic and diverse device environments that drive measurable business impact. Both organizations align on enabling seamless user experiences, proactive security, and scalable IT operations—anchored in a zero-trust framework and AI readiness. This shared strategic approach ensures that enterprises can modernize their workplace with confidence, balancing control with flexibility, and performance with cost-efficiency.

About NTT DATA and Microsoft

According to NTT DATA Global Partnership Report, 2023 — "NTT DATA is recognized as a top Microsoft Global Systems Integrator (GSI), delivering secure digital workplace solutions across over 50 countries."

NTT DATA and Microsoft have been long-standing global strategic partners, working together to help enterprises modernize their IT environments and accelerate business outcomes. By combining Microsoft leading-edge cloud and security platforms with NTT DATA's deep industry expertise and global delivery capabilities, organizations gain access to trusted, end-to-end digital transformation solutions.

NTT DATA brings decades of experience in designing, deploying and managing ecosystems powered by Microsoft across highly regulated and complex environments. From enterprise-wide deployments of Microsoft Intune and Defender, to secure Microsoft 365 Copilot enablement and endpoint governance with Microsoft Purview, NTT DATA ensures that modernization is aligned with security, compliance and long-term business strategy.

Together, NTT DATA and Microsoft deliver the expertise, technology and operational scale required to help enterprises build secure, intelligent and productive digital workplaces — built for today's needs and ready for tomorrow's growth.

Appendix

- **Workforces expect flexible work:** "More than 70% of knowledge workers globally have adopted a hybrid work model or expect one post-pandemic." — Gartner, "Future of Work Trends Post-COVID-19," 2022.
- **Modern device management reduces costs:** "Organizations that consolidate endpoint management see a 30% reduction in operational costs and a 25% decrease in security incidents." — Forrester Total Economic Impact™ Study of Microsoft Endpoint Manager, 2021.
- **Hybrid work has become a standard:** "73% of employees want flexible remote work options to stay." — Microsoft Work Trend Index, 2023.
- **Zero Trust is a strategic imperative:** "By 2025, 60% of organizations will embrace zero trust as a starting point for security." — Gartner, Market Guide for Zero Trust Network Access, 2022.
- **AI drives employee productivity:** "Microsoft 365 Copilot has shown productivity improvements of up to 29% in task completion and writing quality." — Microsoft Copilot Early Access Report, 2023.
- **Compliance and governance are board-level priorities:** "More than 76% of global executives consider data governance critical to business strategy." — IDC Future of Trust Survey, 2023.
- **Digital employee experience (DEX) impacts retention:** "Companies that invest in DEX outperform peers by 22% in employee retention and 17% in productivity." — Qualtrics X-Data and Gartner Workforce Trends, 2023.
- **Sustainability and device lifecycle optimization:** "Extending device life cycles by one year can reduce endpoint carbon footprint by up to 30%." — NTT DATA ESG and IT Asset Study, 2022.
- **NTT DATA + Microsoft partnership:** "NTT DATA is recognized as a top Microsoft Global Systems Integrator (GSI), delivering secure digital workplace solutions across over 50 countries." — NTT DATA Global Partnership Report, 2023.

Learn more about NTT DATA

Visit nttdata.com

NTT DATA is a trusted global innovator of business and technology services, helping clients innovate, optimize and transform for success. As a Global Top Employer, we have experts in more than 50 countries and a robust partner ecosystem. NTT DATA is part of NTT Group.

© 2025 NTT DATA, Inc.