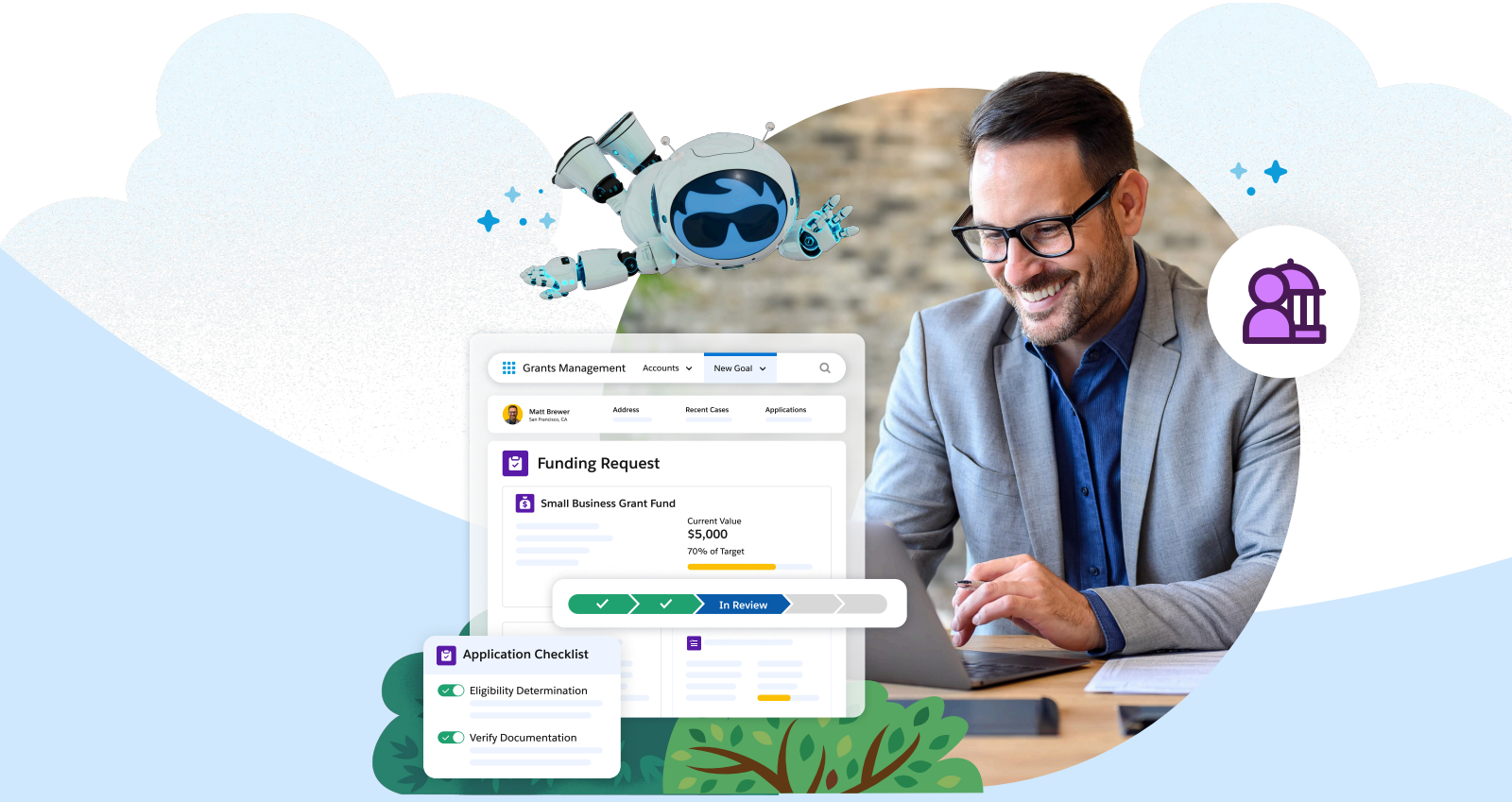
REPORT

The State of IT in the Public Sector

Efficiency, innovation, and workforce challenges in 2025.



Executive Letter

Dear Public Sector IT Leaders,

I've been in your seat. I know what it means to lead in government IT – navigating legacy systems, shrinking budgets, rising expectations, and the constant demand to do more with less. The mission never slows, even when the resources do.

This work is complex, and the stakes are high. Efficiency isn't just a technical imperative – it's a strategic lever. It helps us keep systems resilient, teams focused, and services reliable for the people who rely on us.

The good news? You don't have to tackle this alone. Built-in security, reusable architectures, and AI agents can lift the burden of repetitive tasks – like data entry, reporting, and routine administrative work – by automating them once and replicating that value across your organization. That means less firefighting, and more forward momentum.

Imagine a regular cadence of innovation, patching, and security updates delivered automatically. Imagine reclaiming the hours your teams spend on maintenance – and redirecting that energy toward modernization, service delivery, and impact.

Modern Software-as-a-Service ("SaaS") practices make this possible. And when done right, we can reduce costs and meet high security standards. With the right automation and AI agents in place, you gain faster time to value, reduce administrative burdens, and even uncover inefficiencies that can lead to real savings.

But to get there, we must move AI from aspirational to operational. Start with opportunities to increase productivity grounded in use cases – ones that align to your mission and show immediate value. Our latest report, Public Sector IT in 2025: Efficiency, Innovation, and Workforce Challenges, shares insights from real government leaders who are building capacity, closing resource gaps, and modernizing at speed.

The challenges are real. But so is the opportunity to lead differently – strategically – through this next chapter of modernizing and accelerating government services.

Thank you for your service and for the leadership you bring to the mission every day.

Mia Jordan
Industry Advisor, Salesforce

Table of Contents

01

State of IT in the Public Sector

Today's government is marked by widespread cutbacks, reduction in workforce, and uncertainty across all departments and well-known government programs. Financial constraints are only part of the challenge. IT leaders are also under pressure to keep pace with accelerating technology and rising expectations.

While much of current spend is still tied up in sustaining legacy systems (which are often siloed, costly to update, and difficult to secure), agency CIOs are under mounting pressure to accelerate digital transformation. The focus is now on building cloud-native environments, improving data interoperability, and laying the groundwork for AI and automation at scale.

Salesforce data shows IT project requests in the public sector have increased by 18% year over year, with 29% of projects missing their deadlines due to overload and limited resources. Additionally, 30% of new applications now include an artificial intelligence (AI) component, reflecting the growing importance of AI in government operations. That's not surprising,

In Salesforce's new reports, State of IT: AI & App Development and State of IT: Security, data shows today's AI boom is pulling IT teams across all industries in multiple directions. They are challenged to handle increasingly complex projects with faster timelines, higher expectations, and growing pressure to deliver business value.

IT teams serving the public sector face even more issues, including complex security and privacy requirements, shifting mission priorities, data silos, manual or paper-driven processes, and bureaucratic bottlenecks. These obstacles delay IT service delivery. They also hinder the adoption of solutions that could drive real efficiency gains and bring constituent services in line with modern private-sector services.

Let's take a look at the report's key findings for public sector IT teams.

Digital Transformation & AI Adoption in Government IT

Increase in IT project requests

Projects missing deadlines due to overload/limited resources

New applications that include an AI component

IT professionals who say AI helps complete projects faster

02

Unified Data is Crucial for Future AI Integration.

AI, and agents in particular, have become essential across all industries. Companies embracing the technology are seeing better customer experiences and more efficient operations that allow teams to focus on high-value, strategic work.

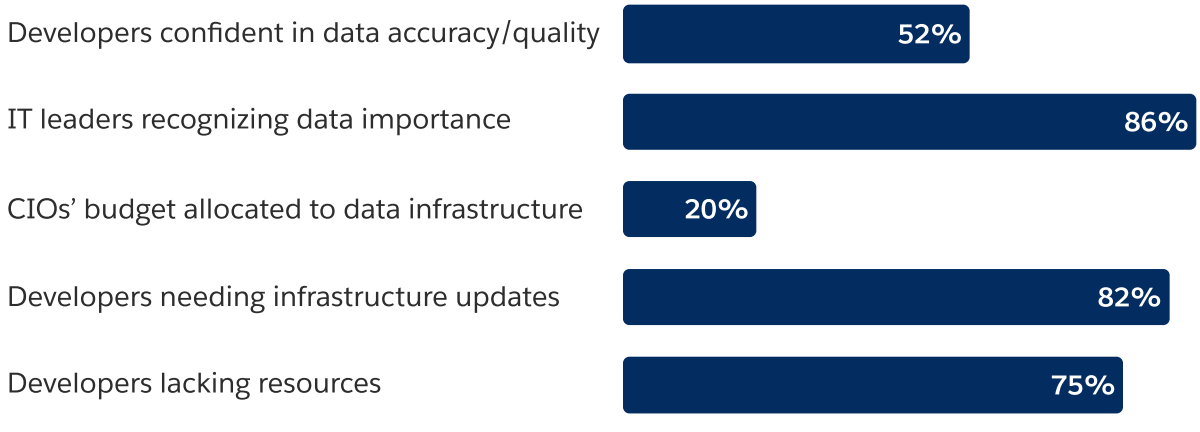
But government agencies that want to roll out autonomous AI agents need the right foundations – including high-quality data, flexible infrastructure, and clear privacy standards – to ensure their agents are reliable, scalable, compliant, and ready for their stakeholders and constituents.

One of the primary hurdles in the adoption of AI is clean, accurate, and relevant data. The lack of good data hampers effective AI and application development. Although 52% of application developers are confident in their data accuracy and quality, many still see a need for improvement.

High quality and high availability of data is essential for the effectiveness of AI, and 86% of IT leaders recognize this. To address these issues, CIOs are allocating 20% of their budgets to data infrastructure and management. This includes adopting new data governance frameworks, data cleansing programs, and data validation processes. Still, there is a significant readiness gap, with 82% of developers stating their infrastructure needs updating to build and deploy AI agents, and 75% lacking the necessary resources. This may be addressed with unified cloud platforms and advanced analytics tools.

A modern cloud infrastructure, stringent security measures, and easy-to-deploy systems are essential for successful AI integration. Addressing these gaps ensures government agencies can fully optimize the potential of AI.

AI Adoption Challenges and Data Readiness



03

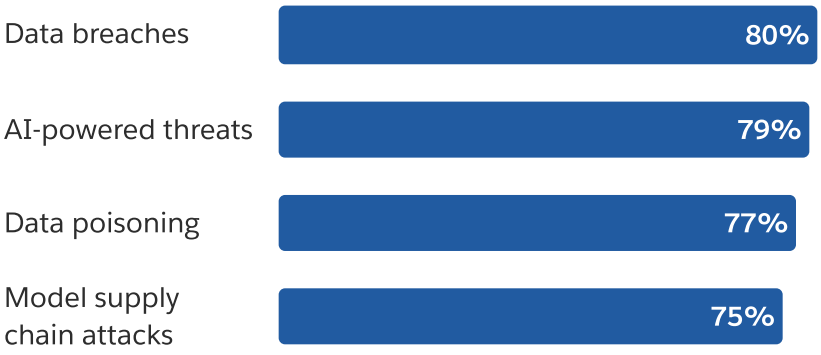
Security and Privacy Remain Foundational Requirements.

In today's threat landscape, security and privacy aren't just compliance checkboxes; they're the load-bearing walls of our digital infrastructure. For federal, defense, state, and local IT leaders, the stakes are high.

Ransomware, data breaches, and AI-enabled threats are evolving faster than legacy defenses can keep up. IT security professionals believe the biggest threats to security in an AI-powered environment include data breaches (80%), AI-powered threats (79%), data poisoning (77%), and model supply chain attacks (75%).

This isn't a fight you win once. Securing sensitive systems and information demands a persistent, always-on strategy – one that embeds cybersecurity from design to deployment. As we integrate AI into government operations, trust must be architected into every layer to safeguard national interests and earn stakeholder confidence.

Biggest Threats to Security in an AI-Powered Environment



03

That's why the shift towards DevSecOps is more than a trend: It's a necessity. Embedding security into every phase of development isn't just about speed or compliance; it's how we future-proof our systems against increasingly intelligent threats. With 85% of IT organizations adopting this model, it's clear that security must move from being a final gatekeeper to a foundational design principle.

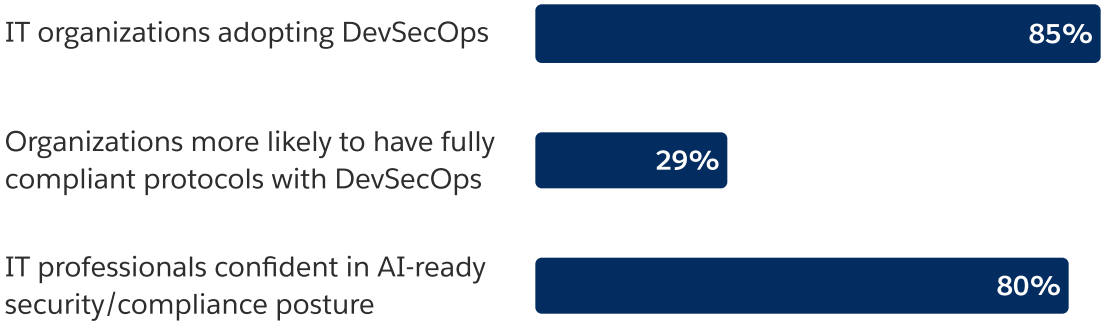
This approach not only boosts security but also increases confidence in building and deploying AI agents. Organizations that adopt DevSecOps are 29% more likely to have fully compliant security and governance protocols. And 80% of IT security professionals believe their security and compliance postures are ready for AI.

To further strengthen this foundation, AI agents can play a crucial role by automating threat detection and response, continuously monitoring for vulnerabilities and identifying areas for compliance with regulatory requirements. Agents can analyze vast amounts of data in real time to identify potential security breaches and flag them for immediate action.

In fact, 84% of security professionals agree AI will provide new security opportunities in the public sector.

Additionally, AI can help in automating the process of data anonymization and encryption, ensuring that sensitive information is protected while still being usable for operational and analytical purposes. When paired with DevSecOps, these AI capabilities create a living, breathing defense posture that adapts, learns, and strengthens over time. Integrating AI into DevSecOps practices transforms security into an intelligent embedded capability, one that builds confidence, earns trust, and protects what matters most.

Impact and Adoption of DevSecOps in AI Integration



04

Agents Partnering with Humans Will Deliver Critical Efficiencies.

The rapid adoption of AI agents is reshaping mission functions and constituent experiences. Data shows 81% of IT leaders are either using or planning to use AI agents within the next two years. These agents are automating routine tasks, freeing up human resources to focus on more complex problem-solving.

Constituent-Facing Applications

AI agents can surface answers in a more intuitive way and then take on low-priority administrative tasks such as summarizing information, generating required forms, and making updates to cases. This can significantly reduce the workload of human staff. Agents can quickly process and route incoming inquiries to the appropriate human worker, ensuring stakeholders receive timely and accurate assistance. This improves operational efficiency and enhances the overall constituent experience by reducing wait times and resolving issues more effectively.

What's more, data shows 64% of developers expect agents to improve stakeholder and constituent experiences. But while constituents are comfortable with AI helping out on routine tasks, for now they prefer to deal with people when critical decisions are involved. AI agents help agencies allocate staff for those real-world discussions.

Guardrails for human involvement and escalation ensure stakeholders and constituents receive personalized and empathetic support, maintaining trust and satisfaction. The human-AI partnership delivers optimal outcomes, combining the strengths of both to achieve mission success.

AI Agent Adoption & Expected Impact

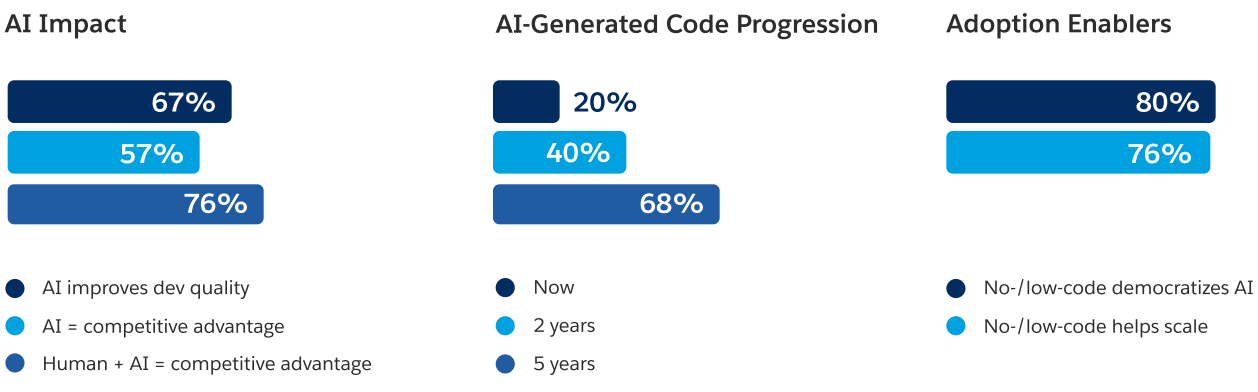
04

Application Development Tools

Our data shows that 67% of developers expect AI agents to improve application development quality, and 57% see it as a competitive advantage. Right now, application developers say 20% of the code developed at their organizations originates with AI. They anticipate that to double in the next two years and reach 68% in the next five. How will they get there? Eighty percent say no- and low-code AI tools will help democratize AI development by allowing business users to build their own capabilities, and 76% say they will help scale AI more efficiently.

Still, the human-AI partnership is a key aspect of this transformation. In fact, 76% believe combining human and AI capabilities is key to building a competitive advantage. Humans are essential for complex problem-solving and critical decision-making, ensuring that AI systems are used effectively and ethically. This collaborative approach is seen as a competitive advantage by 76% of developers, optimizing the best of both human and machine capabilities. This shift enhances operational efficiency and improves employee satisfaction.

AI in Application Development: Current Use & Future Expectations



05

The Strategic Evolution of Agents in Public Sector IT

The challenges facing public sector IT leaders – fragmented data, aging infrastructure, and rising security threats – are significant, but so is the opportunity. We're at a pivotal moment for reimagining the way the government operates by embracing AI-powered agents as part of a larger transformation strategy. The key to success lies in building a unified data foundation, taking advantage of commercial innovations, and embedding AI directly into workflows to break down data silos, update infrastructure, and ensure stringent security measures.

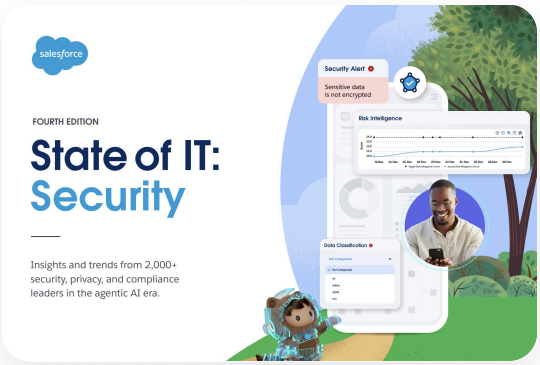
To move forward, IT executives should prioritize realistic and tactical AI initiatives that align with their mission and goals. For example, start first with the agent addressing frequently asked questions. Then, evolve it to act on the information it receives, followed by proactively monitoring and responding to the data it analyzes. By reducing administrative burdens, closing capacity gaps, and delivering faster, more accurate service, agencies don't just improve operations – they earn trust.

With a human-AI partnership and a strategic, integrated approach, public sector IT leaders can navigate the challenges of the current landscape and pave the way for a more efficient and effective future.

Resources

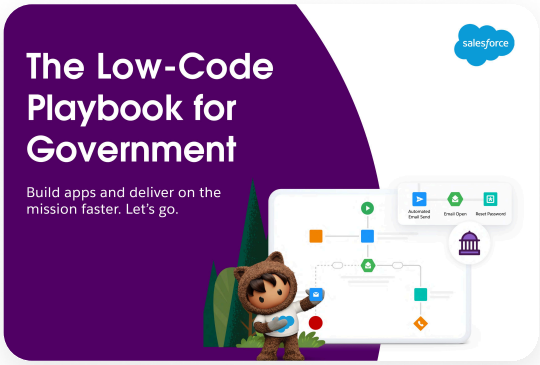
More building, fewer bottlenecks: Learn to use low-code and AI to accelerate app development.

Read the report



Complex threats, simple solutions: See how 2,000+ IT leaders are simplifying security in the age of AI.

Read the report



Learn how to build apps and deliver on the mission faster with The Low-Code Playbook for Government.

Get the guide