Google Cloud

Accelerating modernization and adoption of AI and cloud for public sector

Deliver resilient, optimized digital services in the AI era with F5 and Google Cloud

Contents

Driving change through modernization

Public sector organizations are aligning their digital visions with the possibilities of AI and cloud. To be successful, it also means addressing technical debt that can hold back the adoption of innovation and impede digital transformation.

Reduce technical debt from legacy systems and infrastructure

Government leaders believe outdated software and hardware are some of the biggest barriers to tech modernization efforts at their agency.[3] State CIOs shared that legacy modernization to is a top five priority.[4]

Defend against cybersecurity threats

Ransomware remains a top security risk in the public sector and 79% of leaders say they don't have the necessary workforce to meet current and future demand for managing cloud services.[5]

Lower costs and improve efficiencies

Federal agency leaders agreed that adopting emerging technologies will help increase overall efficiency (86%) and reduce operational costs (77%).[6]

Deliver resilient digital services

Continuing to invest in and deliver resilient digital services is a priority for state CIOs in 2025 which includes improving and digitizing the citizen experience, accessibility, and identity management.[7]

State and local IT decision makers see their top priorities as:[8]

56%
Reducing costs

54%
Improving cybersecurity

47%
Modmodernizing legacy systems

Most federal leaders recognize the importance of investing in emerging technologies,[9] including:

49%
Cloud networks

42%
AI/ML

33%
Generative AI

Exciting trends in AI for public sector

AI has catalyzed a wave of rapid innovation—and the pace shows no sign of slowing. In fact, 94% of state and local governments expect an increase in AI usage in the next 1-2 years.[10] AI's evolving capabilities will continue to drive a radical transformation in how agencies operate and innovate. Google Cloud has analyzed data to identify the top five AI trends and how they can reshape the public sector.

Trend 1

Multimodal AI integrates diverse data sources such as images, video, audio, and text to unlock AI's ability to learn from a broader range of contextual sources with unprecedented accuracy. Google Cloud believes "multimodal AI will enable agencies to analyze local and state-level data and combine it with data from other sources such as Google Earth Engine, Google Maps, Waze, and public data sets to enhance decision-making, preempt climate-related risks, and improve public infrastructure."

Trend 2

We've gone from simple chatbots to **sophisticated AI agents** capable of handling the most complex tasks. In the future, "AI agents will help government employees work and code more efficiently, manage their applications, gain deeper data insights, identify and resolve security threats, and bring their best ideas to life."

Trend 3

AI-powered search is transforming the way we access and understand information. With generative AI, "governments can improve the accuracy and efficiency of searching vast datasets. By investing in semantic search, automated metadata tools, and advanced document transcription, agencies can unlock the value of their data and make it more accessible."

Trend 4

In 2025, "AI will help **improve citizen experiences**. AI-powered tools and technologies can build trust and foster closer citizen-government relationships by enabling citizens to quickly and easily navigate government websites and services—such as applying for permits and licenses—offered in multiple languages and available 24/7."

Trend 5

AI is becoming alarmingly more prevalent in cyberattacks.[11] However, "AI is also a powerful tool for **enhancing security**. By automating threat detection, analyzing vast amounts of data, and responding to incidents quickly, AI can help protect government systems and sensitive information from AI threats such as deepfakes and disinformation."

Source: Google Cloud, 5 AI trends shaping the future of the public sector in 2025

Impediments to modernization with AI and cloud

Attacks on the rise

As legacy systems fail to support critical business requirements, public sector agencies need application modernization. Yet as agencies look to transform through cloud and AI, they are often challenged with balancing speed, innovation, and security. With over 900 public sector data breaches from November 2023 to October 2024, it has never been more important to get digital transformation right. Credential abuse, exploitation of vulnerabilities, and phishing all remain as popular attack techniques, with ransomware seeing a 37% increase from 2023 to 2024.[12] Breaches involving third parties and espionage are also on the rise.

Skilled staffing shortages

While leaders believe their agencies will benefit from modernization and emerging technologies, barriers remain, starting with the workforce. Public sector leaders say one of the biggest barriers to modernization is a shortage of skilled employees (38% for federal, 46% for state and local) and insufficient training (36% for federal, 43% for state and local).[14]

Multicloud complexity

Multiple cloud deployments have become the new norm, offering a flexible approach to modernizing digital services. But as applications and digital services sprawl, managing and securing multiple clouds gets complex. As sophisticated cyberthreats rise, teams face new imperatives for app protection as they modernize in the cloud. Yet without centralized oversight and control in place, IT and security teams cannot keep pace.

The public sector experienced

1,422

security incidents and investigated

946

confirmed breaches[13]

- Growing attack surfaces
- Disparate, proprietary tooling
- Insufficient security posture
- Limited resources and expertise

Accelerate innovation with F5 and Google Cloud

Innovate faster without sacrificing security, compliance, or scale.

To accelerate app modernization efforts, government agencies and educational institutions require automated solutions that improve app delivery in the cloud without sacrificing security. F5 and Google Cloud fuel digital transformation journeys by ensuring mission-critical services stay secure, available, and fast across any environment. With F5 and Google Cloud, you can rapidly develop and deploy new services, actively defend apps, APIs, and networks from advanced attacks, and implement consistent security controls for uniform protection across new and legacy environments.

Defend against cyberattacks

Protect apps, APIs, and networks from automated attacks and OWASP Top 10 threats.

Develop and deploy with speed

Integrate performance, security, and compliance to drive innovation across app development pipelines.

Maintain zero trust security

Meet stringent security and compliance protocols, such as NIST, FIPS140-2, CSfC, Common Criteria, and more.

All 15 executive departments of the U.S. Cabinet rely on F5.

Unified protection and management with F5 and Google Cloud

Proven security and control–wherever your applications live.

Prevent fraud and abuse

Bot defense | Authentication protection
Client-side defense

Identify and mitigate malicious bots and stay ahead of attacker retooling.

Accurately validate users, prevent account takeover, and eliminate unnecessary authentication steps.

Block browser-based attacks, including Magecart, formjacking, skimming, and PII harvesting.

Modernize apps

Secure multicloud networking | DNS
Local traffic manager

Securely and reliably connect apps, services, clouds, and networks at scale.

Increase application resiliency and boost performance with real-time protocol and traffic management.

Accelerate deployments with secure, pre-built integrations.

Modernize security

Web Application Firewall (WAF)
API security | DDoS mitigation
DNS protection | SSL orchestration

Block OWASP Top 10 threats and secure vulnerable or exposed APIs.

Safeguard networks and apps from volumetric L3–7 attacks and prevent downtime or cache poisoning.

Decrypt, encrypt, and inspect SSL/TLS traffic to surface threats.

Secure and optimize your AI journey

AI is ushering in a new era of development, delivery, and security challenges. As agencies begin to build AI models, apps, and agents at scale, the underlying infrastructure gets more complex, resulting in an expanded attack surface. This can make agencies vulnerable to unique AI security risks, escalating cost and infrastructure overhead, and challenges securing data integration across distributed environments.

Accelerate AI development with Google Cloud

Google Cloud eliminates the traditional barriers to building AI-powered applications. Developers can leverage the Google Cloud Vertex AI platform for end-to-end machine learning model development and deployment. Pre-trained first- and third-party models serve as a starting point to build or fine-tune AI initiatives, which can be deployed via Google Kubernetes Engine (GKE)—all running on secure, purpose-built AI infrastructure with high reliability and availability.

Protect AI models and apps without impacting speed

F5 solutions address the unique delivery, security and performance needs of AI apps. These AI-focused technologies provide layered protection, from model security to API connectivity, allowing agencies to innovate without compromising on data protection or regulatory compliance. Wherever AI apps or models are deployed, F5 provides consistent security policies along with capabilities that optimize traffic flow, control resource utilization, and provide deep visibility into AI operations.

Optimize AI application performance and cost

Cost is a top concern for AI workloads. Integrate F5® AI Guardrails with Google Cloud's AI infrastructure to leverage high-performance AI hardware, including Cloud TPUs or NVIDIA GPUs, while maintaining control over costs and performance. AI Guardrails provides smart traffic management and delivery services for AI applications deployed on Google Cloud through:

Intelligent load balancing

Traffic route optimization

Semantic caching

Rate limiting

Edge AI deployments

Reduce multicloud complexity

Consistent protection across every cloud

F5 and Google Cloud enable a foundation to develop, secure, and manage applications. Designed with modernization and efficiency goals in mind, F5 and Google Cloud's joint solutions deliver centralized visibility and control for dynamic and complex hybrid, multicloud IT landscapes. With a rich portfolio of automation, security, and performance capabilities, agencies of every size can create, protect, and operate applications without sacrifice.

- Deploy and safely run apps where you need—in data centers, clouds, and at the edge.
- Streamline protections while keeping pace with changing cloud environments.
- Consolidate management with centralized, universal policies.
- Unify administration and oversight across disparate cloud and on-premises environments.
- Reduce costs, improve operations, and better protect critical apps.
- Drive application reliability and frictionless user experiences.
- Bolster security and actively defend against advanced and automated threats.

Block cyberattacks to protect user experience and privacy.

Drive reliability and performance, from app inception to production.

Stay resilient, reduce attack surfaces, and prevent cyberthreats.

Securely advance the modernization agenda with F5 and Google Cloud

Together, F5 and Google Cloud deliver the security, protection, and connectivity needed for successful infrastructure and application modernization with AI and cloud. F5 and Google Cloud's joint solutions are proven to safeguard apps wherever they run—for consolidated management, consistent policies, and zero trust networking across every industry.

Ensure your apps and services are always:

Connected

Available

Secure

THE F5 AND GOOGLE CLOUD PARTNERSHIP

6+

years of collaboration

Over 50

listings in the Google Cloud Marketplace

Expertise

across security, networking, and industries

Appendix

[1] Verizon, 2025 Data Breach Investigations Report, Public Sector Snapshot, 2025

[2] Ibid

[3] EY, 2024 EY federal, state and local trends report, Feb 2024

[4] NASCIO, State CIO Top Ten Policy and Technology Priorities for 2025, Dec 2025

[5] EY, 2024 EY federal, state and local trends report, Feb 2024

[6] Ibid

[7] NASCIO, State CIO Top Ten Policy and Technology Priorities for 2025, Dec 2025

[8] EY, Government State and Local 2025 Survey Findings, June 2025

[9] EY, 2024 EY federal, state and local trends report, Feb 2024

[10] Google Cloud, Investing in AI, collaboration and the next generation of leaders, Feb 2025

[11] McKinsey & Company, AI is the greatest threat—and defense—in cybersecurity today. Here's why., May 2025

[12] Verizon, 2025 Data Breach Investigations Report, Public Sector Snapshot, 2025

[13] Ibid

[14] EY, 2024 EY federal, state and local trends report, Feb 2024

ABOUT F5

BRINGING A BETTER DIGITAL WORLD TO LIFE

F5, Inc. (NASDAQ: FFIV) is the global leader that delivers and secures every app. Backed by three decades of expertise, F5 has built the industry's premier platform—F5 Application Delivery and Security Platform (ADSP)—to deliver and secure every app, every API, anywhere: on-premises, in the cloud, at the edge, and across hybrid, multicloud environments. F5 is committed to innovating and partnering with the world's largest and most advanced organizations to deliver fast, available, and secure digital experiences. Together, we help each other thrive and bring a better digital world to life.

For more information, go to f5.com.

Learn more about F5 solutions for Google Cloud at f5.com/gcp.