Executive Summary

The convergence of global geopolitical uncertainty and AI disruption creates both opportunities and risks for IT executives such as CIOs, CISOs, and CAIOs. While governments are accelerating their investments in AI-enabled transformation to drive operational efficiency and mission outcomes, they need to rethink how they build and operate cyber-resilient architectures amid evolving regulations and digital sovereignty requirements.

Increasing operational efficiency:

- Governments are seeking to implement advanced digital solutions to streamline operations and reduce administrative burden while maintaining secure citizen interactions when accessing public services, building trust and reliability through enhanced service delivery.

Reinforcing a data and AI-ready organisation:

- Organisations are establishing robust data management and governance frameworks and AI capabilities to enable data-driven decision making, positioning governments to leverage emerging technologies for improved citizen services and operational insights.

Modernising infrastructure:

- Governments are prioritising secure-by-design architectures, which incorporate continuous monitoring and threat intelligence sharing, in their digital transformation roadmaps to defend against state-sponsored attacks and advanced persistent threats targeting critical infrastructure.

Getting ready for the NIS 2 Directive:

- Adhering to evolving cybersecurity regulations and digital sovereignty demands is more crucial than ever. Across Europe, governments are finalising the transposition and enforcement of the NIS 2 Directive, ensuring public service technologies comply with strict security, risk management, and incident reporting requirements.

But transformation comes with challenges:

The expanding attack surface and broadening threat types:

- AI-enabled digital transformation increases vulnerability risks by gathering more data points, necessitating governments to reevaluate security measures and address a broader range of evolving cyberthreats.

Navigating regulations and compliance:

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

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 the citizen experience.