Our Zero Trust Journey

Improving Security in the Justice and Public Safety Sector through Zero Trust

March 12, 2025

ISB
Information Systems Branch

About me: **Ryan Loiselle**

Background:

- Cisco Network Analyst (CCNA/CCNP), Red River College
- *nix SME – Solaris 9, 10, 11 on SPARC
- Applied Computer Science, Business, Rhetoric, University of Winnipeg

Experience:

- **MTS Allstream** (now BellMTS)
  - 7 years Customer Care (all technical roles in residential + business)
  - 8 years Network Management SME (Fault, Configuration, Performance)
- **BC Government**
  - Started on IDIM program, 6 months
  - 2 years as Technical Architect
  - 6 years as Solutions Architect

Context and Situation

CONTEXT: ABOUT ISB ARCHITECTURE

Provide consultative Architecture services to the broader Justice and Public Safety sector, including the Ministries of Attorney General, Public Safety and Solicitor General and Emergency Management and Climate Readiness.

Clients are broad, complex, unique, independent, secure and form the foundation of our justice and public safety systems.

THE SITUATION: THE FOCUS OF TODAYS PRESENTATION

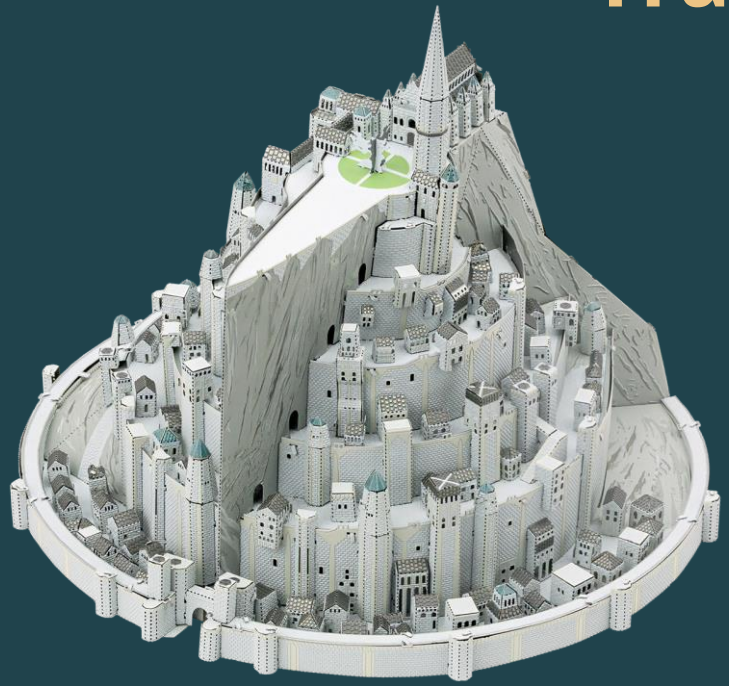
A business area with high volume of data (15+ TB/month), stringent security and legal requirements was adopting one of the sectors first cloud-based applications.

Security by design, performance objectives and the Security Threat and Risk Assessment pointed at the need for something better than the historical approach.

We were outside the castle walls after all…

The Historical Approach

Traditional Castle & Moat



- The classic perimeter security model.
- Some public apps, more private apps.
- VPN or location-based access.
- Static network (IP:port) based decisions.
- Low Identity Assurance.

Once you are in, you are trusted, and we trust all on the network in the same way.

ISB
Information Systems Branch

The evolution: ZERO TRUST?

"The term "**Zero Trust**" (ZT) does not apply to a *single* product, technology, or architecture layer.

Rather, it represents a ***security framework*** for protecting infrastructure and data. ZT's central tenet is that ***no subject (application, user, or device) in an information system is trusted by default***.

Trust must be re-assessed and verified every time a subject requests access to a new resource."

Source: https://www.cyber.gc.ca/en/guidance/zero-trust-security-model-itsap10008

Identity

DIAM

Network

Next-Generation

Device

The Unknown Complexity

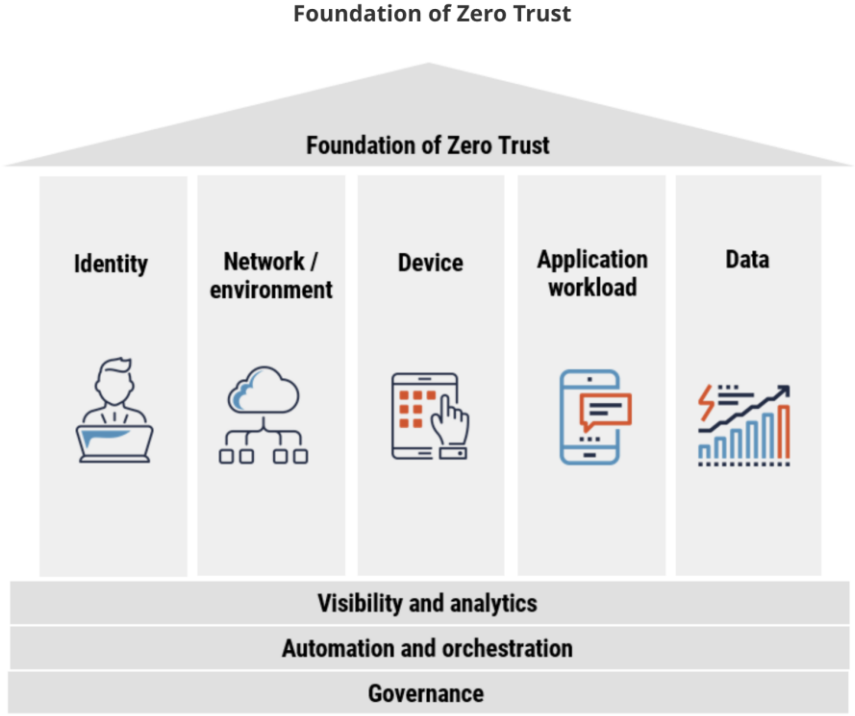
Application

Policy Based Access

Data

Secure Everywhere

Zero Trust?



Source: https://www.cyber.gc.ca/en/guidance/zero-trust-security-model-itsap10008

Zero Trust: **Identity**

Creation of Digital Identity and Access Management strategy, team and services.

Common-SSO:

- Identity Provider brokering
- Identity Protocol translation
- Identity Data Model translation

Access Management provisioning services.

High Level of Assurance Identity Products:

- X.509 certificate based AuthN using OCIO DSC iKey
- Verified Credentials (Law Society of BC) + BC Services Card
- Biometrics (BC Corrections)
- Police IDPs (including their MFA technologies)

ISB
Information Systems Branch

Zero Trust: **Network**

Our Desires:

- Micro segmentation
- Non routable/resolvable
- Tagging/Metadata/Visibility
- Policy Based decisions

Our Journey:

- Micro segmentation & Cloud Native architectures, circa 2018
- Partner with OCIO Platform Services re: Aporeto in OpenShift, circa 2019/2020
- Partner with OCIO hosting to create VM SDN (Vmware + RestNSX), circa 2021/2022
- Partner with OCIO Platform Service to create Emerald OpenShift environment, circa 2023
- SASE/ZTNA adoption by major business unit, circa 2023/2024
- Partner with OCIO Networks on SASE, 2025/2026

Zero Trust: **Device**

This has been traditionally outside the Architecture space, as our work and products are traditionally the destination from enterprise service that we consume (that standard devices and browsers).

However, we can now use device postures and grouping in the process of making policy-based access decisions. This is a new and desirable capability.

This has also been the slowest part of our journey – packaging, testing, deploying and redoing this process is cumbersome and time consuming – not because of any product, but the process.

Zero Trust: **Application/Workload**

Policy Based access using Real Time Identity attributes.

- In terms of access to the application space through the SASE
- Work to surface, expose and modernize the access model that governs access to the data within the eventual application destination, our Legacy Modernization journey.

Enhancements to SDLC (further adoption of DevSecOps) with adoption of GitOps and secure deployment patterns.

Zero Trust: **Data**

- Limiting duplication of sensitive data.
- Rich meta data for all data types, including security tagging and the ability to use this meta data in policy-based decisions.
- Encryption at rest and in transit, and everywhere.
- Starting to talk about and look at Quantum Safe Encryption for data with a long durability.

Zero Trust: **Supporting Services**

- **Visibility and Analytics**: Monitoring and Visibility team and tooling now in place and required on every project.
- **Automation and Orchestration:** Still to do.
- **Governance:** Working to include in SDLC / Emerald standard.

ISB
Information Systems Branch

Zero Trust: **The Challenges**

- **Cost** – new tech and the cost to shift left.
- **Transition Strategy** - big bang or bit by bit.
- **Culture Change** – working in this space involves a different mindset.

ISB
Information Systems Branch

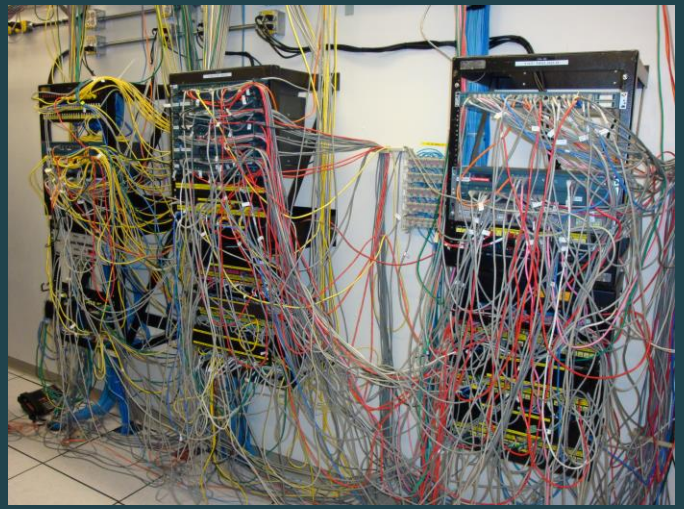
Thanks!

Any questions?

You can find me at:

Ryan.Loiselle@gov.bc.ca

250.380.8656



ISB
Information Systems Branch