IDC Government Insights: Worldwide Government Security, Climate and Resiliency Strategies

Resiliency in government increasingly hinges on a balanced approach to managing risks, emphasizing both climate resiliency and cybersecurity technologies. This includes edge devices, Internet of Things (IoT), digital twins, 5G, and the networks that tie everything together. It also highlights the importance of systems integrators that build complex solutions and ensure the security and resiliency of these solutions as well as the use of AI and GenAI as force multipliers. Increasingly, government systems are coming under attack by bad actors. The security of IT infrastructure is becoming paramount, especially as edge computing systems rapidly evolve. The *IDC Government Insights: Worldwide Government Security, Climate and Resiliency Strategies* program focuses on tracking government technologies pivotal to organizational resilience, climate risk, and cybersecurity to address critical issues facing governments as they manage escalating threats from malicious actors and mitigate climate-related risks. This includes a qualitative and quantitative analysis of key trends, investment priorities, and tech adoption by national, state, and local governments globally. This program provides best practice case studies and objective third-party assessments of solution providers to enable informed strategic decision-making for addressing immediate and long-term challenges in climate resiliency and securing publicly maintained critical infrastructure systems.

APPROACH

This *IDC Government Insights: Worldwide Government Security, Climate and Resiliency Strategies* program is a research advisory service that studies how government infrastructure and advanced technologies can be leveraged to implement and support powerful agency-level trust and resiliency initiatives. This service features government data and analysis based on government surveys and use case studies focused on agency outcomes.

This program delves into the evolving dynamics of government IT systems, focusing on climate resiliency and cybersecurity technologies. It explores the deployment of IT assets across government enterprises, including on-premises and hybrid cloud infrastructure and AI tools as well as the adoption of software-defined networks and systems. These technologies are pivotal in securely navigating the complexities of the modern government IT landscape, ensuring both the protection against cyberthreats and the integration of sustainable practices to foster climate resilience.

TOPICS ADDRESSED

Throughout the year, this service will address the following topics:

- How government agencies and IT vendors can work together to further trust and resiliency in enterprise IT security, sustainability, zero trust connections, network management, edge computing, and connected devices/IoT.
- How government agencies can ensure availability and continuity of services to build trust with the public.
- How public sector organizations and trusted private sector partners can leverage technology to help the populations they represent stay safe from sea level rise, extreme heat, and other environmental factors.
- Global cybersecurity policies drive adoption of tools like SASE, a key component of next-generation network and device security technologies, which combines a variety of technologies including firewalls, intrusion prevention systems, secure web gateways (SWGs), cloud access security broker (CASB), data loss prevention (DLP), and zero trust network solutions.
- How governments are obtaining trust by improving data accuracy and security posture through solutions such as observability, attack surface management, threat intelligence, and secure system access control.

KEY QUESTIONS ANSWERED

Our research addresses the following issues that are critical to your success:

1. How will major systems integrators and service providers evolve their government portfolios and market positions in the coming years?
2. What role government organizations play in ensuring a resilient and sustainable future in the face of climate change?
3. How are trends in the government marketplace, including innovation accelerators such as security, IoT, the secure edge, zero trust, and 5G, affecting buyer priorities, and how should vendors respond?
4. Which vendors are most effectively addressing emerging government system market demands and customer priorities?

WHO SHOULD SUBSCRIBE

This service is designed to aid security and enterprise social governance leaders, offering comprehensive research for agency decision-makers and technology vendors seeking an in-depth understanding of the government IT market and its evolving trends. It is particularly valuable for IT systems integrators and professional services providers, who are at the forefront of designing and constructing these secure and resilient environments. The service delves into industry best practices to foster trust and enhance agency resilience, providing insights into market sizing and spending trends that are essential for IT product and service planners and sales teams aiming to navigate the complexities of government IT with a focus on security and governance.