# SCION for the government sector

Ensuring data sovereignty and security

## Introduction

Governments face increasing pressure to ensure data sovereignty, secure communication, and cyber resilience in a rapidly evolving digital landscape. Traditional internet architectures expose government networks to security vulnerabilities, cross-border data risks, and operational disruptions. SCION (Scalability, Control, and Isolation on Next-Generation Networks) provides a secure, sovereign, and resilient network architecture that ensures full control over data paths, eliminates unauthorized access risks, and strengthens national cybersecurity strategies.

## Key challenges in government networking

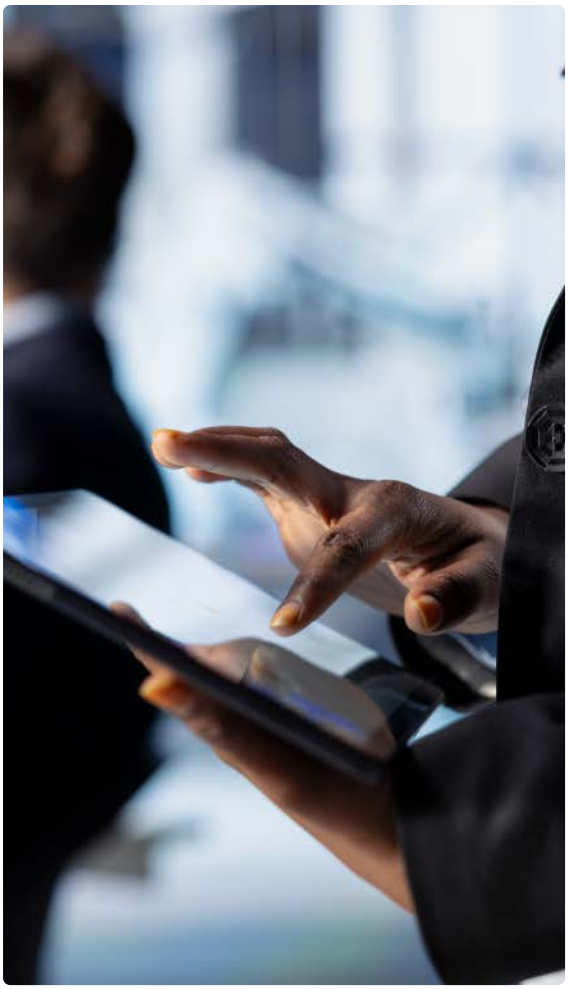
**Data sovereignty and compliance risks**
Governments risk unauthorized data access and regulatory breaches when sensitive data flows through foreign providers or insecure networks.

**Geofencing**
Despite setting digital borders, governments often have little to no control over where data actually travels and data can cross international borders in milliseconds.

**Cybersecurity threats and nation-state attacks**
State-sponsored cyber-attacks threaten government networks, jeopardize confidential data and can paralyze critical infrastructure.

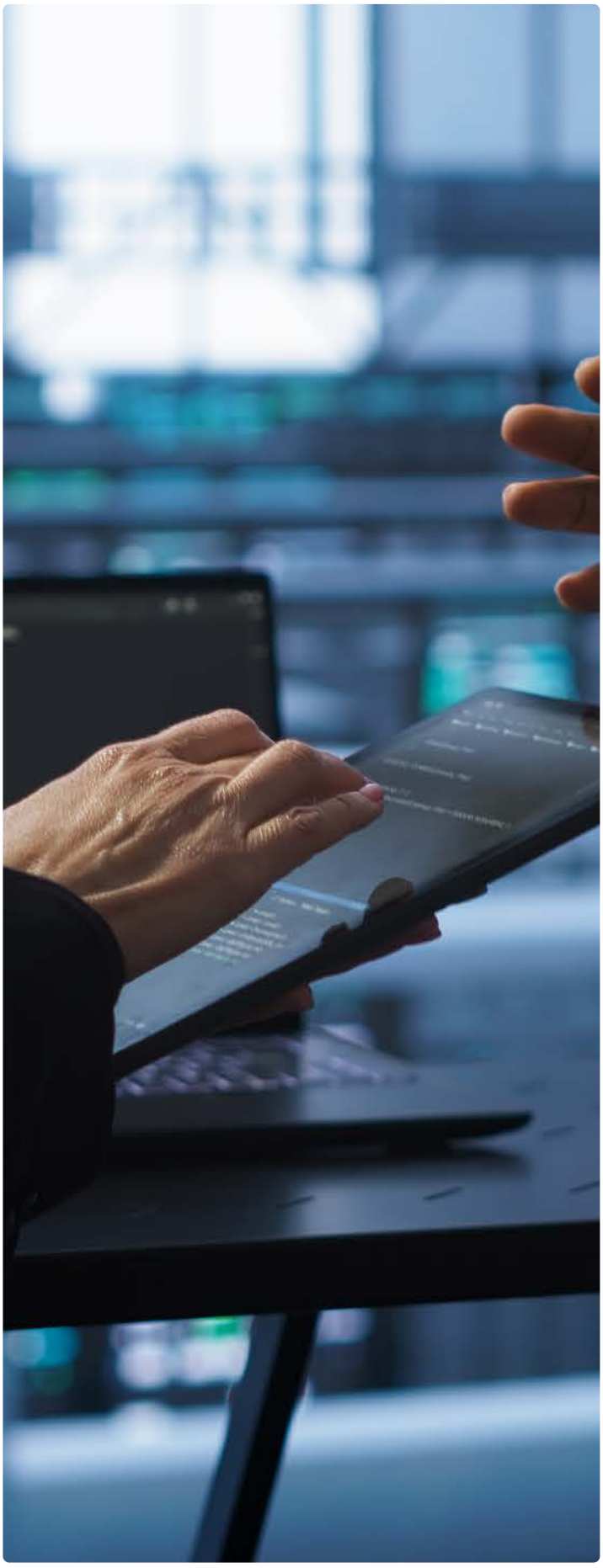
**Low network resilience and geopolitical risks**
Network outages due to cyberattacks, sanctions or geopolitical tensions can significantly impact government services and crisis management.

**Fragmented and insecure multi-agency communication** Inconsistent IT security standards between authorities lead to data leaks, inefficient collaboration and make it difficult to respond quickly in crisis situations.



# SCION for government networks

SCION's unique capabilities and design make it an ideal solution for organizations operating in the critical infrastructure sectors who rely on the traditional Internet for connecting their mission-critical systems. Below, read how Anapaya's SCION-powered solutions help ensure resiliency against cyber threats:



### Define rules around data sovereignty and compliance

Governments can define and enforce trusted network paths, ensuring compliance with national security and data protection regulations.

### Deliver a cyber-resilient and attack-resistant service

SCION's architecture isolates malicious traffic and prevents large-scale attacks like DDoS, ensuring secure, controlled communication.

### Guaranteed uptime and network resilience

Multi-path routing ensures that government services remain operational even if parts of the network are compromised or unavailable.

### Secure cross-agency and international communication

SCION enables trusted, encrypted communication between government entities, diplomatic missions, and defense organizations without reliance on unsecured public internet infrastructure.

## Use cases for government agencies

**Secure digital government services**
Ensure critical citizen services (e.g. voting, public services, and social security systems) operate without cyber disruptions or data breaches.

**Diplomatic and international data exchange**
Enable secure, controlled, and compliant communication between embassies, consulates, and government agencies across borders.

**Military and defense communication**
Protect classified government communications, intelligence sharing, and defense operations with end-to-end secure network routing.

**Public infrastructure protection**
Public operators of critical infrastructure (e.g. energy, water, transport, healthcare) who need to secure their networks against cyber-attacks and geopolitical risks.

## SCION: The secure foundation for future-proof government networks

**Learn how Anapaya can secure government networks**

Contact us at **team@anapaya.net** to learn more.