IDC MarketScape

IDC MarketScape: U.S. State and Local Government Professional Security Services 2025–2026 Vendor Assessment

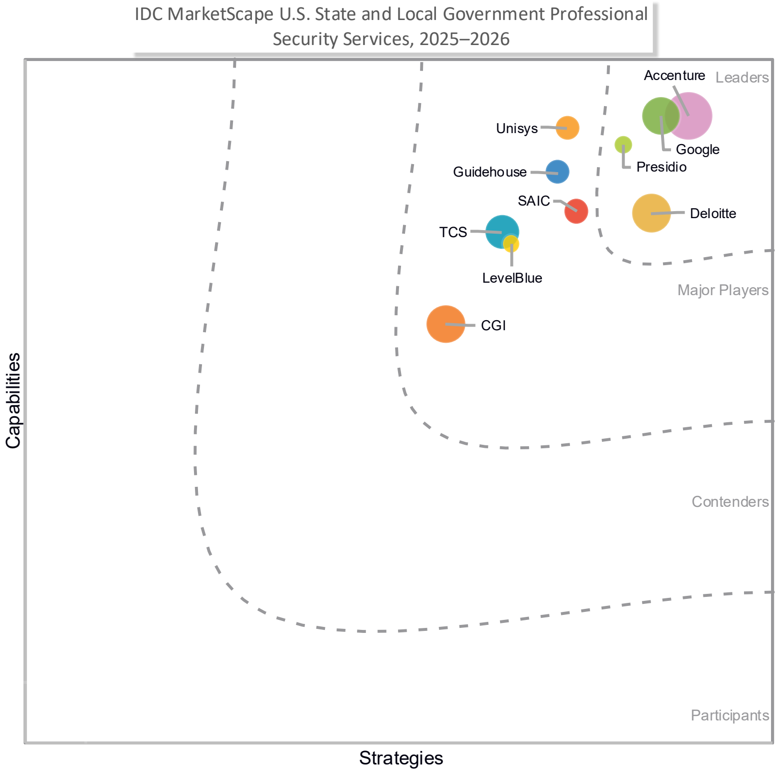
Ruthbea Yesner Alison Brooks, Ph.D. Massimiliano Claps Matthew Leger
Alan Webber

THIS EXCERPT FEATURES ACCENTURE AS A LEADER

IDC MARKETSCAPE FIGURE

Figure 1

IDC MarketScape: U.S. State and Local Government Professional Security Services Vendor Assessment



Source: IDC, 2025

December 2025, IDC #US53891025e

Please see the Appendix for the detailed methodology, market definition, and scoring criteria.

ABOUT THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: U.S. State and Local Government Professional Security Services 2025–2026 Vendor Assessment (Doc # US53891025).

IDC OPINION

U.S. state and local governments (SLGs) are prioritizing cybersecurity and evolving their cyber-resilience in response to emerging technologies and an expanding attack surface resulting from the rapid adoption of edge devices, hybrid and multicloud environments, and the proliferation of APIs and cloud services. State and local governments find themselves under continuous attack, and AI has enabled bad actors to act more quickly and with more sophistication, especially in targeting government workers. This has added substantial work for those tasked with protecting agencywide IT systems by muddying visibility and complicating asset, patch, and device management. On top of these new challenges is a massive shortage of skilled cybersecurity professionals, which impacts state and local governments as they struggle to compete with the private sector to attract workers. These factors are driving a reliance on external security service providers.

The modern cybersecurity service engagement can be complex and can impact every component of an organization's IT ecosystem, especially when efforts are made to have security built into IT environments rather than bolted on. Emerging technologies paint a picture of complete, intelligent protection, while threats to technology and infrastructure paint the opposite. Much effort is needed to demystify the threats facing state and local governments in the United States.

State and local governments desperately need partners with experience in both developing solutions that utilize cutting-edge technology and addressing the unique challenges inherent to operating within the confines of government. In addition, organizations need assistance from providers with deep partner ecosystems across security and cloud infrastructure offerings to achieve holistic security transformation in line with the required efforts outlined in federal, state, and local government mandates.

The following key drivers impact vendor solutions and services:

- **Increased attack surface:** IoT, edge, and operational technology (OT) are three of the largest contributors to attack surface expansion. 5G networks and increases in data in motion have compounded the challenge, making it difficult for agencies to achieve full organizational visibility. Organizations need help from trusted partners to identify and eliminate security gaps without impacting citizen service delivery.

- **Skilled worker shortage:** According to the Cybersecurity and Infrastructure Security Agency (CISA), there are more than 40,000 public sector cybersecurity openings in the United States. States and municipalities struggle to recruit skilled workers as they compete for talent with the private sector, which can offer higher wages and more flexible working conditions.
- **Unfunded mandates and required action:** Executive action taken by the U.S. government, as well as mandates by states and cities themselves, has added new priorities to organizations that were already working to modernize.

Using its MarketScape model, IDC studied 10 organizations that offer professional security services (PSS) to U.S. state and local government organizations and agencies in 2025 and ascertained that most participating firms, if not all, have a comprehensive offering of professional security services, including consulting, assessment, workforce preparedness, and governance, risk, and compliance (GRC) management.

The most complete PSS portfolios designed for U.S. state and local government include:

- Cybersecurity advisory services to improve operational efficiencies and bolster protection through consulting on security strategy, data security and sovereignty, identity and access management (IAM), and cybersecurity modernization
- Assessment services to baseline existing protection and road map improvements to cloud, network, edge, and identity architectures
- Professional security services for incident response readiness, digital forensics, systems integration, and solution implementation and deployment, as well as frameworks and methodologies for efficient and effective service delivery
- Governance, risk, and compliance advisory services related to privacy, governance, risk, compliance, and cyberinsurance management
- Training services, including security awareness training, cyber-range services, and education on new technologies, frameworks, and practices
- Purpose-built tools to address strategic agency challenges, such as zero trust assessment and architecture design, and manage Continuous Diagnostics and Mitigation programs
- Demonstrated success delivering innovative solutions related to AI, 5G technologies, supply chain security, and/or quantum encryption, as well as solutions for protecting emerging technologies such as operational technology, IoT, and edge environments

- Formal partnerships with cloud service providers and technology solution vendors across security markets, including endpoint, network, cloud, application, and data security solutions, as well as identity, privacy, and hardware solution providers

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

Using its MarketScape model, IDC studied vendors that provide professional security services to state and local governments in the United States. The vendors IDC included in the study had to meet certain criteria to qualify for this vendor assessment:

- **Geographic presence:** Participating vendors must be based in the United States or must operate a subsidiary based in the United States.
- **Industry presence:** Vendors must have served the state and local government for at least three years.
- **Industry presence:** Vendors must offer a full suite of project-based professional security services, including consulting, incident management, implementation and integration, and GRC.
- **Government presence:** Vendors must be based in the United States or have a dedicated state and local government business unit with professional teams/SMEs, products/services, go-to-market strategy, and offerings specific to the U.S. state and local government.
- **Vendor agnostic:** The vendor's professional security services offerings must be vendor agnostic.
- **Provider agnostic:** This study excludes hyperscalers and pure-play management consulting firms.
- **Partnership:** Each vendor is required to have partnerships with at least one United States–based public cloud provider.

ADVICE FOR TECHNOLOGY BUYERS

The providers suited to improve technology and outcomes for U.S. state and local governments should demonstrate they have done so before. Providers will offer industry-specific services to meet unique government mandates, regulations, and compliance challenges. A wide range of ecosystem partners will also be key because most security service providers will need to work with partners across security markets to ensure sufficient protection. Further evaluation considerations include:

- **Prioritizing full IT environment visibility:** Achieving complete organizational visibility is a foundational component of understanding cybersecurity maturity and identifying gaps or risks. Organizations that do so lay the groundwork to improve protection in line with zero trust and Cybersecurity Maturity Model Certification (CMMC) frameworks.

- **Understanding your workforce capabilities and external labor needs:** Many resources are available to upskill workers, but the existing shortage of skilled technical staff cannot always be addressed through training. Many agencies need to offload security efforts to trusted third-party service providers. Others may work with providers to identify areas for improving efficiency or automating time-consuming tasks.
- **Utilizing federal government resources and services:** Organizations struggling to find capital resources to invest in modernization should identify federal government–provided services to supplement efforts at low cost. While there have been recent changes to the services CISA, the Defense Information Systems Agency (DISA), and other agencies provide, there are available services for security awareness training, incident preparedness, and evaluating security posture.
- **Establishing a priority-based approach with measurable CMMC and zero trust road maps:** Work with security service providers that have demonstrated success in developing and road mapping enterprisewide security programs. Both CMMC and zero trust frameworks are designed to guide agencies through security updates one step at a time. Providers can help prioritize these efforts to maximize impact and ensure consistent protection.
- **Embracing AI and automation:** AI and automation can greatly improve organizational efficiency and protection by automating monotonous tasks, enabling intelligent monitoring, and providing adaptable defensive capabilities. Suppliers should use these tools themselves to deliver services more quickly and cost-effectively. Still, organizations should proceed with caution as regulations governing the use of AI are still maturing. Eventually, generative AI (GenAI) and agentic AI will provide significant impacts through tools to generate playbooks for security staff, write policy rules, reverse engineer malware, and perform a variety of other tasks.

VENDOR SUMMARY PROFILE

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While IDC evaluates every vendor against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges.

Accenture

IDC has positioned Accenture in the Leaders category in this 2025–2026 IDC MarketScape for U.S. state and local government professional security services.

Background

Accenture employs about 791,000 people, including approximately 30,000 cybersecurity experts, with a specialized Public Service Cybersecurity practice serving clients in more than 120 countries. Its global Public Service practice counts approximately 125,000 dedicated practitioners. Accenture's cybersecurity service portfolio is built around the following capabilities:

- Cybersecurity industry — providing customers with experts who understand the resilience, risk, and compliance context of public service mission areas.
- Cybersecurity solutions — providing customers with methodologies and tools to accelerate modernization, improve business resilience, and optimize costs, including the following professional services areas: security modernization, critical infrastructure security, security function outsourcing (please note that managed security services are not part of this IDC MarketScape evaluation), and global capability center security to help customers build competencies and capacity.
- Cybersecurity services — providing the foundational services expertise at scale for:
  - Security risk and architecture
  - Identity security
  - Secure AI and agents
  - Secure digital core
  - Cyberphysical security
  - Cyberdefense
  - Cyber-resilience management

Accenture is also investing in frontier technology areas, such as advancing post-quantum security technologies, security of space systems, and continuous monitoring and incident response for agentic AI. Accenture supports the Multi-State Information Sharing and Analysis Center (MS-ISAC) for managed security services serving U.S. state and local government, as well as tribal and territorial government. Although a separate legal entity, Accenture Federal Services also provides an avenue to develop expertise. For example, the Cybersecurity and Infrastructure Security Agency's Cybersecurity Division Vulnerability Management Insights Branch enables Accenture to partner with the leading government cybersecurity entity in the U.S. to provide insights and guidance to proactively improve cybersecurity posture across the public sector and the private sector.

In addition to its cybersecurity technical expertise, Accenture maintains a strong focus on mission-specific expertise for state and local governments in social services, revenue, public health, education, cities transportation and infrastructure, and public safety. Accenture's mission-specific expertise helps customers implement cybersecurity solutions in line with operational reliability, regulatory compliance, and trust KPIs.

Accenture relies on both its own expertise and partnerships with technology vendors, such as Microsoft, Google, Palo Alto, CrowdStrike, AWS, and CyberArk. For instance, Google's Mandiant Threat Intelligence feeds are now embedded into Accenture's Adaptive Managed Extended Detection and Response (MxDR) to augment its cyber-resilience services. Accenture made a strategic investment, through Accenture Ventures, in QuSecure, a specialist in post-quantum cybersecurity. Additionally, Accenture continues to develop AI/GenAI and agentic AI solutions for industry, as well as cybersecurity.

Accenture maintains enterprisewide certification under ISO 27001 and ISO 27701. It aligns with the NIST Cybersecurity Framework (CSF) and CSA STAR Gold Level.

Strengths

- **Dedicated state and local government unit and go-to-market structure**: Accenture has a robust North American state and local government go-to-market business unit composed of sales teams, SMEs, and services tailored for cloud, security, and digital transformation for state and local government mission areas.
- **Talent depth**: Accenture's global workforce and dedicated cybersecurity experts provide depth to staff cybersecurity advisory, threat-hunting teams, compliance experts, and technical architects. This depth helps customers scale rapidly during incidents or modernization waves.
- **Strategic alliances and innovation**: Partnerships with global cybersecurity technology vendors enable Accenture to keep up-to-date threat intelligence, AI-driven detection, and incident response, as well as to explore innovative areas such as post-quantum cryptography and security of space systems.

Challenges

- **Cost and procurement complexity**: Although government-specific solutions and expertise can accelerate delivery, agencies may struggle to forecast the total cost of ownership of cybersecurity services contracts across strategy, resilience, protection, and physical security, given the breadth of Accenture's portfolio.

- **Federal-first solutions**: Many of Accenture's cybersecurity innovations are designed with federal government missions first in mind (FedRAMP Marketplace). State and local governments have different threat profiles, procurement rules, legacy systems, and regulatory regimes (e.g., varying CJIS, state privacy laws), requiring states to consider additional resources to be dedicated to adaptations.

Consider Accenture When

- State, local, tribal, and territorial (SLTT) governments need support with end-to-end cybersecurity transformation regardless of organization size, spanning multiple departments and the full life cycle of risk and vulnerability assessment, strategy, resilience and incident response, and knowledge transfer.
- SLTT governments need access to SLTT expertise and a technology partner ecosystem that brings innovative solutions in areas such as threat awareness and detection, automation of incident response, and readiness for post-quantum risks.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services, and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or the strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

IDC weighted capabilities criteria at 75% and strategy at 25% as state and local clients prioritize existing proven, operational excellence over forward-thinking road maps and plans.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores and, ultimately, vendor positions on the IDC MarketScape on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

IDC defines professional security services for this study as project-oriented services — including cybersecurity consulting; security strategy and architecture design; governance, risk, and compliance advisory; assessments and testing; systems and network design and integration; and custom application development and systems integration — delivered to enhance, modernize, and sustain cybersecurity capabilities across IT and operational technology environments. This includes IT consulting, network consulting and integration, custom application development, and systems integration. For this IDC MarketScape report, IDC will consider only project-oriented services directed at designing, assessing, implementing, and integrating cybersecurity programs, platforms, and controls to improve protection, resilience, and compliance within government operations.

IDC defines state/local governments as civilian departments delivering public administration missions, as described by NAICS code 92 and NACE code 84 (Section O), operating at the state and local level. This excludes federal and national departments and agencies, public educational institutions, public healthcare facilities, and public corporations such as utilities or transit authorities.

LEARN MORE

Related Research

- *IDC MarketScape: Worldwide AI Services for State and Local Government 2025 Vendor Assessment* (IDC #US53009325, October 2025)
- *IDC Presentation: Worldwide GenAI Industry Use Case Early Adoptions Trends, 2025: Smart, Sustainable Cities and Communities* (IDC #US53099725, May 2025)
- *IDC MarketScape: U.S. Federal Government Cloud Professional Services 2024 Vendor Assessment* (IDC #US49996223, April 2024)

Synopsis

This IDC study evaluates professional security services (PSS) vendors for state and local governments, highlighting their strategies, capabilities, and alignment with evolving cybersecurity mandates. It emphasizes the growing investment in security consulting, assessment, and implementation services designed to protect government infrastructure, data, and operations. IDC assesses vendors on their ability to strengthen cyber-resilience, modernize security architectures, and support compliance with federal, state, and local regulations. The report underscores the importance of proactive threat management, governance and risk frameworks, and secure integration of emerging technologies in enabling trusted, resilient digital government environments.

"U.S. state and local governments are working on a wide range of modernization and protection initiatives to protect their data, ensure privacy, and deliver mission success. Organizations need trusted partners capable of providing a wide range of solutions developed specifically for state and local governments and including the range of services from advisory and assessment to incident response and purpose-built tools," said Ruthbea Yesner, vice president, Government Insights, Education and Smart Cities at IDC.

ABOUT IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com

Copyright and Trademark Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, and web conference and conference event proceedings. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/about/worldwideoffices. Please contact IDC at customerservice@idc.com for information on additional copies, web rights, or applying the price of this document toward the purchase of an IDC service.