

Zero Trust Strategies for Canadian Federal Agencies and Organizations

Implementing your federal Zero Trust strategy

Canadian federal organizations today face unprecedented security challenges, as highlighted by recent high-profile cyber incidents worldwide. In response, the Canadian government has developed directives to enhance federal cybersecurity frameworks, emphasizing the importance of implementing a Zero Trust strategy.

Achieving these strategic goals should be seen as a continuous journey rather than a final destination. With over 20 years of proven experience in public sector security, Akamai is here to support you on your path toward Zero Trust.

Akamai's Zero Trust advantage

The Zero Trust objectives set forth by the Canadian federal directives are aligned with global best practices, including the Cybersecurity and Infrastructure Security Agency's (CISA) Zero Trust Maturity Model, which outlines five key pillars:

- Identity
- Devices
- Networks
- Applications and Workloads
- Data

As your trusted federal security advisor, Akamai offers the products, expertise, and partnerships to help you achieve your Zero Trust goals.

Identity

Akamai MFA (multi-factor authentication) is our keyless FIDO2 identity solution that protects employee accounts from phishing and other machine-in-the-middle attacks. It ensures that only strongly identity-based authenticated employees can access the accounts they own. Unauthorized access is denied, and employee account takeover is prevented.

Devices

Akamai Guardicore Segmentation is our industry-leading microsegmentation solution, designed to limit the spread of ransomware and other malware. By continuously monitoring and enforcing policies on devices, it verifies device configurations, software installations, and potential vulnerabilities, ensuring that only compliant devices can access the network. Additionally, the solution supports an agentless approach to secure IoT devices.

Akamai Enterprise Application Access is our Zero Trust Network Access (ZTNA) solution, ensuring that only authenticated users and devices can access applications. By verifying the identity and posture of devices, Enterprise Application Access complements the capabilities of Akamai Guardicore Segmentation. If a device is found to be noncompliant or poses a security risk, Enterprise Application Access can restrict its access to sensitive applications.

Zero Trust principles



All entities are untrusted by default



Least-privilege access is enforced



Comprehensive security monitoring is implemented



Networks

Akamai App & API Protector integrates web application firewall, bot mitigation, API security, and Layer 7 DDoS protection into a single solution. It quickly identifies vulnerabilities and mitigates threats across your entire web and API estates.

Akamai Secure Internet Access Enterprise is our cloud-based secure DNS service that ensures your users and devices can securely connect to the internet wherever they are, without the complexity and management overhead associated with other security solutions.

Akamai Guardicore Segmentation provides granular control over network traffic, ensuring that only legitimate traffic is allowed. By segmenting the network at a micro level, it ensures that potential threats are isolated and cannot move laterally within the network.

Applications and workloads

Akamai Enterprise Application Access provides Zero Trust access for your employees, third-party contractors, partners, and mobile users — regardless of their location. It eliminates the operational cost and risk involved in maintaining and patching VPNs or other appliance-based solutions.

Akamai Guardicore Segmentation offers visibility into and understanding of workloads, applications, and processes, as well as the enforcement of secure access policies. Together, Akamai Guardicore Segmentation and Enterprise Application Access provide a comprehensive solution for application and workload security.

Data

Akamai Secure Internet Access provides secure access to data with features like content filtering, advanced threat protection, and data loss prevention. It supports data inventory management by preventing unauthorized access and data leaks.

Proven partners

In addition, you can trust our proven partner relationships to help you meet your Zero Trust directives. Our public sector security team can help you find the right partners and customized solutions to protect your environment.

You can rely on Akamai

Akamai's people, products, and partners will help you achieve your Zero Trust objectives. We assist in building and customizing uncompromised, end-to-end security for your agency or organization. Leading organizations worldwide choose Akamai to build, deliver, and secure their digital experiences — helping millions of Canadians live, work, and connect every day.



To learn more, visit [Getting Started with Your Zero Trust Strategy](#) or contact your Akamai public sector security sales team.