invest IN CANADA | investir AU CANADA

Creating and operationalizing a cloud only organization in GC – Lessons learned 20 months on.

6/19/2019 | Prepared For: Stratosphere 2019

Invest in Canada

As a new federal Corporation dedicated to positioning Canada as a top investment destination, we help global businesses navigate Canada's investment landscape. In bringing together our partners from the federal government, provinces, territories and cities across the country, we ensure global investors get seamless service to support their expansion in Canada.

IM/IT Requirements

Provide IIC Staff with a modern, secure, accessible and automated Information Technology experience that fosters intense collaboration and productivity while minimizing risk and overhead.

Context of our starting point

- Started a new organization without legacy systems, data, processes.

- Wanted to see how far we could go relying on cloud services to run everything.

- IIC is a client of SSC.

- Are a small organization (~70 FTE max), HQ in Ottawa with regionally located staff as well as staff travelling internationally often to meet clients.

Context of our starting requirements

- Needed to get up and running with minimal delay (weeks)

- Needed the most up to date tools to support our ambitious mandate

- Could not justify high overhead costs of on-prem

- Need a fully mobile system that can be managed remotely at the device level

IIC Guiding Principles

Cloud First: IIC will consume Industry provided cloud IT services by default, sharing service delivery accountability with authorised cloud service providers and minimising the need for on-premise components.

Zero Trust: IIC will embrace "never trust, always verify" security by design, protecting IT services and data at the lowest levels. Security will be in accordance with the GC PBMM (Protected B, Medium integrity, Medium availability) profile.

User Centric: IIC will employ modern technologies aimed at enhancing the user experience, deployed in an iterative and agile way, focusing on usability goals, user requirements, mobility, tasks and workflows at each stage of the process.

IIC Guiding Principles, continued

Data is an Asset: IIC will employ a data management strategy that ensures data is protected in all states and accessible to those that need it, when they need it, where they need it. Data protection schemes will include loss prevention, identity+location access control, encrypted pathways, sensitivity and retention labelling.

Automated: IIC IT service management and data lifecycle management will employ automation through self-service interfaces, processes and workflows, including an IIC Corporate Store for software and services.

Modern over Traditional: IIC user experience will be modern, founded on the most current release of features and capabilities of IT products and services. IT service management and support will be modern – easy, always current, proactive and secure – with limited desk-side visits.
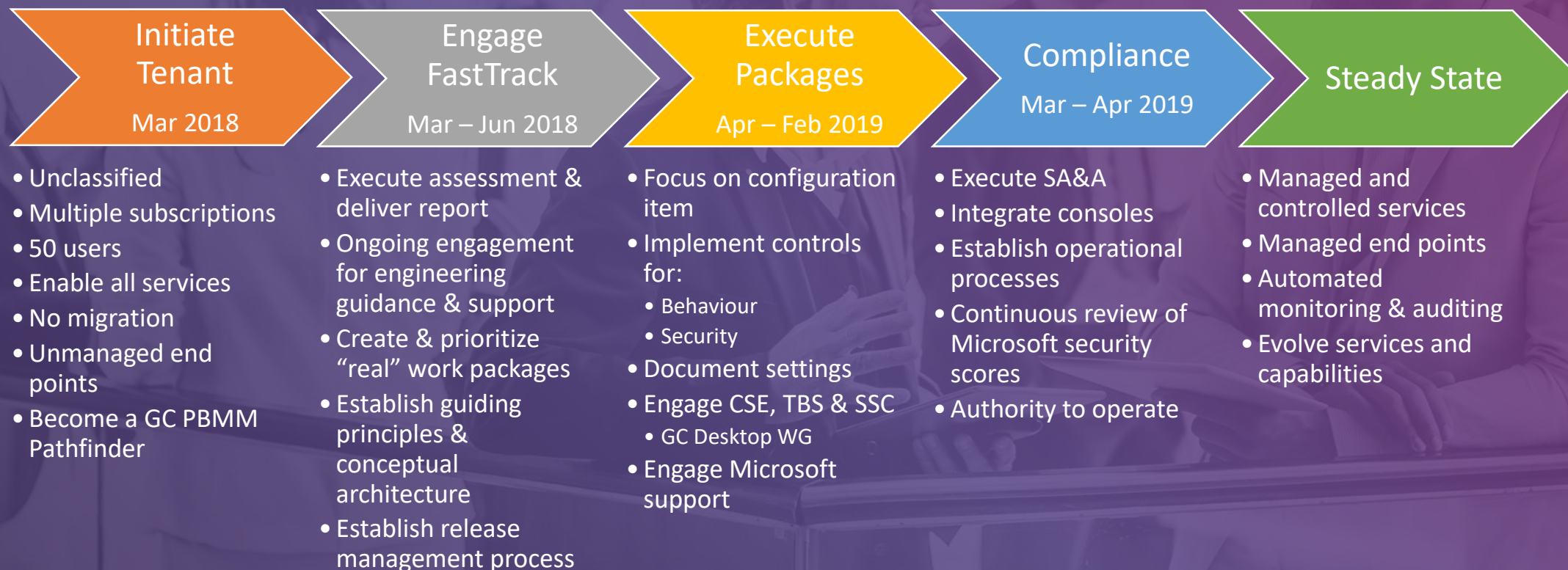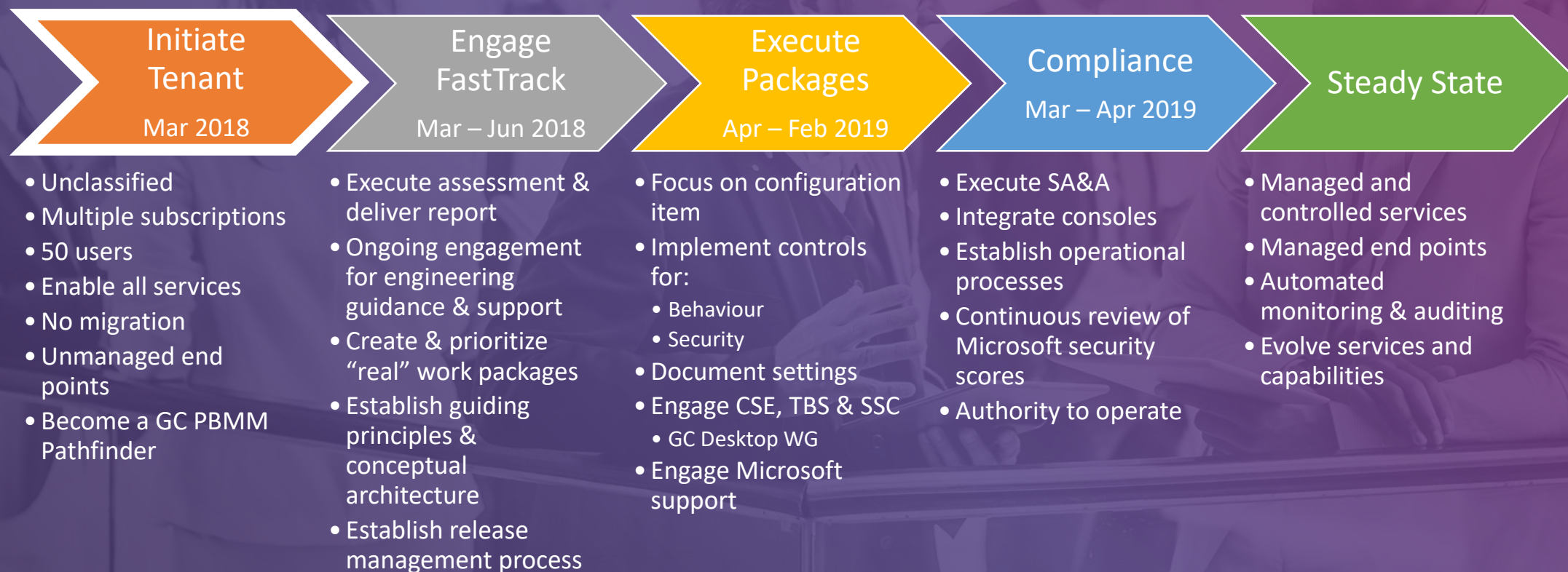
Our Cloud Stack

Office 365 – Journey to PBMM

Initiate Tenant
Mar 2018

- Unclassified
- Multiple subscriptions
- 50 users
- Enable all services
- No migration
- Unmanaged end points
- Become a GC PBMM Pathfinder

Engage FastTrack
Mar – Jun 2018

- Execute assessment & deliver report
- Ongoing engagement for engineering guidance & support
- Create & prioritize "real" work packages
- Establish guiding principles & conceptual architecture
- Establish release management process

Execute Packages
Apr – Feb 2019

- Focus on configuration item
- Implement controls for:
  - Behaviour
  - Security
- Document settings
- Engage CSE, TBS & SSC
  - GC Desktop WG
- Engage Microsoft support

Compliance
Mar – Apr 2019

- Execute SA&A
- Integrate consoles
- Establish operational processes
- Continuous review of Microsoft security scores
- Authority to operate

Steady State

- Managed and controlled services
- Managed end points
- Automated monitoring & auditing
- Evolve services and capabilities

Initiate Tenant
Mar 2018

- Unclassified
- Multiple subscriptions
- 50 users
- Enable all services
- No migration
- Unmanaged end points
- Become a GC PBMM Pathfinder

Engage FastTrack
Mar – Jun 2018

- Execute assessment & deliver report
- Ongoing engagement for engineering guidance & support
- Create & prioritize "real" work packages
- Establish guiding principles & conceptual architecture
- Establish release management process

Execute Packages
Apr – Feb 2019

- Focus on configuration item
- Implement controls for:
  - Behaviour
  - Security
- Document settings
- Engage CSE, TBS & SSC
  - GC Desktop WG
- Engage Microsoft support

Compliance
Mar – Apr 2019

- Execute SA&A
- Integrate consoles
- Establish operational processes
- Continuous review of Microsoft security scores
- Authority to operate

Steady State

- Managed and controlled services
- Managed end points
- Automated monitoring & auditing
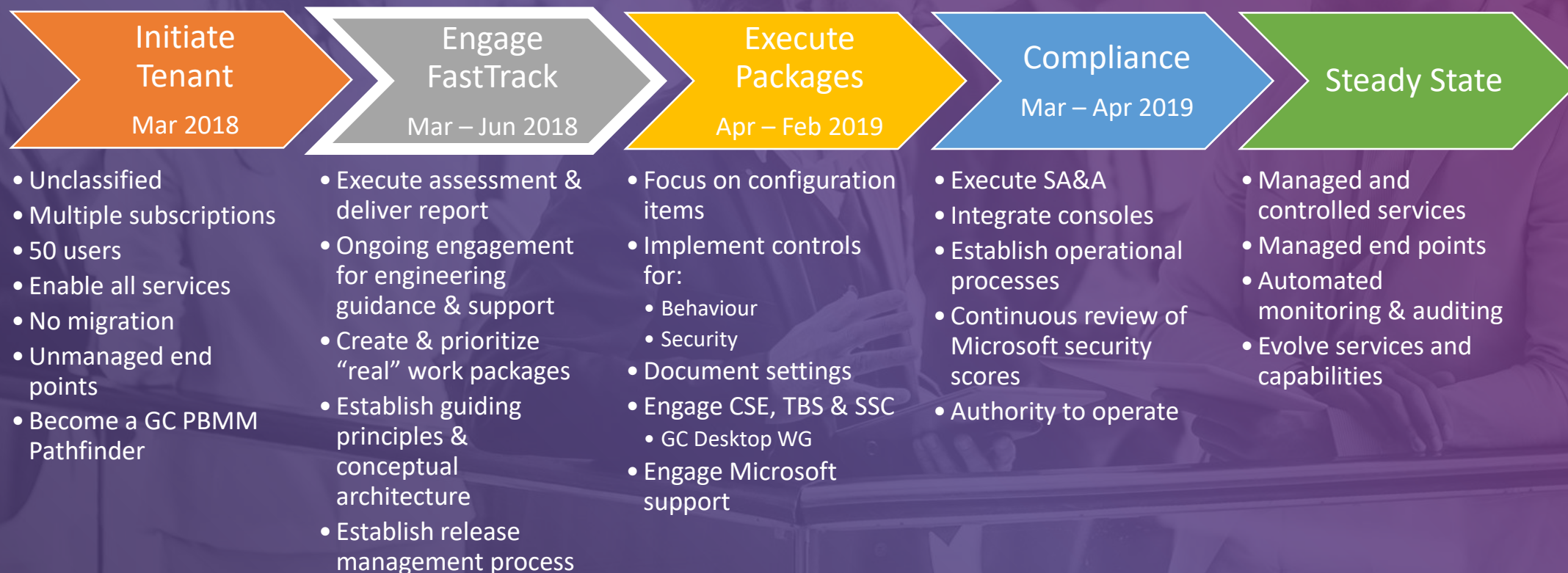- Evolve services and capabilities

Initiate Tenant

- ## Data sovereignty
  - Ensure data is stored in Canada for each service – Exchange, OneDrive, SharePoint, Teams
  - Migration of services can take months to schedule and complete

- ## License management
  - Bundle licenses and apps within licenses
  - Assign and enable based on purpose – use as an access control
  - Apply based on personnel security clearance

- ## Administrative roles
  - Use built in roles
  - Assign roles based on requirement; don't just give Global Admin to staff

- ## Understanding of consoles and PowerShell
  - Multiple ways to implement settings and controls – some work, some don't

- ## Engage expertise

Initiate Tenant
Mar 2018

- Unclassified
- Multiple subscriptions
- 50 users
- Enable all services
- No migration
- Unmanaged end points
- Become a GC PBMM Pathfinder

Engage FastTrack
Mar – Jun 2018

- Execute assessment & deliver report
- Ongoing engagement for engineering guidance & support
- Create & prioritize "real" work packages
- Establish guiding principles & conceptual architecture
- Establish release management process

Execute Packages
Apr – Feb 2019

- Focus on configuration items
- Implement controls for:
  - Behaviour
  - Security
- Document settings
- Engage CSE, TBS & SSC
  - GC Desktop WG
- Engage Microsoft support

Compliance
Mar – Apr 2019

- Execute SA&A
- Integrate consoles
- Establish operational processes
- Continuous review of Microsoft security scores
- Authority to operate

Steady State

- Managed and controlled services
- Managed end points
- Automated monitoring & auditing
- Evolve services and capabilities

Work Packages

1. Foundation
   1. Network
      1. Perimetre Security
   2. IM and Desktop
      Collaboration

2. Global
   1. External Threats
      1. Safe Attachments
      2. Safe Links
   2. GDPR

3. Identity
   1. Information Protection
   2. Multi-Factor Authentication
   3. Single Sign On

4. Messaging
   1. Anti-SPAM
   2. Anti-Malware
   3. Compliance
      1. Data Governance and Retention
      2. Data Loss Prevention
      3. Audit
      4. eDiscovery and Legal Holds

5. Document Management
   1. Desktop Synchronization
   2. Compliance
      1. Data Governance and Retention
      2. Data Loss Prevention
      3. Audit
      4. eDiscovery and Legal Holds

6. Mobility
   1. Device Security
   2. Device Management
   3. Service Expansion
   4. Application Management

7. Desktop Management
   1. Directory Integration
   2. Device Security
   3. Device Management
   4. Application Management

Initiate Tenant
Mar 2018

- Unclassified
- Multiple subscriptions
- 50 users
- Enable all services
- No migration
- Unmanaged end points
- Become a GC PBMM Pathfinder

Engage FastTrack
Mar – Jun 2018

- Execute assessment & deliver report
- Ongoing engagement for engineering guidance & support
- Create & prioritize "real" work packages
- Establish guiding principles & conceptual architecture
- Establish release management process

Execute Packages
Apr – Feb 2019

- Focus on configuration item
- Implement controls for:
  - Behaviour
  - Security
- Document settings
- Engage CSE, TBS & SSC
  - GC Desktop WG
- Engage Microsoft support

Compliance
Mar – Apr 2019

- Execute SA&A
- Integrate consoles
- Establish operational processes
- Continuous review of Microsoft security scores
- Authority to operate

Steady State

- Managed and controlled services
- Managed end points
- Automated monitoring & auditing
- Evolve services and capabilities

Data Sensitivity (as an example)

- ## Staff awareness and education
  - Policy driven and must be completed and maintained
  - Ability to understand the impact of a breach of the information being handled in whatever format – verbal, physical or electronic
- ## Classify, label and mark
  - Azure Information Protection (AIP) and integration with Office 365
  - Move toward Unified Labelling – different consoles, cross synchronization, maturity
  - Government *vs* Commercial
- ## Data loss prevention
  - Built-in policies for financial and personally identifiable sensitive info types
  - Create sensitive info type and policy for Protected B information
  - Automated detection
- ## Data protection
  - Office 365 encryption, access controls and sharing internally and externally
  - Encryption strategy must ensure interoperability with external entities

Modern Management

- ## Device Auto-Enrollment
- ## IIC Corporate Store
  - Application management
  - Patch and update management
- ## Zero Trust Compliance (GC Enhanced Profile)
  - Device authentication
  - Device encryption
  - Device firewall, anti-malware, host intrusion prevention
  - Device restrictions
- ## Automated Windows Update
  - Semi-annual major update channel
  - Immediate security updates

Enterprise State Roaming

Intune / MDM Auto-Enrollment

Windows 10 Azure AD Joined Devices

Initiate Tenant
Mar 2018

- Unclassified
- Multiple subscriptions
- 50 users
- Enable all services
- No migration
- Unmanaged end points
- Become a GC PBMM Pathfinder

Engage FastTrack
Mar – Jun 2018

- Execute assessment & deliver report
- Ongoing engagement for engineering guidance & support
- Create & prioritize "real" work packages
- Establish guiding principles & conceptual architecture
- Establish release management process

Execute Packages
Apr – Feb 2019

- Focus on configuration item
- Implement controls for:
  - Behaviour
  - Security
- Document settings
- Engage CSE, TBS & SSC
  - GC Desktop WG
- Engage Microsoft support

Compliance
Mar – Apr 2019

- Execute SA&A
- Integrate consoles
- Establish operational processes
- Continuous review of Microsoft security scores
- Authority to operate

Steady State

- Managed and controlled services
- Managed end points
- Automated monitoring & auditing
- Evolve services and capabilities

SA&A

Approach

- Clearly define scope – in this case Office 365 and more specifically:
  - Exchange
  - SharePoint
  - OneDrive for Business
  - Teams
- Follow ITSG-33 Protected B, Medium Integrity, Medium Availability (PBMM) profile
- Stack assessments using:
  - Microsoft's FedRAMP control assessment
  - CSE's O365 MT security assessment
  - Automated configuration exports via PowerShell or other tools

Findings

- O365 can be configured to satisfy PBMM
  - Licenses procured under new Microsoft PB enterprise agreement
  - Controls are satisfied by policy, by configuration settings or a combination

Risks

- Azure Active Directory data sovereignty
- On-going compliance as O365 evolves

Initiate Tenant
Mar 2018

- Unclassified
- Multiple subscriptions
- 50 users
- Enable all services
- No migration
- Unmanaged end points
- Become a GC PBMM Pathfinder

Engage FastTrack
Mar – Jun 2018

- Execute assessment & deliver report
- Ongoing engagement for engineering guidance & support
- Create & prioritize "real" work packages
- Establish guiding principles & conceptual architecture
- Establish release management process

Execute Packages
Apr – Feb 2019

- Focus on configuration item
- Implement controls for:
  - Behaviour
  - Security
- Document settings
- Engage CSE, TBS & SSC
  - GC Desktop WG
- Engage Microsoft support

Compliance
Mar – Apr 2019

- Execute SA&A
- Integrate consoles
- Establish operational processes
- Continuous review of Microsoft security scores
- Authority to operate

Steady State

- Managed and controlled services
- Managed end points
- Automated monitoring & auditing
- Evolve services and capabilities

Automated Monitoring, Auditing & Reporting
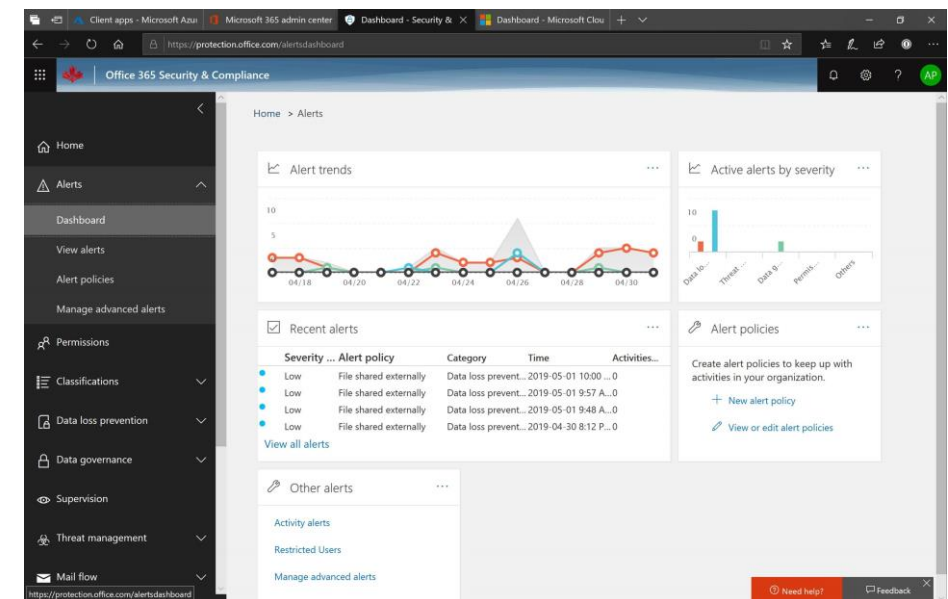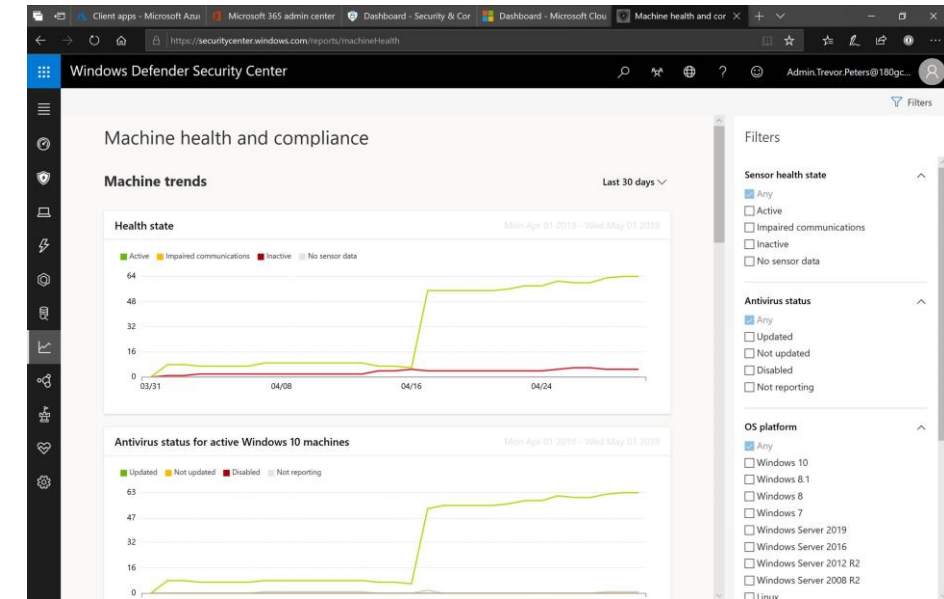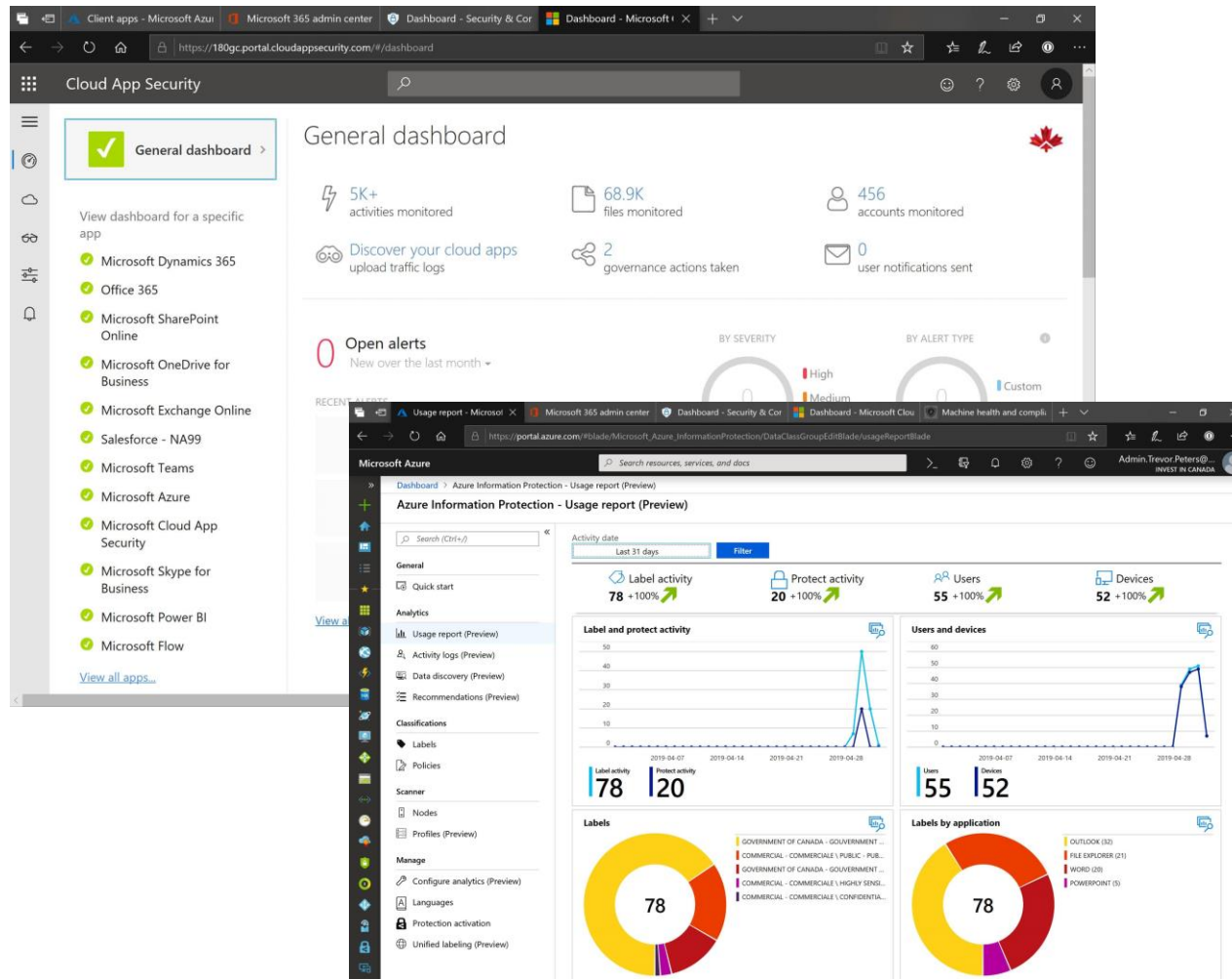
Microsoft Teams - today

Communicate
through chat, meetings & calls

Work with confidence
enterprise level security, compliance, and manageability
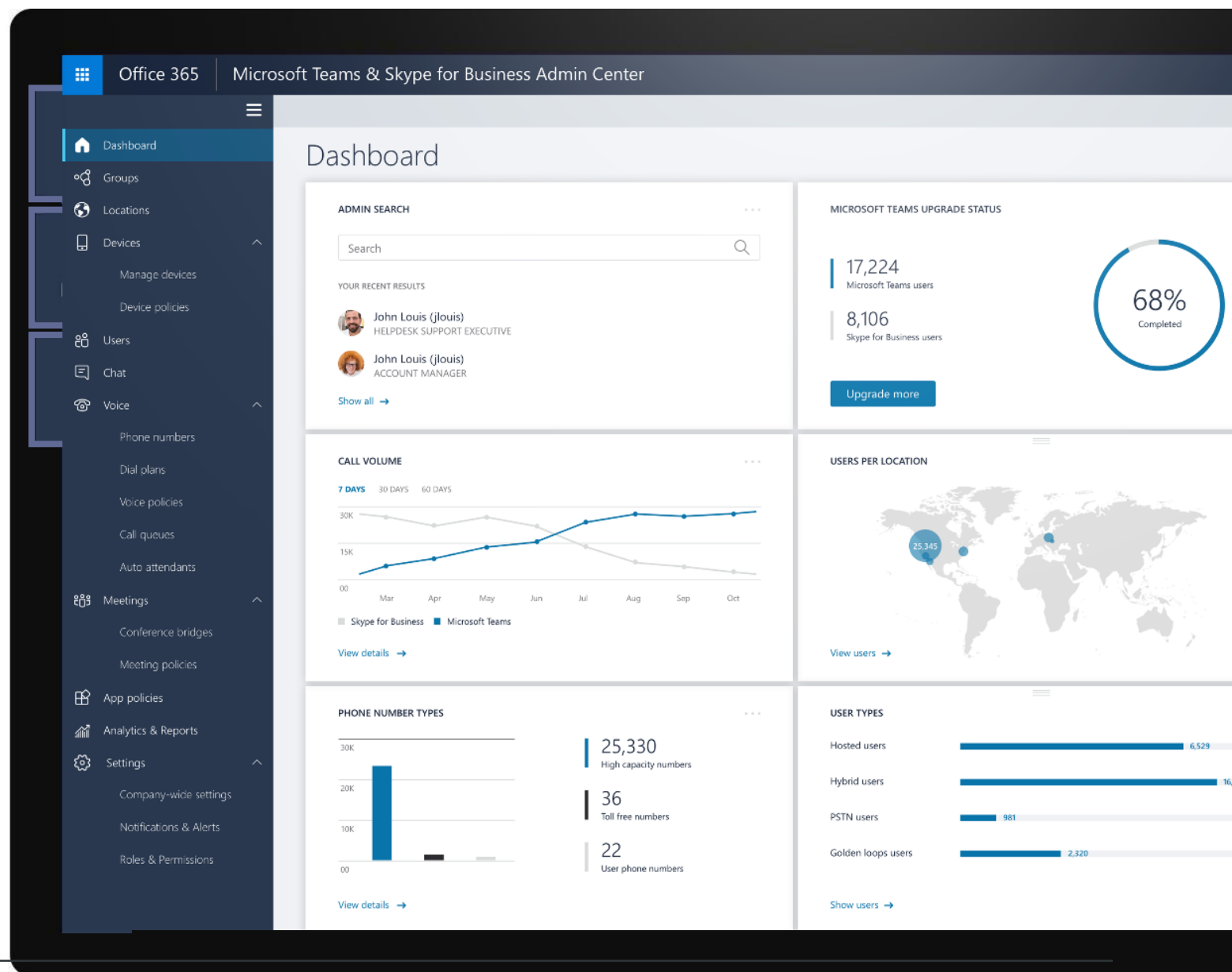
Microsoft Teams - tomorrow

Collaborate
with deeply integrated Office 365 apps

Customize & extend
with 3rd party apps, processes, and devices
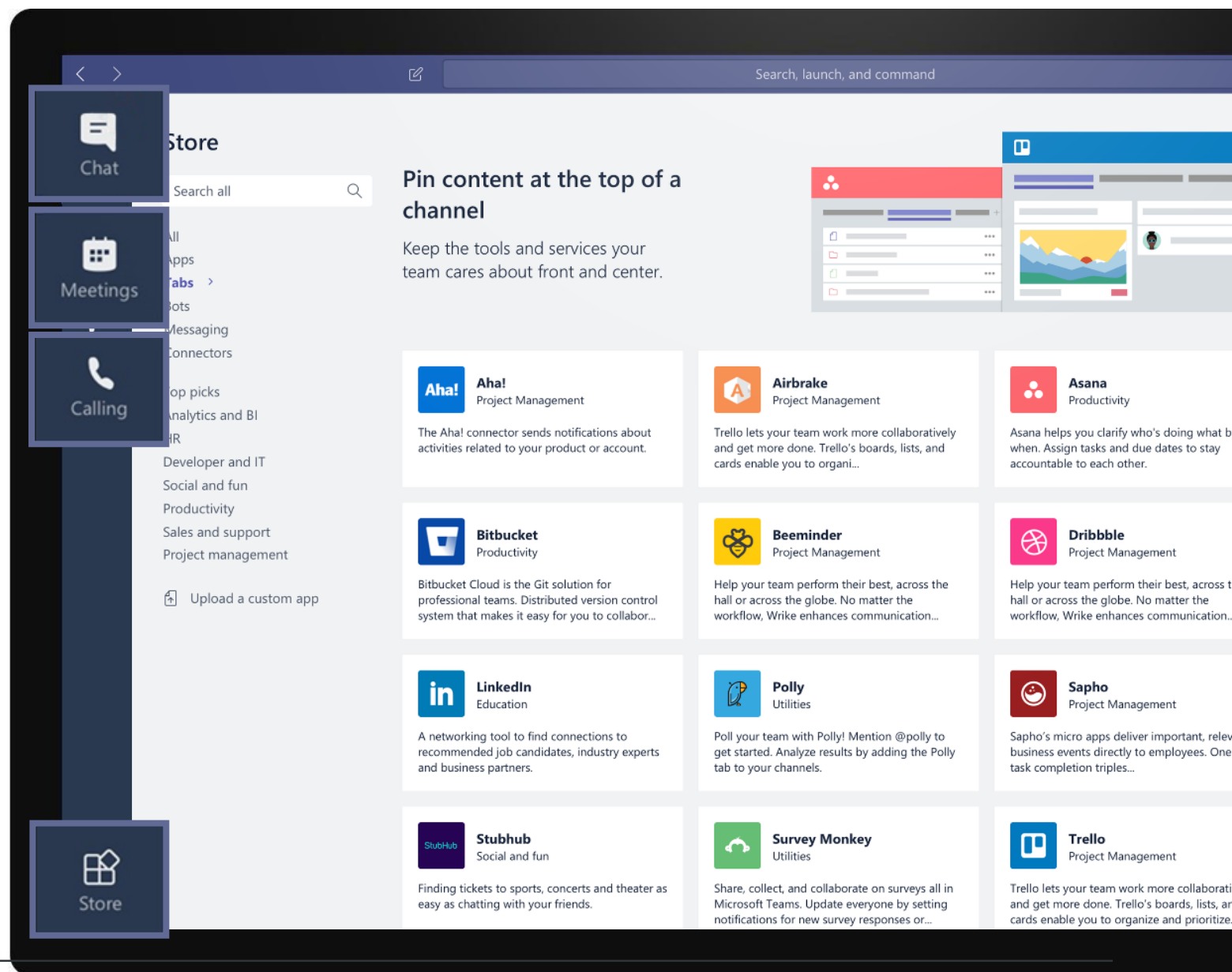
General Observations & Lessons

- Multiple ways to perform an action, need to find the right way – build expertise in PowerShell

- Consoles are continuously evolving as are the services – stay awake!

- Interoperability with Microsoft 365 organizations is fantastic but with non-Microsoft organizations not so much

- Use and take advantage of all the Advanced Threat Protection capabilities

- Expectations may not be reality, e.g. device limit policy or access to AIP protected documents

- Ensure protection, monitoring and auditing of entire service chain, i.e. user, access device, access app, network, service access points, data at rest, in use and in transit

- Get connected with CSE – Canadian Centre for Cyber Security (CCCS)

As a PBMM Pathfinder working with TBS, SSC and CSE, our journey has produced the following GC inputs :

- Detailed configuration documents and exports
- Policy documents
- PowerShell scripts
- Operational processes and procedures
- Test scenarios and results
- Proven SA&A process and tools

Azure PaaS – Data Science Capabilities

Data Strategy

Data Platform

- IIC is building an infrastructure to contain key data that could be of interest to potential investors.
- IIC open access to the lake to key partners:
  - Federal Departments such as GAC
  - Economic Development Offices across the country
- The Lake will use APIs to pull data in from various sources:
  - Statistics Canada
  - Google
- IIC will deliver a PBMM environment for holding this data.
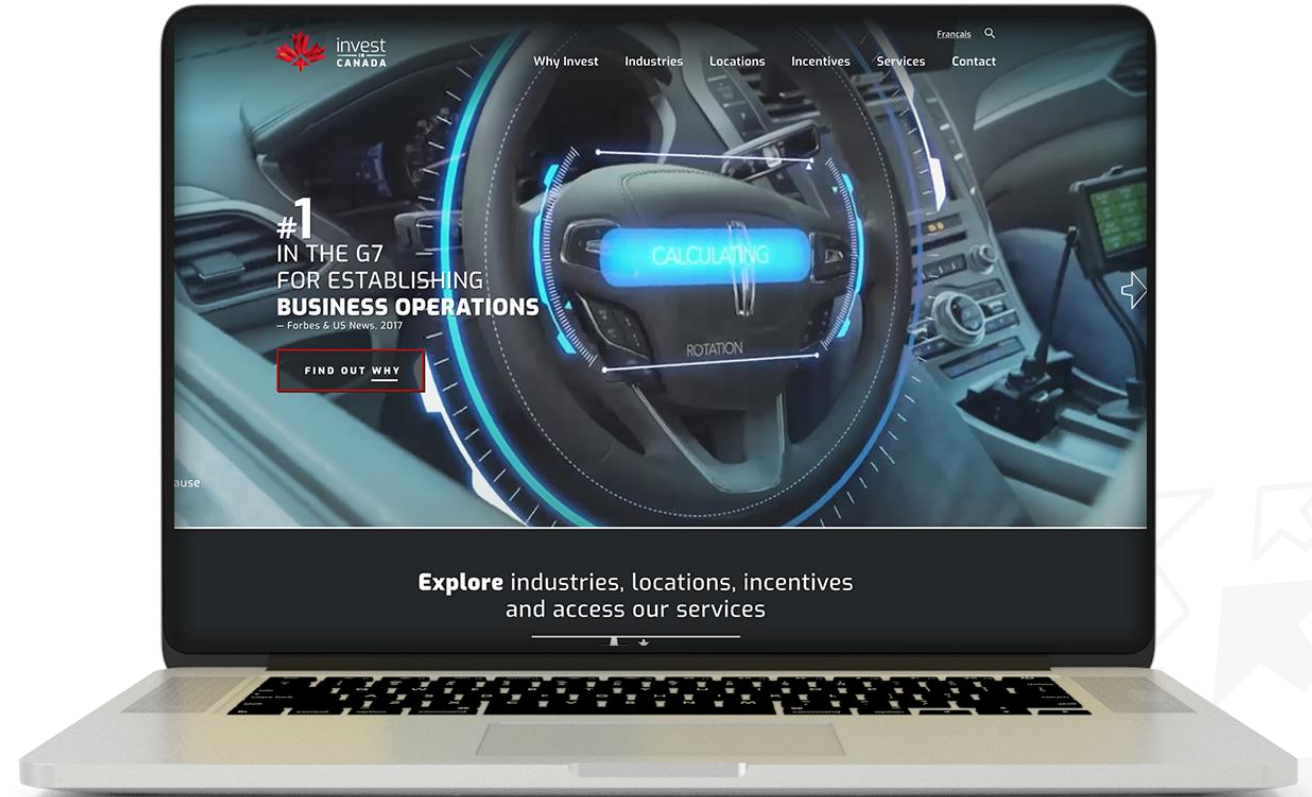
Azure Data Apps

Structured &
Unstructured
Data

Ingest
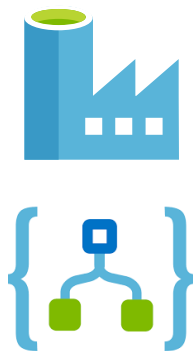
Azure Data
Factory and
Logic App

Store

Azure
Data Lake
(RAW)

**Prep &
Train**

Azure
Databricks

Store

Azure
Data Lake
(CURATED)

Optional

SQL Data
warehouse

**Viz &
Analysis**

COLLISION

ENERCARE CENTRE, TORONTO
MAY 20-23, 2019

"Collision is a crossroads for the world's largest buyers and sellers of technology, alongside many of the world's most disruptive emerging technology companies."

Google Maps API: Companies ecosystem
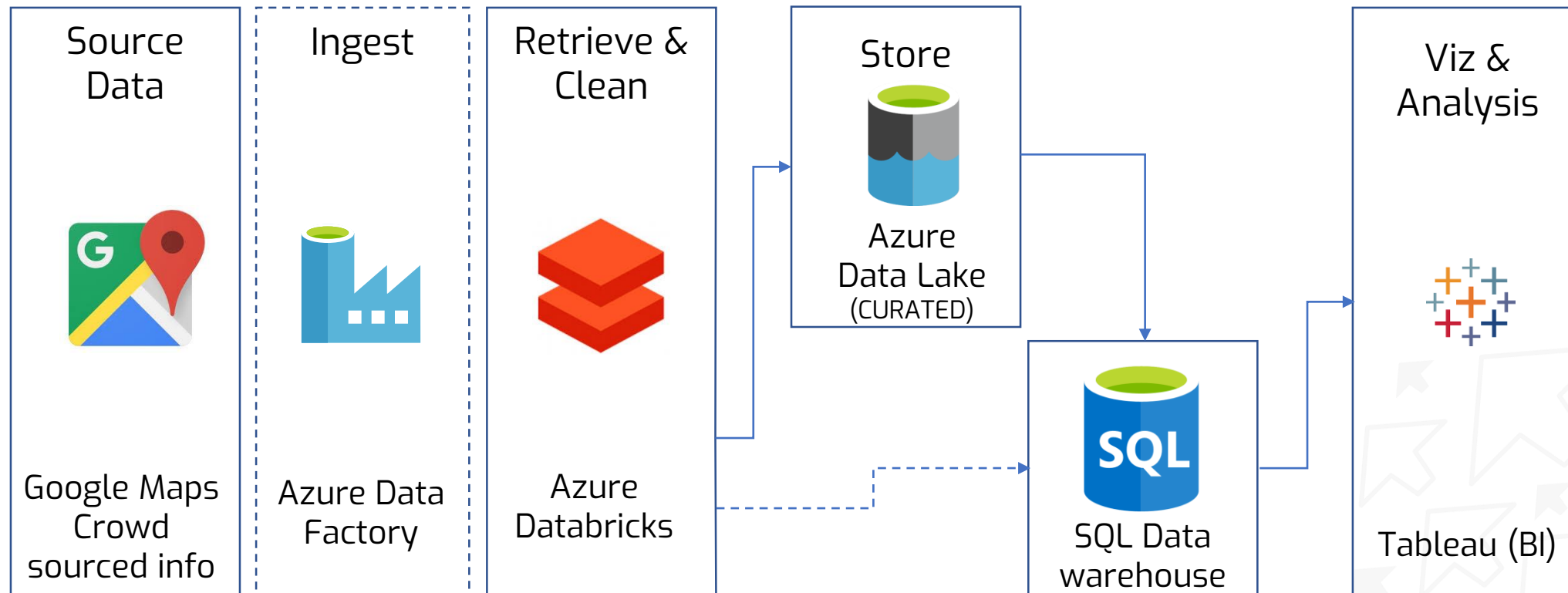
Google Maps API: Companies (CONT'D)

Google Maps API: Companies (CONT'D)
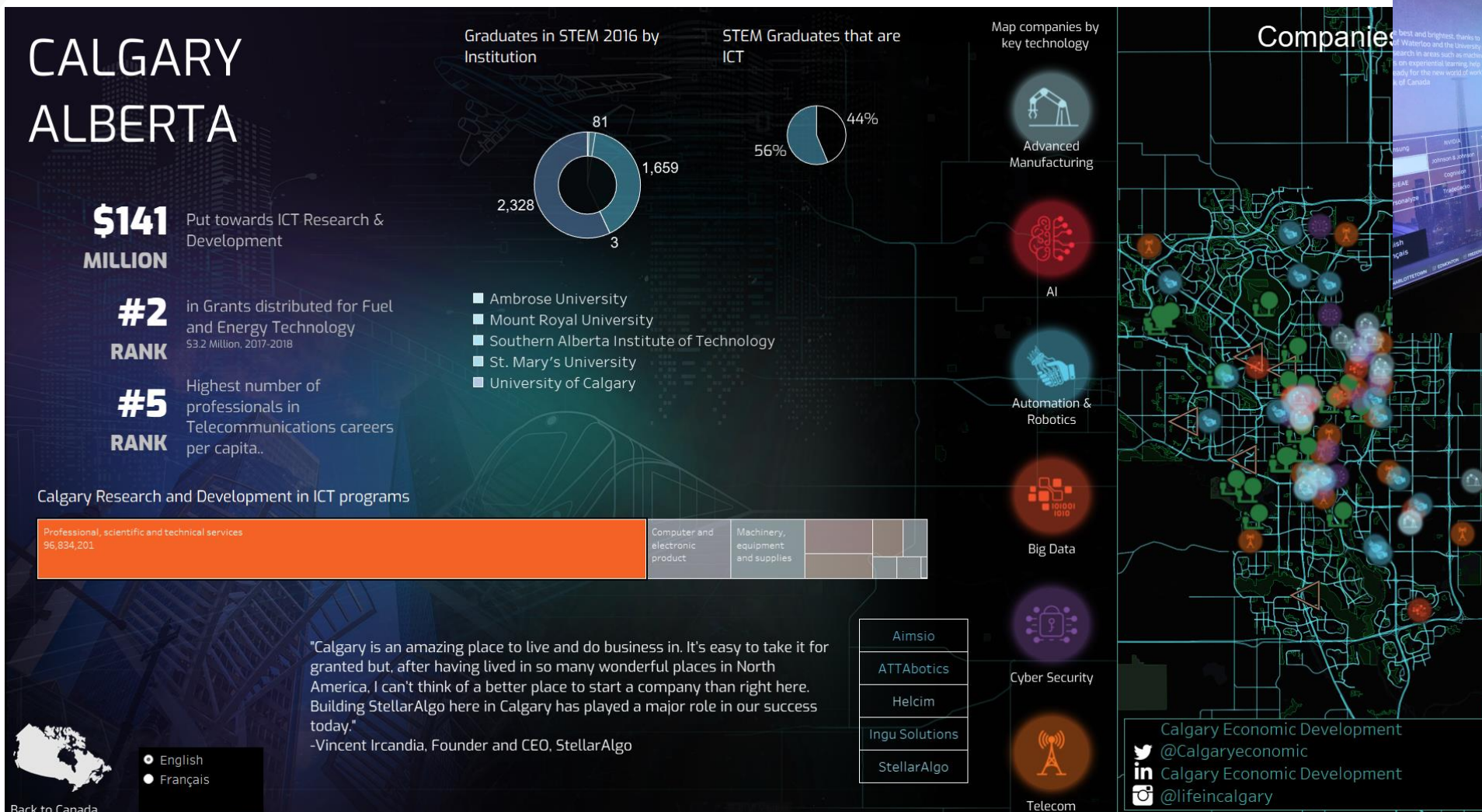
Google Maps API: Companies (CONT'D)

Before Waterloo input
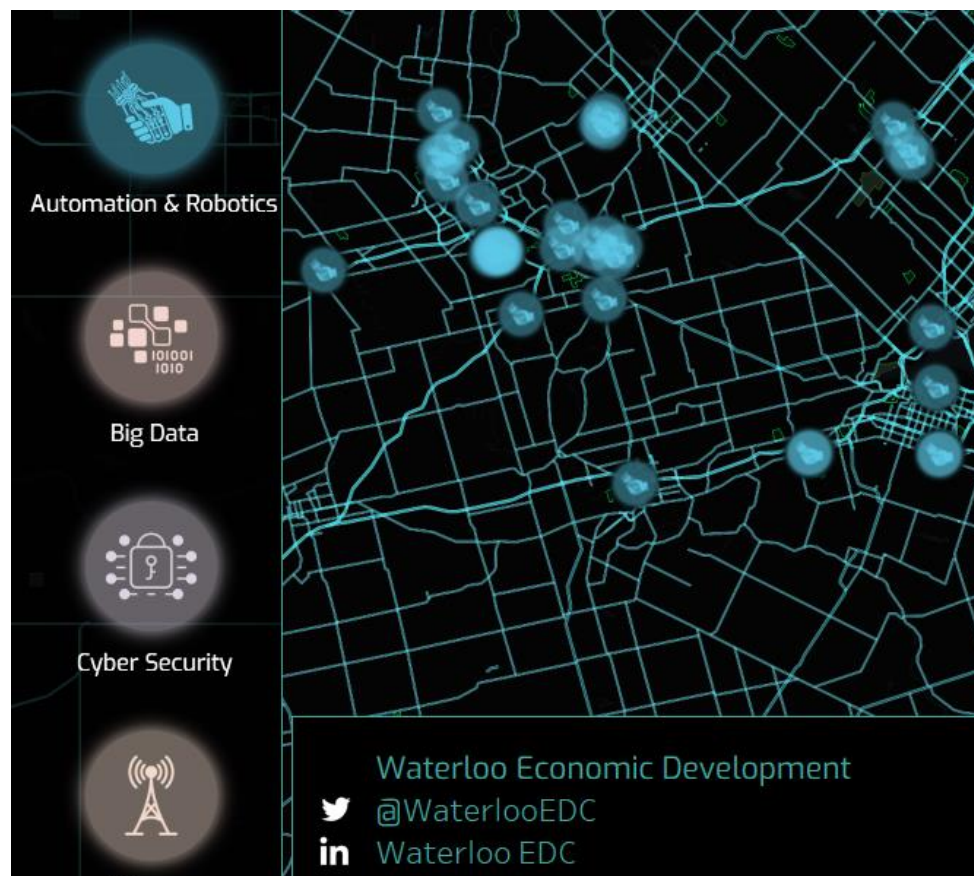
After Waterloo input

Google API: Commute Times

Commute Time Storage & Halifax walking output example:

Halifax-bicycling.csv	34 KB	5/7/2019, 5:53:06 PM			
Halifax-driving.csv	35.3 KB	5/7/2019, 5:53:06 PM			
Halifax-transit.csv	33.1 KB	5/7/2019, 5:53:06 PM			
Halifax-walking.csv	35 KB	5/7/2019, 5:53:06 PM			
Ottawa_Gatineau-bicycling.csv	30.4 KB	5/7/2019, 5:53:06 PM			
Ottawa_Gatineau-driving.csv	31.2 KB	5/7/2019, 5:53:06 PM			
Ottawa_Gatineau-transit.csv	28.8 KB	5/7/2019, 5:53:06 PM			
Ottawa_Gatineau-walking.csv	30.9 KB	5/7/2019, 5:53:06 PM			
Prince_Edward_Island-bicycling.csv	26.9 KB	5/7/2019, 5:53:06 PM			
Prince_Edward_Island-driving.csv	28.3 KB	5/7/2019, 5:53:06 PM			
Prince_Edward_Island-transit.csv	24.5 KB	5/7/2019, 5:53:06 PM			
Prince_Edward_Island-walking.csv	27.7 KB	5/7/2019, 5:53:06 PM			
Regina-bicycling.csv	23 KB	5/7/2019, 5:53:06 PM			
Regina-driving.csv	24.7 KB	5/7/2019, 5:53:06 PM			
Regina-transit.csv	23.1 KB	5/7/2019, 5:53:06 PM			
Regina-walking.csv	24.1 KB	5/7/2019, 5:53:06 PM			
Saskatoon-bicycling.csv	20.9 KB	5/7/2019, 5:53:06 PM			
saskatoon-driving.csv	22.2 KB	5/7/2019, 5:53:06 PM			

CMA	departure_...	origin	origi...	destination	desti...	dista...	duration	distance
Halifax	5:00	Shannon Park, Dartmouth, NS		Downtown Halifax, Halifax, NS			1 hour 25 mins	6.6 km
Halifax	6:00	Shannon Park, Dartmouth, NS		Downtown Halifax, Halifax, NS			1 hour 25 mins	6.6 km
Halifax	7:00	Shannon Park, Dartmouth, NS		Downtown Halifax, Halifax, NS			1 hour 25 mins	6.6 km
Halifax	8:00	Shannon Park, Dartmouth, NS		Downtown Halifax, Halifax, NS			1 hour 25 mins	6.6 km
Halifax	9:00	Shannon Park, Dartmouth, NS		Downtown Halifax, Halifax, NS			1 hour 25 mins	6.6 km
Halifax	10:00	Shannon Park, Dartmouth, NS		Downtown Halifax, Halifax, NS			1 hour 25 mins	6.6 km
Halifax	11:00	Shannon Park, Dartmouth, NS		Downtown Halifax, Halifax, NS			1 hour 25 mins	6.6 km
Halifax	12:00	Shannon Park, Dartmouth, NS		Downtown Halifax, Halifax, NS			1 hour 25 mins	6.6 km
Halifax	13:00	Shannon Park, Dartmouth, NS		Downtown Halifax, Halifax, NS			1 hour 25 mins	6.6 km
Halifax	14:00	Shannon Park, Dartmouth, NS		Downtown Halifax, Halifax, NS			1 hour 25 mins	6.6 km
Halifax	15:00	Shannon Park, Dartmouth, NS		Downtown Halifax, Halifax, NS			1 hour 25 mins	6.6 km
Halifax	16:00	Shannon Park, Dartmouth, NS		Downtown Halifax, Halifax, NS			1 hour 25 mins	6.6 km
Halifax	17:00	Shannon Park, Dartmouth, NS		Downtown Halifax, Halifax, NS			1 hour 25 mins	6.6 km
Halifax	18:00	Shannon Park, Dartmouth, NS		Downtown Halifax, Halifax, NS			1 hour 25 mins	6.6 km
Halifax	5:00	Duffus at Devonshire		5201 Duke St, Halifax, NS B3J 1N9, Canada			42 mins	3.3 km
Halifax	6:00	Duffus at Devonshire		5201 Duke St, Halifax, NS B3J 1N9, Canada			42 mins	3.3 km

Air Traffic Connectivity sample output:

Lessons Learned

- Apply the Data Science Project Lifecycle and develop and explore data and solutions iteratively

- Multiple free learning resources available on the web; such as Github, Google, Microsoft documentation and videos.

- Limited coding knowledge take you further than you might think. (Drag and Drop)

- Overwhelming amount of applications available (some overlap in functionality)

# Federating Cloud Environments

MS Office Integration

To provide ease of access we have federated our Salesforce environment with our M365 tenant and with MS Office Products.

Salesforce uses our AAD credentials to authorize user access to the technology stack:

- This enables SSO

This significantly increased adoption and user productivity.

- MS Outlook & Salesforce
- Sharepoint & Salesforce
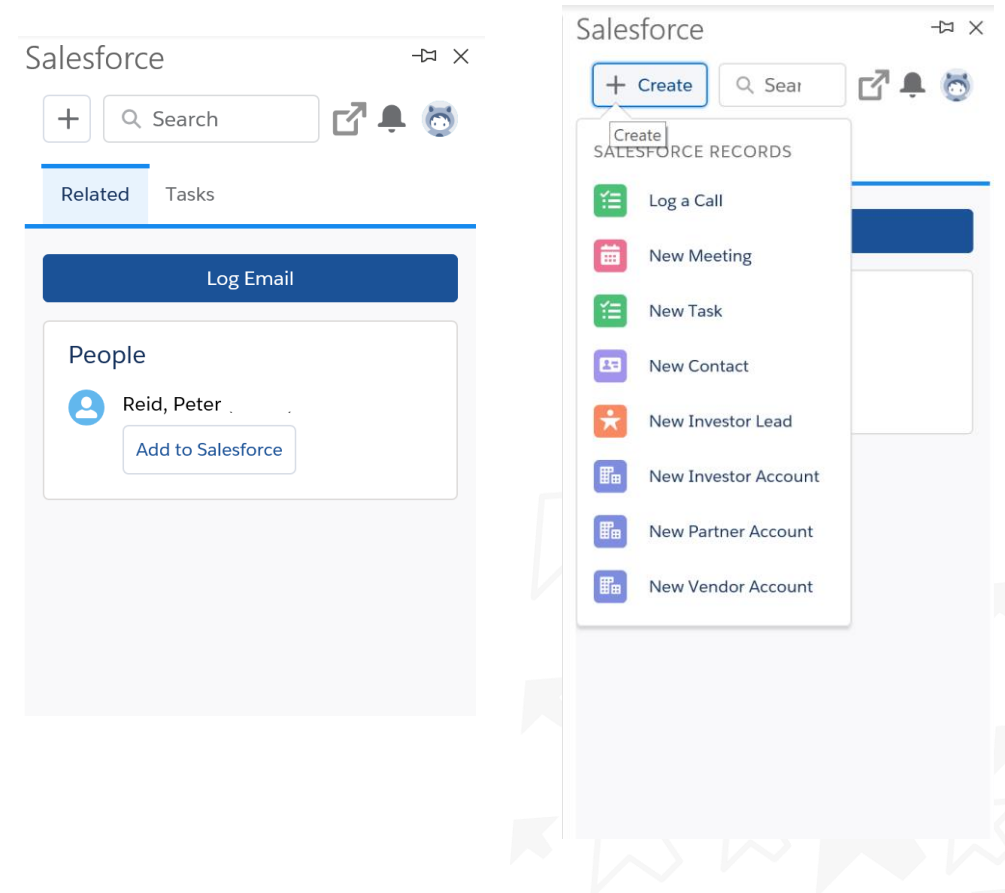
Contact

Gary Devis

**DIRECTOR, BUSINESS SOLUTIONS,
DATA & ANALYTICS**

Gary.Devis@invcanada.ca

C: (613) 323-4815