

Executive Summary

To deliver next-generation public services, European governments must invest in emerging technologies, enhance cyber-resilience, and build trust. This strategic approach aims to achieve practical outcomes:

Improving citizen experience:

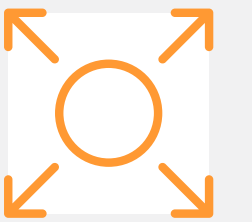
- Governments are adopting modern security measures to provide citizens with secure and seamless interactions when accessing public services, aiming to build trust and reliability.



But transformation comes with challenges:

Expanding attack surface and broadening threat types:

- Digital transformation increases the attack surface, necessitating governments to fortify security measures and address a broader range of sophisticated cyberthreats.



Increasing operational efficiency and resilience:

- Advanced security measures are being integrated to improve operational efficiency and build resilience against evolving threats, ensuring continuous service delivery and protecting critical operations.



Navigating regulations and compliance:

- Adherence to regulations and compliance standards is critical. Governments are navigating this landscape carefully to ensure the secure and lawful deployment of technologies in public services.



Enhancing employee productivity:

- Modernising security architectures is a strategic move to empower government employees with secure and efficient workflows, boosting overall productivity.



Modernising legacy systems with key focus areas:

- Modernisation efforts include advances in cloud security, network security, and zero trust frameworks. These technologies come together to enhance security and elevate citizen experience.



Driving innovation through investment in emerging technologies:

- Proactive investments in emerging technologies aim to accelerate technology-enabled innovation, positioning governments at the forefront of cutting-edge solutions.

