

KEYDATA ENGAGED BY THE CANADIAN FEDERAL GOVERNMENT TO IMPLEMENT A PRIVILEGED ACCESS MANAGEMENT PROGRAM

KEYDATA CASE STUDY | GOVERNMENT

The Government of Canada's Shared Services Canada (SSC) is an agency responsible for delivering strategic I.T. and cybersecurity services to 43 Departments of the Federal Government.

THE OBJECTIVE

As part of ongoing efforts to modernize and secure the Canadian federal government infrastructure and computing resources, SSC was given the mandate to provide a centralized privileged access management (PAM) program for SCC and its 43 Partner Departments.

With assistance from KeyData, SSC developed the concept, technology suite and operating model for a centralized PAM service to allow departments to securely manage privileged access.

ASSESSMENT AND STRATEGIC GUIDANCE

KeyData provided a wide range of services necessary to take the service from inception to deployment.

AT A GLANCE



COMPANY:

Shared Services Canada (SSC)



LOCATION:

Ottawa, Canada



EMPLOYEES:

400,000 employees

10,000 privileged accounts



CHALLENGE:

Develop and deploy a unified IAM/PAM framework for both on-prem and cloud and deploy an integrated technology solution for SSC and its 43 Partner Departments.



SOLUTION:

CyberArk (PAM) & SailPoint (IAM)



SERVICES PROVIDED BY KEYDATA:

- Conducted IAM/PAM current state assessment
- Developed target-state IAM/PAM architecture, strategy, roadmap and implementation plan
- Managed execution of IAM/PAM program
- Developed operating model and client onboarding artifacts for launch of the managed PAM service
- Technical design, solution configuration, integration and customization (off-prem, on prem and cloud)
- Developed and deployed training for admins, end-users, developers and operations

KEY PROJECTS UNDERWAY AND COMPLETED

PAM and IAM Current State Assessment

Conducted a current state assessment against industry-leading IAM and PAM Best Practices to identify gaps. KeyData defined their target state IAM/PAM architecture and developed a phased multi-year roadmap along with an implementation plan. The business priorities and pain points were used to help drive the phases of the IAM/PAM roadmap.

The target-state architecture and roadmap captured the SSC's strategic goals and provided guiding principles for the successful implementation of an integrated solution using industry leading IAM ([SailPoint](#)) and PAM ([CyberArk](#)) technologies.

The roadmap introduced new target-state IAM/PAM processes, which delivered seamless user experience while simultaneously addressing any potential for abuse of privileged accounts across the client's network. KeyData was able to define exactly how the privileged access and enterprise identity management controls would integrate to cover all control gaps using the government's security and controls framework.

Critical PAM Use Case Inventory

As a core deliverable of the assessment, KeyData gathered requirements from multiple stakeholders to develop a comprehensive set of recommendations addressing governance, people, processes and technology. The assessment included detailed recommendations for protecting both personal (i.e., admin accounts owned by a single person) and non-personal privileged accounts (e.g., break-glass accounts/firecall IDs, generic admin accounts). These use cases formed the initial operating capability of the service.

Cloud PAM and IAM Framework Development

To complement existing use cases and workflows, a specific PAM Cloud Framework was developed to consider the unique control requirements of securing privileged accounts in federal public cloud tenants. The framework included use cases that would deliver value to both the human admins managing cloud tenants at scale, and the application and automation processes running within the environments. KeyData created a prototype design of a uniform cloud framework that would then be deployed nationally.

Service Operating Model

In order to deliver this managed service, SSC required an operating model to define the roles and responsibilities of SSC, clients and any third parties involved in the service delivery.

KeyData delivered an operating model that included a detailed RACI, service level parameters, support functions and detailed customer responsibilities. This allowed SSC to present the service when on-boarding other department clients.

From Prototype to Production Deployment

KeyData is leading every phase of the project to design, deploy and enable SSC to operate and maintain the IAM/PAM program.

Along with the technical deployment, KeyData is developing robust test plans, training documentation and educational materials to keep government staff skills current during all phases of this multi-year project.

Production Service Launch

Once the initial phases of the target-state roadmap are deployed, SSC will have the ability to manage and monitor more than 10,000 privileged accounts. The personal privileged accounts will be tightly managed through consistent, reliable and repeatable automated provisioning, self-service access request, and access certification processes.

This represents the largest PAM deployment nationally in Canada and one of the largest in North America.

This program will eliminate hundreds of hours of manual approvals and compliance audit preparation time. By deploying a unified PAM framework across 43 internal government departments, SSC will lower total cost of ownership, reduce risks, as well as rapid time to value.

RESULTS ONCE COMPLETED



Formalize user data and *facilitate automation* and provisioning of personal privileged accounts for employees.



Decrease demand for internal support resources and *eliminate* hundreds of hours of manual approvals and compliance audit preparation time.



Create a consumable service to *reduce risk* across *multiple* government departments



Reduce total cost of ownership, *greater transparency* with a single governance and audit strategy, as well as *rapid time to value*.

ABOUT KEYDATA

Founded in 2005, KeyData has been serving clients for **over 16 years**. KeyData is a recognized North American leader in cybersecurity services, specializing in Identity and Access Management (IAM), Customer Identity & Access Management (CIAM), and Privileged Access Management (PAM). We are committed to providing the best customer experience with every interaction. We strive to offer pragmatic advice that will help organizations protect their assets and maintain a safe and secure environment in which to operate. To learn more, visit our [website](#) for more information or [contact us](#) to get in touch.

- ✓ Uniquely positioned to integrate IAM and PAM solutions
- ✓ Consulting, implementation and managed services experience
- ✓ Deep IAM and PAM technical expertise; certified, secret-cleared resources
- ✓ Customer-centric and trusted advisors