



okta



Nonprofits at Work

2026



Contents

Introduction	02
Summary of Key Findings	04
App Adoption Among Nonprofits	07
Securing Identity Before, During, and After Authentication	12
Securing and Governing Digital Experience	18
Securing AI Agents	26
Protecting Non-Human Identities	30
Conclusion	35
Methodology	38





The world of 2026 is swirling with complex social, political, and technological challenges, and communities around the globe are trying their best to keep up.

Nonprofits are ready to help, as always, but many find themselves facing significant financial headwinds: “Nonprofits today are under more pressure than ever to do more with less,” TechSoup [points out](#). 2025 represented a turning point for nonprofits, marked by massive funding cuts and layoffs, increased government scrutiny, and uncertainty on the world stage, while the needs of vulnerable communities intensified. Inflationary pressures continue to drive up both operational costs and donor scrutiny of their contributions’ impact. This challenging environment means organizations must find new ways to dramatically scale their missions’ reach without a corresponding increase in resources.

The transformative potential of artificial intelligence could be the financial force multiplier that nonprofits urgently need. Like other sectors, nonprofits are already viewing AI as a necessary tool for survival and growth. They’re [actively using AI](#)—often embedded in software solutions—to draft fundraising content, automate

back-office functions, derive new insights from their data, and otherwise reduce workloads for stressed teams. The emergence of agentic AI, including autonomous systems that can manage workflows, communicate on behalf of an organization, and execute other complex tasks, is dramatically accelerating this trend, freeing human talent to focus on high-value, high-touch work that directly serves their missions and communities.

Three out of four nonprofits (76%)
lack a formal AI strategy.

— [TechSoup](#)



However, this promising AI-powered future comes bundled with a new and critical dimension of risk. As organizations consider empowering autonomous agents with access to sensitive systems, including data of donors or vulnerable populations they serve, identity security becomes the most important control plane. A compromised AI agent is not merely a workflow interruption: it can disrupt services, erode public trust, and cause irreparable harm to the communities an organization is meant to protect.

This report explores the intersection of these powerful forces, examining how nonprofits are currently navigating the promise and peril of the agentic age, with a core focus on the identity strategies that can help them innovate safely.



Shameek Bose
VP, Global Impact
Okta



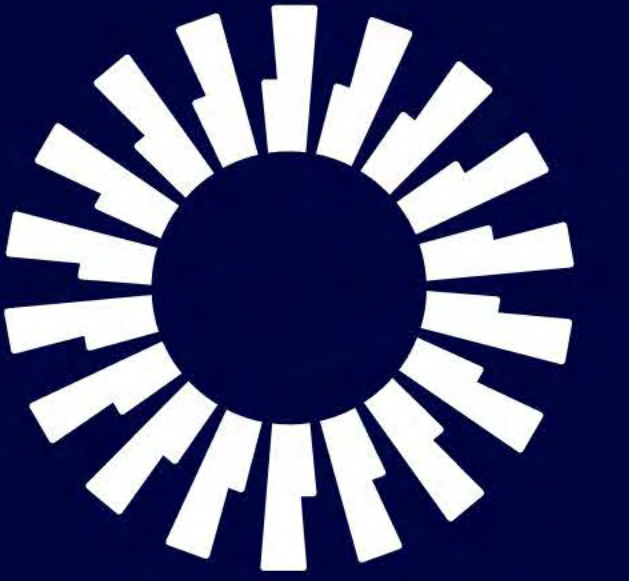
DEFINITIONS

AI Agents

Advanced systems that go beyond traditional chatbots by actively completing tasks based on user-defined goals. An AI agent acts autonomously to achieve specific goals, using reasoning, planning, and tools to complete multi-step tasks without constant human supervision.

Non-Human Identities (NHIs)

A digital identity used by software—like applications, services, or scripts—to automatically access systems and data using credentials like API keys, tokens, and certificates.



Summary of key findings





The rapid rise of enterprise AI solutions, including **agentic AI**, brought new efficiencies to all kinds of functions this past year.



However, safe deployment depends on ironclad identity security, which many nonprofits were still scrambling to achieve. And most sobering of all, fraudsters began targeting nonprofits with broad, large-scale attacks, to the point where the sector has now become the most attacked of all industries. Here's a snapshot of 2025's key trends:

Fraudsters are targeting nonprofits at an astonishingly high rate. Two years ago, the ratio of threats to authentications was 2.6%. Last year it was 18%. This year it was 78%—nearly four out of five attempted authentications to nonprofits were fraudulent, making nonprofits far and away the most-attacked sector.

This year's fastest-growing apps focused on business basics, not security. When we look at all industries, 50% are security-focused. Not so for nonprofits: This year, just like last year, the ten fastest-growing apps are mainly focused on collaboration and business services, with just one security app among them.

High-assurance, phishing-resistant authentication is growing fast. Continuing a trend of the last few years, nonprofits have been busily upgrading their low-assurance authentication factors for higher-assurance ones like Okta FastPass. Two years ago, just 28% of nonprofits were using higher-assurance factors; today it's nearly half.

Nonprofits are leveraging AI to reduce human workloads. Around the world, agentic AI is helping nonprofits perform repetitive tasks and analyze large datasets. Today, adoption is slower among nonprofits than other sectors, and the AI they're adopting is often a built-in function of third-party software solutions rather than a standalone strategic investment, for now.

But there are significant concerns about governing AI activity. When considering the challenges of AI, 46% of nonprofit leaders cite governance and oversight as their top concern—a number that rises to 57% when considering agentic AI in particular. The sector wants the efficiencies that AI promises, but is leery of agentic AI's potential to do harm.



“For years, the sheer volume of information nonprofits manage has outpaced their ability to process it. AI agents have the potential to bridge that gap, enabling even the smallest teams to transform their raw impact data into real-time strategy. But this added capacity doesn't come without risk,

and it's critical that organizations develop AI policies that help to ensure the data that they have been entrusted with remains protected.”

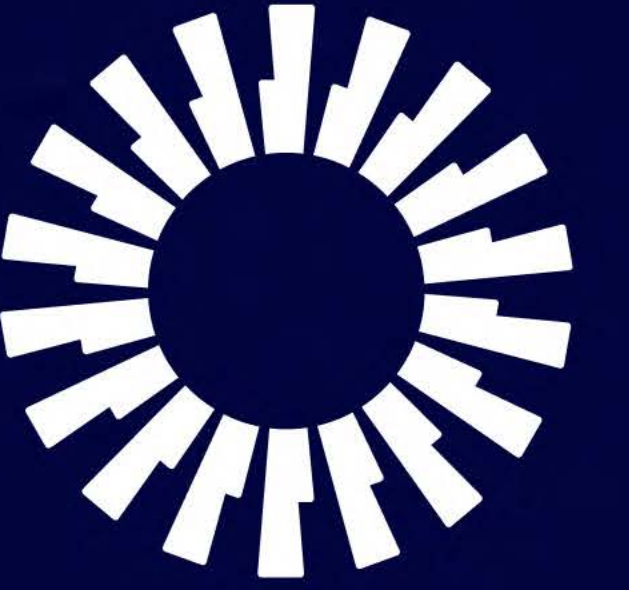


Wojciech Rusteki

Vice President, Digital Solutions and Services

TechSoup



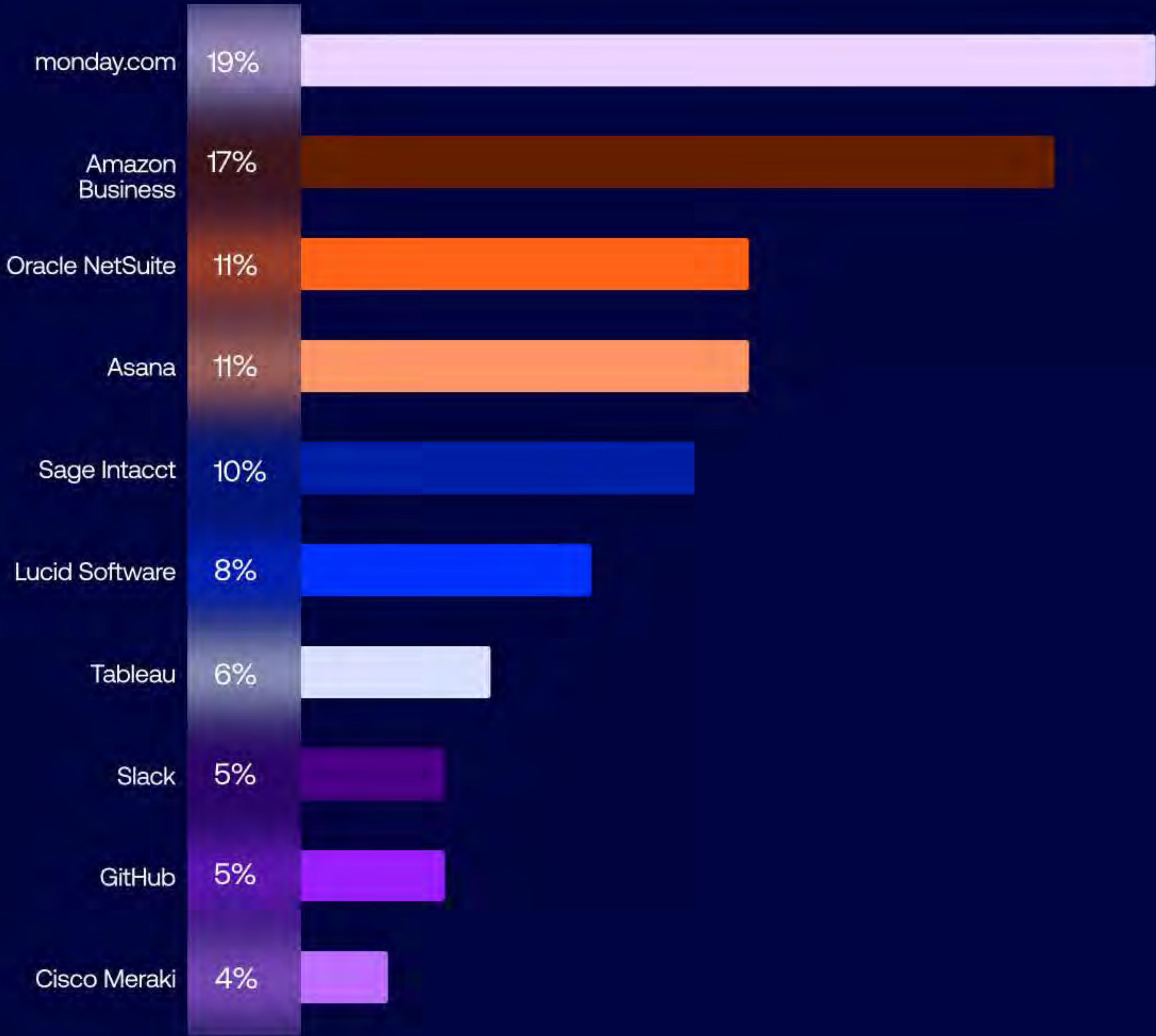


App adoption among nonprofits





Fastest-growing apps, by number of customers



For nonprofits, technology is not merely a tool for productivity; it’s also a powerful engine for effective and efficient mission delivery. Getting the right apps and platforms in place helps companies squeeze the most value out of every donation and grant, making it particularly critical to get the mix right during times of budgetary stress or insecurity. The average nonprofit in the Okta Integration Network (OIN) today deploys 40 apps, though usage is much higher for larger nonprofits, which have steadily risen from 102 apps per customer in 2022 to 139 today.

The emergence of autonomous agents that can analyze data, manage workflows, and engage with constituents has further raised the stakes. An Okta survey of 61 nonprofit leaders in December 2025 showed that current AI investment and planning by nonprofit organizations (not including unsanctioned use of risky shadow AI) is focused on SaaS applications with built-in AI functionalities (87%) and Large Language Models (LLMs, 77%). More than three out of five report also planning to invest in NHIs (62%) and SaaS applications or platforms with built-in autonomous agents (61%).

This powerful technology offers a potential force multiplier for impact, but it also magnifies existing challenges around budget, expertise, and security, particularly for nonprofits that are in earlier stages of their identity maturity journey. This section explores how nonprofits are modifying their solution sets to tackle the persistent barriers they face.

Year-over-Year Growth



Nonprofits set their sights on efficiency with collaboration and finance apps

The applications experiencing the fastest growth in the nonprofit sector paint a clear picture of organizations focused on operational excellence and productivity. Leading the charge is collaborative project management platform monday.com, sporting an impressive 19% YoY increase in adoption. Amazon Business, a platform dedicated to streamlining procurement and purchasing, follows close behind with 17% YoY growth. Both apps were on last year's fastest-growing apps list as well, and nonprofits' continued investment in them may reflect a more urgent need to be efficient with scarce resources.

These two top business optimization apps aren't outliers: This year, 30% of nonprofits' fastest-growing apps are focused on collaboration (monday.com, Asana, and Slack), and finance and banking apps make up another 20% of this year's list (Oracle NetSuite and Sage Intacct). This suggests that these organizations are dedicating themselves to optimizing fundamental business processes, freeing up time and resources to redirect toward mission-critical activities. This back-to-basics approach is in stark contrast to the focus across all industries, where security makes up fully 50% of the fastest-growing apps. (For nonprofits, just one security app made the list this year: Cisco Meraki, at No. 10.)



Three out of four humanitarian practitioners, in a recent survey across 120 countries, say they use AI daily or weekly for work—yet fewer than one in ten say they work at an organization where AI is widely integrated.

– Humanitarian Leadership Academy 2026



Why aren't AI apps like ChatGPT and Microsoft Copilot showing up in the data? Because while usage of apps like these is widespread among nonprofit team members (and in the wider business world), it's primarily free tools that are being used by individuals, not managed enterprise accounts, effectively creating "Shadow AI". These GenAI tools are not behind SSO, and are often not accessed in a logged-in or business account state. "So far we see mostly individual use cases, where members of staff utilize generative AI tools to support and automate their individual workflows," says Daniela Weber, Director of the NetHope Center for the Digital Nonprofit.

"Organizations must take a much more strategic approach to AI, identifying transformative use cases that can generate benefits at scale, and ensuring they put the appropriate governance and security frameworks in place so they use AI safely and responsibly." And the risks if they don't? SSO and MFA can't be enforced, meaning sensitive data is more at risk to attackers. If something goes wrong, there's no way of knowing which AI tool accessed what and when, and no way to shut it down. This becomes even more critical as agentic tools are adopted.

"Organizations must take a much more strategic approach to AI, identifying transformative use cases that can generate benefits at scale, and ensuring they put the appropriate governance and security frameworks in place so they use AI safely and responsibly."



Daniele Weber

Director

NetHope Center for the Digital Nonprofit



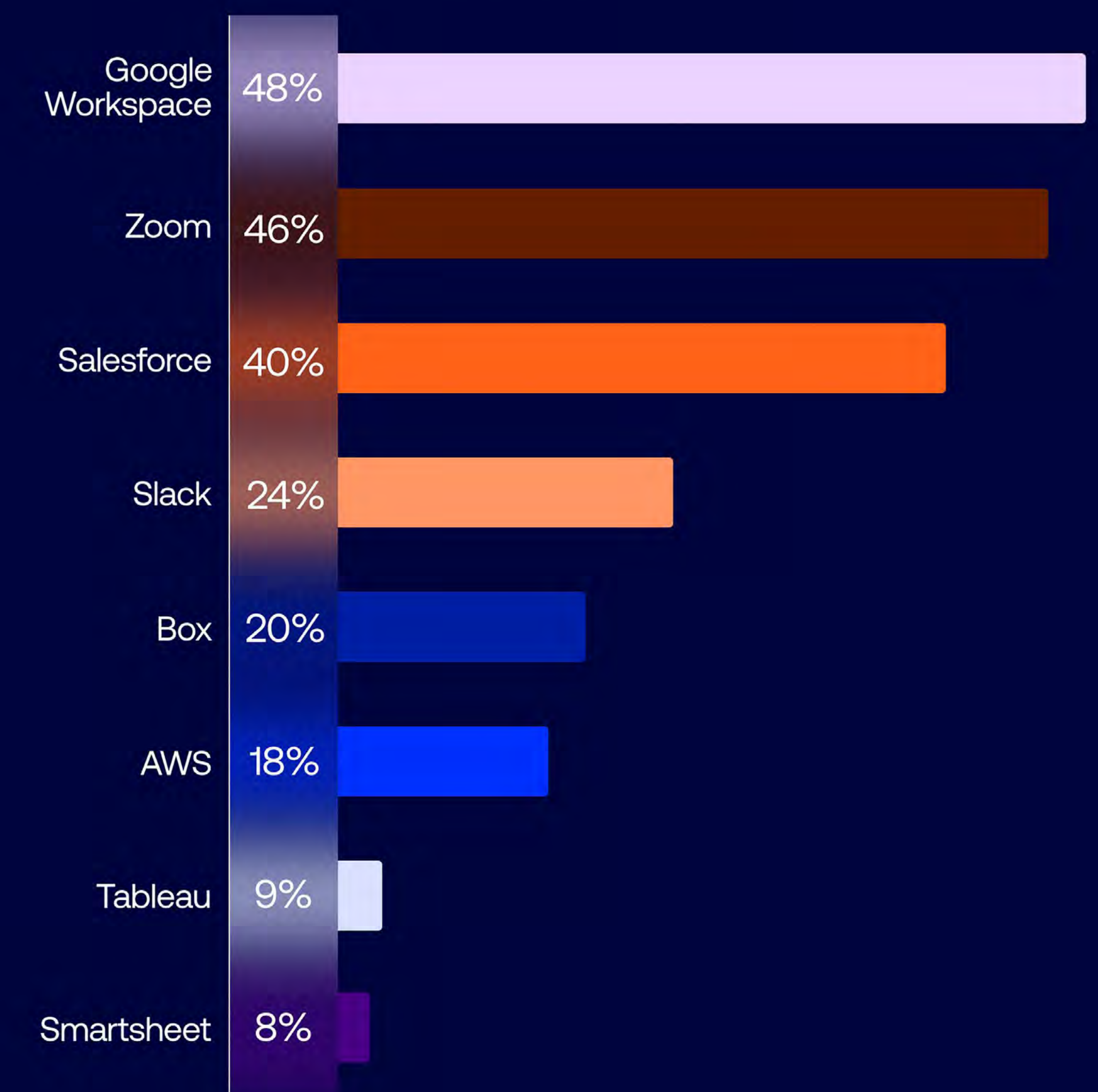
Supplementing the suite with best-of-breed tools

Is the era of relying on a single, monolithic software suite over? Microsoft 365 still serves as a foundational productivity platform for many, but nonprofits, like their counterparts in other sectors, are embracing a more flexible, powerful best-of-breed strategy to supplement their suites. Nearly half of nonprofits that use Microsoft 365 also use Google Workspace, for example (48%, up from 43% last year).

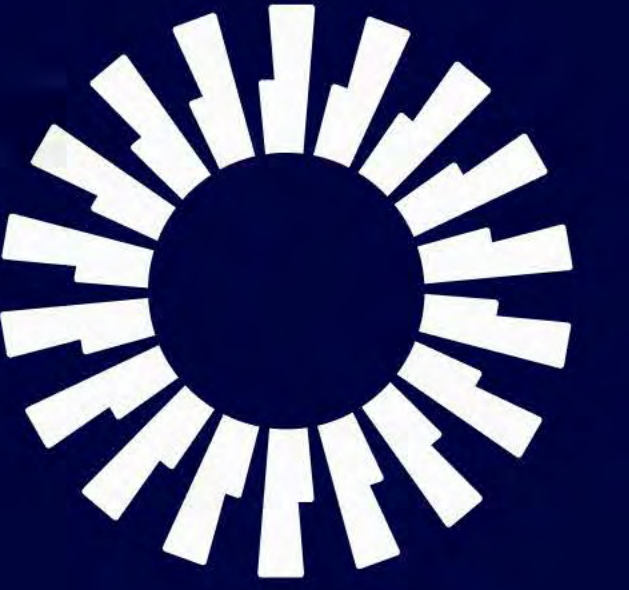
This is not redundant spending: it's a deliberate choice to leverage the unique collaborative strengths of Google's tools for specific teams or projects, as companies increasingly recognize that the best solution for one task may not come from the same vendor as another. This best-of-breed approach extends to other critical business functions as well. Zoom and Salesforce were also adopted by 40% or more of Okta's Microsoft 365 customers, highlighting the tremendous value nonprofits place on managing donor, volunteer, and community relationships with specialized best-in-class tools.

This trend is reflective of a broader enterprise shift away from single-vendor lock-in, which makes more sense than ever: Now that AI agents are being created and connected everywhere, companies will want to preserve the ability to upgrade their AI agent-building platforms, and other emerging tech solutions, whenever it makes strategic sense to do so. The [Flexera 2025 State of the Cloud Report](#) noted that the vast majority of organizations now operate with a multi-cloud, multi-vendor strategy, seeking to optimize costs and functionality while avoiding dependencies. For nonprofits, this strategy is crucial. It allows them to assemble an efficient digital toolkit tailored to their specific needs, so they can maximize the impact of every dollar spent while ensuring their teams are equipped with the best tools to advance their missions.

Okta's Microsoft 365 nonprofit customers with best-of-breed apps



Percentage of Okta's Microsoft 365 Customers with App



Securing identity before, during, and after authentication





Fully 69% of survey respondents now call identity and access management **important to the successful adoption of AI.**

The advent of agentic AI marks a pivotal moment for organizations of all kinds, and nonprofits are no exception.

As philanthropic organizations explore how to leverage the power of AI to amplify their missions, they must also come to terms with the expanded threat landscape it represents. Standing up virtual armies of AI agents that can act autonomously on behalf of human users (or other agents) gives agentic workflows the power to scale. But it also transforms the traditional security paradigm, especially since AI is also helping attackers perfect their phishing and scale their attacks. A single compromised, over-entitled identity can now become a launchpad for a wide range of automated attacks, making strong identity and access management (IAM) more critical than ever.

In Okta's recent survey of nonprofit leaders, it was clear that this danger is top of mind. Fully 69% of survey respondents now call IAM important to the successful adoption of AI. This section explores the growing challenge for nonprofits: to shore up foundational security and close any identity management gaps, while simultaneously adopting the advanced, continuous identity verification models required to safely manage AI agents and proactively mitigate rising threats.





Nearly half of nonprofits now use high-assurance factors

When contemplating a new explosion of identities, the first line of defense is strong authentication you can safely scale. The [2025 NetHope State of Humanitarian Cybersecurity Report](#) notes that “Credential-based attacks—particularly phishing—have surged, affecting 94% of organizations.” Shifting away from low-assurance multifactor authentication (MFA) methods like SMS and email has long been a key security goal for nonprofits, and our data shows that they have made commendable progress on this front. The share of nonprofits that use high-assurance factors like Okta FastPass, FIDO2-based security keys, or biometrics has surged from 28% just two years ago to 45% today. This significant and necessary step forward demonstrates a clear commitment to hardening defenses against common credential-based attacks that exploit weaker authentication factors.

Definitions of factor groupings

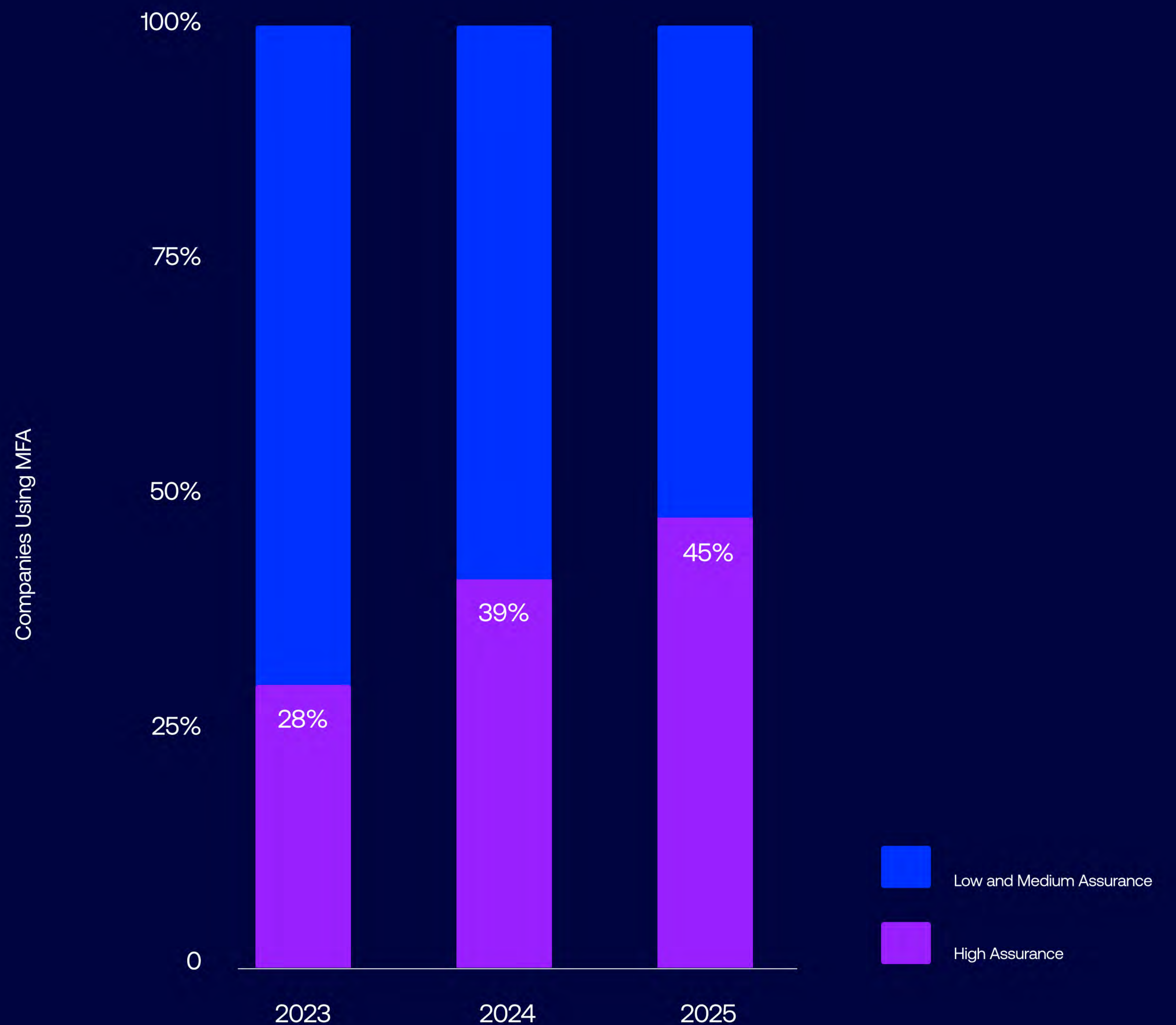
Factor grouping	Factors included	Assurance level	Phishing-resistant
Okta FastPass	Okta FastPass (with and without Biometrics)	High	Yes
Security Key or Biometrics	WebAuthn (FIDO2), YubiKey (FIDO2), Touch ID	High	Yes
Okta Verify (OTP and Push)	Okta Verify (OTP and Push) includes Okta Verify with One-Time Passcodes and Okta Verify with Push Notifications	Medium	No
Other OTP	Duo Security, Google Authenticator, HOTP, RSA SecurID, Symantec VIP, YubiKey OTP	Medium	No
Email	Email	Low	No
Security Question	Security Question	Low	No
Phone (Voice Call/SMS)	SMS or Voice Call	Low	No



However, this 45% adoption rate of high-assurance factors for nonprofits lags significantly behind the 58% adoption rate for all industries combined, and leaves more than half of nonprofits without this baseline level of protection. AI is helping attackers as well, turbocharging existing threat vectors like phishing and spearphishing, and enabling criminal organizations to reach a dizzying scale and improve the accuracy of their fraud strategies. As nonprofits prepare for an agentic AI future, closing this gap and standardizing on phishing-resistant, high-assurance factors is not just a best practice, anymore—it is a foundational prerequisite for security and resilience that mission-based organizations can rely on.

The share of nonprofits that use high-assurance factors like Okta FastPass, FIDO2-based security keys, or biometrics has surged 21% YoY, but the threats are growing faster.

MFA factors by assurance level

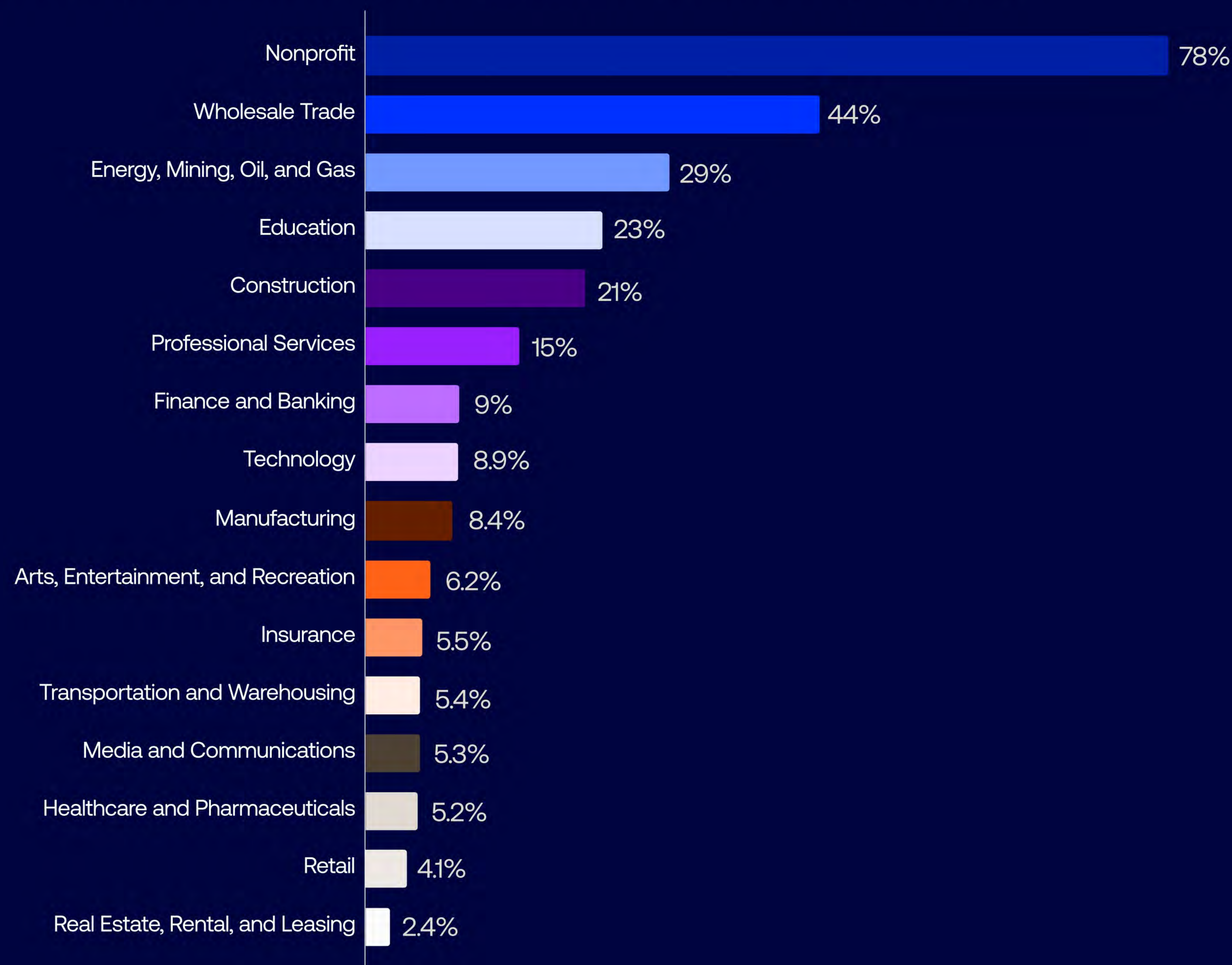




Nonprofits soar past energy in the ratio of detected threats to authentications

This year's data reveals a grave reality: Nonprofits are now the most-attacked industry in our dataset. The threats-to-authentication ratio (the percentage of detected threats per every 100 authentications) has skyrocketed to 78% for the nonprofit sector. To put this in perspective, just last year this figure stood at 18% for nonprofits, with the most-attacked industry (energy, mining, oil & gas) at 32%. This exponential rise in threat activity against nonprofits may mean that attackers now, more than ever, see the sector as a target-rich and potentially less-defended environment. Before nonprofits can fully unleash the power of AI agents, they must first secure the identities those agents will be tied to.

Ratio of detected threats versus authentications, by industry



Ratio of Detected Threats to Authentications

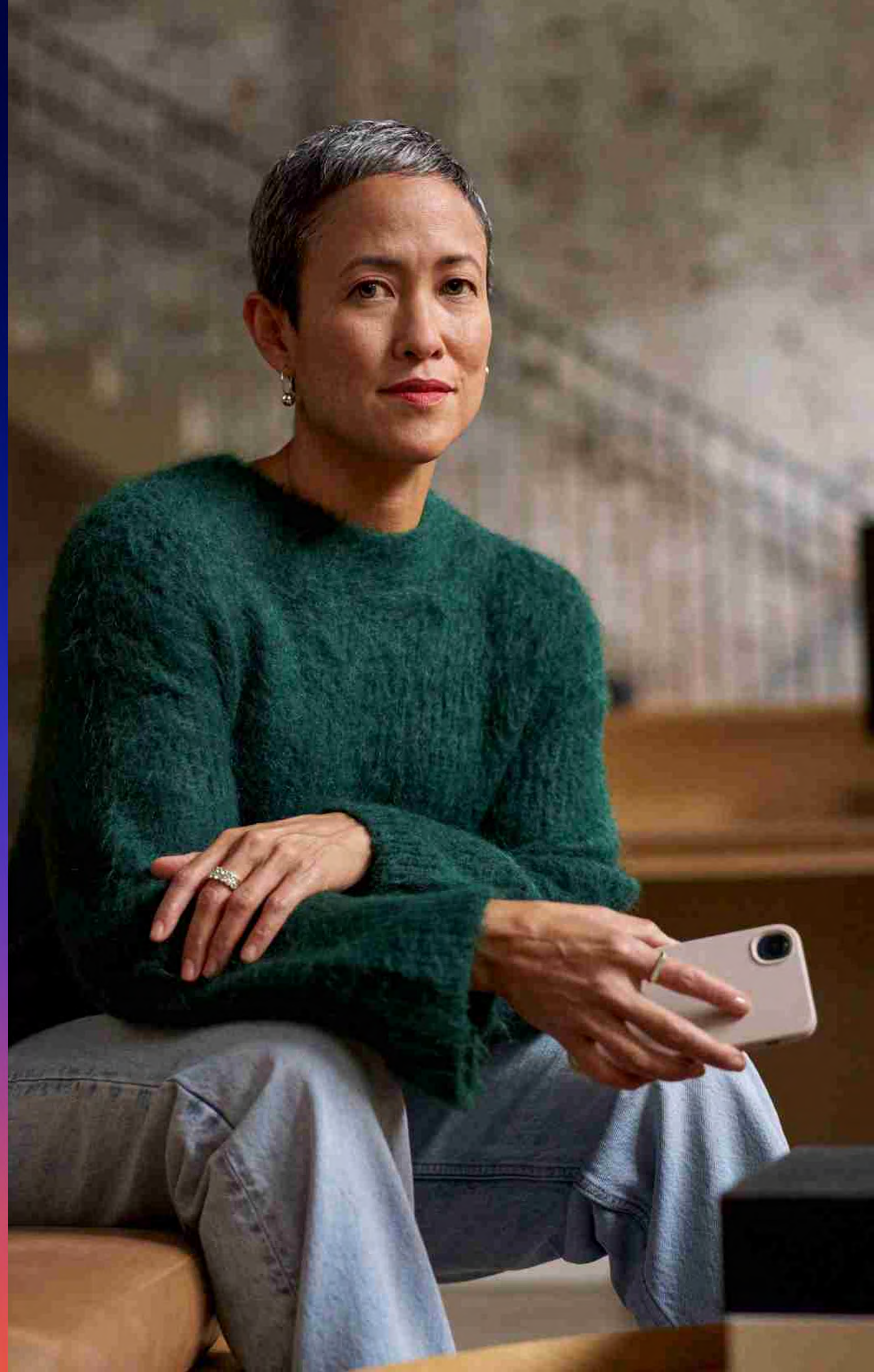
Based on 1 year of cumulative data
Percentages over 10% have been rounded

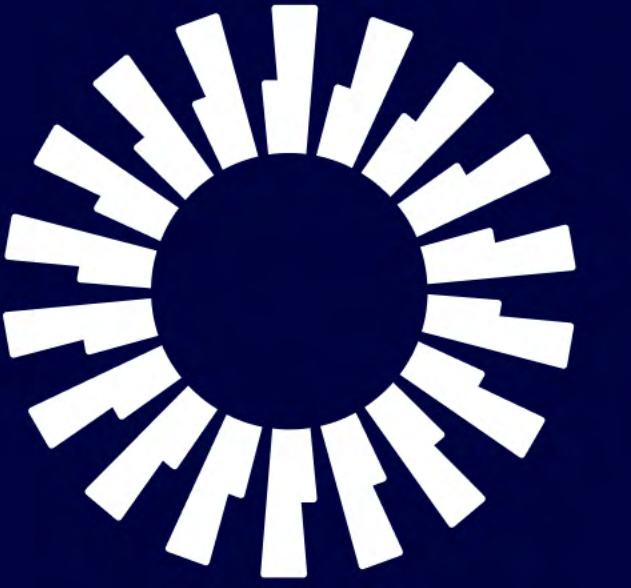


Still, even in the face of this onslaught, nonprofits are addressing this critical security risk, and the sector is aggressively adopting and prioritizing essential identity technologies. In this year's nonprofit data, we see a staggering 98% year-over-year growth in the total number of FastPass passwordless authentications, outpacing the 81% growth across all industries. Nonprofits' shift toward enhanced biometric protection is even more pronounced, with 142% YoY growth (compared to 84% for all industries) and in the use of adaptive MFA (AMFA, up 524% over the past two years). AMFA is particularly important for securing AI deployment, as it represents the critical "during and after" security layer that enables continuous, risk-based authentication, allowing companies to assess the posture of each user or non-human identity long after initial login.

Nonprofits' impressively high adoption rate of both passwordless and adaptive MFA provides a powerful counterpunch to the rising tide of attacks currently targeting nonprofits preferentially. It shows that leaders in this sector are thinking ahead: proactively hardening security by building stronger front doors, and weaving a flexible identity fabric that can continuously verify every identity at scale. Strengthening these foundational security features will help close today's authentication gaps, supporting the dynamic AI agents and other non-human identities (NHIs) just beginning to enter the story.

This year's data reveals a grave reality:
**Nonprofits are now the most-
attacked industry in our dataset.**





Securing and governing digital experience





AI holds significant promise as a force multiplier for nonprofits. Empowering AI agents to act on their behalf could help mission-driven organizations automate complex tasks and scale their impact without a linear increase in resources.

However, this scaling potential comes bundled with a commensurate rise in risk, as well as the burden of managing a more complex digital ecosystem with an ever-expanding attack surface. AI agent creation is unusually democratic: anyone in your organization, theoretically, can spin them up and connect them to existing tools, apps, and data. This puts added pressure on IT and security teams to simultaneously roll out AI quickly and put appropriate guardrails in place.

Alarming, our nonprofit AI survey found that 58% of nonprofits have no restrictions in place for the use of AI tools—this aligns with IBM’s 2025 Cost of a Data Breach Report, which found that 63% of organizations lack AI governance policies. And even when organizations do have an AI policy, it doesn’t always specify tools that have been approved for use—many only provide general advice on things like what such tools should or should not be used for, or what types of information not to put into the prompt.





The survey also showed that about two in five nonprofits have at least general guidelines or training, but that's not enough to counter the risks of AI; effective security in the age of agentic AI requires both securing access and governing the actions that follow. (A good start for organizations looking to spin up an AI usage policy can be found [here](#).) At the moment, the nonprofits sector is making good progress adopting the foundational tools of modern identity management, like password managers (up 17% YoY) and infrastructure monitoring (up 12% YoY). But implementing lifecycle management automation and workflows remains an important opportunity to drive greater automation, productivity, and cost savings, without rushing to adopt AI before its use can be managed and governed at scale.

Here's a closer look at nonprofits' current security concerns and the tools they're adopting to address them.





Security is a primary consideration of AI adoption (including agentic AI), cited by nearly half of all nonprofit leaders as one of their top three issues. That concern is well-founded: 97% of organizations without proper AI access controls reported AI-related security incidents. For specifics on the governance coverage gaps particular to nonprofits, see NetHope's AI Governance and the Nonprofit Sector: Mapping the Missing Middle, a report that describes what a mature sector-wide nonprofit AI governance layer requires: shared principles and norms, regulatory translation, operational tooling, evidence and learning, community and coordination, and sector voice in global governance.

For **general AI adoption**, top concerns most often cited by nonprofit leaders are AI governance and oversight (46%), data loss prevention and unsanctioned shadow AI usage (both 33%), and compliance and regulatory requirements (31%).





In our survey, the data around nonprofits' AI-related concerns reveals a clear desire for control and visibility.

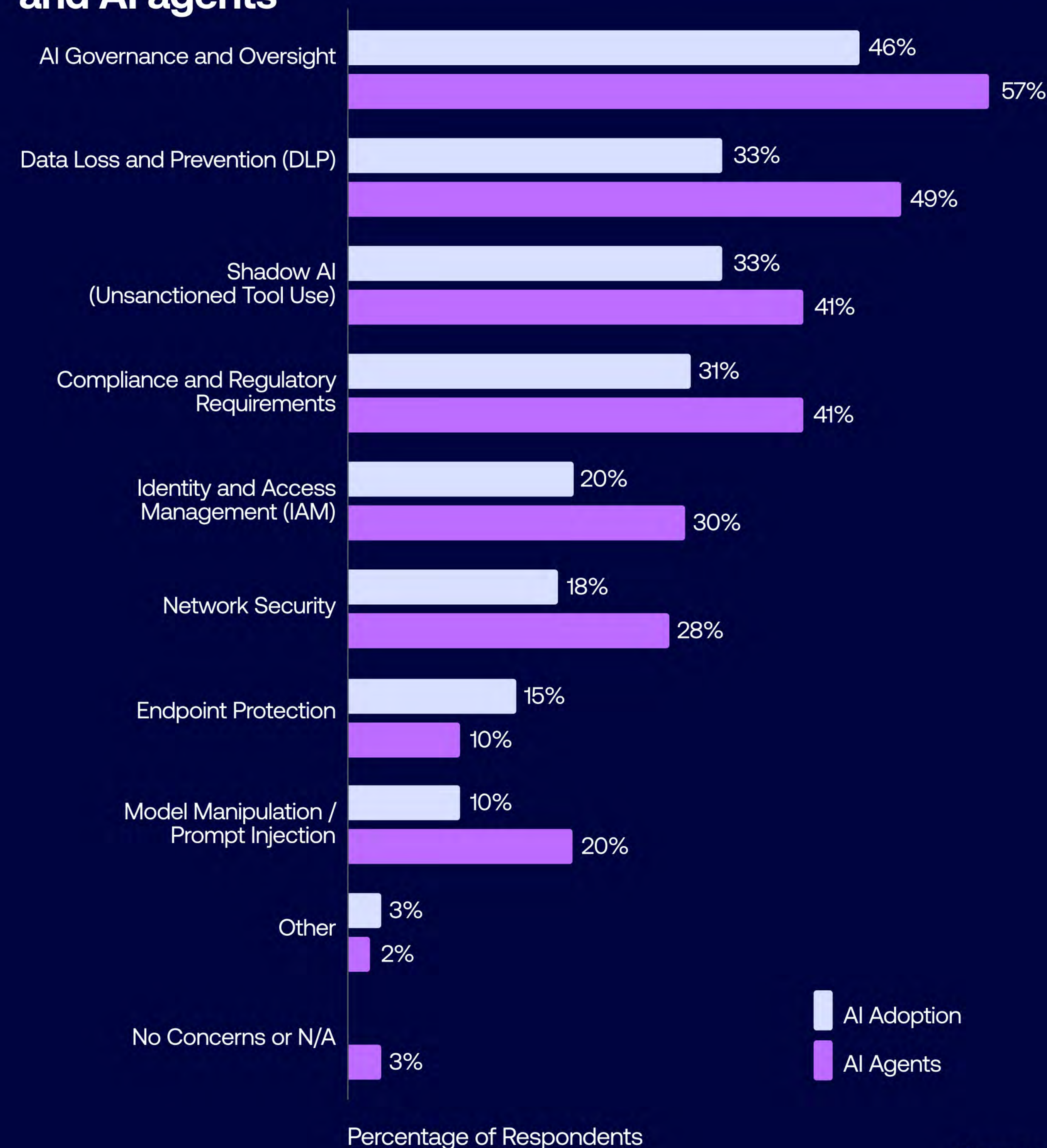
For **general AI adoption**, top concerns most often cited by nonprofit leaders are AI governance and oversight (46%), data loss prevention and unsanctioned shadow AI usage (both 33%), and compliance and regulatory requirements (31%). These reflect a foundational need to understand specifically who is using what AI, with what data, and under what policies, to provide the visibility nonprofits need to adequately govern AI usage.

For **AI agents**, the same four concerns dominate the list, but with an even higher consensus. Nearly three out of five nonprofit leaders (57%) say they consider AI governance and oversight a pressing security concern; other top concerns include data loss prevention (49%), unsanctioned shadow AI usage (41%), and compliance and regulatory requirements (41%).

Nonprofits are right to be more concerned about agentic AI: An employee using generative AI to draft an email represents one level of risk, but an AI agent that's authorized to access systems and execute entire workflows or sets of tasks instantly is a next-order challenge. And when organizations have not established clear privileged access management policies or provisioned role-based access permissions, this can give AI agents more privilege than they need for the workflows they're designed to administer, adding risk.

Nonprofit leaders recognize that the move to agentic systems will require a deliberate, robust governance framework, such as the AI Trust, Risk, and Security Management (AI TRiSM) framework that [Gartner champions](#) for operationalizing AI management.

Most pressing security concerns related to AI adoption and AI agents



Based on 1 year of cumulative data
Percentages over 10% have been rounded



Password managers: Securing identities while reducing user friction

Nonprofits are continuing to evolve their security stacks in response to an ever-changing threat landscape. Foundational tool adoption remains strong, and staples like security training (at No. 1) and VPN/firewall (at No. 2) lead the pack. But the big story this year is the rapid YoY growth of password managers, up 17% YoY. This may signal a growing recognition that, in an environment of constant phishing and credential-based attacks, tools that work with your identity solution to bolster security while simplifying the user experience are compelling. Password managers aren't the whole solution, however. Other success stories include infrastructure monitoring, which grew 12% YoY, and secure web gateway solutions, which grew 9% YoY. These rankings among nonprofits are similar to those we see across all industries.

The big story this year is the rapid growth of password managers, **up 17% YoY.**



Top 10 security tool categories by number of customers

In ranked order:

1. Training
2. VPN / Firewalls
3. Endpoint Management and Security
4. Password Managers
5. Email Security
6. Secure Web Gateways
7. Data Loss Prevention
8. CDN Providers
9. Infrastructure Monitoring
10. Security Analytics



Lifecycle management: Making progress from a small base

When it comes to preparing for an agentic AI future, nonprofits may be behind the curve, starting with a significant lag in adopting basic identity automation. Consider lifecycle management (LCM)—the automated processes of onboarding, offboarding, and managing user access. Here, nonprofits rank last among all our focus industries (16 out of 16) in the average number of LCM events (i.e., user lifecycle triggers that initiate automated identity processes) per customer. The arts, entertainment, and recreation category tops the list, with more than 5.5M LCM events per customer, compared to fewer than 1M LCM events per customer for nonprofits. However, the gap may be closing: Okta's internal data shows that the nonprofit sector's LCM-using customer base is growing at 5% per year, ranking it No. 9 for YoY growth (insurance is growing the fastest, at just over 10% YoY).

Nonprofits rank last among all our focus industries in the average number of LCM events per customer.

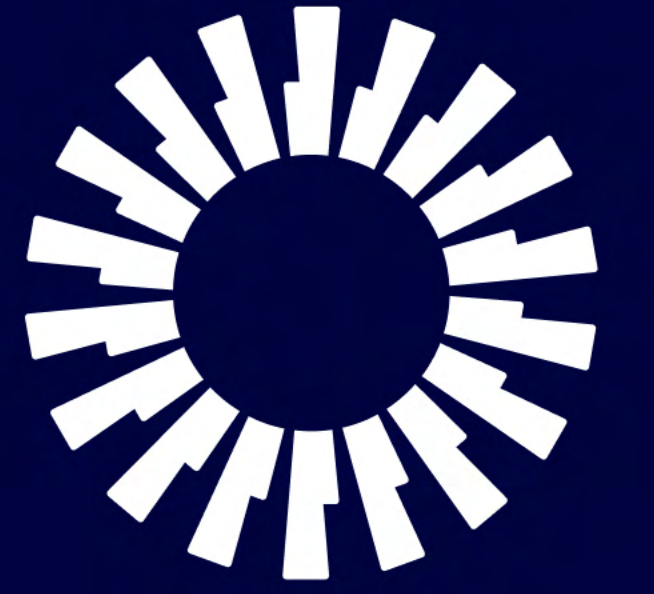




Workflows: An opportunity for automation

As nonprofits catch up on the LCM front and close existing security gaps, they'll be better positioned to safely leverage automation. Adoption of Okta Workflows, for example, is currently very low for the nonprofit sector, with an average of just 28 active flows per company. Technology leads the pack this year (97 workflows per company), followed by transportation (59) and media and communications (57). This data paints a picture of a sector that's still a bit behind on automation, but is making targeted investments in advanced, flexible automation platforms. This strategy can help nonprofits build scalable, event-driven governance engines to securely manage human and machine identities. After all, automation doesn't have to involve cutting-edge AI, and organizations often have access to underutilized automation tools they can leverage before considering more costly AI solutions.





Securing AI agents





Nonprofits often find themselves charged with finding creative ways to **do more with less**, and the promise of AI as a tool for efficiency generally resonates with them.

Our survey found that many nonprofits are already piloting and experimenting with AI agents, with a majority in the early phases of exploration. 13% are actively deploying AI agent solutions, 39% are piloting/experimenting, 16% are exploring/researching, and 23% are considering future AI agent adoption.

These forward-looking investments signal a shift in priorities: Nonprofits are actively exploring their ability to empower AI agents to act on their behalf, to achieve new efficiency and productivity gains to help scale their missions. This section explores how organizations are using agents today and the identity-centric security challenges they must address to unlock agentic AI's full potential.

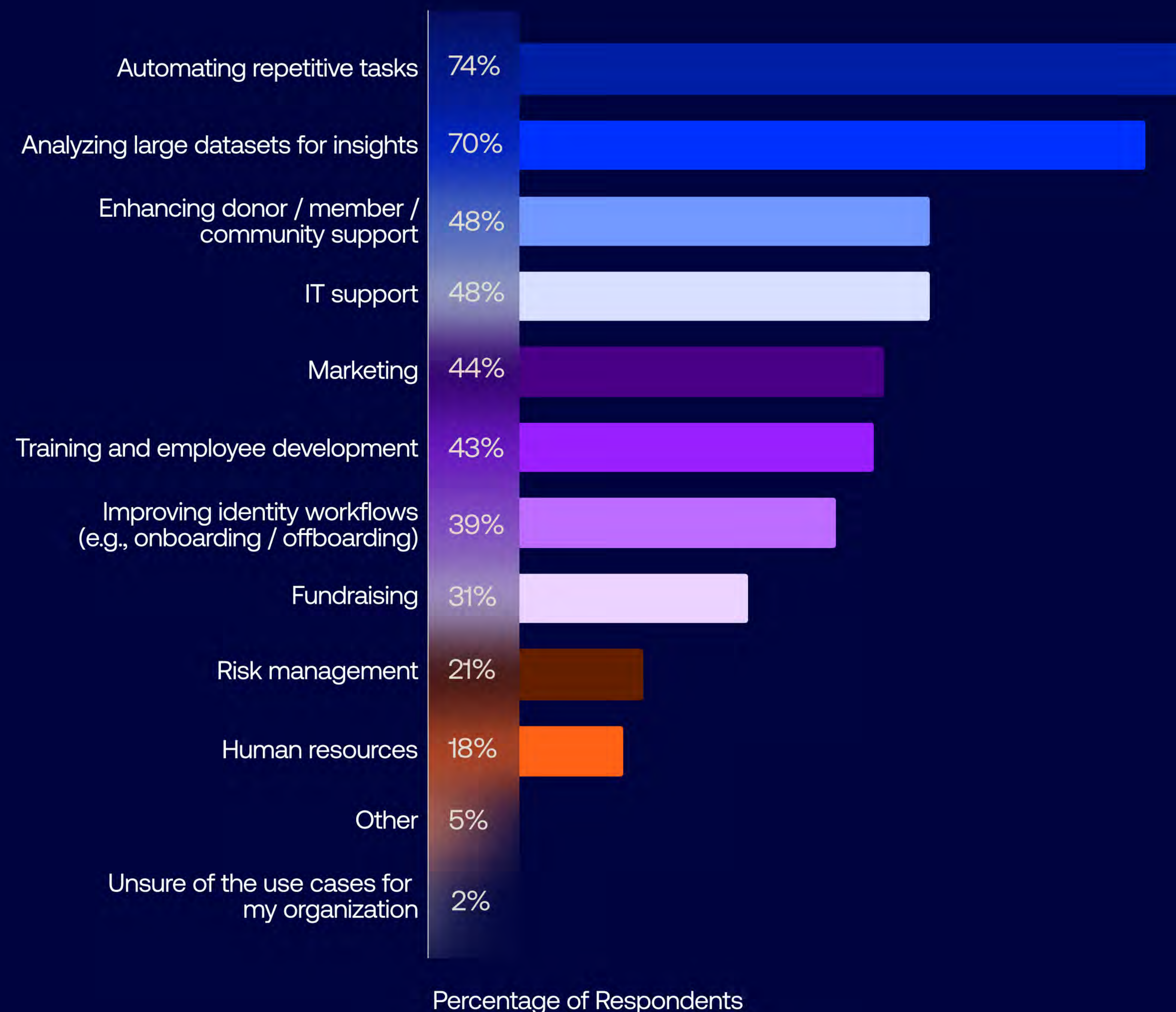




Nonprofits currently use AI agents for repetitive tasks and large datasets

How are nonprofits using AI agents today? Nearly three in four (74%) use them to automate repetitive tasks, similar to data across all industries, where this is also the top result (81%). Nonprofits also use AI agents at a high level (70%) to analyze large datasets for insights—higher than the 42% average across all industries who report this as a primary use case. Another distinctive AI agent use case for nonprofits is training and employee development (43%, vs. 22% for all industries).

Primary use cases for AI agents

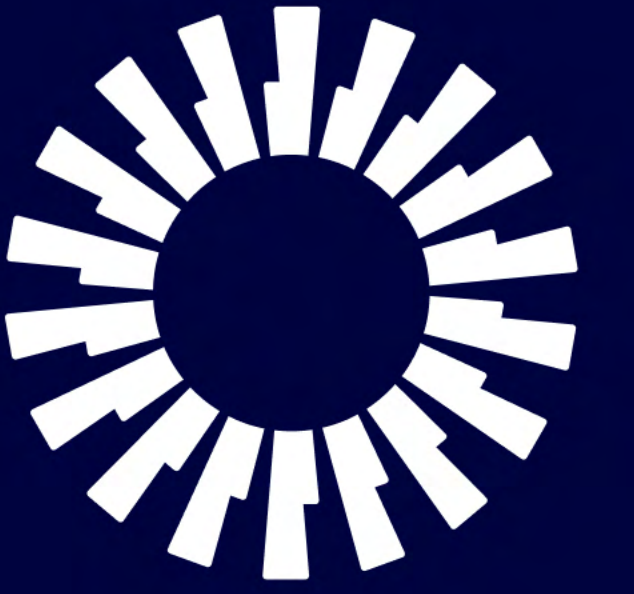




This strategic divergence highlights the unique position of nonprofits, which are often resource-constrained but rich in program, donor, and impact data. They're overindexing relative to peers in other industries on leveraging AI agents to efficiently unlock latent data value, turning their datasets from a management challenge into a source of actionable insights for fundraising, program optimization, and demonstrating impact. They're also leveraging agentic AI at a relatively high rate to help them upskill their workforce and enhance institutional knowledge. "Nonprofits used to be dependent on experienced data analysts—a constrained resource—to create actionable insights," notes Daniela Weber of NetHope. "They can now utilize AI to generate value out of their wealth of data, by automating data processing and analytics tasks, and by enabling easy access for anyone in the organization who needs data insights for decision making."

Agentic AI promises to open new pathways to data-driven strategy and operational efficiency, but adoption is, at the moment, heavily influenced by organizational size. Larger nonprofits (with over 200 employees) are overwhelmingly leading the agentic AI charge, with 80% actively deploying or piloting agents, compared to just 26% of their smaller counterparts. As AI agents shift from merely advantageous to mission-critical, smaller nonprofits must find ways to close this gap. McKinsey's [The State of AI in 2025](#) report shows that organizations with ambitious AI agendas are already seeing tangible benefits, such as efficiency gains, growth, and innovation. Establishing and securing agentic workflows—ensuring each agent has a verified identity and appropriately scoped permissions—is the foundational step to realizing these benefits securely and at scale.

Nonprofits use AI agents at a high level (70%) to analyze large datasets for insights—higher than the 42% average across all industries who report this as a primary use case.



Protecting non-human identities





The rise of agentic AI is accelerating a trend that has been building for years: the explosion of non-human identities. The modern digital ecosystem runs on a vast, often invisible, workforce of NHIs: the digital credentials assigned to applications, the API keys that connect services, the service accounts that run automated backups, and the agents tasked with executing complex workflows. As nonprofits scale their adoption of cloud services and AI, they inevitably inherit a burgeoning population of these machine identities, each representing a potential pathway to sensitive data, and every API key or service account that acts on an organization's behalf is an identity that must be secured, managed, and governed. Our data reveals that nonprofits are navigating the start of their NHI journey and are focused on building a strong foundation to secure all identities.





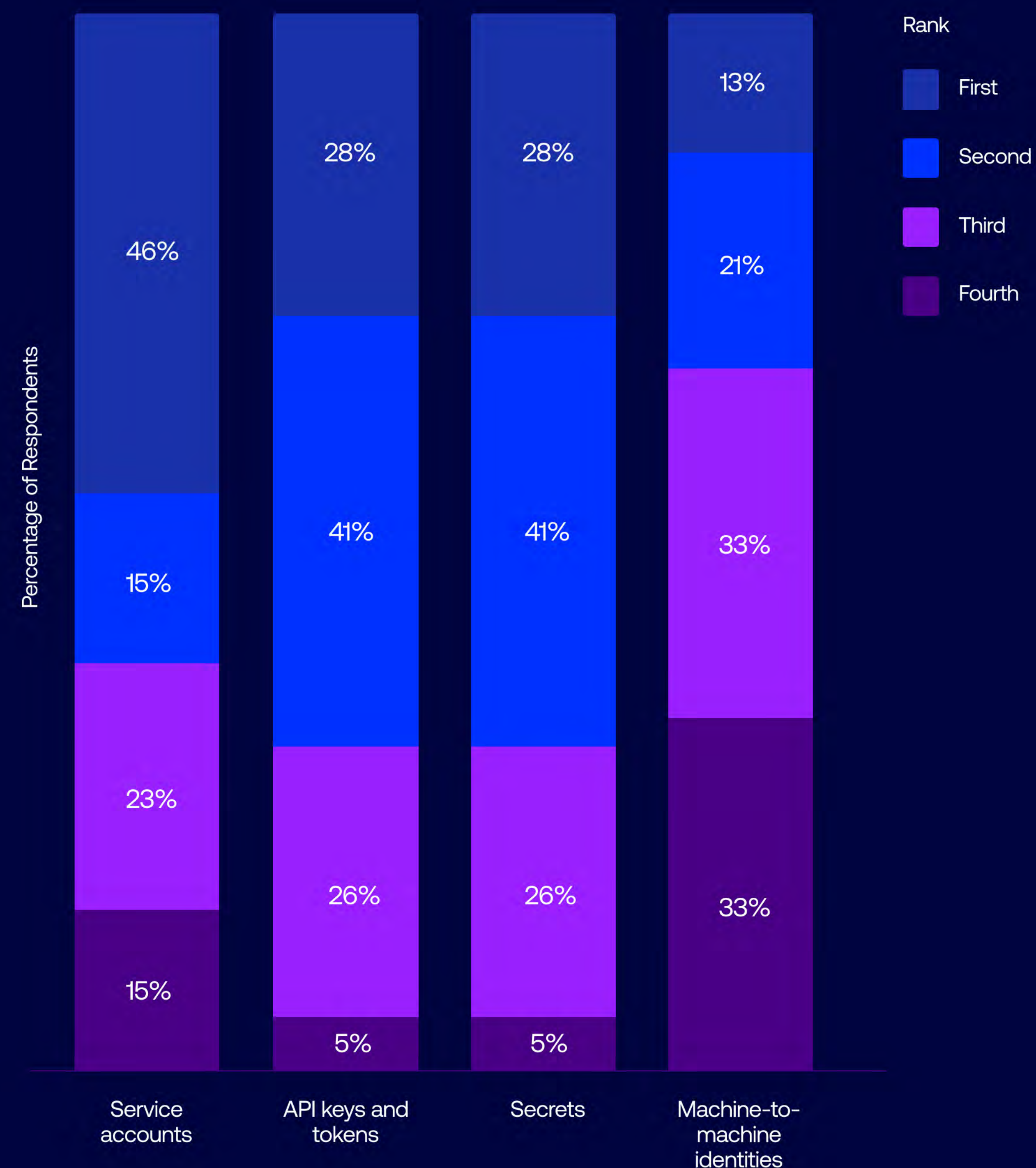
For nonprofits, service accounts top their current NHI usage

Compared with other industries, nonprofits have been much more cautious and deliberate in adopting NHIs: Just 3% of nonprofit leaders report “widespread” use, and another 15% report “moderate” use, compared with 42% and 55% in the broader market. These tentative initial explorations into the world of NHIs reveals a deliberate and pragmatic strategy. Asked to rank the importance of different NHI types, nonprofit leaders place service accounts at the top, with 46% citing them as their most critical need. (API keys and tokens hold the top spot among all industries.) Nonprofits seem to be focused on first securing the identities of core internal systems and legacy applications—often managed via service accounts—before expanding to the more complex, API-driven, interconnected web of modern cloud services.

Service accounts are generally bound by privileged access restrictions associated with the service that they were engineered to manage, unattended by a human. With limited resources, prioritizing service accounts is a logical first step: Before fully leveraging external AI agents via APIs, nonprofits must first secure the privileged accounts that underpin their existing infrastructure.

This approach also strategically prioritizes access risk. “The explosion of AI agents and non-human service accounts is creating an attack surface too large for rules-based security,” [worries](#) Arun Shrestha, CEO and co-founder of BeyondID. “Organizations will need autonomous, AI-native identity defenses that can detect and adapt at machine speed.” For nonprofits, whose service accounts may hold the keys to sensitive donor and constituent data, the proper governance of these identities is not just a pragmatic first step—it is a mission-critical security imperative.

Most important types of NHIs in current use for nonprofits



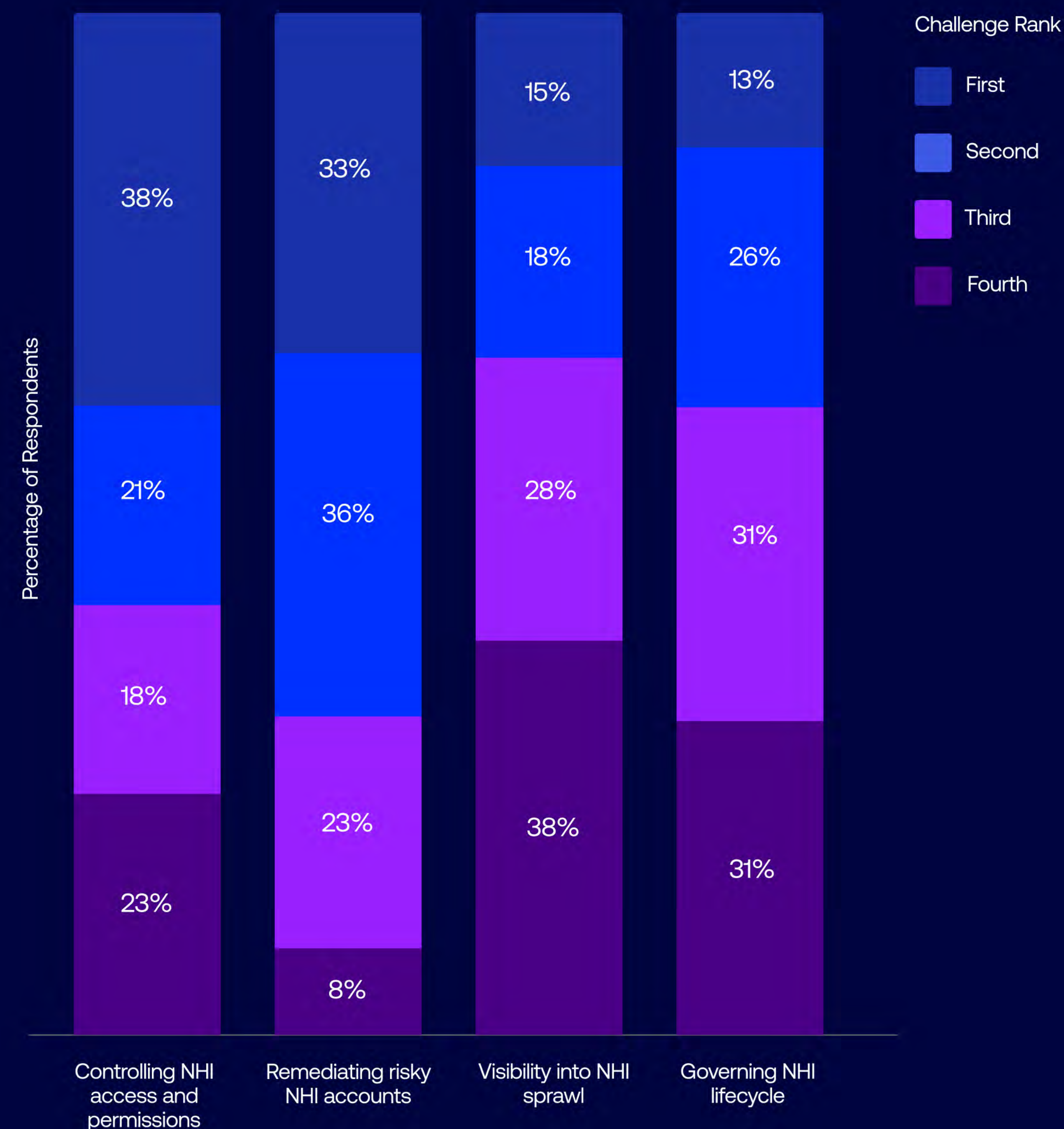


Most pressing security concerns for securing NHIs

When it comes to security concerns around NHIs, nonprofit leaders are focusing on immediate, tangible risks. Controlling NHI access and permissions is their top concern, ranked first by 38% of respondents (and either first or second by more than half). This is also the top concern across all industries. The second-highest priority for nonprofits is remediating existing risky NHI accounts, ranked first by another 33% of respondents. In the broader market, however, remediating risky NHI accounts ranks only fourth among top concerns.

Controlling NHI access and permissions is **nonprofits' top NHI security concern**, ranked first by 38% of respondents.

Nonprofits' most pressing security concerns related to NHIs

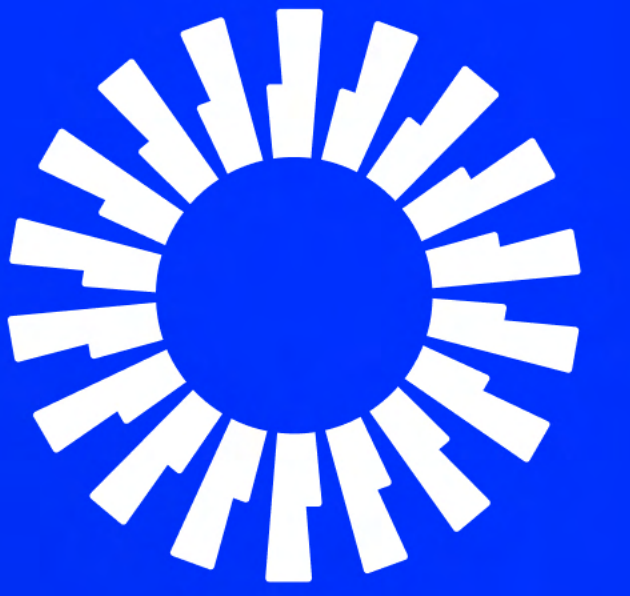




Nonprofits' relatively high focus on cleaning up and improving visibility before engaging too deeply in governing the NHI lifecycle (only 13% of nonprofits named this as their No. 1 concern) suggests their IT teams are reckoning with identity debt. When organizations begin moving to the cloud, for example, legacy on-premise systems that may have more exposure to sensitive data may be left unmanaged and unattended. Old or overly privileged machine identities can accumulate over years of evolving IT environments, and these dormant or misconfigured accounts can represent a significant, often invisible attack surface.

Smaller IT teams can lack the sophisticated, expensive discovery and lifecycle management tools common in larger commercial enterprises, and need to prepare for expanding NHI lifecycle management by shoring up their identity foundations. Without automated governance, the number of unmanaged machine identities will inevitably sprawl, creating unacceptable risk, making it critical for nonprofit leaders to lay the groundwork to deploy automated governance at scale.





Conclusion





Resources for laying a secure identity foundation

- [Nonprofit AI Readiness Assessment](#) (NetHope 2026)
- [AI Usage Policy Framework and Template](#) (TechSoup 2023)
- [Identity Maturity Model for Nonprofits](#) (Okta 2026)
- [AI Governance and the Nonprofit Sector: Mapping the Missing Middle](#) (NetHope 2026)
- [Maximizing the Reach and Impact of AI Agents for Nonprofits](#) (Okta 2026)

The story of the nonprofit sector has always been one of resilience and ingenuity, and the dawn of the agentic age is no different. Throughout this report, we've seen a clear and consistent narrative: nonprofit leaders are pragmatic, security-conscious, and relentlessly focused on their missions. They face a 78% threat-to-authentication ratio—by far the highest of any industry—and are meeting this challenge by aggressively adopting phishing-resistant MFA and passwordless solutions. They recognize the immense potential of adopting AI agents, but are first ensuring their organizations can govern and oversee them. They are building the foundation for a secure, AI-powered future by focusing on what matters now, including adopting best-of-breed applications to optimize efficiency and developing frameworks for governing the non-human identities that will power automated workflows in the years ahead.

For nonprofits, this pragmatic approach to leveraging AI is the key to safely navigating the path forward—it's a marathon, not a sprint. Scaling for the efficiency gains to come must be founded on a bedrock of strong identity security. The quiet thesis of this report—that the move to agentic AI requires identity security readiness—is borne out by the data. Nonprofits need to continue investing in modern, phishing-resistant authentication for all users, build robust governance for human and non-human identities alike, and, when safe to do so, embrace automation to manage the complexity of this fast-evolving landscape. By placing identity at the center of their strategy, nonprofits can unlock the full, transformative potential of AI to protect their people and assets, expand their reach, stretch their budgets, and deepen their impact within their communities.



The conclusion is unavoidable:
Agentic AI readiness *is* identity
readiness. **Are you ready?**

Take our [AI Readiness Assessment](#) to find out.

[Contact Okta for Good](#) if you have any questions.



To create this nonprofit-specific report and our all-industry Businesses at Work reports, we rely on data from Okta customers. We anonymize data from our network of thousands of customers, applications, IT infrastructure integrations, and millions of daily authentications and verifications worldwide. Our customers and their employees, volunteers, partners, and external communities use Okta to securely log in to devices, websites, apps, and services and to leverage security features to protect their sensitive data.

Nonprofits at Work mainly focuses on data from our 501(c)(3) nonprofit customers — organizations that hold current 501(c)(3) status in the US or their country's equivalent, as validated by our partner, Goodstack. Unless otherwise specified, the data included in this report is limited to Okta customers who have deployed at least one app to users through the Okta Integration Network. In some charts and data in this report, “nonprofits” are defined by industry sector tagging; in others, they are defined as companies in the OIN that are validated nonprofits by our partner Goodstack. Unless otherwise noted, this report looks only at apps deployed for corporate use.

As you read this report, remember that this data only represents Okta's customers, the applications and integrations they authenticate to through the Okta Integration Network, and how users access these tools through our service. Throughout this report, we use the terms “app” and “tool” to refer to applications, services, and integrations available through the Okta Integration Network. The trends we describe for Okta customers who use Microsoft 365 may differ from those of Microsoft 365 customers who don't use Okta (i.e., those using Azure Active Directory or other identity platforms).

Unless otherwise noted, this report presents and analyzes data from November 1, 2024, to October 31, 2025, which we refer to as “this year,” “today,” and “in 2025.” Similarly, when we refer to “last year” or “in 2024,” we mean data from November 1, 2023, to October 31, 2024.

The report also incorporates survey data from two Okta surveys of IT and security C-suite leaders, conducted by third-party research firms on our behalf. A nonprofits-focused survey of 61 leaders from large and small nonprofit organizations, largely in North America, explored technology adoption trends, AI priorities, and security challenges. Additional insights in this report incorporate findings from Okta's AI at Work 2025 research, which examined enterprise adoption of artificial intelligence and autonomous systems, research which helps contextualize how emerging technologies such as AI agents and automated workflows are influencing identity usage and security requirements across organizations.



Safe Harbor Statement

This report contains "forward-looking statements." These statements are not historical facts but rather are based on Okta's current expectations, estimates, and projections about our industry, business, and the technology landscape. Forward-looking statements can often be identified by words such as "believes," "expects," "anticipates," "estimates," "intends," "plans," "seeks," "will," "may," "should," "predicts," "projects," "targets," "will likely result," or the negative of these terms or other comparable terminology.

These statements include, but are not limited to, predictions and observations regarding:

- The future adoption, growth, and impact of agentic AI and other artificial intelligence technologies.
- Trends in application usage, security practices, and identity management.
- The future evolution of the threat landscape and cybersecurity responses.
- Projections about customer behavior and technology investment priorities.
- The expected performance and integration of various technologies and platforms.

These forward-looking statements are subject to a number of risks, uncertainties, and assumptions that could cause actual results to differ materially from those described in the forward-looking statements. These risks and uncertainties include, but are not limited to:

- The pace of technological change and market acceptance of new and developing technologies, including AI.
- Changes in the competitive landscape and the strategies of our competitors.
- Uncertainty in the global economic environment.
- The evolution of and changes to the regulatory and legal landscape, particularly concerning data privacy and artificial intelligence.
- Our ability to accurately interpret and analyze the underlying data from the Okta Integration Network and other third-party sources.

Okta undertakes no obligation to update any forward-looking statements in this report, whether as a result of new information, future events, or otherwise. In light of these risks and uncertainties, we caution you not to place undue reliance on these forward-looking statements.

Third-Party Trademark Notice

The "2026 Nonprofits at Work" report mentions various third-party companies, products, services, and applications for identification and illustrative purposes only.

All third-party trademarks, service marks, trade names, product names, and logos appearing in this report are the property of their respective owners. The use of any third-party trademarks does not imply an affiliation with, endorsement by, or sponsorship of Okta by such third parties.

Okta does not claim any ownership rights in these third-party marks. Any reference to third-party products, services, or companies is for informational and analytical purposes only and should not be construed as a recommendation or endorsement.



How to cite the Okta Nonprofits at Work 2026 report

We love it when people share Nonprofits at Work insights. Here's how to properly cite data, statistics, and any other information found in the Okta Nonprofits at Work 2026 report:

Give us credit: Please cite the source as "Okta Nonprofits at Work 2026 report" when referencing any content.

No modifications: Content must be cited exactly as it appears in the report. If you wish to paraphrase, we'd appreciate it if you contact us for approval.

Please share: If you'd like to share the report with others, please provide a link to our [download page](#).

We appreciate your helping us keep our insights accurate and accessible to everyone.

About Okta

Okta, Inc. is The World's Identity Company™. We secure identity, so everyone is free to safely use any technology. Our customer and workforce solutions empower businesses and developers to use the power of identity to drive security, efficiencies, and success—all while protecting their users, employees, and partners. Learn why the world's leading brands trust Okta for authentication, authorization, and more at okta.com.