IDC MarketScape

IDC MarketScape: U.S. National Government Professional Security Services 2024 Vendor Assessment

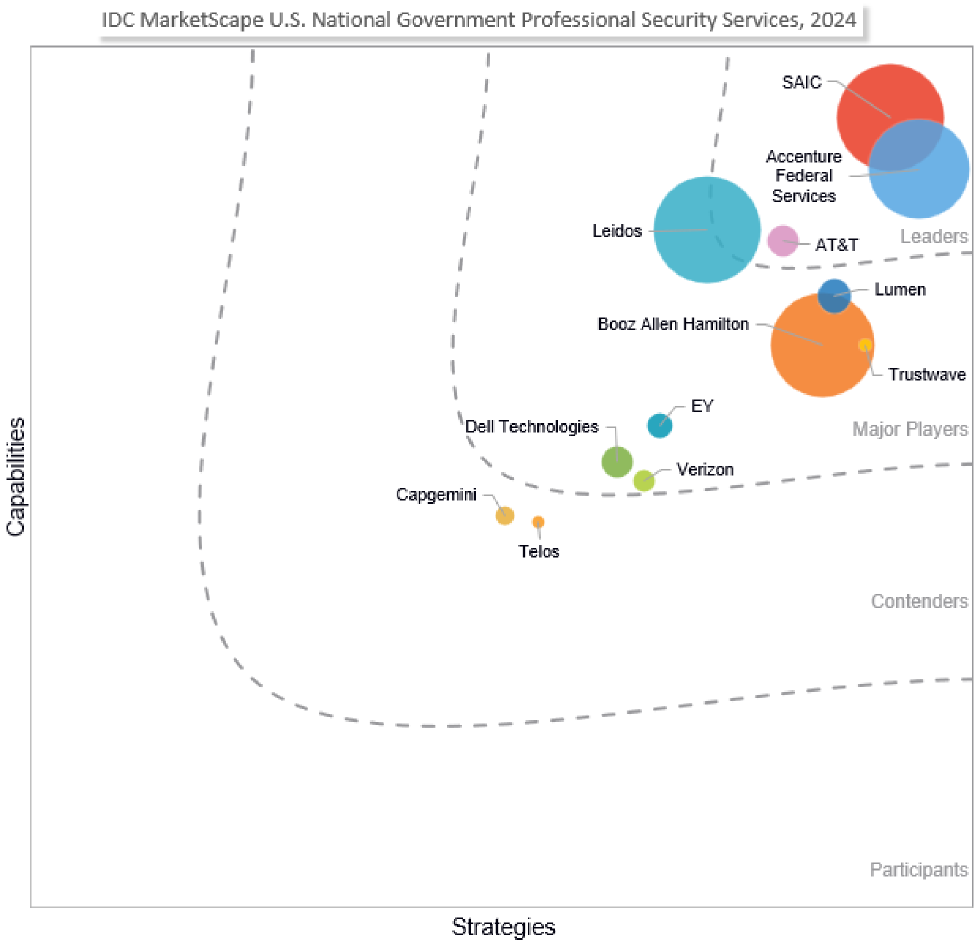
Aaron Walker

THIS IDC MARKETSCAPE EXCERPT FEATURES LUMEN

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape U.S. National Government Professional Security Services Vendor Assessment



Source: IDC, 2024

February 2024, IDC #US51875423e

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

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: U.S. National Government professional Security Services 2024 Vendor Assessment (Doc # US51875423). All or parts of the following sections are included in this excerpt: IDC Opinion, IDC MarketScape Vendor Inclusion Criteria, Essential Guidance, Vendor Summary Profile, Appendix and Learn More. Also included is Figure 1.

IDC OPINION

Cybersecurity practices and services continue to evolve in response to emerging technologies and an expanding attack surface resulting from the rapid adoption of IoT devices and hybrid and multicloud environments and the proliferation of APIs and cloud services. 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 across markets — particularly in the federal government space as agencies typically provide less pay, benefits, and flexibility than the private sector workforce.

The modern cybersecurity service engagement can be incredibly complex and can impact every component of an agency's IT ecosystem, especially when working to have security built into IT environments rather than bolted on. Emerging technologies paint a picture of complete, intelligent protection, while threats to the nation's technology and infrastructure paint the opposite. Much effort is needed to demystify the threats facing federal agencies in the United States. And agencies 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 the federal government. In addition, agencies are seeking assistance from providers with deep partner ecosystems across security and cloud infrastructure markets to achieve holistic security transformation in line with the required efforts outlined in federal mandates.

It should also be noted that several companies evaluated in this document have had breaches in recent years exposing government data and personally identifiable information (PII). The companies in this document have all provided required breach notifications and cooperated or are cooperating with federal investigators. It is important that agencies ensure their partners have a track record of properly reporting, investigating, and remediating data breaches as they occur.

The concepts that were found to be the key drivers impacting the market's evolution include:

- **Increased attack surface.** IoT and operational technology (OT) are two of the largest contributors to attack surface expansion. 5G networks and increases to data in motion have compounded the challenge, making it difficult for agencies to achieve full organizational visibility. Agencies 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. Agencies have struggled to recruit skilled workers from private sector technology companies capable of providing higher wages, added benefits, and more flexible working conditions.

- **Unfunded mandates and required action.** Executive action taken by the U.S. government, and the Biden administration in particular, has added new priorities to agencies that were already working to modernize. Executive Order 14028, Improving the Nation's Cybersecurity, and Executive Order 14017 on America's Supply Chains require action be taken to improve national cybersecurity but do so without directly allocating financial resources to federal agencies.

Using the IDC MarketScape model, IDC studied 12 organizations that offer professional security services (PSS) to U.S. federal agencies from 2022 to 2023 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. federal agencies 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), cybersecurity modernization, and supply chain resilience
- 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
- 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, achieve continuous authority to operate (ATO), and manage Continuous Diagnostics and Mitigation (CDM) programs
- Demonstrated success delivering innovative solutions related to artificial intelligence (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 the IDC MarketScape model, IDC studied vendors that provide professional security services throughout the world. The vendors 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 national government for at least five years.
- **Industry presence:** Vendors must offer a full suite of project-based professional security services including consulting, incident management, implementation and integration, and governance, risk, and compliance.

- **National presence:** Vendors must be based in the United States or have a dedicated federal government vertical business unit with professional teams/SMEs, products/services, go-to-market strategy, and offerings specific for the federal government.
- **Vendor agnostic:** The vendor's professional security services offerings must be vendor agnostic.
- **Provider agnostic:** Exclusions include hypervisors (e.g., Microsoft, AWS) and management consulting firms (e.g., BCG, McKinsey).
- **Partnership:** Each vendor is required to have partnerships with at least one United States-based public cloud provider.

ADVICE FOR TECHNOLOGY BUYERS

When evaluating professional security service providers, consider partnering with providers capable of delivering a wide range of services directly related to the common challenges facing U.S. federal agencies. The providers best suited to improve technology and outcomes within the federal government should demonstrate they have done so before. Top-tier providers will even offer industry-specific services to meet unique government mandates, regulations, and compliance challenges. A wide range of ecosystem partners will also be key as most security service providers will need to work with partners across security markets to ensure sufficient protection. Further:

- **Prioritize full IT environment visibility.** Achieving complete organizational visibility is a foundational component of understanding cybersecurity maturity and identifying gaps or risks. Agencies that do so lay the groundwork for mandated efforts related to improving protection in line with zero trust and Cybersecurity Maturity Model Certification (CMMC) frameworks.
- **Understand 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 to improve efficiency or automate time-consuming efforts.
- **Utilize agency resources and services.** Federal agencies struggling to find capital resources to invest in modernization should identify services provided by the federal government to supplement efforts without breaking the bank. Numerous services provided by CISA, the Defense Information Systems Agency (DISA), and other agencies are available for security awareness training, incident preparedness, and evaluating security posture.
- **Establish a priority-based approach with measurable CMMC and zero trust road maps.** Agency leaders should work with security service providers that have demonstrated success 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.
- **Embrace AI and automation.** AI and automation can greatly improve organizational efficiency and agency protection by automating monotonous tasks, enabling intelligent monitoring, and providing adaptable defensive capabilities. Still, agencies should proceed with caution as regulations governing the use of AI are still emerging. Eventually, generative AI (GenAI) will provide significant impacts with tools to generate playbooks for security staff, write policy rules, and reverse engineer malware.

VENDOR SUMMARY PROFILES

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

Lumen

Lumen is positioned in the Major Players category in this 2024 IDC MarketScape on professional security services for the U.S. national government.

Quick facts about Lumen include:

- **Employees:** 29,000+
- **Years in business:** 94
- **Ecosystem/alliances:** AWS, Microsoft, Google Cloud, Palo Alto, Zscaler, Fortinet, Cisco

Lumen Technologies leaders believe the largest challenges facing federal agencies today include the growing complexity of networks, the expanding threat landscape, compliance requirements, and legacy environment constraints. Lumen offers assessment, planning, design, and deployment capabilities to address virtually any modernization or protection initiative. Lumen is working to continuously simplify and integrate offerings, bolster threat intelligence, and increase access to on-demand retainer services.

Lumen's professional security services include custom security solution development, testing, deployment, integration, and support for large federal civilian agencies and SLED customers in the public sector. In addition to the standard product components offered under the EIS contract, Lumen Professional Services include incident response, risk management, penetration testing, vulnerability scanning, forensic analysis, security assessments, log management, threat correlation against the Black Lotus Labs threat feed, and threat hunting; Lumen offers assessments for security architectures, vulnerabilities, compliance readiness, privacy, risk, business impact, and security program and control. Lumen's managed security services include managed SOC, security information and event management (SIEM), firewall, DDoS protection, TICS, EDR, secure access service edge (SASE), and managed trusted internet protocol services (MTIPS). Lumen also operates Black Lotus Labs, its threat intelligence arm.

Strengths

- Lumen offers a wide range of services across professional services, consulting, and GRC capabilities. Lumen's range of services includes advisory engagements for planning and assessment of all current-state systems from data and privacy to cloud and network components. Project-based efforts include design, implementation, and deployment of most major solution categories. And managed services range from vulnerability, identity, and log management to engineering and program management.
- Networking capabilities are inherently strong based on Lumen's origin as a pure-play network service provider across industries. In terms of security, Lumen has robust offerings for implementing zero trust and secure access service edge architectures, a standard most agencies are working toward.
- Innovation is a strength as Lumen can deliver numerous innovative solutions and protection for emerging technologies. Zero trust and SASE offerings lead the way for network defense.

On the road map are IoT and OT solutions for secure privileged access, XDR to address multicloud threats, AI to increase efficiency and efficacy, and supply chain security to reduce risk.

- Industry participation is a strength for Lumen; the company's executives hold numerous leadership positions in industry organizations. Lumen is involved with CISA's Joint Cyber Defense Collaborative, the President's National Security Telecommunications Advisory Council, and the Federal Communications Commission's Communications Security, Reliability, and Interoperability Council (CSRIC), among others.
- Lumen has purpose-built solutions to improve compliance management through a streamlined authorization service called Lumen Authority to Operate (ATO) as a Service. The offering is aligned with NIST 800 to streamline, but not automate ATO security authorization processes. Lumen's STIG Hardening Services can also help agencies reduce the company's attack service, improve protection, and maintain authority to operate.

Challenges

- Lumen has market presence but much less share in the U.S. federal market than many competitors in the document. Lumen has comparable overall government contracting at over $1 billion annually, according to the Federal Procurement Data System, but much of that is from internet and networking services rather than professional security services.
- Lumen can successfully address many compliance challenges and supports most regulatory frameworks, but the company does not provide specific services for achieving continuous authority to operate, managing CDM requirements, or managing FIPS. Still, Lumen supports compliance services with frameworks and standards that include PCI DSS, HIPAA, ISO 27001, FedRAMP FISMA, NIST, SP800-53, GDPR, and CCPA.

Consider Lumen When

- With less than 5ms latency for 95% of U.S. customers and numerous success stories providing connectivity solutions for federal agencies, Lumen should be strongly considered for network security modernization efforts. Lumen has also demonstrated success in securing connections to critical information apps and developing secure cloud-based VOIP systems.
- Lumen is well qualified to support full SASE implementation featuring software-defined wide area networking (SD-WAN). Lumen offers both professionally managed and self-managed SASE offerings delivered in partnership with either Fortinet, VMware, or Versa Networks and potentially others in the future.
- Federal agencies that are struggling to maintain an adequate cybersecurity workforce should consider Lumen for both SOC modernization and incident response services. Lumen's virtual SOC provides 24 x 7 SIEM monitoring, incident handling, and remediation recommendations. The company's on-demand retainer services include emergency incident response services, security leadership advice, and assistance leveraging emerging technologies.

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, here and now. 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 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 this IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed. For this IDC MarketScape, vendor size represents market share within the U.S. federal civilian agency market and was determined by data in publicly available tax documents, Washington Technology's 2021 and 2022 largest government contractors report, and IDC's Worldwide Semiannual Services Tracker.

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

This IDC MarketScape provides a vendor assessment of security professional services at the U.S. federal civilian government level (primarily security advisory, security assessment, and awareness services). The companies must be based in the United States because of U.S. federal requirements. The referenced professional security services include security strategy and planning, compliance and auditing, security policy assessment and development, vulnerability tests, penetration testing, network architecture assessment, and incident response planning and forensics. For the purpose of this study, the professional security services exclude the implementation services that often refer to the installation and configuration services of security software or hardware products.

LEARN MORE

Related Research

- *IDC PeerScape: Free Federal Cybersecurity Resources Practices to Manage Agency Regulation* (IDC #US51365123, November 2023)
- *AI and Cybersecurity in Federal, State, and Local Governments* (IDC #US51309423, November 2023)
- *IDC FutureScape: Worldwide National Government 2024 Predictions* (IDC #US50296223, October 2023)

- *Top 5 Technology Trends to Watch in National Cybersecurity and Privacy, 2023* (IDC #US51204823, September 2023)
- *IDC's Worldwide Digital Transformation Use Case Taxonomy, 2023: National Civilian Government* (IDC #US49229623, August 2023)
- *IDC PlanScape: Leveraging AI to Address the Skills Gap in Federal Agencies* (IDC #US50308423, June 2023)
- *Software Supply Chain Security in U.S. Federal Government* (IDC #US50518323, April 2023)

Synopsis

This IDC study highlights the evolving cybersecurity landscape due to emerging technologies and the rapid adoption of IoT devices and hybrid and multicloud environments and the proliferation of APIs and cloud services. This document emphasizes the need for agencies to partner with experienced providers to address these challenges and achieve holistic security transformation. It also notes the importance of properly reporting, investigating, and remediating data breaches. Key market drivers include the increased attack surface due to IoT and operational technology, a shortage of skilled cybersecurity professionals, and unfunded mandates and required action.

"Federal agencies are managing a wide range of modernization and protection initiatives to ensure mission success and protect the nation's data. Agencies need trusted partners capable of providing a wide range of solutions developed specifically for the challenges federal agencies face," said Aaron Walker, research manager for Worldwide Government Trust, Security, and Resilience program at IDC. "The most comprehensive services portfolios include cybersecurity advisory services; assessment services; professional security services for incident response readiness; governance, risk, and compliance (GRC) advisory services; training services; and purpose-built tools."

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