



State of Digital Workspace 2026



Observability emerges as an essential component for scaling digital work

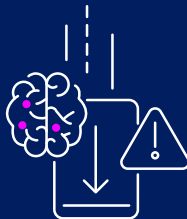


Table of contents

3	Introduction
4	Device choice
5	OS platform and OEM adoption differ by industry
7	Device form factor preference varies by industry
8	Device lifecycle duration varies by OS platform
9	Device configuration is shaped by user requirements
11	The shadow perimeter
12	Unsanctioned AI apps are prevalent in the enterprise
12	Personal communication tools are blurring professional lines
13	Browsers are quickly becoming the new endpoints
13	Windows system bloat may hinder user utility
15	Security hygiene
16	Patching velocity is inconsistent across OS platforms
17	Critical industries are lagging behind on OS updates
18	Desktops have alarmingly high levels of unencryption
20	Employee experience
21	DEX baselines differ across desktop systems
21	System instability imposes a “forced interruption tax”
23	Conclusion

Introduction

The **Omnissa State of Digital Workspace 2026** report reveals a fractured end-user computing (EUC) landscape defined by a distinct bifurcation of strategy: As organizations pursue operational efficiency through AI and automation, they are simultaneously overlooking the essentials of the digital workspace—allowing shadow apps, device noncompliance, platform instability, and hidden hygiene gaps to actively undermine their ability to manage risks. This dichotomy can create a visibility gap, suggesting that management based solely on standards and policies may not be sufficient. Under these circumstances, management powered by deep, **end-to-end observability** becomes absolutely essential. After all, how can you secure and optimize an environment that you can't fully see?

This inaugural report synthesizes telemetry data from millions of endpoints from enterprise environments using Omnissa solutions. The analysis of this data provides an empirical baseline of the modern digital workspace, highlighting four areas where greater observability can help organizations improve end-user computing operations:

1. **Device choice** – Evolving device choice programs from employee perks to persona-based procurement policies that optimize costs.
2. **The shadow perimeter** – Adjusting governance approaches to include policies that can help counter the explosion of unsanctioned AI and shadow app usage.
3. **Security hygiene** – Helping IT teams move from reactive auditing to more proactive remediation against compliance drifts.
4. **Employee experience** – Identifying sources of digital friction that may contribute to lost productivity and user experience.



The report findings all point to a broader shift: Today's IT teams must move from simply managing assets to achieving greater visibility across the digital workspace environment. Deep, end-to-end observability is no longer optional—it's a fundamental way to drive efficiencies in cost, productivity, and compliance.

Methodology

This research is based on anonymized and aggregated telemetry data analyzed across millions of endpoints between **January** and **December 2025**. The dataset includes enterprise environments across **the globe** and **17 uniquely tracked industries**, including high tech, retail and wholesale, healthcare, pharmaceuticals, financial services, manufacturing, education, and government.

Omnissa Workspace ONE® telemetry signals were derived from device, application, and system activity across supported endpoints and operating systems. All data used in this report was analyzed in aggregate to identify trends across the digital workspace environment.*

* Based on anonymized and aggregated telemetry data from enterprise environments using Omnissa Workspace ONE technologies. Only non-personally identifiable data collected through administrator-enabled settings was included. Findings reflect observed trends within the analyzed dataset and may vary by organization.

1 Device choice

Shifting from a “perk” to a persona- and performance-based procurement approach can optimize costs and productivity

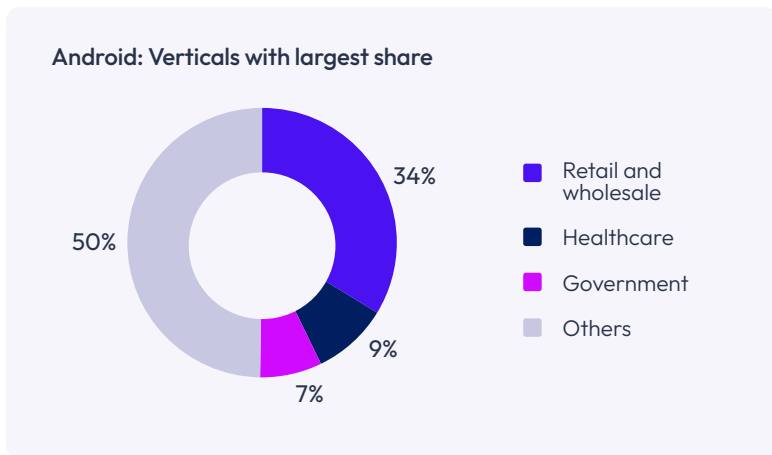
Our data suggests that organizations are increasingly treating device choice as an operational consideration rather than solely an employee benefit. By moving from a standard, “one-size-fits-all” hardware strategy to persona-based device allocation, organizations can more accurately align device investments with workforce needs and operational requirements. This observation is informed by four patterns identified in device adoption and lifecycle telemetry:

1. OS platform and OEM adoption differ by industry.
2. Device form factor preference varies by industry.
3. Device lifecycle duration varies by OS platform.
4. Device configuration is shaped by user requirements.

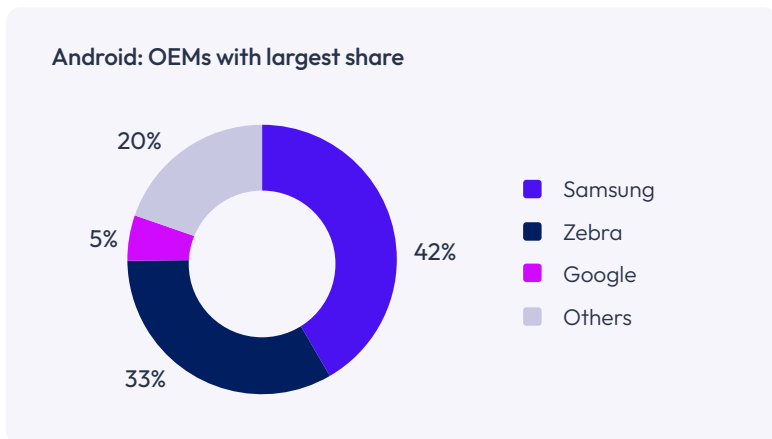


OS platform and OEM adoption differ by industry

Our research shows a concentration of specific operating systems and device manufacturers within specific industries, suggesting platform selection may sometimes be influenced by an industry’s particular operational requirements. For example, we see a higher concentration of Android devices in the retail and wholesale and healthcare sectors where ruggedization is a priority, while adoption of Apple devices is observed to be consistent and widespread across industry verticals.



We also observe that a full three-fourths of Android devices used in the enterprise are made by just two manufacturers—a duopoly led by Samsung (42%) and Zebra (33%).



Samsung sees broad enterprise adoption

The widespread enterprise adoption of Samsung may reflect the company’s “dual-use” strategy of serving both knowledge workers via the Knox-secured Galaxy S series and frontline staff via the Galaxy XCover ruggedized series.

Google Pixel has a breakout year

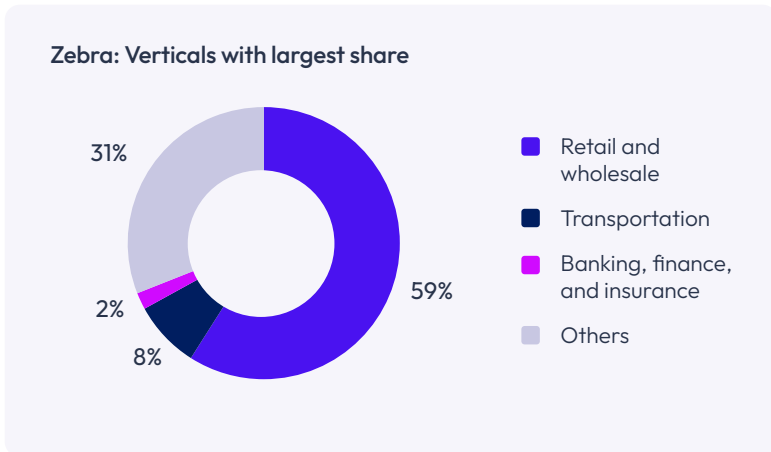
Although they started from a smaller base, **Pixel devices have experienced a year-over-year (YoY) growth of 988%** to claim a 5% share of Android devices. This growth is particularly pronounced in government and retail verticals. The surge in the government sector aligns with the recent placement of Google Pixel on the Department of Defense Information Network (DoDIN) Approved Products List (APL).



The growth of Pixel devices may indicate a shift in IT preference toward first-party hardware-software integration, likely driven by the need for rapid security patching and AI-ready hardware.

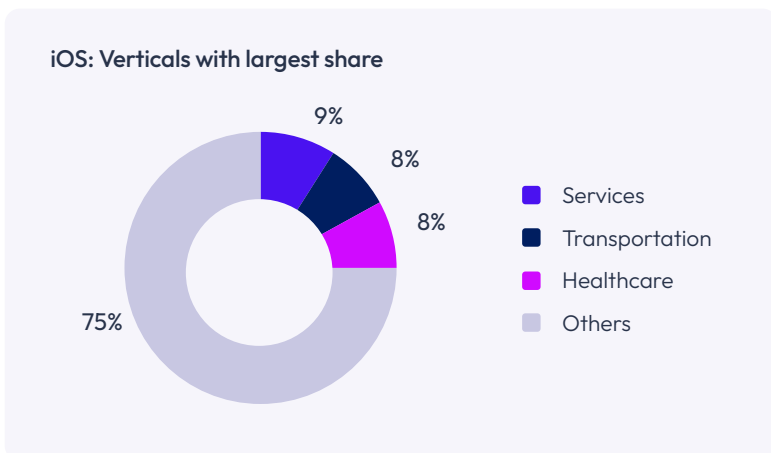
Zebra adoption remains strong where ruggedization is a priority

Our research shows that frontline verticals such as **retail and wholesale and transportation are strongholds for Zebra devices**, likely driven by their physical attributes such as device durability, hot-swappable batteries, and integrated barcode scanning capabilities.



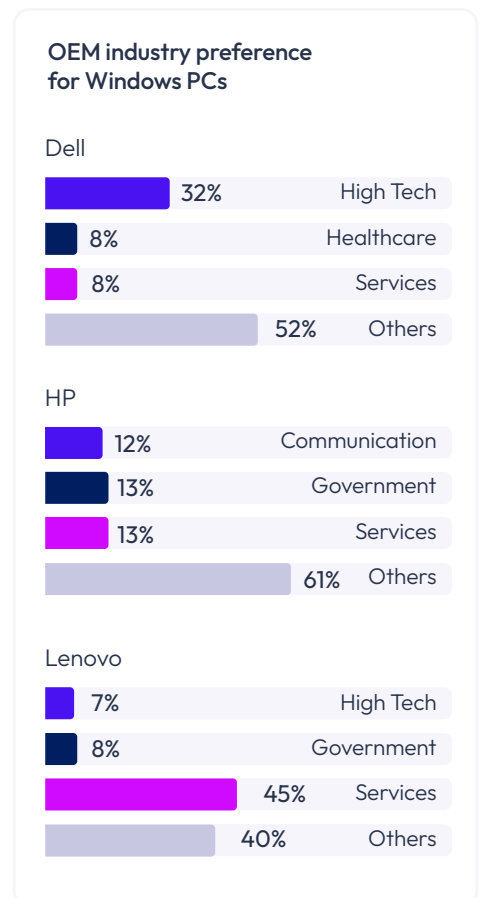
Apple adoption is consistent across industries

Compared to the Android ecosystem, our data suggests that Apple devices—particularly iPhones and iPads—have become a “utility infrastructure” of enterprises. Much like electricity or email, the adoption is consistent and widespread across the enterprise.



Different industries prefer different Windows PCs

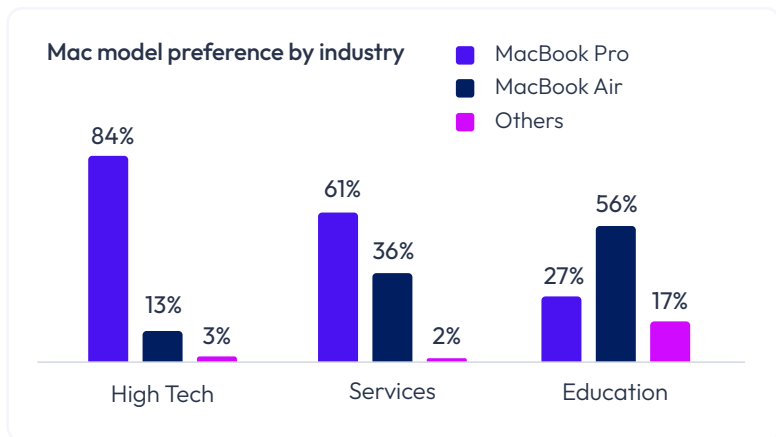
While the Windows ecosystem is broadly dominated by the “big three,” with **Dell, Lenovo, and HP taking 86% of the enterprise share**, the telemetry also reveals deep, industry-specific loyalties rather than generic distribution. For example, the high-tech sector overwhelmingly standardizes on Dell, while the services industry shows a distinct preference for Lenovo and government organizations choose HP.



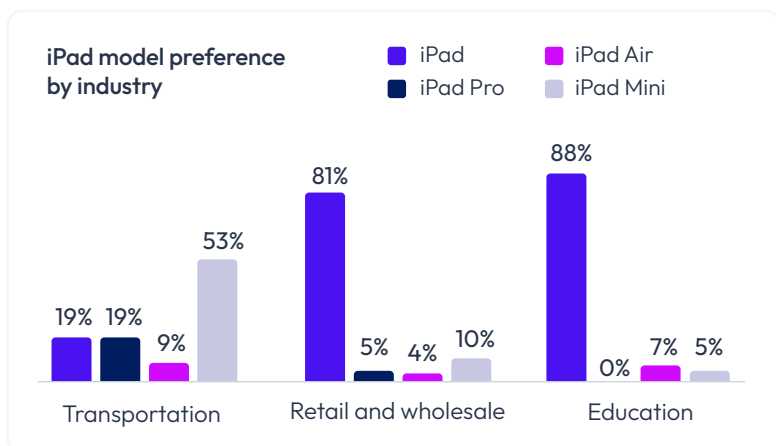
Device form factor preference varies by industry

Our research shows variations in device form factor preferences across sectors, suggesting that hardware selection is influenced by persona and performance needs rather than a standardized corporate catalog.

For example, our top three Mac verticals—high tech, services, and education—all show strong preferences when it comes to the particular models they choose. **MacBook Pro is the clear choice in the high-tech (84%) and services (61%) sectors**, suggesting that organizations are willing to pay the Pro premium when high performance—for tasks like engineering, design, and analysis, for example—and talent retention are paramount. On the other hand, **MacBook Air is the preference (56%) in the education sector**, where cost-efficiency and portability considerations may influence procurement decisions.



A similar economic and operational divide is evident in our top three iPad verticals: Transportation, retail, and education. **In the transportation sector, organizations favor the highly portable iPad Mini (53%)** for field mobility, supplemented by the premium iPad Pro (19%) for resource-intensive logistics and routing. Conversely, **the standard, base-model iPad is the predominant form in the retail (81%) and education (88%) sectors**, where mass deployment, single-app kiosks, and cost-efficiency are primary concerns.



Desktop growth is strong in the government sector

While enterprise mobile growth appears to be relatively uniform across most verticals, desktop adoption demonstrates significant variance. The government sector is a massive outlier, with a staggering **2x desktop growth**. This trend aligns with broader public sector procurement cycles and security mandates that emphasize secure, stationary endpoints for classified workflows, strict supply chain regulations, and “clean desk” policies.¹



Glanceable workflows likely on the rise

Like desktops in government, the **Apple Watch has emerged as another outlier enterprise endpoint, showing significant YoY growth (36%)**, led primarily by its adoption across transportation and pharmaceuticals. This surge potentially indicates a transition from “pilot” to “production” for hands-free or glanceable workflows, as enterprises deploy apps for shift management, two-factor authentication (2FA), and critical alerts. For example, in transportation and logistics, wearables can be seen replacing bulky handhelds for notifications, simple acknowledgments, and hands-free picking, improving efficiency and worker safety.²

Device lifecycle duration varies by OS platform

Our telemetry indicates stark differences in hardware longevity and lifecycle duration across operating systems. Since device lifecycles fundamentally alter the total cost of ownership (TCO) calculus, factoring in device longevity can help organizations optimize their budgets over a period of time.

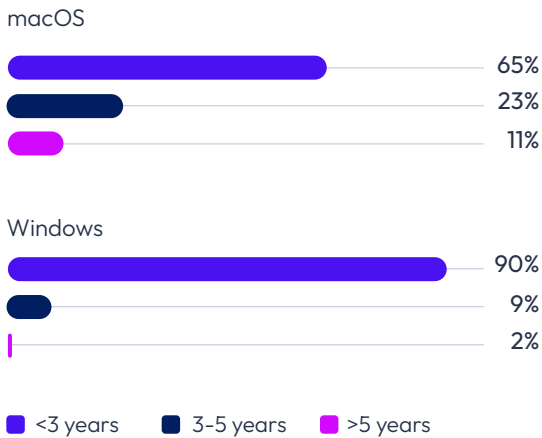
Our research looks at the device enrollment age as a proxy to the lifecycle to identify how long a device has been “in service.” For desktop platforms, data suggests **a healthy percentage (11.5%) of Macs remain viable even into year 6**, compared to Windows devices (1.8%).

The difference is less prominent in mobile platforms, with approximately 75% of new iOS and Android devices being enrolled within the last 3 years. However, **the data suggests that iOS devices display longer service life, with twice as many devices in service into year 6.**

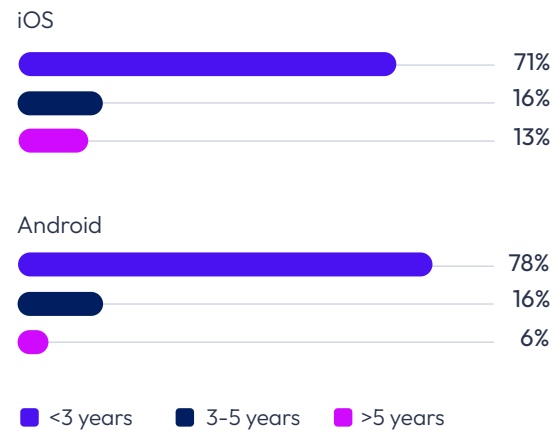


Compared to Windows, 6.5x more Macs are seen in service into year 6, and 3.3x more Macs are seen in service into year 3+.

Desktop device enrollment age by OS platform



Mobile device enrollment age by OS platform



While our data provides significant support that Macs outlast Windows PCs, **with Macs often being a five-plus-year asset compared to a Windows PC being a three-year asset**, this longevity could be a function of both hardware build quality and software support timelines. Historically, Apple has supported OS updates for 6+ years, whereas 2025 saw the official end of life and hardware support for Windows 10.³



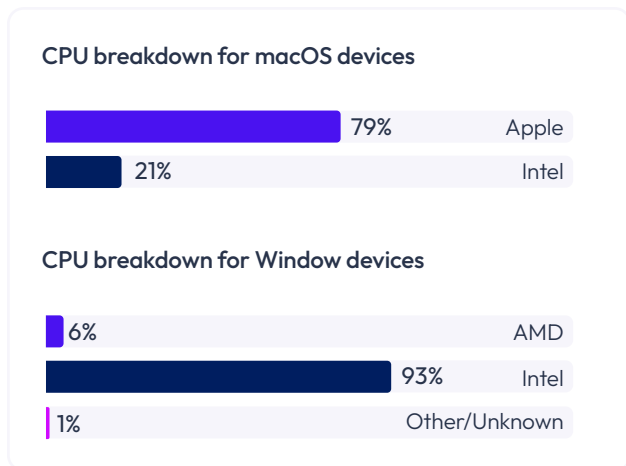
Organizations can leverage insights into device lifecycles to pivot toward refresh policies grounded in platform longevity, application fit, and performance requirements.

Device configuration is shaped by user requirements

Beyond lifespan, the telemetry also reveals a divergence in how devices across OS platforms are internally configured. Based on our findings, organizations are intentionally configuring devices with distinct silicon architectures, memory, and storage capacities based on the thermal and computational demands of the user’s role.

Apple embraces the performance advantage of silicon

The enterprise Mac fleet has transitioned away from Intel, with **79% of devices now running on custom Apple silicon (M-series) processors**. Conversely, the Windows fleet remains heavily entrenched in legacy x86 architecture, with 93% utilizing Intel processors and only 6% using Advanced Micro Devices (AMD).



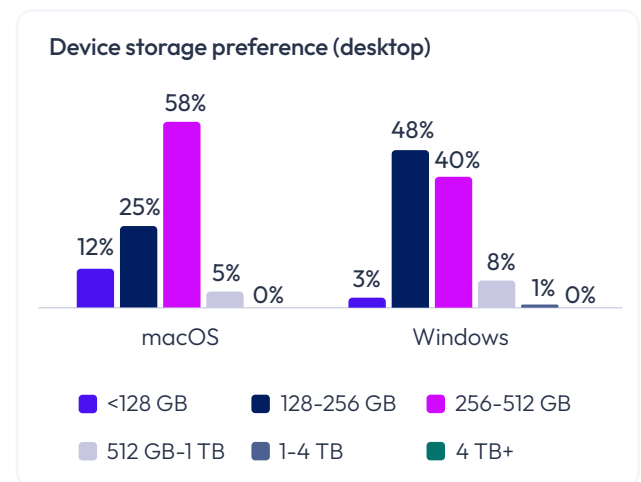
The rapid adoption of Apple silicon seems to indicate a strong enterprise appetite for ARM-based architecture, which delivers a distinct **“thermal advantage”** (higher performance-per-watt). This translates to less energy loss, lower cooling requirements, and longer usable device life.



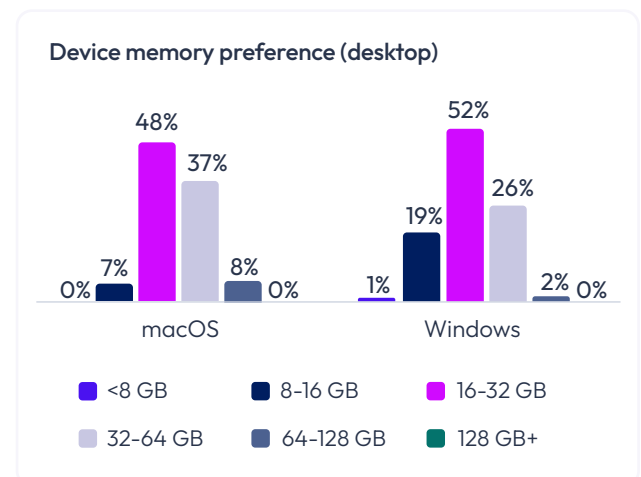
Our data shows that Intel chips in enterprise Macs average thermal outputs of **65.2°C**, while **Apple M-series silicon stays cool at just 40.1°C**, effectively eliminating the performance/thermal trade-off.

Persona drives storage and memory capacity

The telemetry shows that the “sweet spot” for macOS devices sits firmly in the 256 GB–512 GB range (58% of the fleet). Windows devices are much more evenly distributed across the 128 GB–512 GB tiers (88% of the fleet).



Research also reveals a noticeable gap in memory provisioning. Macs boast a weighted average of 28 GB of RAM, compared to 21 GB for Windows devices.



Storage and memory sizing is a clear indicator of the worker’s persona. The data suggests that macOS endpoints may be preferred for pro users—for example, developers and creators who require substantial local caching for rich media, large codebases, or complex datasets. Meanwhile, the flatter distribution of Windows PCs points to a broader mix of “utility” workers, frontline staff, or users highly reliant on cloud/VDI storage where massive local drives are an unnecessary expense.

Section summary: Observability is key to optimizing device choice

The pivot toward persona-based, highly diversified hardware fleets creates a massive new challenge for IT, as **it's impossible to optimize what you cannot observe**. In a heterogeneous environment in which a frontline worker requires a ruggedized Android scanner and a developer requires a 32 GB M-series Mac, relying on static spreadsheets and assumed refresh cycles could lead to immense capital waste. Without deep observability into actual device performance—such as daily memory utilization, thermal throttling, and true battery degradation—procurement teams may be left guessing.

By continuously measuring the actual hardware performance and consumption of the workforce, organizations can transition from reactive and scheduled asset management to a dynamic, persona-based management approach that helps optimize the dollars spent while keeping employees rightly provisioned, productive, and satisfied.



2 The shadow perimeter

The growing use of AI and unsanctioned apps has created new, unseen risks

The way employees discover, acquire, and use their apps has fundamentally shifted. Instead of tightly controlled software procurement, we now see a decentralized, user-driven ecosystem. Apps are being downloaded from websites and mobile app stores as employees prioritize speed and innovation above all else.

This shift may empower the workforce, but it also creates a complex challenge for IT decision-makers as traditional governance models struggle to keep pace. Our research has uncovered a **“shadow app” economy that introduces risks that the standard security perimeters fail to see**. Organizations must quickly adapt their governance policies to counter the widening gap between the tools IT sanctions and the tools employees adopt. There are four key observations that have led us to this conclusion:

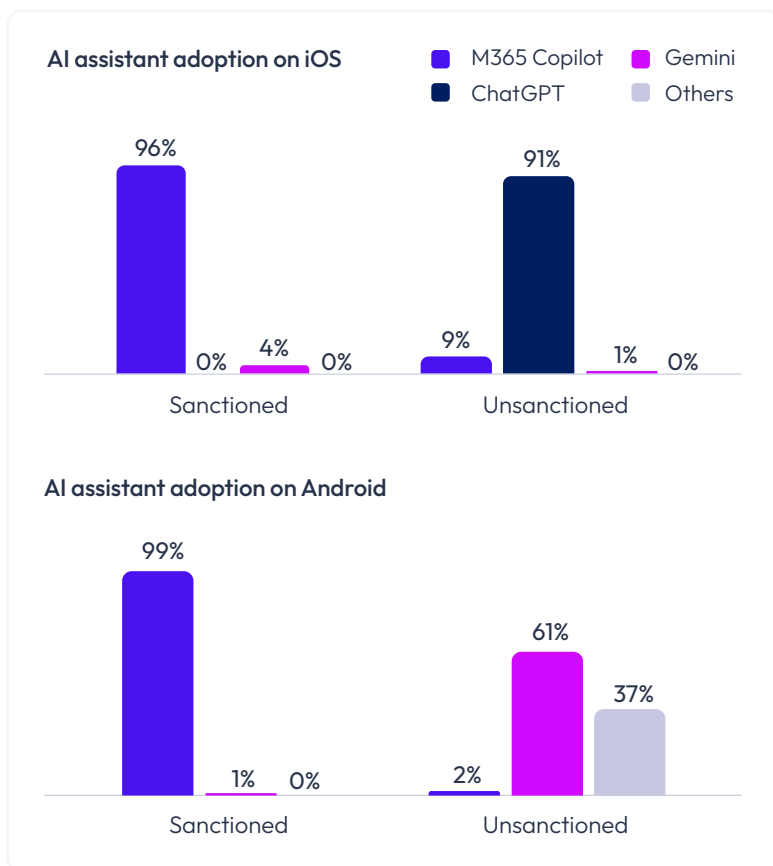
1. Unsanctioned AI apps are prevalent in the enterprise.
2. Personal communication tools are blurring professional lines.
3. Browsers are quickly becoming the new endpoints.
4. Windows system bloat may hinder user utility.



Unsanctioned AI apps are prevalent in the enterprise

While the use of business and productivity apps has remained stable, GenAI powered AI-assistants are by far the fastest-growing app category in our CY25 dataset, notching a **near 1,000% growth across most OS platforms**.

However, adoption patterns reveal a stark dichotomy between the corporate agenda and user preference. As IT departments move quickly to deploy sanctioned, enterprise procured AI tools—primarily Microsoft Copilot—employees are aggressively adopting publicly available apps like ChatGPT and Gemini on enterprise-managed devices, outside of IT’s view.

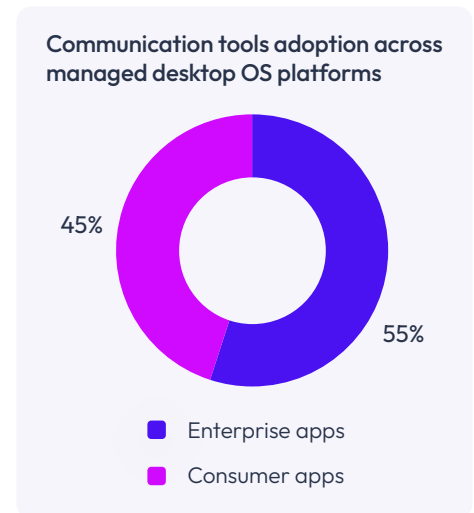


Microsoft’s integration of Copilot into their enterprise bundles (Microsoft 365) clearly gives it a distribution advantage in the enterprise, as indicated by their high 90%+ share in the sanctioned category. However, **the divide in sanctioned vs. unsanctioned apps may indicate a gap in user satisfaction**, with employees possibly seeing the corporate-sanctioned tools as either insufficient, restrictive, or lacking in features they need to get their work done. Consequently, they are turning to unsanctioned alternatives.

This, of course, introduces risk. Employees feeding proprietary data into unsanctioned AI models, coupled with the rapid growth of these tools, makes “shadow AI” a primary vector for potential data exfiltration.

Personal communication tools are blurring professional lines

Just like with AI apps, many employees are creating potential compliance blind spots by adopting consumer messaging and communication tools on enterprise-managed devices. While enterprise standard apps like Microsoft Teams, Zoom, and Slack dominate the sanctioned apps landscape, our research shows a high prevalence of consumer messaging apps on these corporate devices.



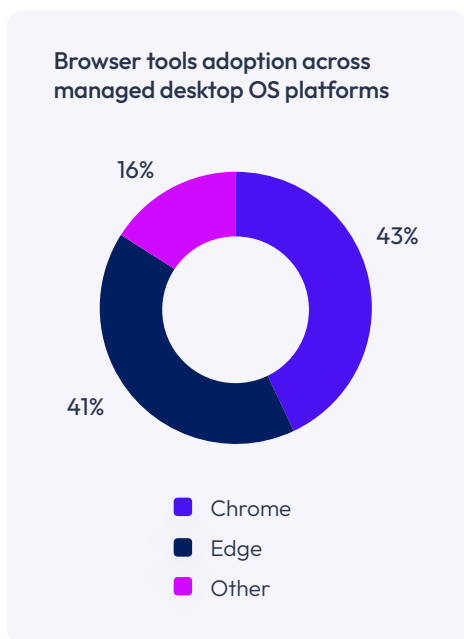
The use of unmonitored consumer messaging apps constitutes a significant compliance risk, especially in industries with strict record-keeping requirements such as financial services and healthcare.



When business decisions happen on encrypted, unmanaged platforms, organizations lose the ability to audit, archive, or secure those communications.

Browsers are quickly becoming the new endpoints

Google Chrome remains the dominant browser across all desktop platforms. On Windows, Microsoft Edge has solidified its position as the runner-up, displacing legacy Internet Explorer completely. Niche “enterprise browsers” like Island and Talon are appearing in the data, albeit with small share.

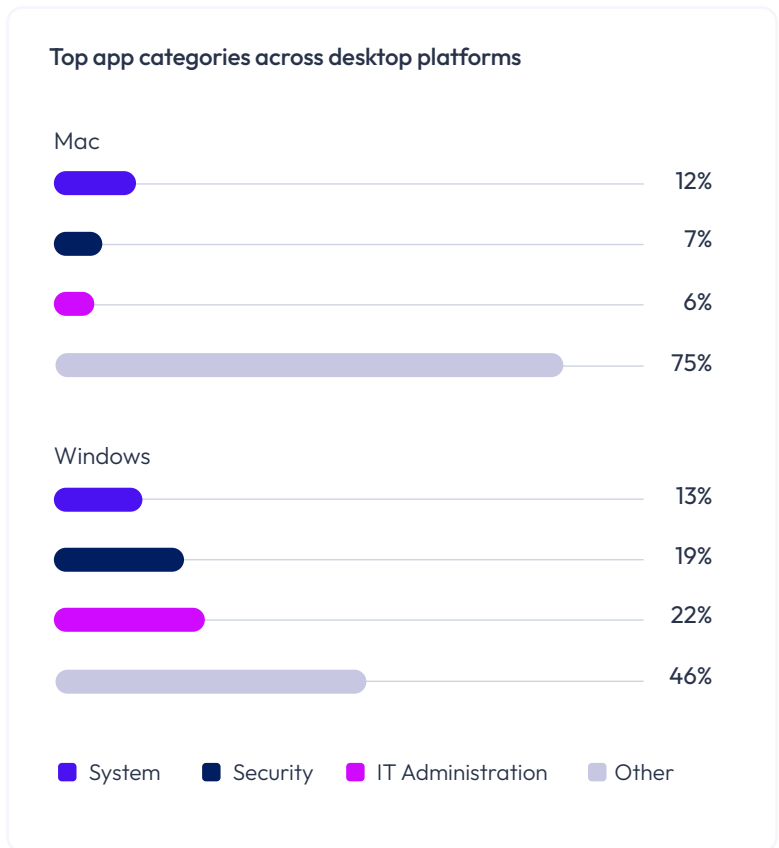


With the explosion of SaaS apps like Salesforce, Workday, and ServiceNow, the browser is effectively the new operating system and the endpoint for the modern worker. The presence of niche enterprise browsers suggests IT is attempting to regain control over this “last mile” of data presentation, moving security controls from the device level to the browser level.

Windows system bloat may hinder user utility

On the desktop front, particularly within Windows environments, the data also surfaces a different kind of app challenge: **agent fatigue**.

Our analysis of Windows app packages reveals that **IT administration, security, and system tools make up nearly two-thirds of the deployed software stack**. This “bloat” often competes for resources with the productivity apps employees rely on to do their jobs.



The abundance of management and security agents creates a paradox: While IT deploys more agents to gain more control, these agents often cause a degradation to the employee experience. It’s a cycle in which the attempt to manage risk may inadvertently hinder productivity.

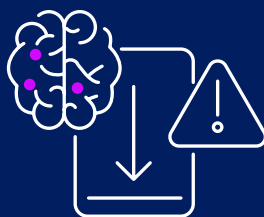
Section summary: Seeing into the shadows with observability

The “shadow perimeter” findings prove that using traditional, static blocklists for unauthorized apps is a failing strategy. Users will always find the path of least resistance to get their work done, whether that means pasting proprietary code into an unsanctioned AI prompt or collaborating on a rogue messaging app. This presents yet another challenge to IT: **You can't secure a perimeter that you can't see.**

The solution isn't to impose stricter lockdowns, which can stifle innovation and frustrate talent, but to achieve real-time observability across the app landscape so IT can transition from a department of “No” to a secure enabler for the workforce. Comprehensive observability can enable organizations to:

- **Shine a light on shadow AI usage**, allowing IT to sanction popular tools or provide secure alternatives rather than issuing blanket bans.
- **Rationalize the app stack** by identifying redundant agents on Windows devices to improve performance without compromising safety.
- **Implement adaptable data governance policies** that can keep up with—or even anticipate—unsanctioned IT usage.

Organizations must pivot from being gatekeepers to being enablers. With deep visibility into app adoption—sanctioned or otherwise—IT can manage both enterprise risk and user productivity at the speed of human innovation.



3 Security hygiene

Moving from reactive audits to proactive remediations is essential to keeping the enterprise secure

The data shows digital work fragmentation across diverse devices, form factors, OS platforms, apps, and even ownership models. It also sheds light on the emergence of a dangerous byproduct: the **erosion of foundational security hygiene**.

Our research reveals that traditional, policy-based controls are failing to keep pace with today's digital work sprawl, leading many organizations to operate under a false sense of security while harboring alarming rates of non-compliance.

Without cohesive visibility, security gaps will appear where teams least expect them, creating opportunities for threats to go undetected. This means **organizations must shift from reactive policy and audit controls toward a security posture powered by continuous observability**, enabling them to proactively identify and remediate these evolving risks with confidence. We have arrived at this conclusion by observing three critical failures in enterprise hygiene:

1. Patching velocity is inconsistent across OS platforms.
2. Critical industries are lagging behind on OS updates.
3. Desktops have alarmingly high levels of unencryption.

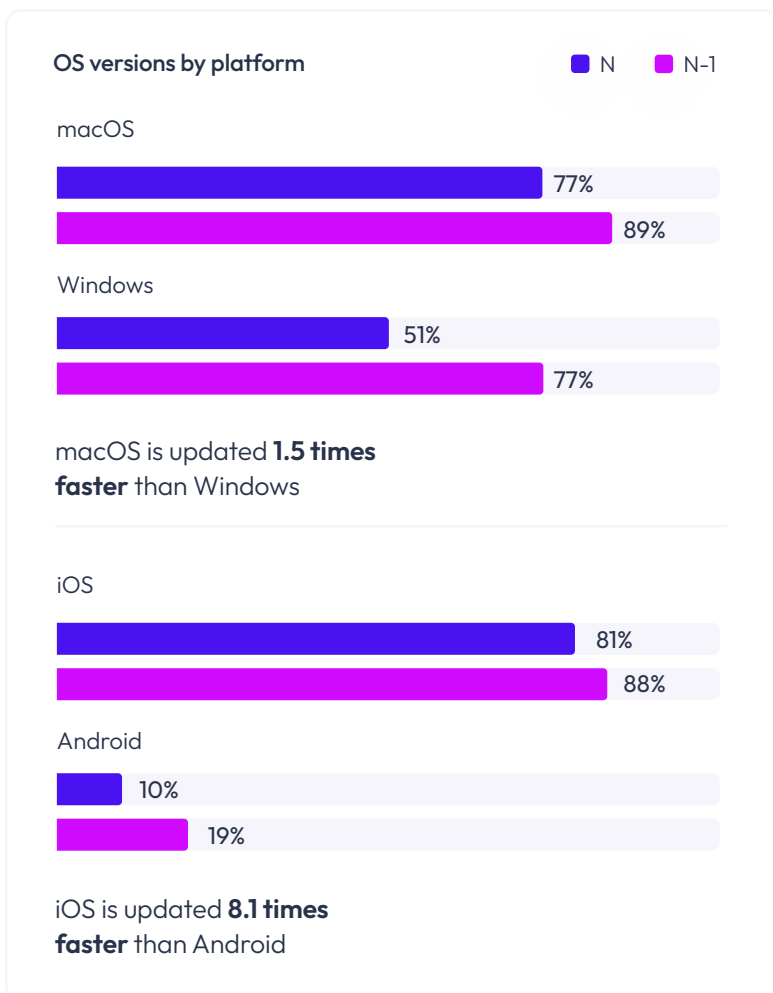


Patching velocity is inconsistent across OS platforms

In a landscape defined by zero-day vulnerabilities, keeping operating systems current is a foundational metric of security hygiene. Yet our research shows that many organizations are falling behind on this critical security practice, creating a significant window of vulnerability.

The data reveals a stark contrast in patching velocity across OS platforms, with Windows and Android platforms lagging in comparison to their Apple counterparts, even within highly regulated sectors.

Here are the results when we look at the disparity in how fast the mobile and desktop operating systems are updated to their latest (referred to as “N”) or the previous (referred to as “N-1”) versions:



The disparity in patching velocity could be structural

Apple controls the entire update stack, whereas Android updates are likely fragmented across OEMs and device types (smartphones, ruggedized handhelds, etc.). As observed in section 1, our data does show a higher concentration of Android devices in frontline and regulated sectors, which may prefer longer-term servicing of updates for app compatibility and fewer user disruptions in critical workflows. On Windows devices, the strict hardware requirements (e.g., TPM 2.0) for Windows 11 could be forcing enterprises to delay upgrades coinciding with hardware refresh cycles.



The rapid adoption of macOS updates (often within 90 days) suggests that Mac users are culturally conditioned to update, or that OS update controls for macOS are centralized, less obstructive, and more reliable than the bifurcated Windows Server Update Services (on-premises) and Windows Update Client Policies (cloud) approach for Windows patching.

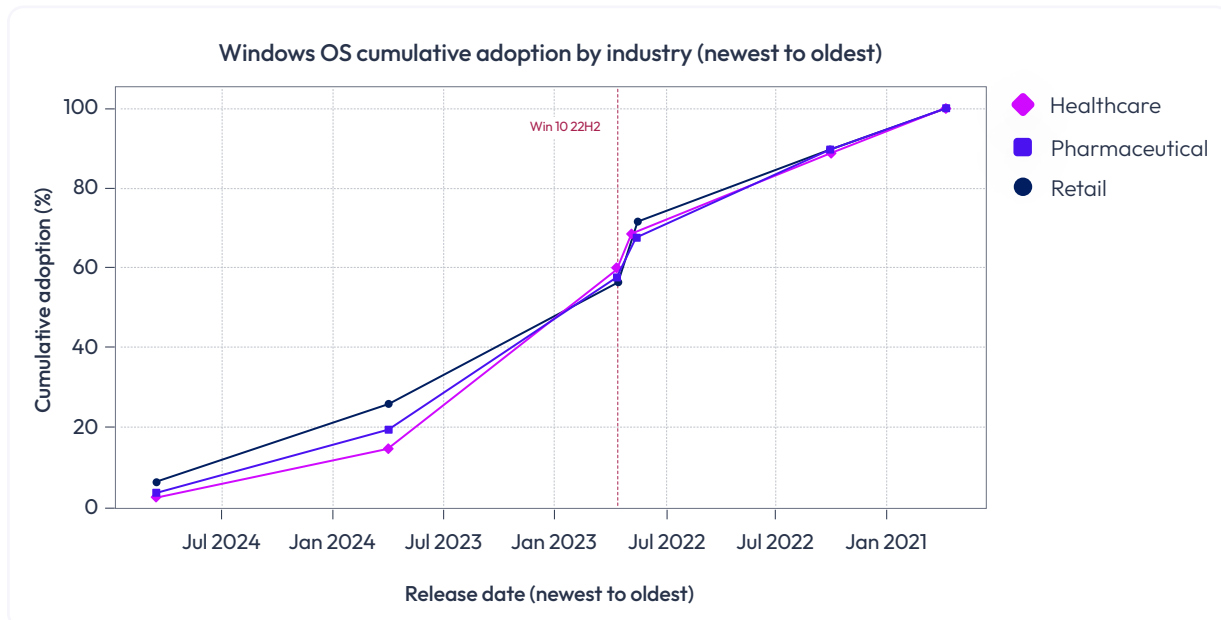
Critical industries are lagging behind on OS updates

When looking at OS version adoption by industry, an alarming pattern emerges: The industries that house the most sensitive data are ironically the furthest behind in basic OS patching.

Critical industries like healthcare, pharmaceuticals, and retail and wholesale consistently let their operating systems languish. In the Android ecosystem, these three verticals have the highest percentage of devices running versions that are N-4 or N-5 (four to five generations old).



A similar observation can be made for how up to date these industries are on their Windows PCs.



This points to a severe operational bottleneck, with the fear of breaking mission-critical legacy apps, such as those used in medical charting or retail inventory, overriding the need for critical OS updates. This bottleneck may be a symptom of vendor lock-in versus IT competency, with software vendors for these specialized apps often slow to certify new OS builds. However, by choosing operational uptime over basic security hygiene, these industries may very well be leaving devices exposed to exploits.

Desktops have alarmingly high levels of unencryption

While encryption is a non-negotiable layer of data protection, our research shows that **desktop devices have significantly higher rates of missing encryption** compared to their mobile counterparts. This is likely due to the added effort in managing native encryption tools, such as BitLocker and FileVault, in comparison to the passcode-enforced, built-in simplicity of mobile OS encryption.



Regardless of device type, the education and government sectors show high rates of unencryption—**20% of government desktops are unencrypted and over 50% of education desktops and mobile devices are unencrypted.**

Across sectors—including those managing highly sensitive intellectual property and citizen data—the percentage of unencrypted desktops is alarmingly high.

High rates of unencrypted desktop devices

Banking, finance, and insurance



Healthcare



High tech



Media and entertainment



What could explain this encryption gap?

In education, one of the most attacked industries globally,⁴ the encryption gap is likely due to the prevalence of shared carts and older devices where encryption impacts performance. This is also validated by our data that shows education as having one of the highest percentages (51%) of older devices (>3 years in service).

For banking and healthcare, the encryption gap may indicate a false negative, as these industries have the highest concentration of secure virtual desktop sessions, often accessed via thin or zero clients. Our data also points to a staggering **36% YoY growth in virtual desktops**, a likely indicator of organizations pivoting to VDI driven by Windows 10 end-of-life and the need for newer OS-ready hardware.

Regardless, the sheer amount of unencrypted devices across these regulated industries makes them soft targets for a major compliance failure waiting to happen.

Section summary: Observability can help proactively mitigate risk

The widespread failure of basic security hygiene we have observed indicates that traditional compliance models are broken. IT cannot rely on point-in-time compliance checklists or the assumption that a policy pushed is a policy enforced. Configuration drift is inevitable in a fragmented workspace. By unifying observability across the digital workspace, organizations can:

- **Detect hygiene gaps instantly** – Identify and remediate unencrypted devices or disabled firewalls the moment they appear, regardless of the operating system.
- **Quantify risk exposure** – Know exactly how many devices are vulnerable to a specific CVE and prioritize patching based on risk.
- **Monitor compliance continuously** – Replace periodic audits with continuous monitoring that alerts IT to compliance gaps before they become incidents.

End-to-end observability transforms security from a reactive scramble into a proactive, data-driven operation that keeps the enterprise safe, compliant, and ready for what's next.



4 Employee experience

Digital “micro-frictions” are causing an undetected productivity gap in the enterprise

In pursuit of operational efficiency, IT teams have historically relied on binary metrics like device uptime and service tickets. However, our research reveals a critical blind spot in this approach: **A device can be technically operational while user productivity is actively hindered.** Digital micro-frictions like app crashes, app hangs, and system slowdowns can cause significant productivity drains that directly impact business outcomes.

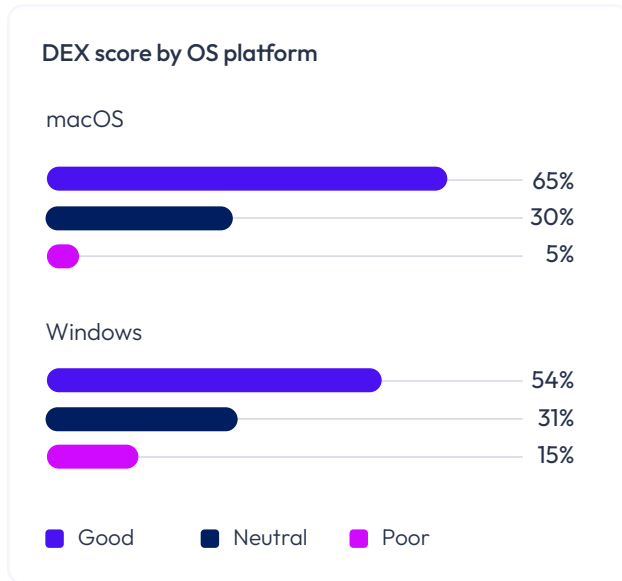
Deep observability is required to help organizations effectively quantify this productivity gap and justify the ROI of their digital employee experience (DEX) investments. We have arrived at this conclusion after making the following two observations:

1. DEX baselines differ across desktop systems.
2. System instability imposes a “forced interruption tax.”



DEX baselines differ across desktop systems

Our research reveals a measurable difference in DEX scores across platforms, indicating that Mac devices consistently deliver a higher baseline of positive user experience compared to Windows devices.



The DEX score is not an abstract feeling or user sentiment score—it is a measurable output of hardware and software synergy. For Apple, the tighter integration of their silicon, OS, and hardware ecosystem (the “Apple silicon advantage”) is likely resulting in a higher baseline of health. Conversely, the complexity of the “Wintel” ecosystem—a multi-vendor combination of OEM hardware, peripherals, third-party drivers, and configuration agents—potentially drags down the health score for the Windows platform.



In measuring users’ experience with their devices, the “Good” score for Mac stands 1.2x higher than for Windows. The Windows “Poor” score is 3x that of Mac.

System instability imposes a “forced interruption tax”

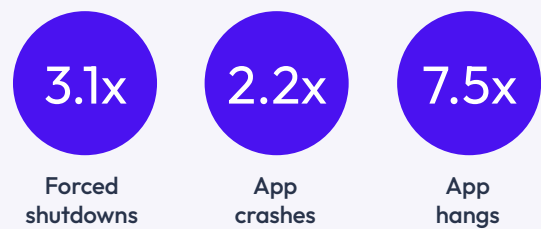
Besides the composite DEX score, we have also analyzed critical system failures such as forced system shutdowns, app crashes, and app hangs.



Studies show that it takes an average of **23 minutes and 15 seconds to refocus after a disruption**.⁵ When these events happen daily across thousands of employees, the cumulative effect is a massive, invisible “productivity tax” paid by the organization.

The telemetry reveals that Windows devices **exhibit 3.1x more total forced shutdowns** (including system crashes and unexpected restarts) than macOS devices. A forced shutdown is much more than an IT support ticket—it’s a disruption to an employee’s work that translates directly into lost work hours. What IT may see as a 60-second device reboot could very well be a 20- or 30-minute “refocus penalty” of lost business output.

Windows system failures compared to Mac



The productivity gap extends into the app layer. Telemetry shows that **Windows devices experience 2.2x more app crashes and a staggering 7.5x more app hangs** (unresponsive software states) than Macs. In contrast to a full system crash, app hangs are often the “silent killers” of productivity, as a user sitting and waiting for an app to respond does not trigger a traditional IT alert.

Section summary: Observability can help quantify the productivity gap

The stark disparities in system crashes and app hangs highlight a critical failure of traditional IT monitoring that leaves organizations bleeding through a continuous, unmeasured productivity gap. End-to-end observability is the key to effectively mitigating this lost time and definitively justifying the ROI of DEX initiatives. This allows organizations to:

- **Quantify the experience** – Translate technical hiccups like a 15-second app hang or a blue screen into quantifiable business metrics, such as “hours of lost productivity” and “dollar value wasted.”
- **Diagnose root causes** – Correlate performance data from multiple sources to pinpoint the exact cause of slowdowns, whether it’s a buggy app, a network bottleneck, or a failing hardware component.
- **Optimize proactively** – Make data-driven decisions to optimize procurement decisions and address potential issues before they impact the workforce. By understanding how resources are used, IT can make informed decisions about hardware refreshes, app rationalization, and policy changes.



Conclusion

We are entering the era of radical visibility

The Omnissa State of Digital Workspace 2026 report makes one thing abundantly clear: The era of “management by standard” is over. The enterprise perimeter has dissolved, the hardware catalog has fractured into specialized ecosystems, and the digital employee experience has become the primary territory for organizational productivity.

Across every chapter of this report, the telemetry tells a consistent story of a widening gap between IT policy and operational reality.

- **For devices**, we see how “standard” hardware procurement can ignore persona-based performance needs, and how reliance on yesterday’s refresh paradigms comes at a high cost.
- **For apps**, we observe a rapidly expanding “shadow perimeter” effectuated by the rise of unsanctioned AI and communication tools, creating significant data exfiltration and compliance risks.
- **For security**, our research exposes the illusion of compliance, revealing an alarming percentage of unencrypted endpoints and delayed uptake of new OS versions, including in highly regulated industries.
- **For experience**, the data quantifies inconsistent performance across platforms, marked by frequent crashes and hangs and directly eroding employee productivity.

To navigate this complexity, organizations must build a digital workspace strategy centered on end-to-end observability—across every device, app, security layer, and user experience. This can enable organizations to understand the real risks, and make intelligent, data-driven decisions that optimize and secure the digital workspace, without stifling innovation.

1. Government Executive. “5 Must-Know Government Technology Trends in 2025.” January 30, 2025.
2. Scope Technical LLC. “Logistics Innovation: The Impact of Wearable Technology.” January 19, 2025.
3. Microsoft. “Windows 10 support has ended on October 14, 2025.” 2025.
4. DeepStrike. “Data Breaches in Education 2025: Why Schools are the #1 Cyber Target.” Mohammed Khalil, August 18, 2025.
5. Gloria Mark, Daniela Gudith, and Ulrich Klocke. “The Cost of Interrupted Work: More Speed and Stress.” April 2008.

Looking ahead

As our inaugural data report, this year's analysis establishes a crucial empirical baseline for the industry. By synthesizing pure telemetry from millions of endpoints over a 12-month period, we have moved beyond the noise of survey-based conclusions to provide a data-driven, ground-truth view of how the digital workspace actually operates today.

As the digital workspace continues to evolve at an unprecedented velocity, we look forward to the next edition of this report. In future iterations, we aim to explore further:

- **AI hardware readiness**, tracking deployment and utilization of hardware as organizations prepare for on-device AI workloads.
- **Useful life of device**, doubling down on device lifecycle by correlating performance scores to time in service.
- **Sustainability and carbon impact**, measuring the environmental, social, and governance (ESG) implications of device lifecycles, refresh rates, and power consumption across varying platforms.
- **Compliance risk factors**, discovering the top reasons for non-compliance across platform types and industries.
- **Segment analysis**, understanding the impact of these digital workspace measurements across different organization sizes.

The modern digital workspace is too complex, too diverse, and too critical to leave in the shadows. The future belongs to the organizations that choose to see it clearly.

omnissa®