

EBOOK

Ping
Identity®

Identity powers
trusted AI.

Did you just approve an
invoice from DevGroup Inc?

Yup! You delegated that task
to me. Should I put it on hold?

No, I'm just verifying
that it's on track.

I did block a suspicious request.

Please send the report.

...

AI Agents Explained: Types, Trust, and Identity

Meet the next generation of intelligent digital actors —
and see how identity makes them trustworthy.

Table of Contents

- 03 The Rise of AI Agents
- 04 Key Types of Agents
- 05 The Personal Assistant
- 06 The Digital Assistant for Consumers
- 07 The Digital Assistant for Workforce
- 08 The Digital Worker
- 09 What Next?

From Prediction to Action: The Rise of AI Agents

AI has evolved from supporting human decisions to making them. Where generative AI produced content, agentic AI takes action. These intelligent entities can plan, reason, and complete real-world tasks on behalf of users or organizations. They're reshaping how we engage customers, support employees, and automate business operations.

This evolution is more than technological. It's operational, cultural, and strategic. AI agents are already being embedded into daily workflows, customer journeys, and backend systems. They are taking on tasks that previously required human intuition and oversight. From triaging service tickets to personalizing product recommendations, their scope is rapidly expanding.

But with action comes risk. Enterprises need to ensure that every AI agent operates under its own identity – never a human's – so that every action is accountable and governed. Trust in the agent economy begins with identity.

“Credential sharing is an exceptionally (we use this term intentionally) high-risk method for enabling AI agents to act on behalf of humans, and it is inconsistently effective.”

Gartner, [How to Securely Delegate Access From Humans to AI Agents](#),

Nathan Harris and Arif Khan, 20 August 2025

Four Types of AI Agents Powering the Modern Enterprise

AI agents fall into four distinct categories, each with different responsibilities, control levels, and trust implications. Whether customer-facing or enterprise-bound, all must be recognized, verified, and governed through identity.

These categories reflect both ownership and operational scope. Personal agents are unmanaged and act solely for the user. Consumer digital assistants are managed by the enterprise but serve users externally. Workforce assistants are embedded internally, aiding employees under IT governance. Digital workers are the most autonomous — executing backend processes independently and continuously.

What changes is how they access systems and whose authority they carry. What stays the same: they must never act without accountability. For each agent type, identity defines what they can do, who authorized them, and how their actions are logged and reviewed.

Personal Agent

(Unmanaged)

Your agent works for you

Consumer Digital Assistant

(Managed)

Our agent works for you

Workforce Digital Assistant

(Managed)

Our agent works for us

Digital Worker

(Autonomous)

Our agent works autonomously

01 Personal Agent

Examples of Personal Agents

Personal Travel Agent



Books flights, hotels, and transport based on your preferences. Uses delegated access to payment and loyalty accounts—never your credentials—and follows secure travel and spending policies.

Personal Shopping Agent



Finds deals, applies discounts, and checks out within your spending limits. Accesses your accounts via scoped tokens, ensuring secure, permission-based purchases.

Tax Preparation Agent



Pulls income data from authorized accounts and pre-fills tax forms. Uses secure delegation—not impersonation—with full audit trails and final user sign-off.

Your Agent Works for You

These user-owned agents are digital proxies. They book flights, buy groceries, file claims—all on behalf of the individual. But they live outside the enterprise trust boundary. That makes identity essential.

Today's consumers are empowering these agents with increasing autonomy. The agent might be configured by a user but deployed across dozens of services. This creates a fragmented identity model where enterprises don't control the agent, but must still respond to it securely. When a personal agent initiates a transaction, it must do so with a verifiable identity and bounded permission set.

Enterprises must authenticate the agent as its own distinct identity, while verifying that any actions are tied back to an authenticated human user. That means no shared credentials. Only securely delegated access, limited by purpose, time, and context. This delegation must be ephemeral and auditable to reduce risk, prevent impersonation, and ensure compliance.

02 Digital Assistant for Consumers

Examples of Digital Assistants for Consumers

Insurance Plan Assistant



Helps customers compare health, auto, or life insurance options by analyzing personal data and recommending plans. Operates with delegated access and prompts the user for final selection and consent.

Digital Banking Concierge



Assists users with account summaries, fund transfers, and fraud alerts. Interacts via secure chat or app, with step-up verification for sensitive actions like wire transfers

Travel Rebooking Assistant



Proactively offers rebooking options during delays or cancellations, pulls current itineraries, and proposes alternatives. Requires confirmation before finalizing new reservations or charges.

Our Agent Works for You

These are your digital frontline workers. Chatbots that answer questions, solve problems, and complete transactions. Customers expect them to work instantly — and securely.

These agents must reflect your brand's authority, tone, and policy. If they retrieve customer data, initiate refunds, or perform sensitive actions, they must do so under scoped permissions and transparent identities. Their actions must be attributable, logged, and reversible if needed. Without this discipline, even a helpful bot can erode trust or cause regulatory exposure.

They need enterprise-issued identities, scoped permissions, and auditable logs. Each interaction must be traceable to the agent that performed it — not just the user it served. Role-based access, consent verification, and human approval gates are critical for agents handling private data or executing irreversible actions.

03 Digital Assistant for Workforce

Examples of Digital Assistants for Workforce

HR Assistant Agent



Answers employee questions about PTO balances, benefits, and policies. Can initiate time-off requests and update contact details with employee approval.

Finance Assistant Agent



Automates expense report preparation by pulling transactions and receipts. Flags policy violations and submits reports for approval, maintaining audit trails throughout.

Onboarding Assistant



Guides new hires through orientation tasks—account setup, training modules, and benefits enrollment. Coordinates across departments while logging progress and actions.

Our Agent Works for Us

Workforce assistants are enterprise-managed AI agents that support employees inside the trust boundary. They act as digital coworkers — surfacing insights, drafting content, resolving tickets, or automating workflows — always under IT's governance and within organizational policy.

These assistants accelerate productivity by handling repetitive or complex tasks. But because they can access sensitive systems and data, identity governance is critical. Each assistant must have a unique enterprise-issued identity, with role-based permissions mirroring a human counterpart.

They also need continuous monitoring. Actions should be logged and attributed to the specific assistant identity, ensuring every automation is auditable and reversible. By extending workforce identity policies to AI, enterprises can scale intelligence safely while maintaining compliance and trust.

04 Digital Worker

Examples of Digital Workers

Compliance Monitoring Agent



Scans communications, transactions, or logs for policy violations or regulatory triggers. Escalates anomalies and produces compliance reports on a regular schedule.

Inventory Replenishment Agent



Monitors stock levels, forecasts demand, and places restock orders within approved thresholds. Adjusts based on seasonality or supply chain signals without human intervention.

Customer Feedback Analyzer



Reviews surveys, call transcripts, and reviews to extract insights and sentiment. Summarizes trends for CX teams and triggers alerts for urgent issues.

Our Agent Solves Tasks Autonomously

Digital workers are the most autonomous class of AI agents. They execute business processes end-to-end — reconciling invoices, provisioning accounts, or orchestrating multi-system workflows — often without direct, real-time human oversight. These agents don't just assist; they operate as digital team members.

Because of their autonomy, identity becomes the cornerstone of governance. Each digital worker must have a persistent, verifiable identity that defines its authorization scope, operational boundaries, and accountability chain. Without this, even small misconfigurations can propagate errors or expose data.

Identity systems enable lifecycle management for digital workers — from creation to retirement. They ensure every action, API call, and decision is traceable to a specific, credentialed entity. Through continuous authentication and least-privilege access, enterprises can trust digital workers to execute complex operations safely and predictably.

Ready to Build Trust Into Your AI Strategy?

AI agents will power the next decade of business innovation and every stage of the agent journey depends on identity. Each agent type operates differently — but the foundation stays the same.

Ping Identity is tackling the challenges enterprises face when adopting AI agents, removing the guesswork and providing the foundation to deploy them responsibly, efficiently, and at scale.

AI agents are already acting on behalf of your users. Make sure your identity strategy — and your trust framework — are ready.

[Explore the Ultimate Guide to Identity for AI →](#)

