TEHAMA

**Compliant and Secure Virtual Desktops for Your Global Workforce**

—

# Securely Accessing Distributed Financial Data for Analysis

## Eliminate the Risk of Data Exfiltration with Policy-Based Access to Data Sources

Canada's data collection and analysis agency is leading a world class strategy to better understand individuals' behaviours and trends that can be used to define and influence government policy. While this is a necessary and exciting task in the Statistics Canada mandate, it comes with data privacy, policy, and disclosure concerns for many private citizens. Requiring financial institutions to hand over hundreds of thousands of transaction records creates anxiety for any private citizen with respect to individual profile disclosure, but also for fear of data breaches and leaks. Individuals trust their financial institutions to protect and secure their private data. With this data in the hands of Statistics Canada and no longer under the control of the financial institution, Canadian citizens become concerned about the duty of care that is being applied to their sensitive data.

Data breaches are fast becoming an unfortunate commonplace in the news cycle, whether the root cause is a result of well funded state-sponsored attacks, malicious hackers, malware unknowingly being installed by a careless end-user, or the result of malicious intent by an insider to gather and share private information for profit. Knowing that one's personal information has been sold on the 'dark web' must be a devastating worry to the millions who have experienced this, and the trend will likely continue under the current mechanisms for data gathering, sharing, and analysis.

**With more than 75 percent of consumer activity being conducted online by Canadians, macro-level analysis to generate and provide the public with timely and quality statistics in areas such as the housing market, debt levels, and the emergence of the gig economy becomes a difficult task. Data needed for such macro-level analyses is spread across many disparate, and distributed data systems, managed and protected by just as many financial and payment processing organizations.**

Having access to such data places a significant burden on the entity, and individuals, gathering and processing the data -- not just due to the unsurmountable sensitivity of such data, but also exacerbated by the legal and political ramifications of a potential breach which may arise due to many factors such as inadvertent mis-handling, poor classification of data, or security systems and procedures incapable of protecting such data due to legacy security designs.

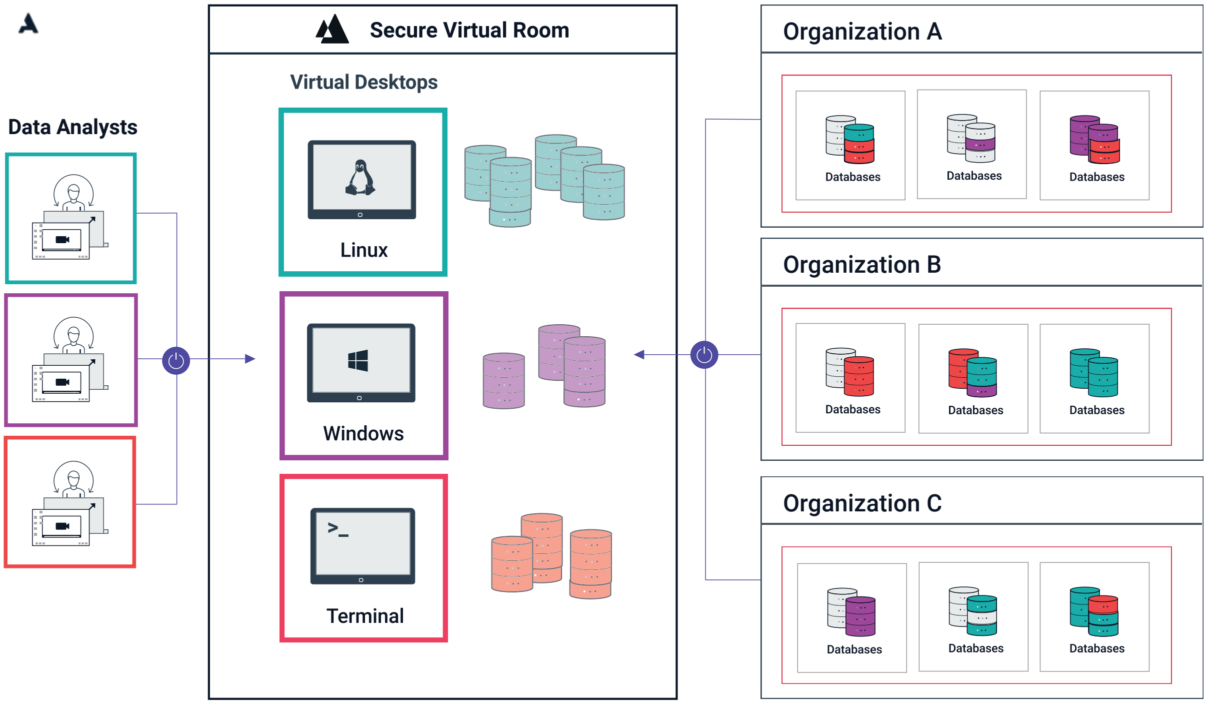
Macro-level analysis and decision-making processes are fast evolving to require data inputs from an ever broadening set of disconnected, disparate data sources spread nationally or globally across an unlimited number of databases. These analyses processes require modifications to respect the sensitivity and the dispersed nature of the information in order to continue providing meaningful results.

> ***A mechanism by which decision-making processes may continue to provide meaningful and insightful information in a distributed data landscape needs to evolve.***

A mechanism by which data can be securely accessed, anonymized, and used for insightful analysis by specific authorized personnel for specific authorized and controlled purposes, for specific periods of time, while having no possibility of data leakage, data copying, or mis-handling of the master data is a necessary evolution to support these decision-making processes.

To support such a distributed and controlled data access mechanism, a holistic security model must be in place to protect the individuals represented by the information while allowing access to the information - a necessary evil for the analysis process:

- **Consumer and individual data must not be copied; rather subsets of the data presented in a controlled manner to enable anonymized aggregation for analysis. Equally important is the requirement to have a very clear control and access genealogy with no broken chain. The access logs must show all approvals and workflow associated with the access and data requests and who granted the requests. Ultimately, organizations must ensure all data lineage from initial data capture to data analysis or sharing is visible to the data steward and data depositor.**
- **The information access and sharing model needs to support roles-based data access policies.**
- **The results of analyses must be contained in a secured manner which has no potential of unauthorized data exfiltration.**



## Holistically Aggregated Access to Data

Data providers - institutions which perform and protect the financial and payment transaction data, for example, must define the rules of engagement for access to their data by applying access policies to their Data Sources. Such policies allow for:

**a) the specification of the Organization from which the data is being accessed;**
**b) the specific role or purpose for the access and approval for that purpose and individuals; and**
**c) to which internal data may be accessed.**

In this manner, there is a precise security model in place which allows for the remote access to subsets of the data, while the data provider retains control over specifically what data may be accessed and by whom. This maintains the level of burden for the protection of the information on the data provider, where it needs to stay.

This mechanism of policy-based aggregated data access removes the need for entire database copies to be performed.

## Roles-Based Information Sharing

Presently, the organizations controlling consumer financial transaction data must provide such information in its complete form for external analysis - after which access control over the information is lost; no form of identity access or permission based on individuals' roles may be enforced.

Placing strict roles-based access to such data places the data access and analysis into a 'zero-trust' and need-to-know model where only individuals permitted to access the data may actually gain access to the data and to the results of any analysis performed on the aggregate data sets.

## No Potential of Unauthorized Data Exfiltration

The pitfalls of copying data need no further explanation; an environment which supports secured access to authorized individuals, supporting high levels of user authentication and identity management, and supporting secured encrypted storage access permits the analysis of the data, and removes the possibility of data being exfiltrated and falling into the wrong hands. All analysis necessary for collaboratively creating timely and quality statistics for Canadians can be performed in air-lock-like secured networked environments through which the national data sources may be accessed.

Access to these secured compute work environments is permitted only to authorized individuals through presentation-layer network protocols removing any possibility of malware infection, network snooping, and data exfiltration from these environments.

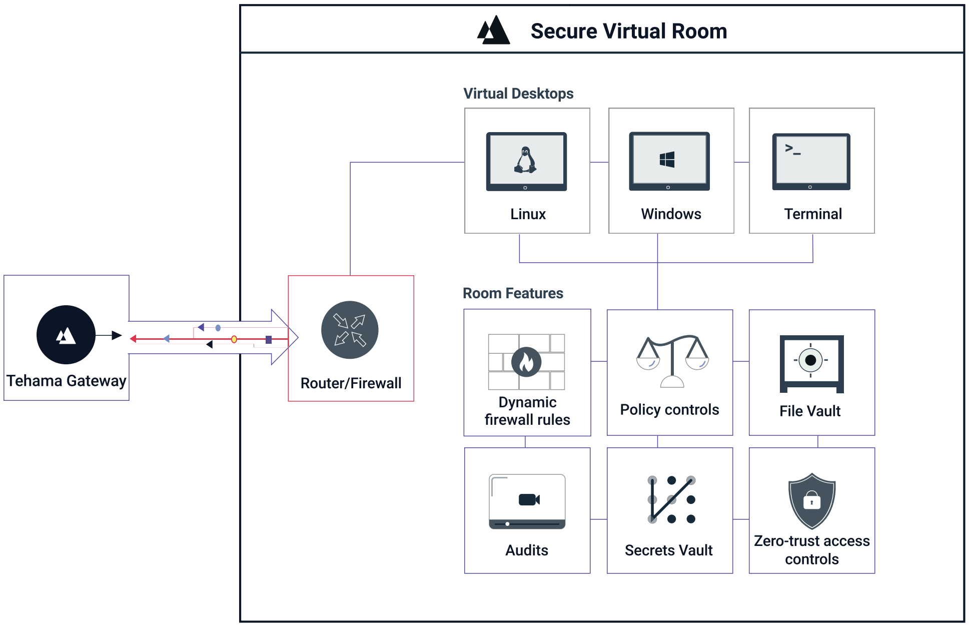
For **Statistics Canada**, Tehama could be used to access financial institutions' data within an airlock like architecture for data. Meaning, financial institutions could grant access to data via the Tehama platform where Statistics Canada analysts could run the models, aggregate the data, analyze, and synthesize the data with full protection of the data and complete visibility into who accessed the data, when the data was accessed, and what actions were performed on that data.

## The Tehama Platform

The Tehama platform is an in-market solution that provides all of the above-mentioned capabilities to support an airlock like data access and security model necessary for an organization to perform analysis on globally or nationally distributed and disparate data sources, supporting a security model that has been adopted by over 150 CIOs/CISOs globally to protect their core intellectual property and internal revenue-generating critical processing systems.

The Tehama platform allows for institutions which may be required to share data with third parties to offer subsets of data - only what is needed, for access rather than direct data copy. All analysis may be performed on the data without a need to copy the data, allowing large sets of reports to be created based on heterogeneous, disparate, and distributed data sources, all supporting strong information sharing models.
Offered as a cloud model, the Tehama platform scales up from individual usage to multiple organizations and distributed teams, with minimal investment.

Tehama meets SOC 2 Type II compliance, allowing it to be used, and relied upon for the processing and analysis of the most private of financial and consumer data.



## *Summary*

Today's methods for performing analysis on data which is spread across a multitude of disparate and distributed databases housed by many external entities and organizations unduly removes the standard of care regarding the information from those charged with protecting it, and represents several ways for such information to land in the wrong hands.

A mechanism which allows the data providers to share data, without copying it, only to trusted individuals, and allows the data providers - those charged with due standard of care for such data - to prescriptively isolate certain fields from sharing, allows for analysis jobs and reports to be created, and larger business and macro-level decision making to be performed based on large sets of data, while removing the need for directly copying the data.

There is no one single vendor that offers all the requirements described herein for securely accessing remote database systems in a single product like Tehama. Assembling all the capabilities into a functional and manageable suite will be prohibitively expensive, time consuming, and will contain a high level of risk as integration gaps between the subset capabilities will be undocumented and invisible, making them hard to uncover under penetration testing. In addition, there will be pricing and licensing complexities with the unavoidable multi-vendor approach.

Tehama represents a holistic approach to enforcing the security boundaries of large sets of data while providing organizations with the ability to perform deep analysis across such data, in a single, secure, and trusted platform.

**About Tehama**

Tehama provides compliant and secure virtual desktops on the cloud, enabling enterprises to quickly onboard, scale, manage, and audit a global workforce. With Tehama, enterprises quickly connect with increased security through virtual and secured perimeters that extend zero-trust network access to global employees and 3rd-party IT services providers.

For more information on Tehama, visit tehama.io or contact tehama@tehama.io