

Building Resilient Digital Government Across Asia/Pacific



Massimiliano Claps
Research Director, IDC



Ravikant Sharma
Research Director, IDC



Table of contents



Click any title to navigate directly to that page.

Executive summary	3	Resilience maturity: AP market clusters	12
Resilience as a strategic imperative	4	Key recommendations for tech leaders	13
The expanding threat landscape	5	Looking ahead: From planning to operations	14
IDC digital resilience framework	6	About the IDC analysts	15
Securing the core: Defense in depth	7	Message from the sponsor	16
AI: Expanding both threats and defenses	8		
Governance and execution gaps	9		
Sovereign cloud: The new resilience pillar	10		
Building secure-by-design government	11		

Executive summary



Resilience anchors digital transformation.

AP governments are accelerating modernization, but resilience, cybersecurity, and digital sovereignty are now foundational requirements. Internal resilience and critical infrastructure protection rank among the top five strategic priorities for governments across the region over the next two years.



Governance and skills gaps constrain progress.

Budget pressures, tool complexity, and cyberskills shortages fragment security architectures. Decentralized decision-making and regulatory burden delay execution, creating persistent gaps between cybersecurity strategy and operationalization across ministries.



Escalating threats demand urgent action.

Eighty-nine percent of AP government organizations reported ransomware attacks in the past year, outpacing the 77% rate across other industries. AI-enabled threats such as automated phishing, deepfakes, and model manipulation are rapidly expanding the public sector attack surface.



Sovereignty and secure-by-design are the next frontier.

Forty-five percent of AP governments are prioritizing sovereign cloud for AI workloads. The region's next modernization phase requires a shift toward secure-by-design architectures, zero trust operating models, and cross-border threat collaboration.



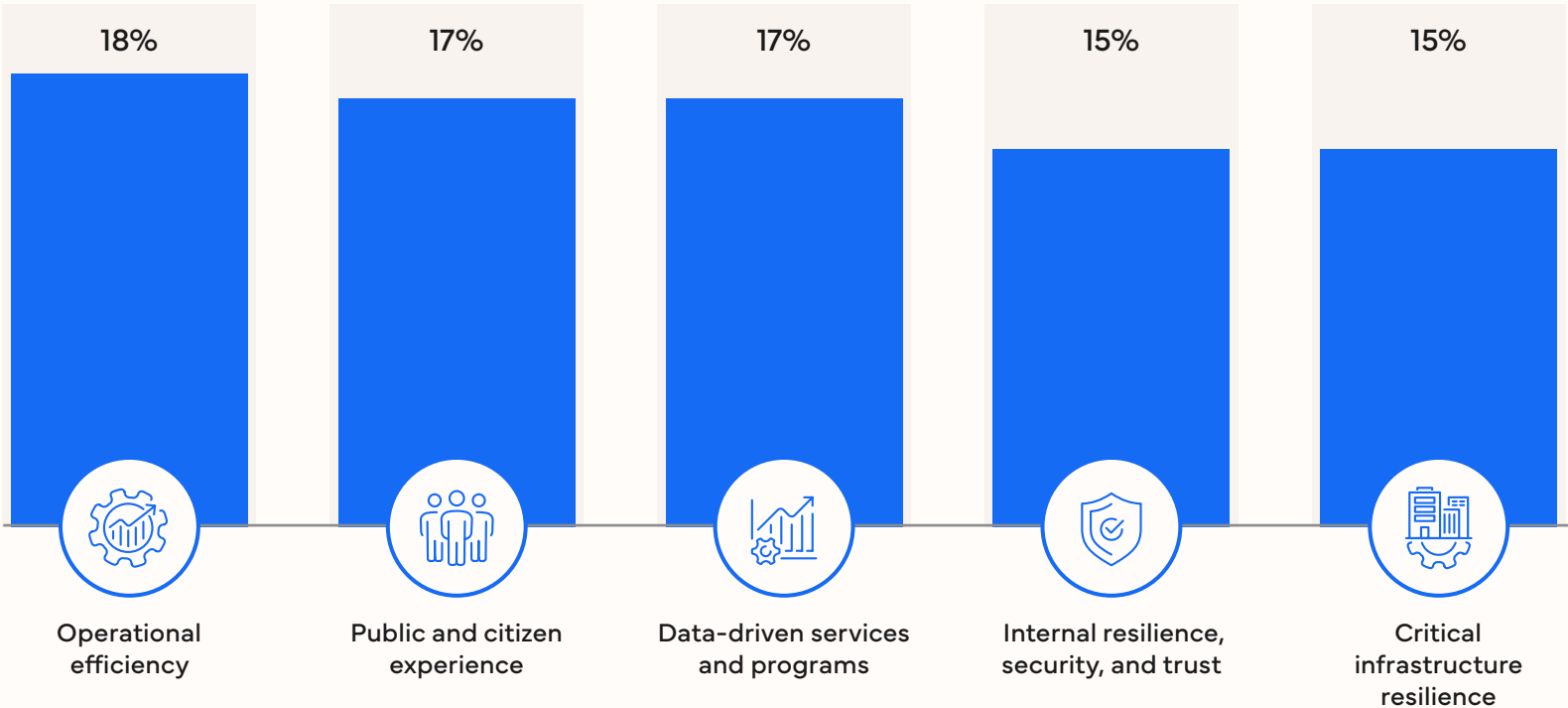
Resilience is now a top government priority



Over the next two years, AP governments will intensify their focus on operational efficiency, citizen engagement, and data-driven services to accelerate modernization.

Critically, **internal resilience and critical infrastructure resilience rank among governments’ top five priorities**, signaling that secure, reliable, and adaptive government foundations are viewed as essential to sustaining digital transformation.

AP government top priorities [% selecting as top priority]



Source: IDC’s Industry Intelligence — Government Survey 2025; Australia, India, Japan, Korea, New Zealand, Singapore (n = 262)

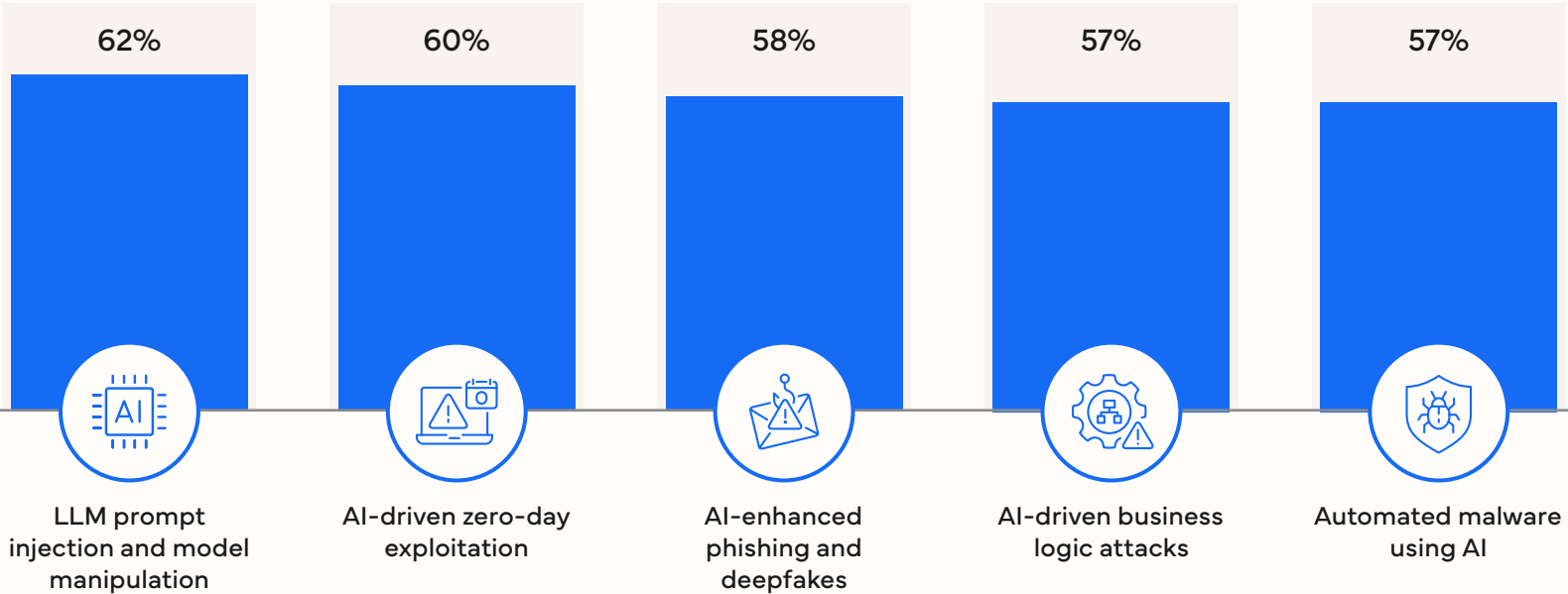
Governments are high-value targets in an AI-expanded threat landscape



of AP government organizations experienced ransomware attacks in the past year, versus 77% across other industries.

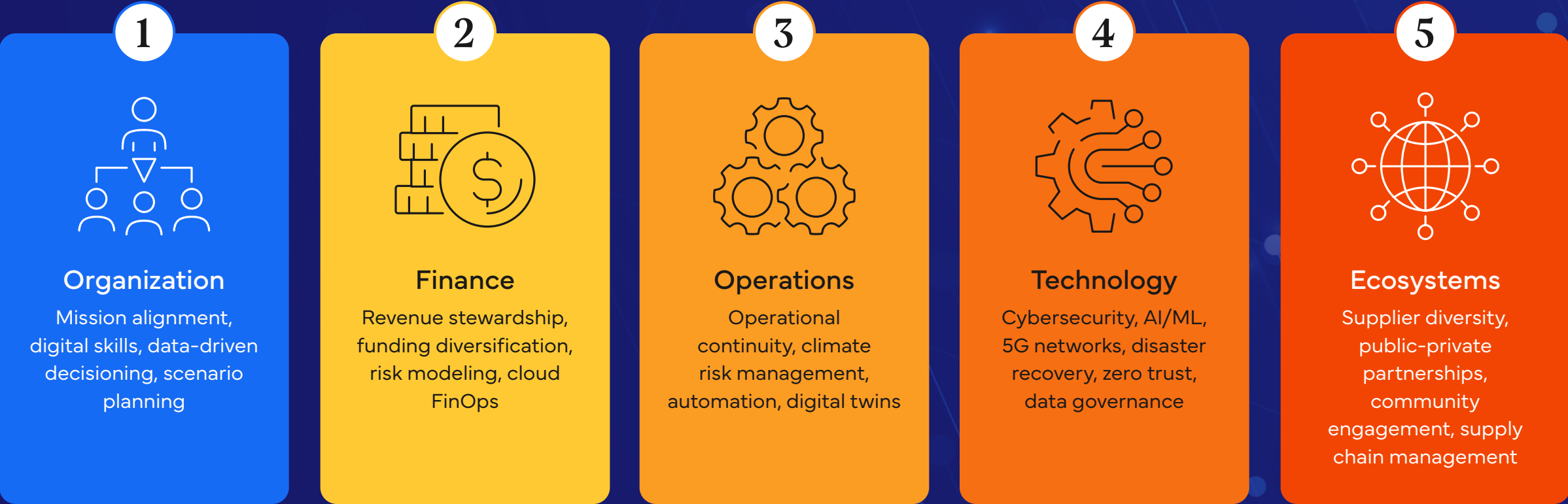
AI-enabled threats are widening the public sector attack surface. Governments must embed adaptive, intelligence-driven defenses combining AI-powered threat detection and real-time intelligence sharing to stay ahead of rapidly emerging attack vectors.

Top AI-driven threats concerning AP governments [% concerned]



Sources: IDC's FERS Survey Wave 5, 2025; IDC's AP Security Study, 2025

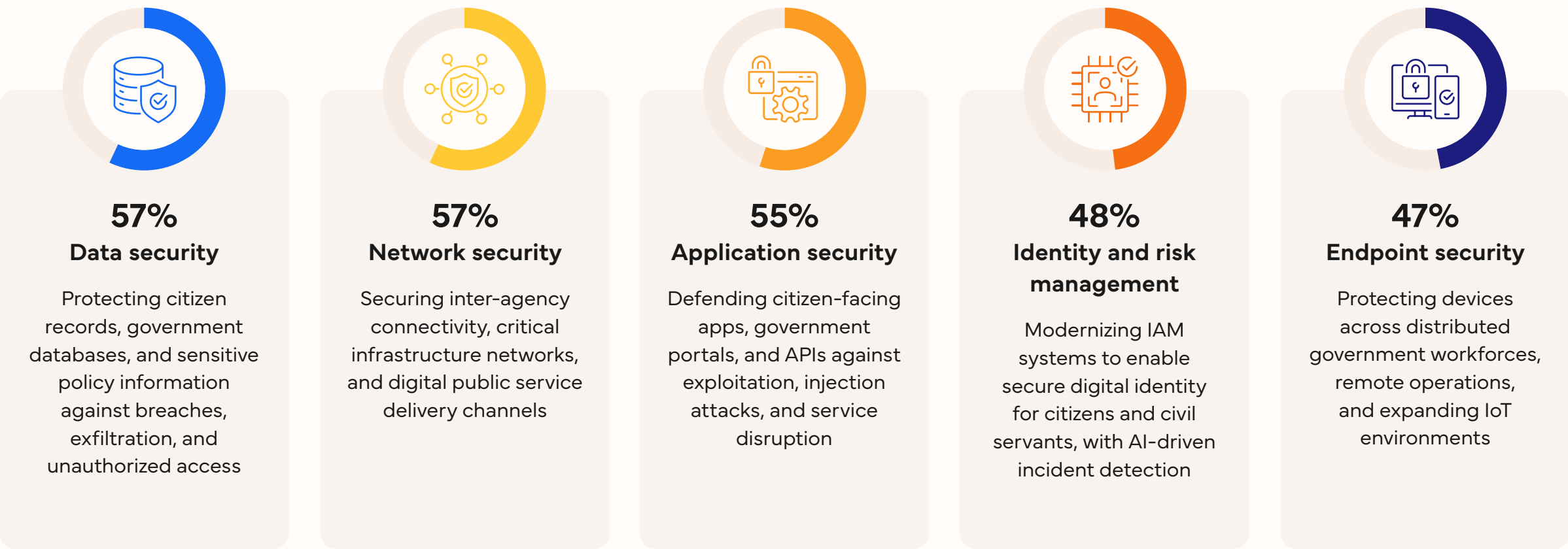
IDC’s government digital resilience framework



Source: IDC's Governmental Digital Resilience Framework 1.0

Securing the core: A defense-in-depth approach

AP governments are reinforcing existing security foundations across five core domains, reflecting a defense-in-depth strategy focused on optimization and resilience rather than adopting unproven tools.



Source: IDC's Industry Intelligence — Government Survey 2025; % already using solution (n = 262)

AI: Expanding both threats and defenses



AI adoption in government security

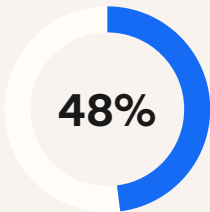


73% of AP government organizations have already invested in AI/GenAI, with deployments increasingly embedded in integrated threat management and critical infrastructure protection.

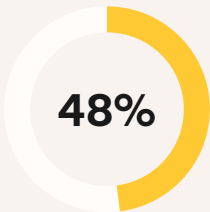
Key AI security use cases include real-time threat detection, AI-powered incident response, ML-assisted web application firewall, and continuous vulnerability monitoring.

Source: IDC's Industry Intelligence — Government Survey 2025 (n = 262)

Barriers to AI security adoption



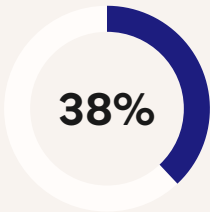
Lack of trusted vendors and verified solution providers



Regulatory uncertainty around AI security governance



Concerns about transparency, compliance risks, and AI hallucinations



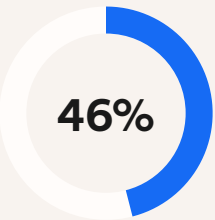
Integration challenges with legacy security stack

AP security study 2025

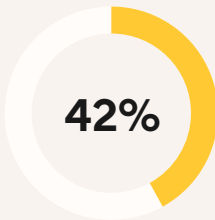
Source: IDC's AP Security Study 2025 (n = 65)

Governance and execution gaps constrain resilience

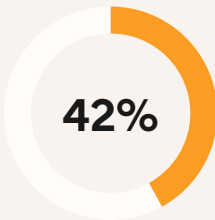
Structural integration barriers



Cost and budget restrictions on cybersecurity tooling



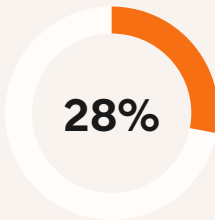
Complexity from AI/automation layers within existing stacks



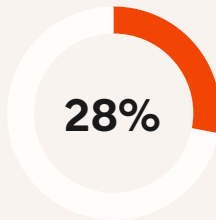
Lack of in-house skills to manage integration

These structural barriers fragment security architectures and impede the operationalization of resilience strategies across government ministries.

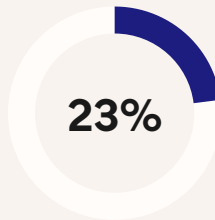
Internal governance constraints



Security decisions being made outside the region/country



Navigation of complex and fragmented regulatory requirements

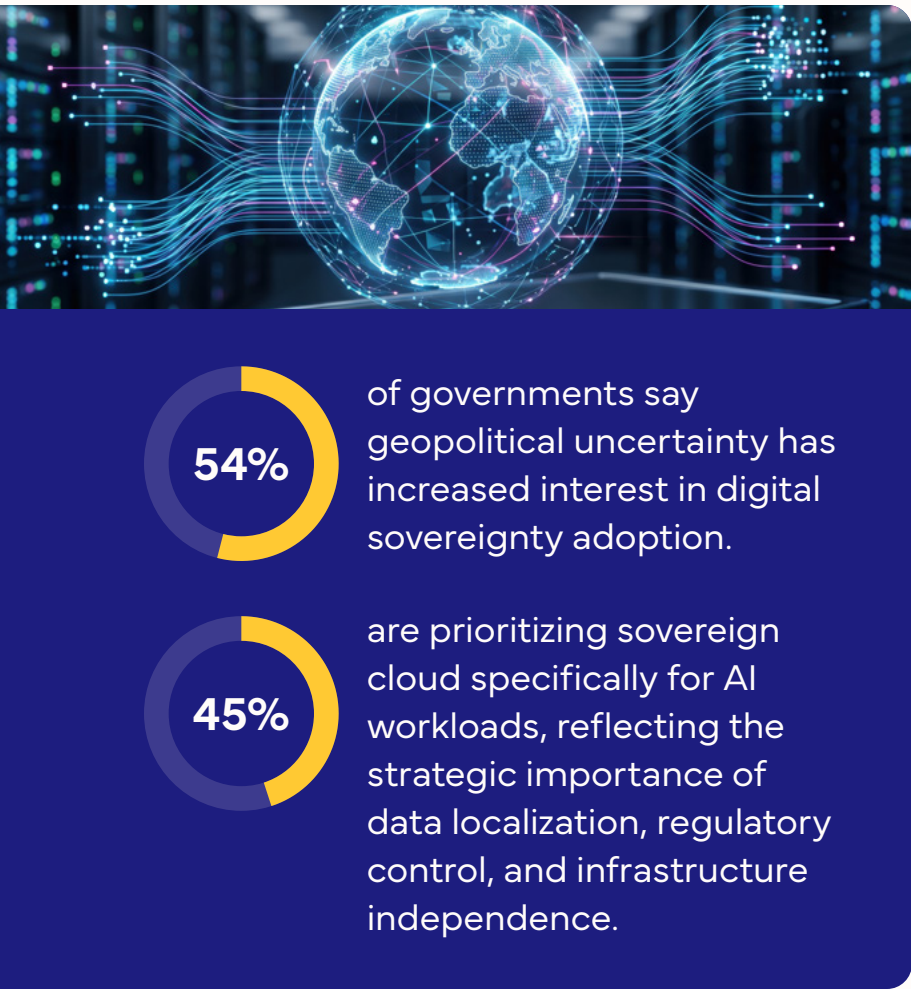


Limited executive sponsorship or prioritization of security

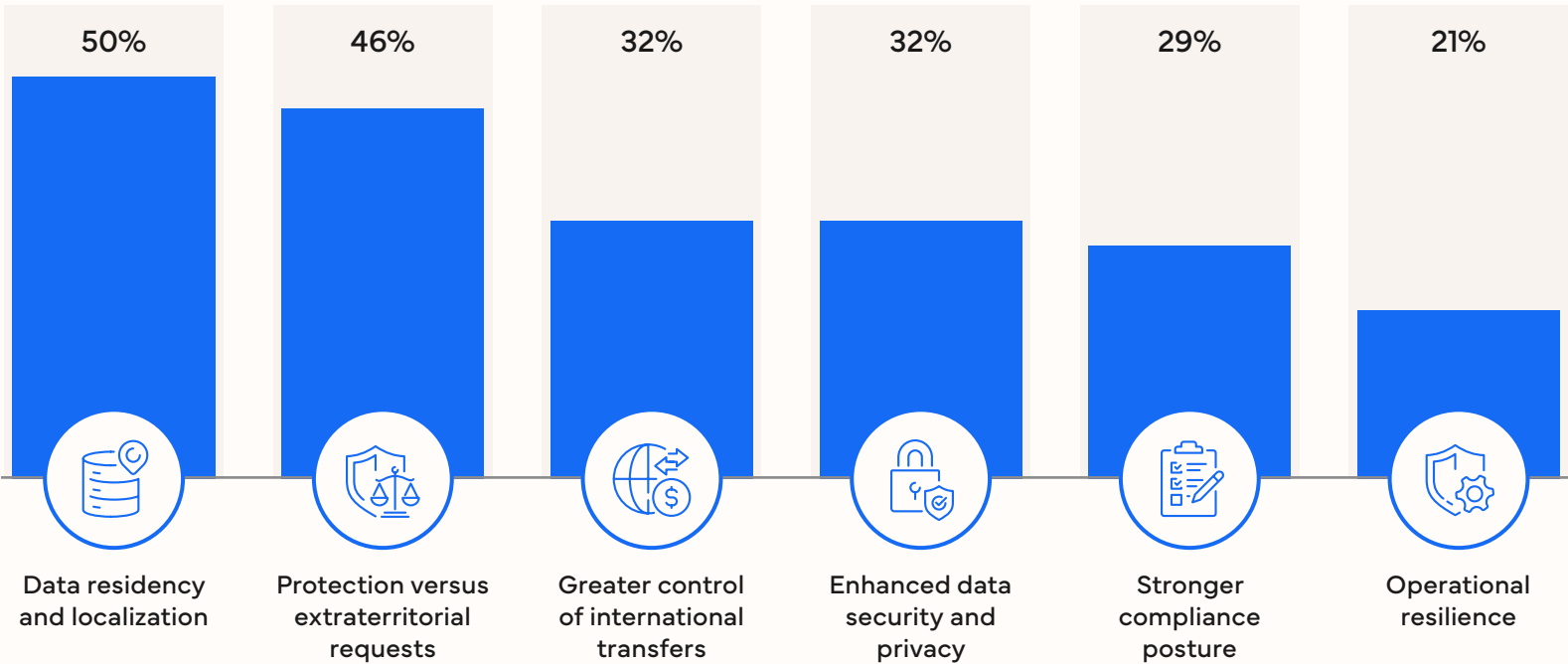
Governments must adopt simplified, interoperable security platforms and empower localized, accountable cybersecurity governance, aligning funding, skills, and decision authority with operational risk realities.

Source: IDC's AP Security Study 2025 (n = 65)

Sovereign cloud: The new resilience pillar



Top advantages of sovereign cloud adoption (%)



Source: IDC's Industry Intelligence — Government Survey 2025; Australia, India, Japan, Korea, New Zealand, Singapore (n = 262)

Building secure-by-design government

Where governments are today

Cybersecurity spending across the region remains largely **risk-driven and defensive**, responding to threats and compliance mandates rather than re-architecting resilience from the ground up.

Top investment drivers cited by governments reflect this reactive posture:



37%
Increase in
cyberthreats and
attacks



36%
Evolving citizen
expectations around
privacy



32%
Regulatory
requirements driving
compliance spend

Source: IDC's Industry Intelligence — Government Survey 2025 (n = 262)

The shift required

The next phase of government digitalization demands a fundamental re-orientation from security as a response mechanism to security as an architectural principle embedded in every initiative from the outset.

- ➔ **Secure-by-design architectures:** Designing in resilience, not bolting it on
- ➔ **Zero trust operating models:** Replacing perimeter-based thinking with continuous verification
- ➔ **AI assurance frameworks:** Ensuring trustworthy, explainable, and bias-free government AI
- ➔ **Cross-border threat collaboration:** Sharing intelligence to protect regionally interdependent digital infrastructure
- ➔ **Edge-distributed infrastructure:** Reducing dependency on centralized cloud concentration and single points of failure

Resilience maturity across Asia/Pacific market clusters

IDC segments AP public sector markets by digital maturity and sovereignty orientation.



Singapore and Australia

Advanced digital maturity |
Open to innovation

Innovation-led resilience

These regions have high digital maturity, performance-driven procurement, and strong innovation culture. PDPA/IM8 (Singapore) and IRAP (Australia) compliance are non-negotiable gating criteria. These regions benchmark against hyperscaler-native stacks and have a focus on co-innovation, ML-assisted WAF, and API security expansion.



Japan

Advanced digital maturity |
Sovereignty-centric

Trust-governed sovereign

Japan has high digital maturity but strong domestic orientation. ISMAP and APPI accreditation determine vendor eligibility. SI-led architecture recommendations shape all vendor selection. This requires deep localization, patient trust-building, and vendor-agnostic multicloud positioning.



India and Indonesia

Emerging digital maturity |
Sovereignty-centric

Sovereignty-led digital infrastructure

These regions have rapid digital expansion paired with strong localization mandates (India DPDP Act, Indonesia GR 71/2019) and a preference for domestic alignment and cost stability. They focus on compliance-aligned architecture, in-country PoPs, and interoperability with digital public infrastructure.



Malaysia and Thailand

Emerging digital maturity |
Open

Value-led digital expansion

These regions are developing digital ecosystems with budget sensitivity and are open to foreign vendors but price-conscious. Security maturity varies by ministry. Foundational security (DDoS, WAF) is the entry point. City-building workshops and TCO comparisons against hyperscalers accelerate adoption.

Key recommendations for technology leaders

- 1** **Treat resilience as infrastructure, not an add-on.**
Embed cybersecurity, continuity planning, and sovereign alignment into the architecture of every new digital government service. Resilience is not a project but a design principle.
- 2** **Consolidate from fragmented tools to integrated platforms.**
Replace siloed point solutions with interoperable security platforms that span data, network, application, and identity layers. Simplicity reduces gaps and lowers the skills burden on stretched government teams.
- 3** **Prioritize identity modernization as the new perimeter.**
With cloud-based citizen services eliminating traditional network perimeters, IAM and zero trust principles are the new security backbone. Invest in AI-assisted identity and incident management as a foundation.
- 4** **Build sovereign cloud and compliance into procurement criteria.**
Data localization, in-country infrastructure, and vendor certification alignment (ISMAP, IRAP, and IM8/PDPA) should be formal procurement requirements, not afterthoughts.
- 5** **Shift from reactive defense to secure-by-design architecture.**
Move beyond threat response toward proactive resilience. Mandate secure-by-design architecture for all new digital public infrastructure, embed AI assurance frameworks, and establish cross-border threat intelligence sharing.
- 6** **Close the skills and governance gap through structured investment.**
Partner with industry to establish cybersecurity academies, localized training programs, and clear governance accountability. Decentralized decision authority must be replaced by empowered, accountable security leadership.



Looking ahead: From resilience planning to resilience operations

Asia/Pacific governments stand at a critical inflection point. The foundations of digital government (citizen services, data infrastructure, and AI-enabled policy) are now inseparable from the question of resilience. The threats are real, the gaps are documented, and the pressure to act is mounting from every direction amid geopolitical volatility, evolving regulatory frameworks, and adversaries' rapidly changing capabilities.

The next phase is not about planning for resilience but about operationalizing it. This means moving from reactive cyberdefense to continuous, proactive resilience management, including zero trust architectures that adapt to shifting threat surfaces, AI assurance frameworks that keep public sector AI trustworthy and secure, sovereign cloud deployments that give governments control without sacrificing capability, and cross-border intelligence sharing that treats regional interdependence as a strength, not a vulnerability.

The governments that will lead this transition are those that choose the right technology partners: those who understand regional regulatory complexity, invest in a local presence, and can integrate seamlessly with evolving national digital architectures. **Resilient government is not a destination but a continuous capability.**



About the IDC analysts



Massimiliano Claps
Research Director, IDC

Massimiliano (Max) Claps is the research director for the Worldwide National Government Platforms and Technologies research in IDC’s Government Insights practice. In this role, Max provides research and advisory services to technology suppliers and national civilian government senior leaders in the US and globally. Specific areas of research include improving government digital experiences, data and data sharing, AI and automation, cloud-enabled system modernization, the future of government work, and data protection and digital sovereignty to drive social, economic, and environmental outcomes for agencies and the public.

[More about Massimiliano Claps →](#)



Ravikant Sharma
Research Director, IDC

Ravi Kant Sharma serves as the Research Director for Government Insights for Asia/Pacific (excluding Japan and China) (APEJC) at IDC’s office in Bangalore, India. He is tasked with guiding public sector agencies and the tech industry by collaborating with them in strategic planning. He has led numerous complex consulting engagements, represented IDC at industry events, and hosted workshops focusing on understanding how digital investments impact key economies in Asia/Pacific within the context of global trends — all while collaborating with IDC’s global Government Insights teams.

[More about Ravikant Sharma →](#)

Message from the sponsor



Akamai is the cybersecurity and cloud computing company that powers and protects business online.

Our market-leading security solutions, superior threat intelligence, and global operations team provide defense in depth to safeguard enterprise data and applications everywhere. Akamai’s full-stack cloud computing solutions deliver performance and affordability on the world’s most distributed platform. Global enterprises trust Akamai to provide the industry-leading reliability, scale, and expertise they need to grow their business with confidence.

Learn more at akamai.com and akamai.com/blog or follow Akamai Technologies on [X](#) and [LinkedIn](#).

akamai.com

akamai.com/blog

[!\[\]\(41b4206cc8026cb67be14dc277248f9f_img.jpg\) Akamai](#)

[!\[\]\(02e4544a00d6eb28889af71fb4810a2d_img.jpg\) Akamai](#)

IDC Custom Solutions

IDC Custom Solutions produced this publication.

The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies.

This IDC material is licensed for external use and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.



[IDC.com](#)

[IDC on LinkedIn](#)

[IDC Blog](#)

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 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.

©2026 IDC. Reproduction is forbidden unless authorized. All rights reserved. [CCPA](#)