jumpcloud™ Google Workspace

eBook

The Enterprise Unification Gap: Why 87% of IT Leaders Would Switch Productivity Suites

How JumpCloud and Google Workspace Deliver the Integrated Foundation for Simplicity and Zero Trust

Modern Productivity Suites Promise Simplicity. IT Knows Better.

Any IT leader knows that "simple" is rarely simple. Productivity suites remain essential to identity, collaboration, and access, yet they are also one of IT's biggest sources of operational friction.

Productivity suites function as the backbone of day-to-day operations. But keeping them running smoothly, especially when locked into legacy technology, requires continued oversight, policy tuning, and integration work across complex environments. The findings in this report, from a survey of 250 U.S. enterprise IT decision-makers, show how deep that burden runs: **only 6% report a truly seamless experience, and nearly one-third (28%) say their suite meets their needs but only with significant cost or complexity.**

IT has tried to close the gaps with connectors, add-ons, and third-party tools. These efforts can help, but they also layer on administrative work, increase cost, and expand the attack surface. This steadily erodes the simplicity that suites were meant to deliver. According to recent industry research, organizations on average now rely on 9.3 tools to manage their core IT functions, and only 5% use fewer than four.[1]

The market is ready for change: **Almost nine in ten of IT decision-makers would consider migrating to a more modern productivity suite if a better, unified solution existed.** That signals a clear demand for an operating model that prioritizes simplicity, verifiable security, and time-to-value over yet more features.

About the survey

Results are drawn from a survey of 250 U.S. IT decision-makers at organizations with 2,000+ employees and are exclusive users of either Microsoft 365 (61%) or Google Workspace (39%).

Respondents included C-suite,senior leadership,IT directors, managers, and admins with purchasing power. Company size distribution includes 53% with 2,000–4,999 employees, 37% with 5,000–9,999, and 10% with 10,000+. Industry mix reflected a broad cross-section. The study was fielded with 95% confidence and a ±6.2% margin of error.

The Current Enterprise Productivity Landscape

Productivity suites sit at the core of enterprise IT, connecting people, devices, and data. They are indispensable and increasingly difficult to manage at scale.

Working ≠ Effortless

Only **6%** have *no challenges* with their suite

Nearly **1 in 3** say it "works" **only with significant cost / effort**

For most enterprises, "working" still means ***working harder.***

As a result, IT teams spend valuable time maintaining integrations, managing licenses, and troubleshooting identity or device conflicts instead of enabling innovation.

Where complexity lives

Microsoft-centric environments often deliver rich functionality but also accumulate administrative layers, licensing tiers, and policy sprawl, increasing costs and reducing agility. Over time, incremental add-ons across identity, endpoint management, and security enforcement create operational drag and dependency that is difficult to unwind.

Google Workspace environments are built on a cloud-first, collaboration-driven architecture that provides a leaner operational base and greater adaptability. Yet without unified management of identity, devices, and access, even these environments can fragment as scale and security demands grow.

Breaking the cycle of complexity

Enterprise IT leaders are now questioning not just what their productivity suite can do, but how much work it takes to keep it working. The next stage of modernization lies in unifying AI, collaboration, identity, and device management into a single control plane. This removes layers of complexity that slow productivity and inflate costs.

New partnerships, such as the collaboration between Google Workspace and JumpCloud, reflect how the industry is beginning to deliver on that vision by simplifying the foundation rather than adding to it.

The Price of Patchwork IT

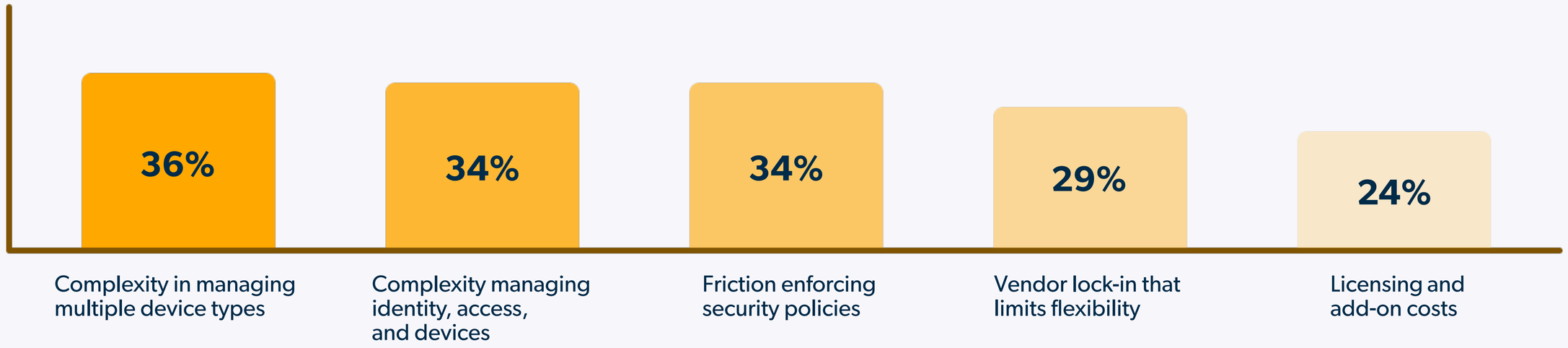
IT teams have learned to live with fragmentation, keeping systems online despite layers of disconnected tools and policies. Every workaround has a price in time, risk, and money.

Microsoft-heavy organizations feel the strain.

With more than 3.7 million companies worldwide on Microsoft 365, that translates to roughly 1.3 million organizations struggling with multi-device complexity, 1.3 million with identity and policy management, 1 million with vendor lock-in, and nearly 900,000 contend with escalating licensing costs.

Among managed service providers, 70% say Microsoft 365 requires more administrative time than Google Workspace—evidence of the same inefficiencies from a partner's perspective.[2] With an estimated 150,000 MSPs, even incremental inefficiencies in managing Microsoft 365 could have a significant ripple effect across the ecosystem.[3]

Which of the following best describes the gaps or challenges your IT team faces with your current IT set up?



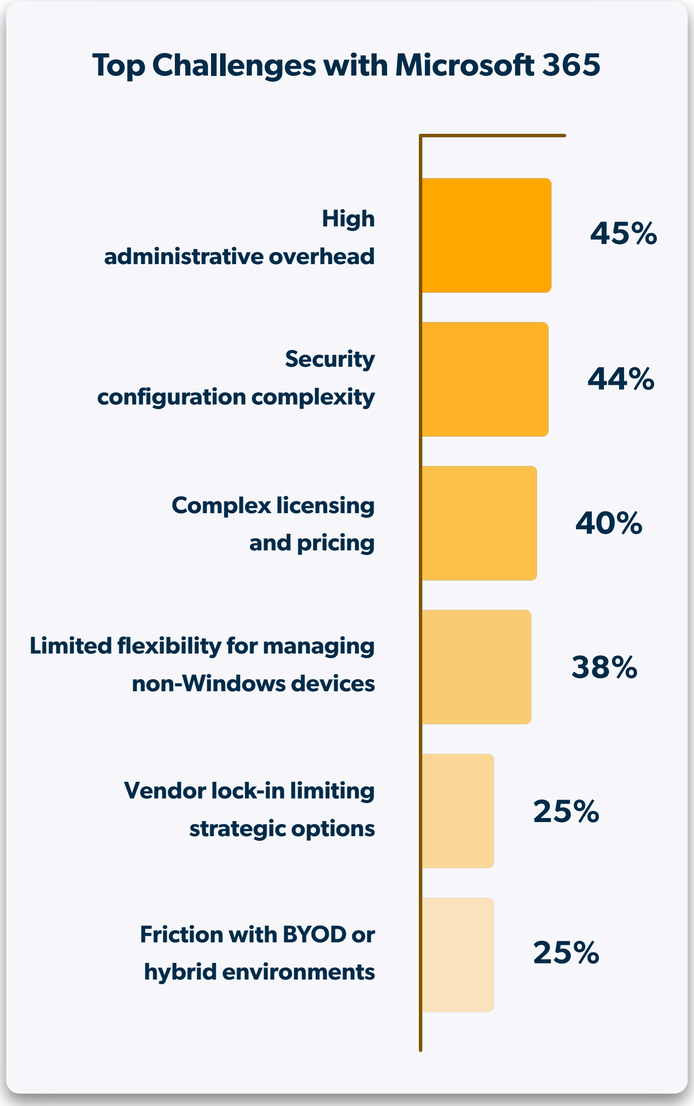
The Price of Patchwork IT

This picture aligns with JumpCloud's broader IT Trends research. **Only 2% of IT professionals have not explored alternatives to Microsoft.** Organizations' top three challenges with Microsoft 365 were high overhead (45%), security configuration complexity (44%), and complex licensing and pricing (40%).[1]

Alternatives such as Google Workspace offer significant benefits, with JumpCloud's IT Trends research showing that almost two-thirds (64%) of organizations use it alongside Microsoft 365. Many enterprises deploy both suites in parallel—using Google Workspace for collaboration and Microsoft 365 for legacy workflows or license entitlements—highlighting the demand for flexibility rather than full replacement. IT professionals said the top three benefits they associate with using an alternative to Microsoft 365 were improved end-user experience (64%), increased agility (57%), and easier automation (52%).

However, JumpCloud's survey findings reveal that Google customers face friction too: citing multi-device management challenges (47%) and tool sprawl (43%). But these issues are primarily operational rather than architectural and can be resolved by unifying device and identity management. Recognizing these operational rather than architectural gaps, Google introduced the Work Transformation Set with JumpCloud to unify identity, device, and policy management under one control plane.

Every disconnected tool widens the administrative surface, multiplies licensing costs, and opens new security gaps. The organizations that will thrive in the next phase of enterprise IT will stop patching complexity and design for unification, consolidating identity, device, and policy under one cohesive model.



The Unification Gap

Many organizations believe they have achieved unification, but most are operating a patchwork of connectors, manual syncs, and loosely coupled systems. True unification, where identity, device, and policy operate seamlessly, remains uncommon.

The state of unification today

Despite consolidation efforts, true end-to-end unification is the exception rather than the rule:

Identity:
46% are **not** fully unified

Device management:
62% are **not** fully unified & automated

Security policy enforcement:
64% are **not** fully unified

Compliance management:
66% are **not** fully unified

Over half (58%) of organizations report that their IT unification is unsustainable. Another **38%** report it only works with high ongoing administrative effort, and nearly one in five still have major security, compliance, or audit gaps. On average, organizations manage **9.3 tools** across core IT, which raises cost, adds manual oversight, and increases risk exposure.

58%

of organizations report that their IT unification is unsustainable.

The Unification Gap

Why unification is hard

Microsoft environments

Microsoft environments often combine several distinct products—such as Active Directory or Entra ID, Intune, Defender, and Purview—each with its own policy model and administrative console. This creates a multifaceted ecosystem that requires deliberate configuration and orchestration to maintain consistency.

IT teams must define clear ownership and precedence across systems—such as which platform governs device posture, which manages application access, and which enforces data loss prevention—to avoid overlap or policy conflict. When those boundaries aren't well established, administrative effort tends to increase as teams reconcile configurations across tools.

Over time, this can result in multiple layers of policy and enforcement models that add complexity and operational overhead. While these tools individually provide strong functionality, their distributed nature can make end-to-end visibility and unified control more difficult to achieve.

Google Workspace environments

Google Workspace starts from a cloud-native, collaboration-first foundation with fewer moving parts and cleaner interoperability. For enterprise requirements such as identity, device management, and policy enforcement, Google now offers an expanded enterprise layer through the Work Transformation Set with JumpCloud that establishes a single control plane with clearer policy ownership and precedence.

This model supports consistent automation and alignment with Zero Trust principles while helping reduce policy drift, multi-console overhead, and administrative burden. Historically, organizations often addressed these needs through a mix of third-party tools and manual integrations; the combined Workspace and JumpCloud approach represents an evolution toward a more unified architecture rather than an overlay of additional components.

DIY Unification Does Not Scale

Add-ons and workarounds keep systems running, but they rarely simplify them. IT leaders have invested significant effort to streamline their environments, yet most simplification has been achieved through connectors, point add-ons, and third-party tools rather than through a single operating model.

Nearly 79% of enterprises have attempted DIY unification using add-ons or third-party tools, but 58% say the effort has been unsuccessful. Microsoft environments often rely on overlapping tools such as Active Directory, Entra ID, and Intune as well as third party solutions to fill gaps.

DIY approaches may keep the lights on, but they do not make operations easier. Technical debt accumulates. Integrations need care and feeding.

Teams spend more time maintaining brittle links than improving core systems. “Good enough for now” becomes the norm, and the organization loses its ability to scale or adapt with confidence.

Over time, these fragmented connections also create security exposure points—inconsistent policy enforcement, outdated connectors, and unclear ownership of access controls—all of which weaken an organization’s ability to detect, prevent, and respond to threats. What begins as an operational workaround can quickly become a security liability.

Short term, DIY unification can preserve continuity. But long-term, it undermines resilience. The path forward is not more connectors. It is a unified operating layer for identity, device, and policy that eliminates overlapping tools and replaces integration work with a durable architecture.

A pieced-together IT solution will never be as secure, easy to manage, or scalable as a unified one.

Security and Compliance Breakpoints

Security and compliance are the pressure tests for every IT architecture. When tools do not talk to each other, gaps open in visibility, enforcement, and confidence.

More than 60% of IT leaders report gaps in access governance, MFA coverage, or device compliance.

Only about one in three say their compliance processes are fully unified and automated, and have greater audit exposure. Even mature IT environments struggle to maintain control when enforcement is distributed across disconnected systems.

Why these gaps translate into risk

Split consoles mean no single view of who has access to what from which device, creating real exposure:

- **Higher breach risk:** MFA gaps, stale accounts, and unmanaged devices raise the chance and blast radius of compromise.
- **Slower response:** Fragmented logs/policies delay detection and containment, increasing incident impact.
- **Audit & revenue risk:** Incomplete governance/compliance drives findings, penalties, and remediation cost.

Unifying identity, device posture, and access policy under one control plane shrinks attack surface and provides audit-ready proof.

Unifying enforcement, strengthening trust

Modern IT security benefits from a model where identity, device, and policy enforcement operate as a single, coordinated system. That is the foundation of the collaboration between Google Workspace and JumpCloud.

Through the Work Transformation Set, enterprises have:

- AI-powered productivity and collaboration through Google Workspace with Gemini.
- Cross-platform device visibility and compliance through centralized unified endpoint management.
- Zero Trust identity and access management through JumpCloud's platform.

And it's all delivered under a single Google Workspace contract with integrated support and pricing.

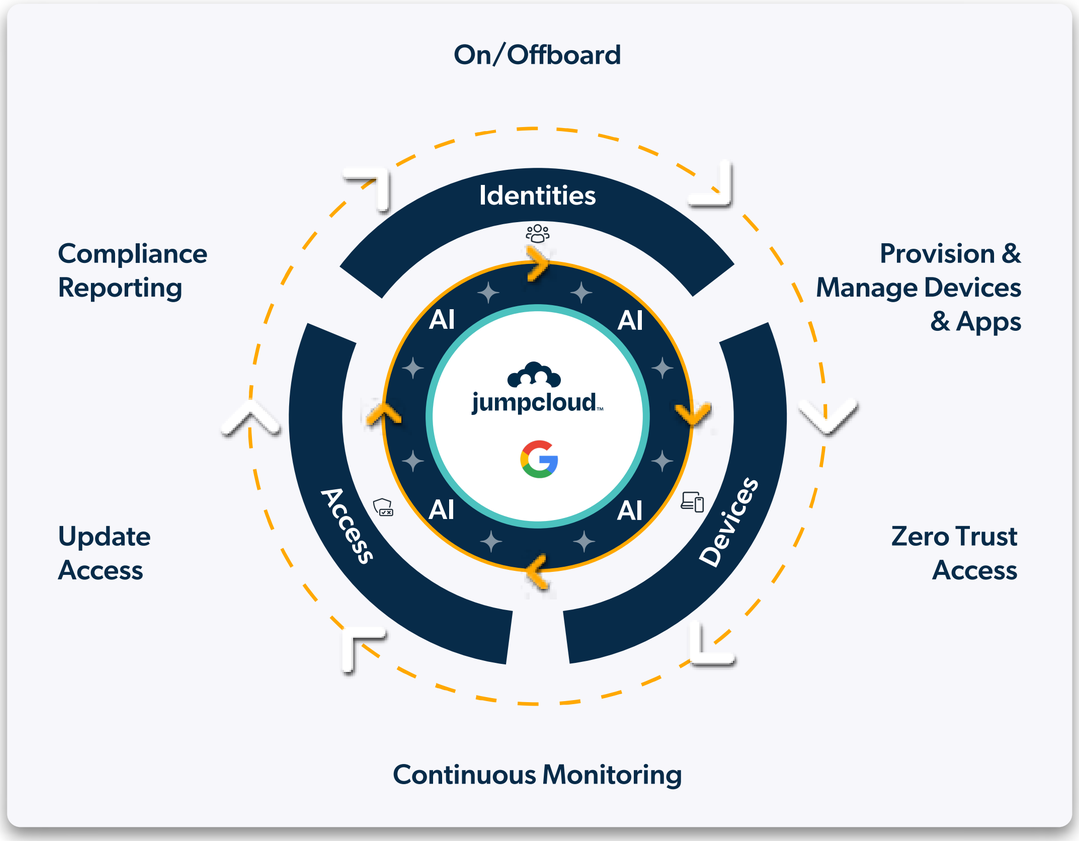
Together, Google Workspace and JumpCloud provide a cloud-native architecture that strengthens security while simplifying it, eliminating policy drift, reducing enforcement gaps, and removing multi-console overhead that makes compliance costly and complex.

A New Model for Unified Productivity

IT leaders are clear: progress depends on making identity, device, and collaboration operate as one system. An overwhelming 87% would consider migrating if a better unified solution were available, and over half (54%) say they are ***very likely*** to do so.

The collaboration between Google Workspace and JumpCloud introduces a new model for enterprise productivity—one designed to simplify operations by aligning collaboration, identity, device, and policy management within a single, cloud-first framework.

This unified architecture brings together Google Workspace with Gemini for AI-driven productivity and JumpCloud for cross-platform identity, access, and device management grounded in Zero Trust principles. Together, they demonstrate how a tightly integrated foundation can reduce administrative effort, strengthen security posture, and lower total cost of ownership.



This architecture illustrates how this model connects collaboration, security, and management under one cohesive control plane—representing a significant evolution in how enterprises can manage complexity at scale.

A New Model for Unified Productivity

From patchwork to one integrated architecture

This collaboration replaces a web of connectors and add-ons with a single operating model where identity, device, and policy enforcement share one control plane.

Challenge	Impact	Unified Solution
High admin burden	Increased cost and slower onboarding	Centralized identity and device management
Fragmented enforcement	Policy gaps and audit risk	Unified enforcement and reporting
Vendor lock-in	Limited flexibility	Modular, cloud-first foundation
DIY complexity	Ongoing maintenance and patching	One integrated architecture replaces add-ons

Work Transformation Set gives enterprises the migration path they're asking for—a single, auditable, cloud-first suite that unifies collaboration, identity, device, and policy while simplifying procurement and support.

“

As a rapidly scaling fintech, we needed an IT stack that could keep up with our growth without sacrificing security or adding complexity. The collaboration between JumpCloud and Google Workspace has been a game-changer.

We’ve cut employee onboarding time by 70%, eliminated manual password resets, and achieved 100% compliance across all our devices.

— Renjith Radhakrishnan, Head of IT Business Solutions, Tamara

Simplify to Strengthen

Productivity suites still power enterprise IT, but complexity is holding them back. Fragmentation, add-ons, and manual oversight have turned management into a full-time job. IT leaders are ready for a unified foundation that strengthens security, reduces overhead, and simplifies operations.

Work Transformation Set from Google Workspace and JumpCloud delivers that shift: a cloud-native, Zero Trust architecture that unifies collaboration, identity, device, and policy so teams can run simpler and safer while moving faster.

Ready to transform?

Discover how this powerful collaboration between JumpCloud and Google Workspace can be your final move away from the constraints and compromises of the past.

Learn More →

Appendix

[1] Q3 2025 IT Tech Trends Report

[2] 2025 MSP Performance Report

[3] How Many MSPs Are There?

About JumpCloud®

JumpCloud® delivers a unified identity, device, and access management platform that makes it easy to securely manage identities, devices, and access across your organization. With JumpCloud, IT teams and MSPs enable users to work securely from anywhere and manage their Windows, Apple, Linux, and Android devices from a single platform.

Learn more: https://www.jumpcloud.com/

Follow us: Blog | Community | Podcast | X | LinkedIn | YouTube | Resources

Click here to get started with JumpCloud.

About Google Workspace

Google Workspace is a suite of productivity apps, including Gmail, Drive, Calendar, Docs, Meet, Vids, and more, that are trusted by over 11 million paying customers. Google Workspace helps people and teams do their best work across any device, from anywhere. AI has been used in Google Workspace for years to improve grammar, efficiency, security, and more with features like Smart Reply, Smart Compose, and malware and phishing protection in Gmail. Now, Google Workspace with Gemini brings AI into the entire suite.