2025
IT Insights:
Identity, AI, and the Cloud

How leaders are securing the new perimeter and operationalizing artificial intelligence.

burwood group, inc.

Cybersecurity & Risk

EDUCATION AND USER BEHAVIOR ARE A STRUCTURAL CYBER GAP

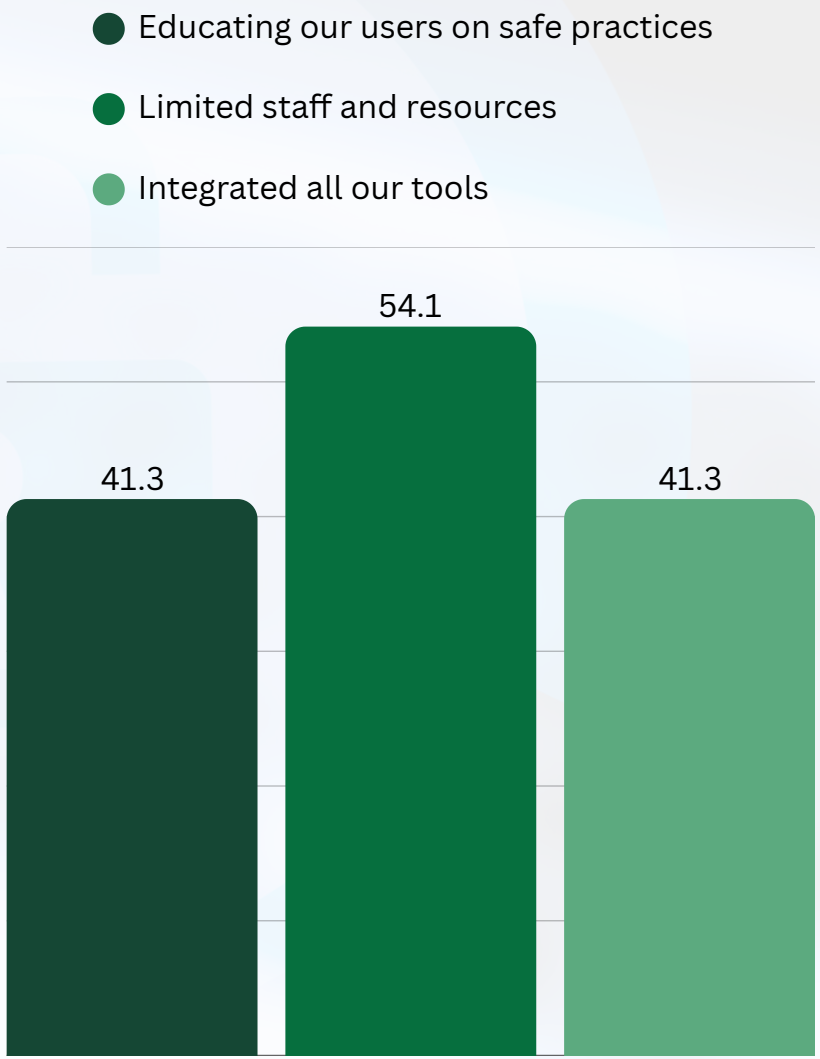
What the data shows:
When asked the top 3 Cybersecurity challenges, IT leaders reported human factors as 2 of the top 3. IT teams are walking a tightrope, balancing improving their security posture against growing threats while also educating their users. Notably, "protecting our network from internal threats and vulnerabilities" is 5th on the list, highlighting the duplicated effort when education isn't sufficient.

Why it matters:
AI-driven phishing, deepfakes, and shadow IT make users a prime target for attacks. Annual training is insufficient for today's threat landscape.

CIO Insight

Adopt continuous, contextual coaching in collaboration tools, deploy adaptive phishing simulations, and use human-risk scoring to prioritize interventions.

TOP CYBERSECURITY CHALLENGES



1

NETWORK AND CYBER RATINGS ARE DECENT—YET FRAGILE

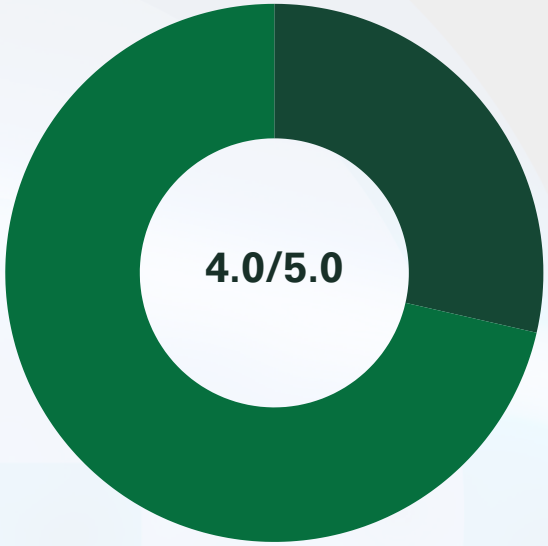
What the data shows:
Respondents rate their organization's cybersecurity preparedness at an average of 4.0 out of 5, and their IT network health at a similar 4.0. These self-assessments suggest confidence in current controls, but some leader's comments highlight concerns about legacy debt, infrastructure complexity, and the ability to recover from incidents or adapt to rapid change.

Why it matters:
Solid ratings can mask underlying fragility, especially when teams are stretched or processes are untested. As seen in the top cybersecurity threats, staff, resources, and budgets are limited. As threats increase and IT needs expand, cybersecurity can't be left lagging.

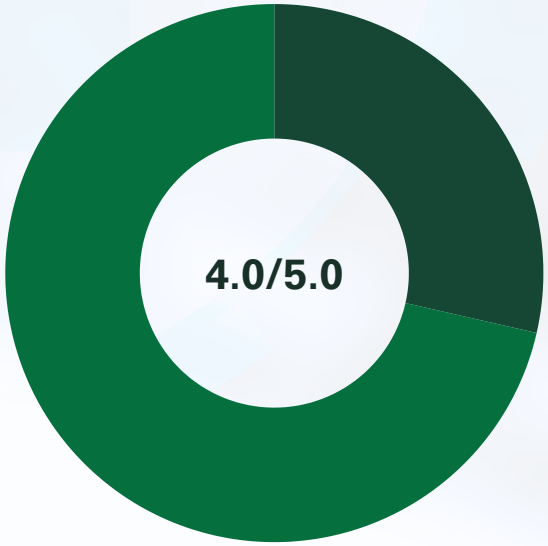
CIO Insight

Define resilience objectives beyond uptime. Include recovery time for identity, network, and data services. Run quarterly tabletop exercises and chaos testing to validate runbooks before major 2026 rollouts.

Cybersecurity Preparedness



IT Network Health

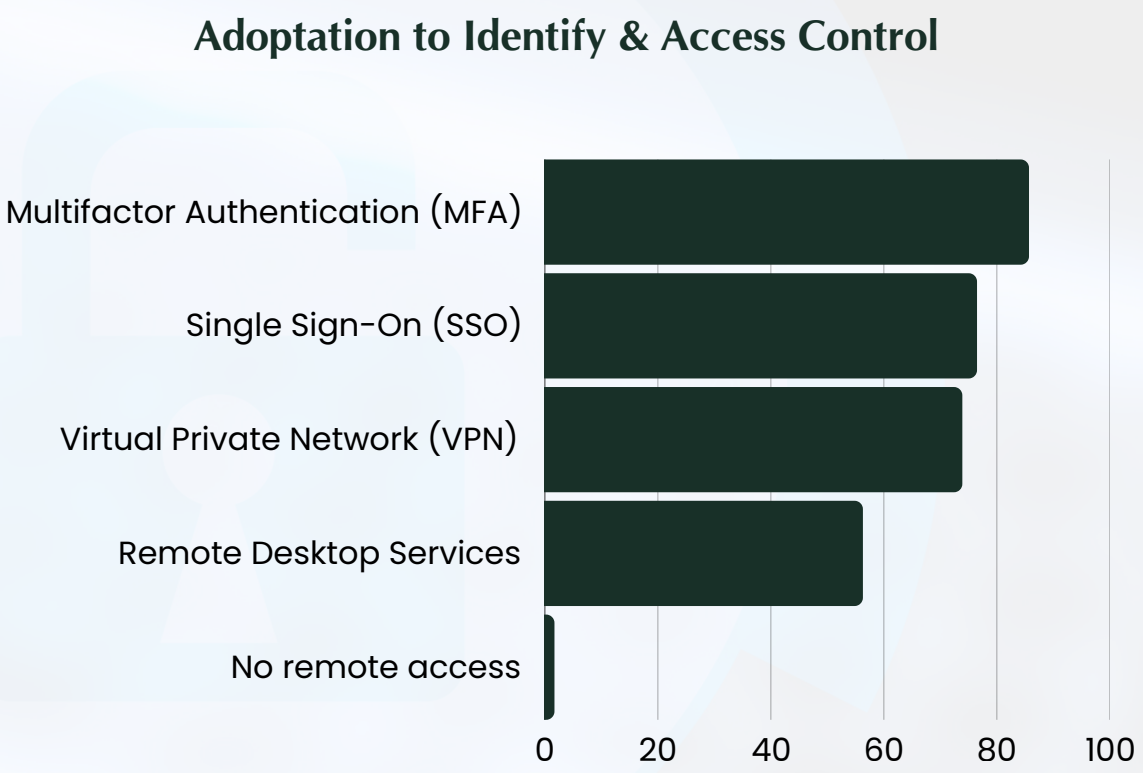


IDENTITY IS THE NEW PERIMETER—AND YOU'RE ALREADY ALIGNED

What the data shows:
A remarkable 85.7% of organizations report using Multifactor Authentication (MFA) to manage access to internal applications. Single Sign-On (SSO) is also widely adopted (76.5%), followed by Virtual Private Network (VPN) access (73.9%) and Remote Desktop Services (56.3%). Only 1.7% say they do not allow remote access at all.

This demonstrates that identity-centric controls are now the norm, not the exception, across a diverse respondent base.

Why it matters:
With identity as the new perimeter, organizations are well-positioned to implement Zero Trust strategies. The high adoption of MFA and SSO means most enterprises have the foundation for continuous verification and adaptive access policies.



THE REAL BRAKES ON AI AND SECURITY: SKILLS, CAPACITY, AND GOVERNANCE

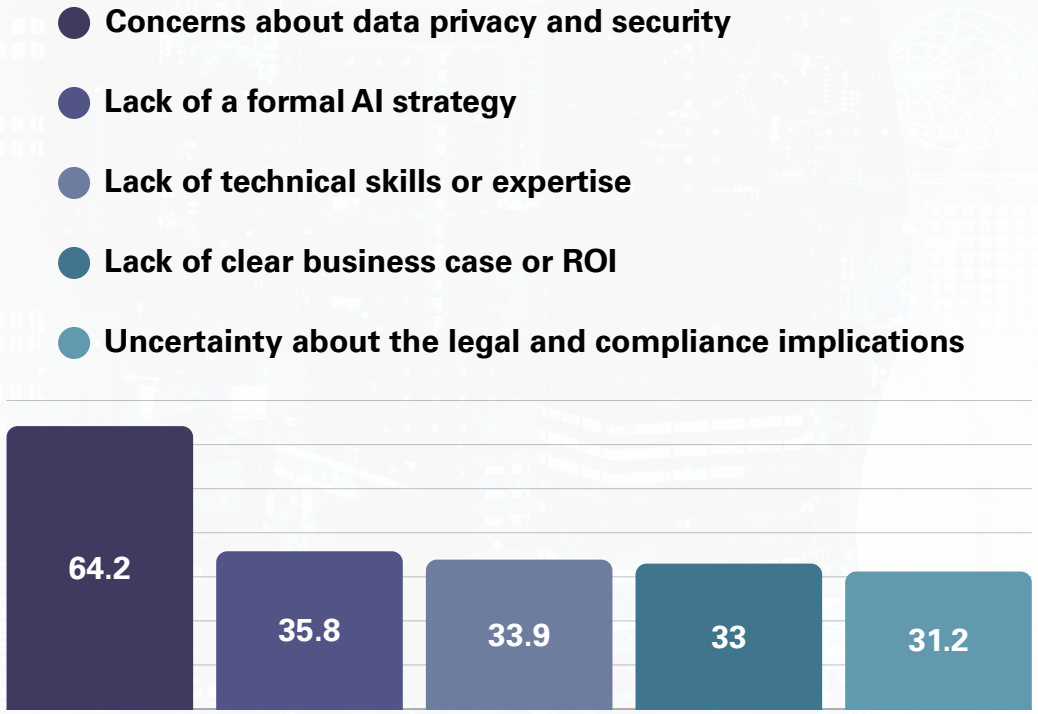
What the data shows:

The top barriers to AI adoption and effective cybersecurity are overwhelmingly about people and process, not technology. “Concerns about data privacy and security” is cited by 64.2% of respondents, “Lack of a formal AI strategy” by 35.8%, and “Lack of technical skills or expertise” by 33.9%. “Lack of clear business case or ROI” (33.0%) and “Uncertainty about the legal and compliance implications” (31.2%) are also significant. These findings are echoed in cybersecurity challenges, where “Limited staff and resources to manage all our security tools” is one of the most frequently selected pain points. Open-text responses reinforce that tool sprawl, integration complexity, and hybrid/multi-cloud environments are stretching teams thin.

Why it matters:

Even with strong tool adoption, both security and innovation could be undermined by operational debt, talent shortages, and unclear governance. Every additional console or manual process increases risk and slows response. These hurdles are systemic, not sector-specific, and reflect the need for governance and enablement as much as technology.

Top AI Barriers to Adoption



CIO Insight

Consolidate overlapping solutions, standardize on integrated platforms, and invest in managed services for 24×7 coverage. Stand up a private AI sandbox (tenant-isolated, logged, content-filtered), fund enablement (prompt design, red team, evaluation harness), and require ROI and control milestones for production promotion. Track improvements in mean time to detect/respond (MTTD/MTTR) and reduction in manual handoffs.

EARLY AI ADOPTION IS REAL—BUT MEASURED

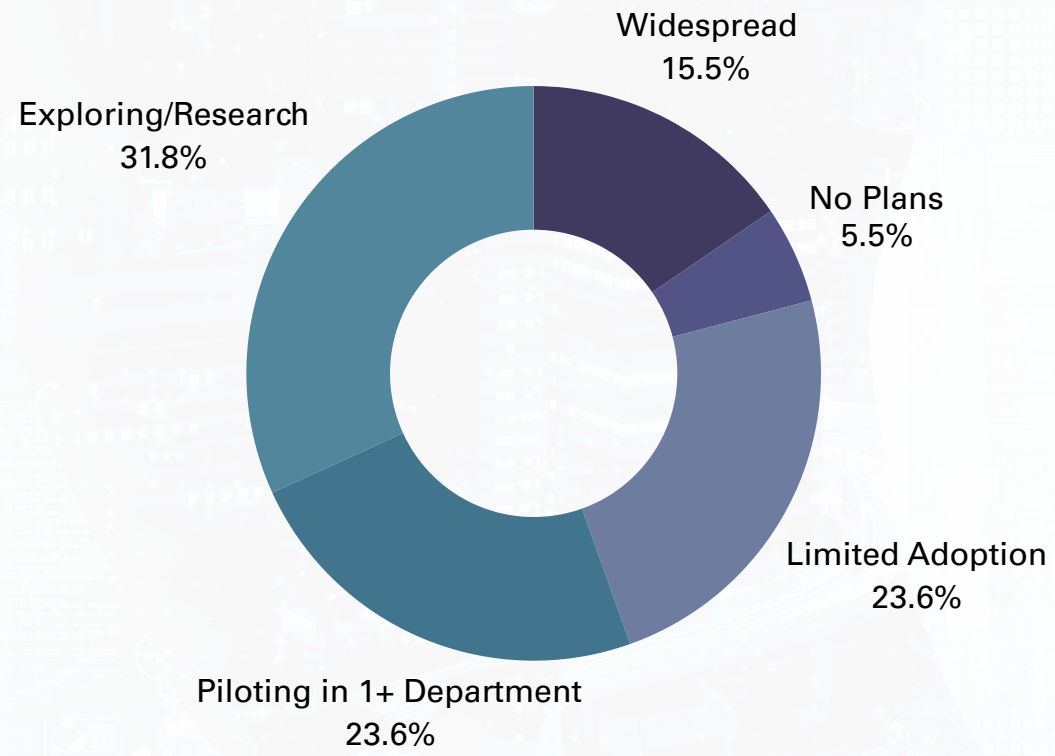
What the data shows:
31.5% of organizations are "Exploring or researching AI tools," 23.4% are "Piloting/testing AI tools in 1+ departments," and 23.4% report "Limited adoption, with a few departments using AI tools." Only 15.3% have "Widespread adoption across multiple departments or the entire organization," and 5.4% have "No plans to adopt AI."

Why it matters:
While the world feels overtaken by AI, the reality is that most organizations are in the very early phase of adoption. As adoption expands, the key is to a pragmatic approach that prioritizes governance and measurable value over speed.

CIO Insight

Create an AI intake & governance board with explicit go/no-go gates (data tiers, auditability, evaluation protocols, ROI thresholds) and treat pilots like products with owners and success criteria.

Current State of AI Adoption



PLATFORM-LED ASSISTANTS LEAD ENTERPRISE AI USAGE

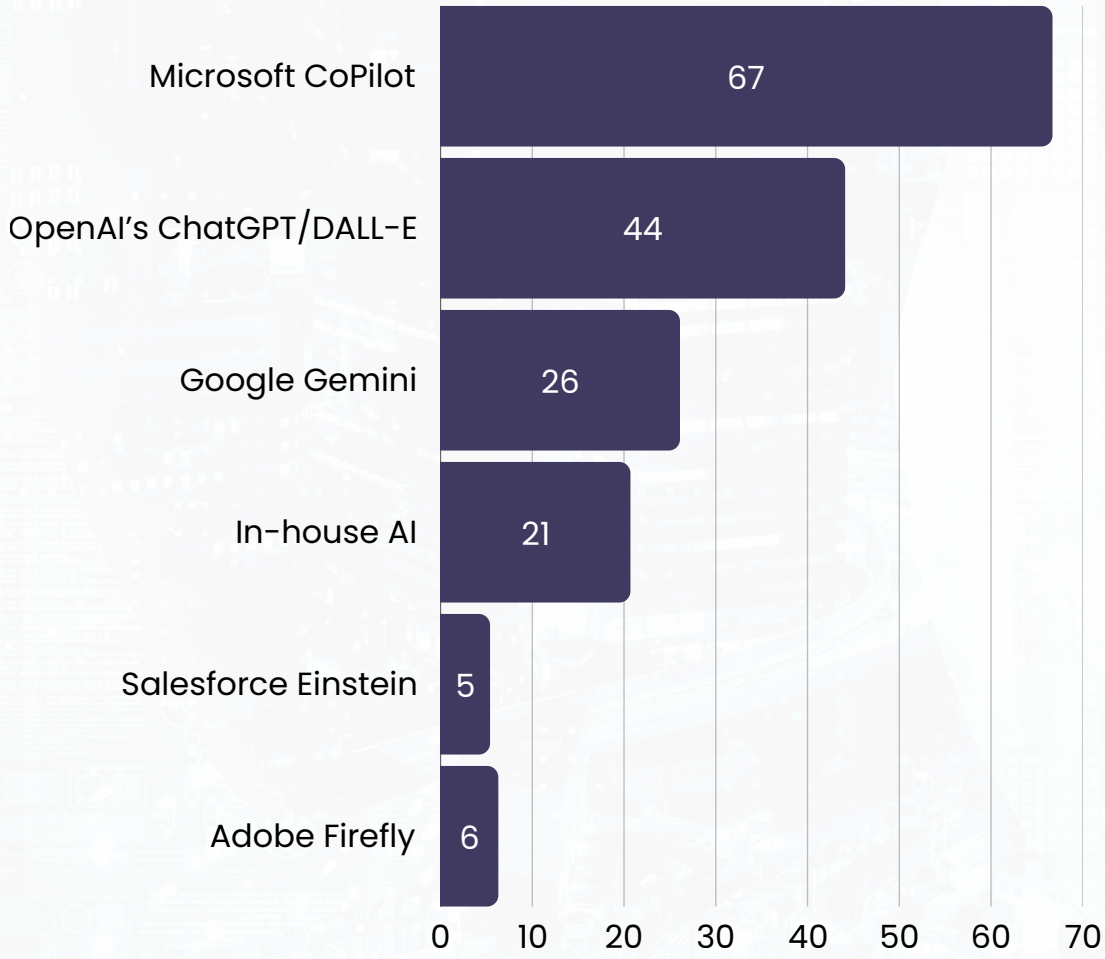
What the data shows:
Microsoft Copilot is the most widely provided AI tool (66.7%), followed by OpenAI's ChatGPT/DALL-E (44.1%), Google Gemini (26.1%), and custom/in-house AI solutions (20.7%). Salesforce Einstein (5.4%) and Adobe Firefly (6.3%) are less common.

Why it matters:
Organizations, in this initial phase of adoption, prefer AI tools that are natively integrated with their productivity and security suites, reducing friction and centralizing governance.

CIO Insight

If you're standardized on Microsoft 365, treat Copilot as the default productivity layer and complement with domain-specific models where they create clear value. Ensure sensitivity labels and access policies flow into assistant contexts and treat pilots like products with owners and success criteria.

Most Widely Provided AI Tools



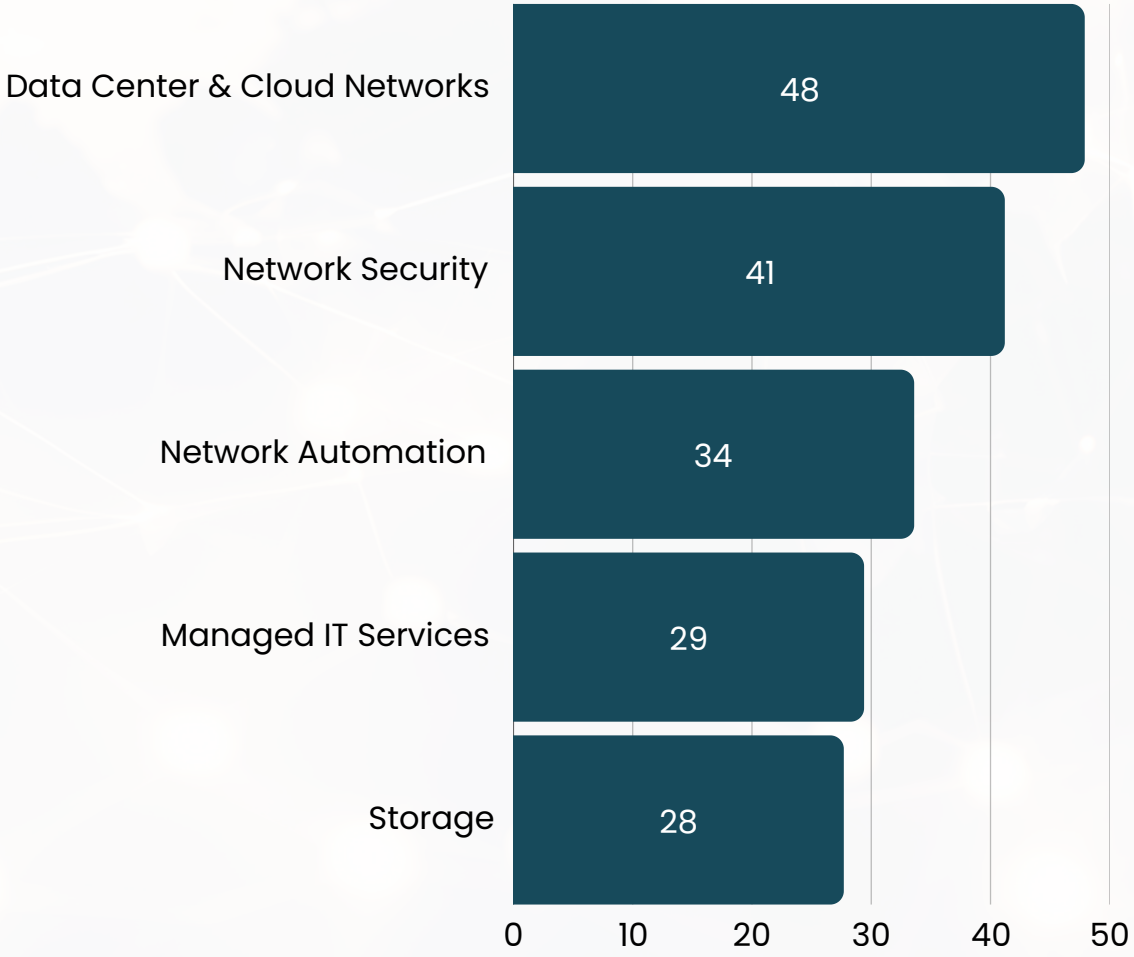
Network, Infrastructure & Operations:

2026 INVESTMENT INTENT: SECURE THE CLOUD AND AUTOMATE THE NETWORK

What the data shows:
The most frequently considered network technologies and services for the next 12 months are Data Center & Cloud Networks (selected by 47.9% of respondents), Network Security (41.2%), and Network Automation (33.6%). Managed IT Services (29.4%) and Storage (27.7%) also rank high. This reflects a clear focus on hybrid architectures, automation, and outcome-based sourcing.

Why it matters:
Automation and cloud-centric investments are now mainstream priorities, not just for scale but for resilience and agility.

Top Network Priorities (Next 12 Months)



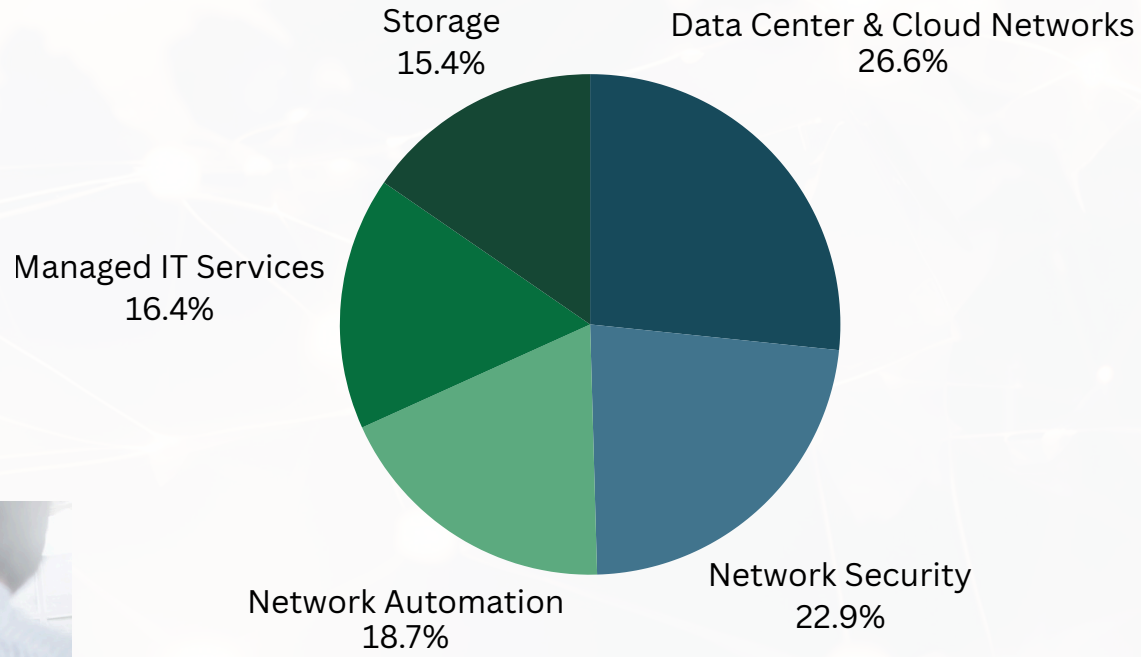
Network, Infrastructure & Operations:

2026 NETWORK PROGRAMS: SD-WAN REFRESH + OBSERVABILITY

What the data shows:
Looking towards the next 12 months, the most considered network technologies that leaders are planning on purchases in: Data Center & Cloud Networks (47.9%), Network Security (41.2%), Network Automation (33.6%), Managed IT Services (29.4%), and Storage (27.7%).

Why it matters:
Modernization efforts are focused on hybrid connectivity, automation, and managed outcomes, with an emphasis on resilience and visibility.

PLANNED NETWORK PURCHASES FOR THE NEXT 12 MONTHS.



Network, Infrastructure & Operations:

CO-SOURCING IS ACCELERATING: MANAGED SERVICES ARE ON THE ROADMAP

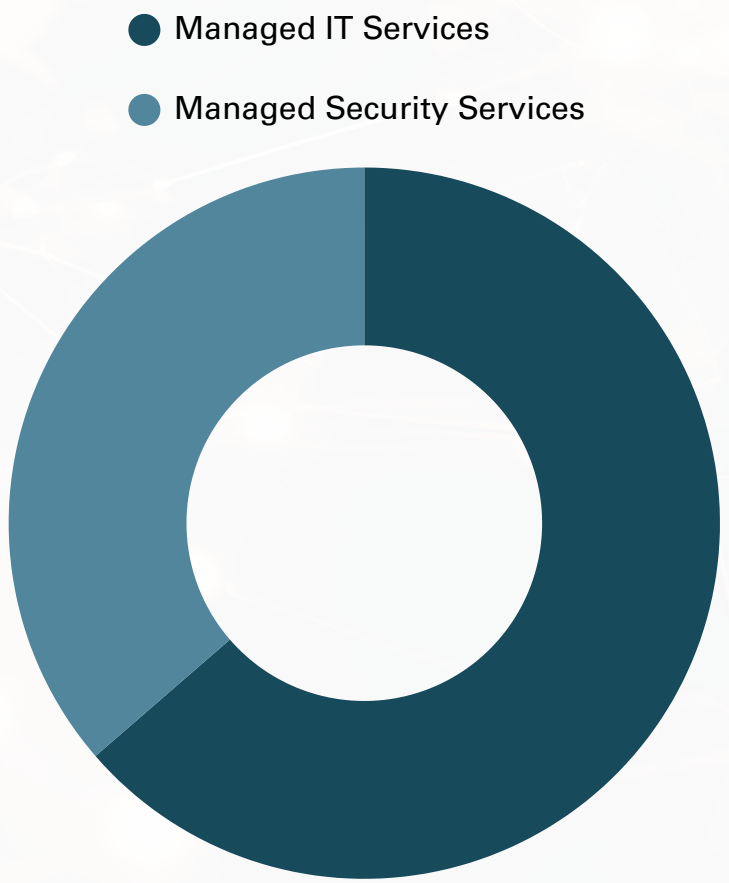
What the data shows:
Managed IT Services are being considered by 29.4% of organizations, and Managed Security Services by 16.8%. This shift from tool acquisition to outcome acquisition is echoed in open-text comments about staff shortages and the need for 24×7 coverage.

Why it matters:
Co-sourcing expands capacity without expanding headcount, which is essential when internal teams face coverage and skills gaps.

CIO Insight

Define outcome-based SLAs (e.g., time-to-contain, patch compliance windows), insist on shared-telemetry access, and align incentives to resilience metrics rather than ticket volumes.

Managed Services Adoption



About Burwood Group

For over 25 years, Burwood Group has established itself as a distinguished IT consulting and integration firm. With an unwavering comm tment to excellence, we have been providing exceptional services to our clients. Our core focus centers on enabling businesses to harness the power of technology, revolutionizing their operations, to achieve their business goals.

burwood group, inc.

Contact Us

burwood.com/contact

info@burwood.com 877-BURWOOD @burwoodgroup