



Ensuring and Securing Canadian Data Sovereignty

Safeguarding digital infrastructure and data

Summary

In times of geopolitical uncertainty, data storage and flows still need to continue. Global distribution of data infrastructure contains costs and drives efficiency—however, it also creates vulnerability when you can't be sure where infrastructure is located. Data sovereign solutions are becoming increasingly important to provide assurance to customers that their data is in a single jurisdiction and is protected, both from unauthorized intrusion and from foreign governments.

Global Connectivity and National Challenges

In the age of digital warfare, data sovereignty is essential. Prosperity and national security rely on data. Governments need to keep information safe and secure to sustain operations and daily activities. Military and national security information needs to remain secure to maintain advantage over adversaries and prevent interference in planning and operations. Intellectual property is essential for industry to be competitive globally and to enjoy the benefits of research and development investment. For daily life, things like global financial infrastructure, GPS navigation, the security of air traffic control, and the reliability of traffic lights and cameras require secure data. Personal privacy requires data security for a wide range of personal, financial and health information.

In a world that is contested and competitive, having digital infrastructure secured within national borders is more important than ever. Data sovereignty means securing data and digital infrastructure, bringing that infrastructure home to prevent unauthorized access by foreign governments.

Canada has made clear that the Department of National Defence (DND) and the Canadian Armed Forces (CAF) have responsibility to ensure all mission-critical, operational, intelligence and defence-related information (data) is governed, stored and processed according to the requirements of Bills C-26 and C-27. This is foundational to Canada's position on safeguarding data and data infrastructure.



Building and Delivering Data Sovereignty

Data sovereignty means safeguarding all aspects of our digital and data infrastructure and securing it at home. For Canada's defence, this means data sovereignty is essential to control, govern and restrict access to sensitive defence-related data across cloud, AI, communications and operational networks.



Offshore digital infrastructure creates layers of bureaucratic process for managing foreign regulatory and legal requirements. Relying on domestic data sovereign solutions eliminates the compliance challenges with offshore storage.



Calian Data Sovereign Capabilities

Calian delivers secure-by-design data storage for facilities, infrastructure, networks and devices. For defence customers, we provide solutions for large military headquarters down to forward-deployed units using data solutions at-the-edge. We tailor and scale our solutions to meet any digital infrastructure and data security need. With real-time monitoring of cybersecurity threats and emissions security threats, we deliver secure solutions for enterprise or local needs. No matter the application, Calian delivers sovereign solutions to keep your data safe and secure.



Domestic Cloud

We deliver robust cloud-based solutions that protect digital infrastructure and data, hosted in domestic cloud with the appropriate security technologies and solutions to keep data secure. We deliver scalable solutions to meet your needs today and offer a strategic future-proof solution that can be adapted for changing needs and new technology.

Calian's zero-trust framework uses multi-factor authentication, identity and access management (IAM), least-privilege access, and continuous monitoring of network activity to keep your network secure. This approach ensures that only authenticated and authorized users and devices can access applications and data, thus significantly reducing the attack surface. Zero trust is particularly relevant for today's cloud-based services and mobile access, where the traditional network perimeter has become increasingly irrelevant. By assuming that there are always potential threats, zero trust provides a proactive and adaptive security stance.

We deliver solutions with exclusive resource usage, with infrastructure dedicated to your organization. We also deliver hybrid cloud solutions that combine public and private environments. Hybrid cloud solutions are very useful for effortlessly surging data capacity requirements to accommodate a rapid increase in demand.

Private Cloud with Managed Backup

Our private cloud environment is hosted within Canada, offering defence customers a place to ensure data sovereignty. Coupled with our fully managed backup, our solution ensures data resiliency and business continuity across your environments.

We take a multi-tiered backup model approach that combines hot storage for rapid recovery and S3-compatible archival for long-term retention. This service includes 24x7x365 monitoring, proactive issue resolution, and full backup lifecycle management.

With secure-by-design in mind, our managed backup adheres to AES-256 and TLS encryption, zero-trust access, immutable storage, and ransomware protection. The cloud environment is monitored 24x7x365 by a SOC compliant with PIPEDA, GDPR and Controlled Goods Program.

SOC/NOC

Calian's managed security operations centre (SOC) delivers continuous services that monitors networks, devices, appliances and information storage wherever your information is stored. Our managed SOC acts as a centralized function within your organization, integrating people, process and technology to monitor and improve your security posture, while preventing, detecting, analyzing and responding to cybersecurity incidents.

With 24x7x365 monitoring, we provide continuous protection against threats, and offer the strategic insights to improve cybersecurity planning and compliance. For prevention, we deliver threat-hunting services through networks and datasets to isolate advanced threats before they materialize. With a clear threat profile, we anticipate your security posture using existing systems, regardless of your data environment.



Emissions Security

Calian delivers emissions security (EMSEC) solutions, recognized by the Canadian government and by TEMPEST standards. We protect facilities, infrastructure, networks and devices to safeguard sensitive data from electrical and electromagnetic threats. Starting with a harmonized threat risk assessment to identify where your facilities, infrastructure and equipment could be vulnerable to electronic intrusion. We deliver zoned assessment for any facility—government or industrial—that has zones with higher security requirements embedded in lower security facilities.

We tailor our security solutions—including products—by modifying off-the-shelf equipment to meet your specific needs, all while meeting TEMPEST certification standards. We secure workstations, routers and switches, printers and scanners, ruggedized and non-ruggedized laptops and tables, and provide RF lockboxes.



Cyber Training

We deliver training to equip organizations and individuals with the knowledge, skills and strategies to prevent, detect and respond to cyber threats. Calian approaches cyber training and readiness in two fundamental ways—through a simulation environment and tabletop exercises. Today, our simulation environment supports the military with real-world cyber threats, giving your team the benefit of an immersive training environment for incident response. Accessible via a sovereign cloud environment, this training can be scaled to provide introductory training to develop new operators or to provide more challenging training to test the skills of seasoned operators onsite or in the field.

Tabletop exercises are another training resource offered and best-done face to face. This scenario-based exercise enables key stakeholders to work together to resolve complex security challenges before they occur, essentially building a real-world playbook for the future.

Ethical AI and Sovereign Data

Today's challenges go beyond securing data under a sovereign mandate. Today, it includes ethical AI and how data is being used as it aligns with Canadian laws, values and public trust. Where and how the data is being stored is the starting ground for ethical AI and without a sovereign approach to data you can't guarantee an ethical use of AI.

Calian's AI and data experts also provide custom solutions built based on the premise of a secure and centralized data lake where machine learning algorithms can rapidly enable critical insight through tools like predictive modelling or trend analysis.



Customers and Sectors



Defence & National Security

We provide data sovereign solutions for defence and national security customers in Canada to protect installations, infrastructure and networks. They trust us when they cannot fail.



Space

The ground station is the most vulnerable part of the space ecosystem. Our solutions protect physical infrastructure on the ground to keep satellites on-time and on-target.



Health

Our Canadian healthcare industry is a complex, multi-layered environment, but appetizing to bad actors. Calian is known within healthcare as the go-to cyber and cloud modernization solutions company, that is there 24x7x365 to protect individual healthcare IP.



Transportation

Supporting this critical infrastructure is something Calian does every day. Managing security and network operational environments, cloud management back up and redundancy, and RF emissions control enables airports to operate and service civilian demands with minimal risk.

Our Certifications

Calian SOC and IR Teams' Certifications

- Certified Threat Intelligence Analyst (CTIA)
- Certified Digital Forensics Examiner (CDFE)
- Certified Incident Handler (GCIH)
- Certified Information Systems Security Professional (CISSP)

Microsoft Certifications

- Microsoft Security, Compliance and Identity Fundamentals (SC-900)
- Microsoft Azure Fundamentals (AZ900)
- Microsoft Security Architects Expert (SC100)
- Microsoft Security Operations Analyst (SC200)
- Microsoft Identity and Access Administrator (SC300)
- Microsoft Information Protection Administrator (SC400)
- Microsoft Azure Security Engineer Associate (AZ500)



For over 40 years, Calian has delivered mission-critical solutions when failure is not an option. Trusted worldwide, we empower organizations in critical industries to overcome obstacles, manage risks and drive progress. By combining the expertise of our people, proven industry insight, cutting-edge technology, bold innovation and global reach, we deliver tailored solutions that solve complex challenges. Headquartered in Ottawa, Canada, with over 5,000 people around the world, Calian's solutions protect lives, strengthen security, foster global connectivity and drive economic progress, making a lasting impact where and when it matters most.