CANADIAN CENTRE FOR CYBER SECURITY

Zero Trust

Who we are: Canadian Centre for Cyber Security (CCCS)

- The Canadian Centre for Cyber Security (the Cyber Centre) is part of the Communications Security Establishment. We are a single unified source of expert advice, guidance, services and support on cyber security for Canadians.

Who we are: CCCS Security Architecture

- Advice and guidance on how to architect and design systems with security in mind.
- Lead on various CCCS publications
  - ITSG-33 – IT security risk management: A lifecycle approach
  - ITSP.80.022 – Baseline security requirements for networks security zones
  - ITSG-38 – Network security zoning – Design considerations for placement of services within zones

What is Zero Trust?

What is Zero Trust? – From NIST SP800-207

What is Zero Trust? – From NIST SP800-207

- *Zero trust (ZT)* provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.
- *Zero trust architecture (ZTA)* is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan

What is Zero Trust? – From an AI chatbot

What is Zero Trust? – From an AI chatbot

- It is like a secret club where you need to give your password every time you want to get in, even if you are already recognized as a member of the club.

Zero Trust is explicit

- In the Zero Trust model, the trust to access and consume resources, like data, is granted **explicitly**. There is *zero* **implicit** trust granted.

Zero Trust is explicit

- In the Zero Trust model, the trust to access and consume resources, like data, is granted **explicitly**. There is *zero* **implicit** trust granted.
- Zero Trust requires **explicit** trust for each *subject* to access and execute an action on a *resource*.
  - A subject can be a person, a workload/application, or a device. A resource is something accessed by the subject, such as data or a workload.

Zero Trust is explicit

- In the Zero Trust model, the trust to access and consume resources, like data, is granted **explicitly**. There is *zero* **implicit** trust granted.
- Zero Trust requires **explicit** trust for each *subject* to access and execute an action on a *resource*.
  - A subject can be a person, a workload/application, or a device. A resource is something accessed by the subject, such as data or a workload.
- The trust allows a subject to carry out an action requiring the *least privileges*.

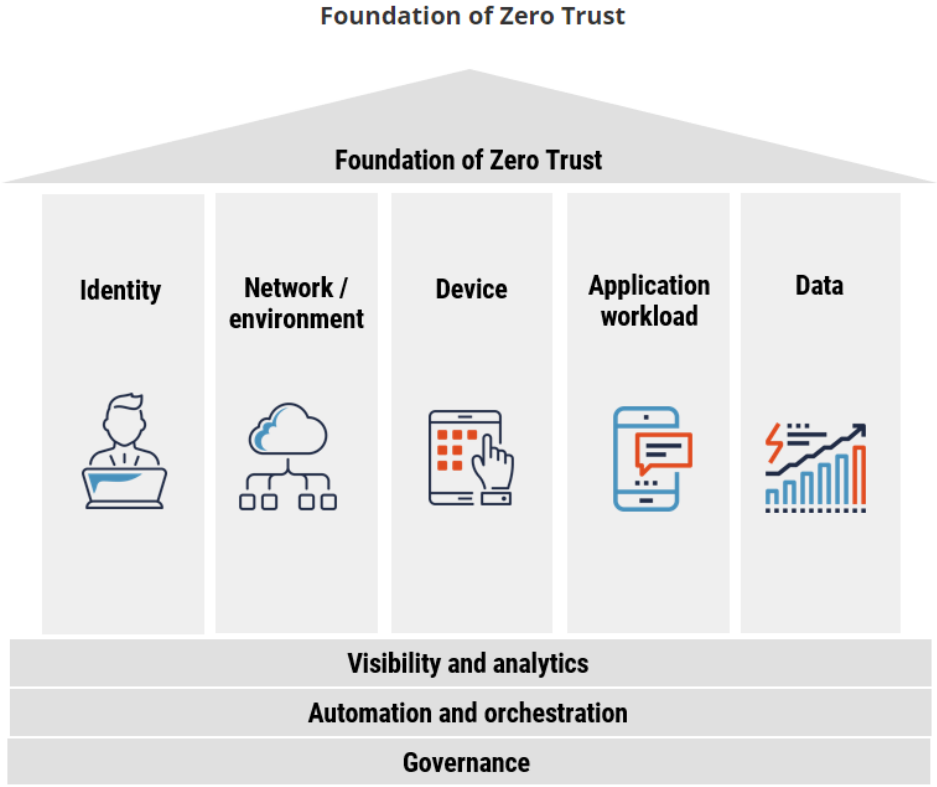
Zero Trust is explicit

- In the Zero Trust model, the trust to access and consume resources, like data, is granted **explicitly**. There is *zero* **implicit** trust granted.
- Zero Trust requires **explicit** trust for each *subject* to access and execute an action on a *resource*.
  - A subject can be a person, a workload/application, or a device. A resource is something accessed by the subject, such as data or a workload.
- The trust allows a subject to carry out an action requiring the *least privileges*.
- The trust is *constantly* and *automatically* evaluated and dynamically updated to ensure the subject is trusted for the *current context*.

What Zero Trust is not

- Zero trust is not a product
  - There is no silver bullet solution, zero trust is a set of concepts and ideas.
- Zero trust is not static
  - There is no set it and forget it point
- Zero trust is not impossible
  - There is a roadmap to success

Building Zero Trust

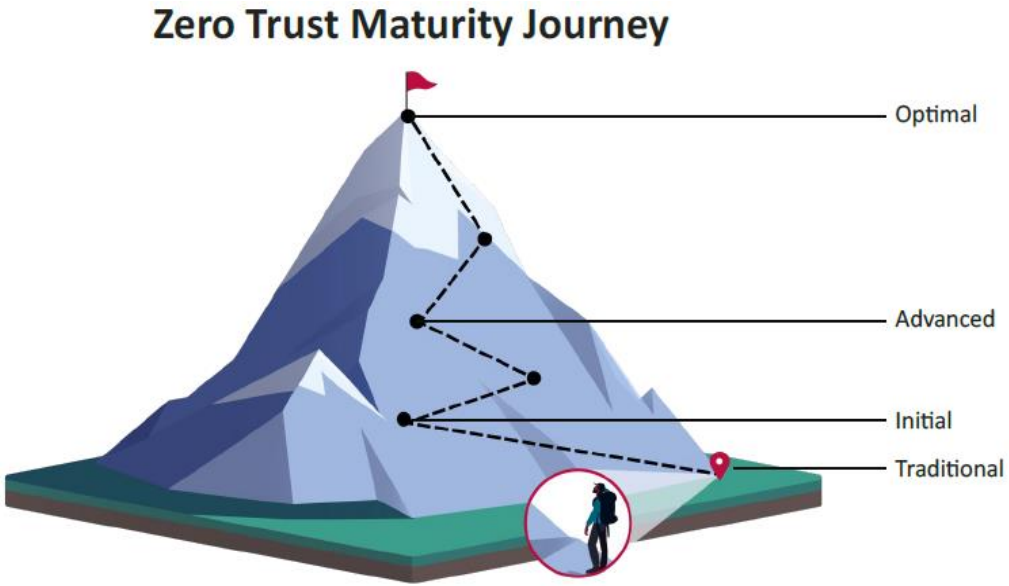


Building Zero Trust

- Zero trust is a marathon not a sprint.

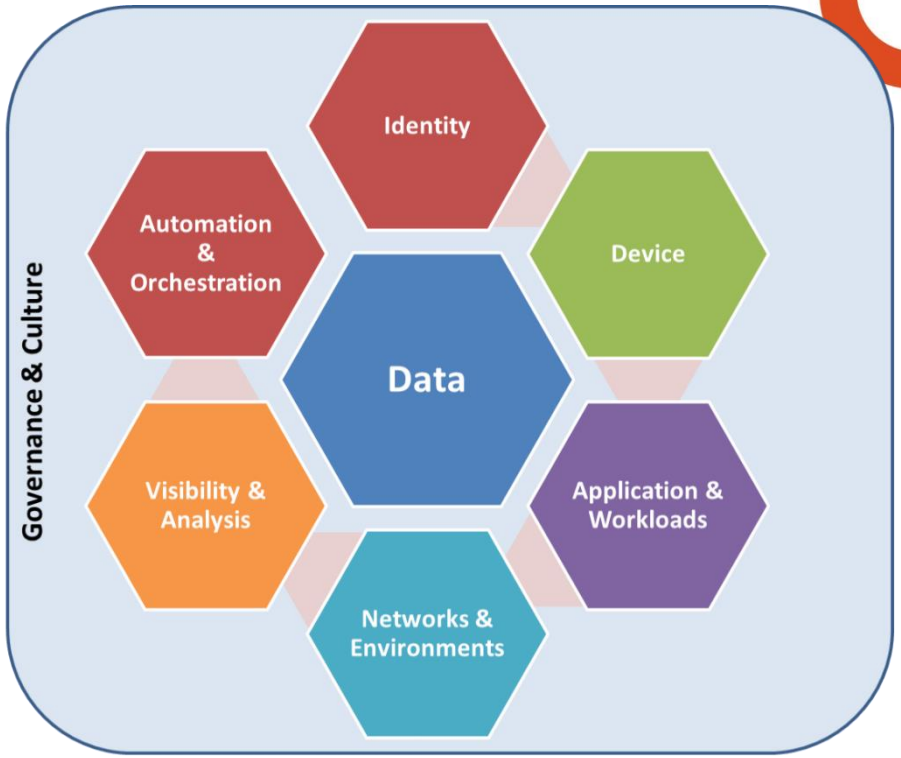
Building Zero Trust – Zero Trust Maturity Model

- Zero trust is a marathon not a sprint.
- Zero trust maturity model



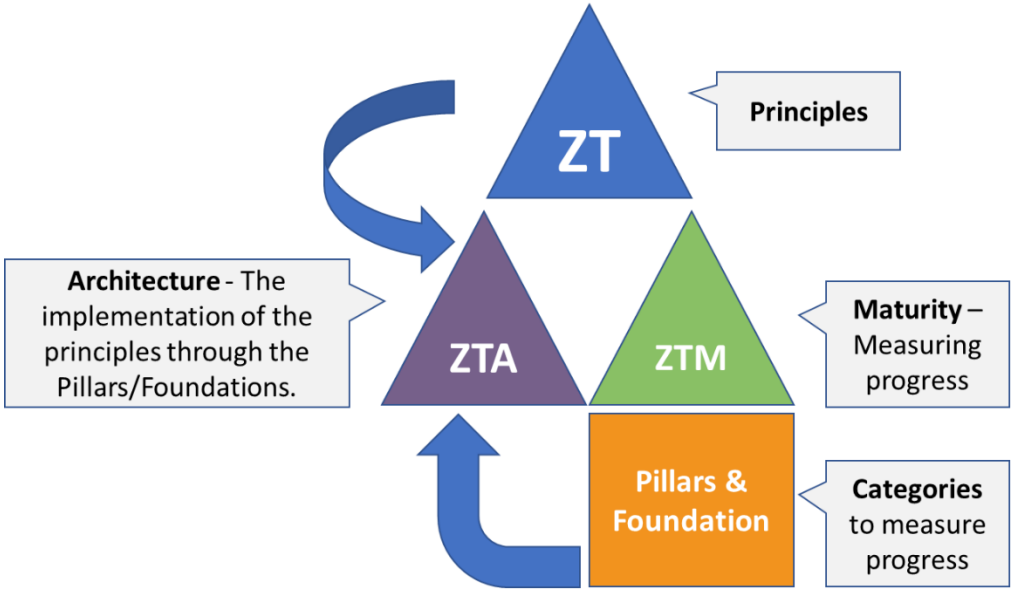
Building Zero Trust – Zero Trust Maturity Model

Level	
0	The initiative is undocumented and performed on an ad hoc basis with processes undefined. Success depends on individual efforts.
I	The process is documented and is predictably repeatable, using lessons learned in the initial phase.
II	Processes for success have been defined and documented.
III	Processes are monitored and controlled; efficacy is measurable
IV	Focus is on continuous optimization



Zero Trust Architecture

- Zero Trust Architecture is the implementation of the principles an concepts in the pillars and foundation to and organization's IT landscape.



Where does CCCS fit in?

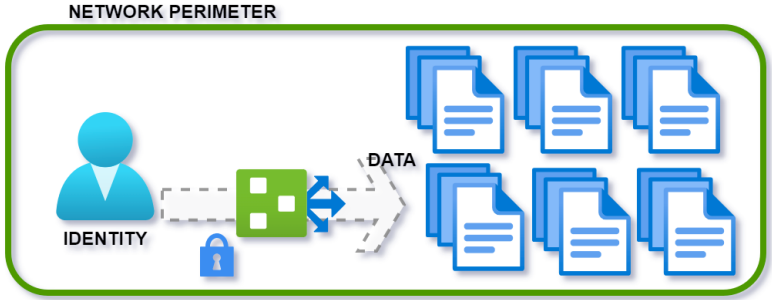
- CCCS has published
  - ITSAP.10.008 - Zero Trust security model
  - ITSM.10.008 - A zero trust approach to security architecture
- CSE and CCCS are internally progressing on our path towards a Zero Trust architecture
- Working in collaboration with TBS and SSC on the GC's approach to Zero Trust

Questions?

John.Parker@cyber.gc.ca

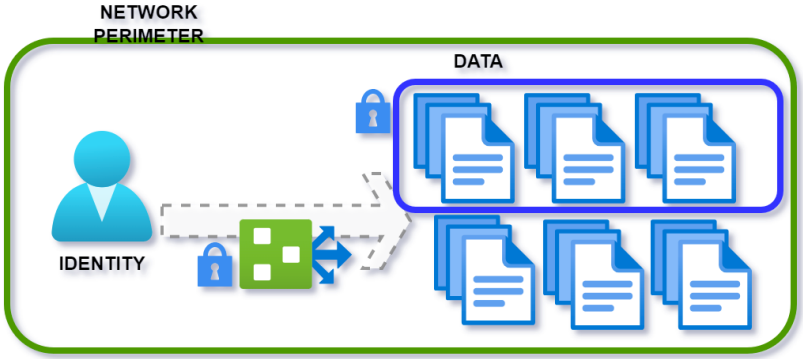
In the beginning (Network-centric)

- Identity Authentication: IP address & user account
- Permission Level: Based on network access
- Frequency of authentication: Upon accessing resource (network). Renewal not enforced.
- Perimeter Type/Trust Boundary: Network
- Resource location: On premise
- Data Access: Network based
- Authentication Time frame: Persistent
- Level of Trust: Implicit based on network.



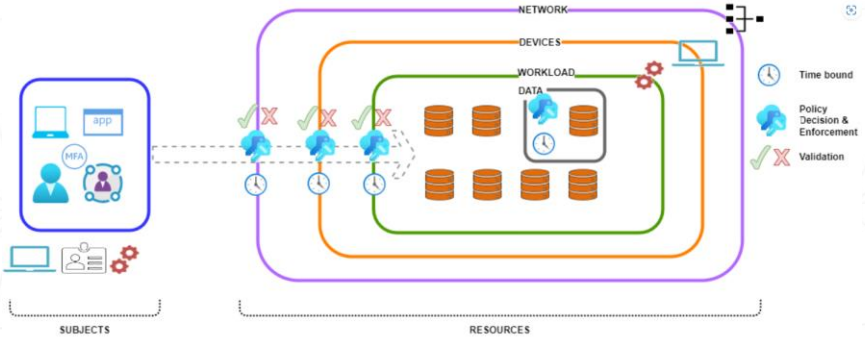
Role Based Access (RBAC)

- Authentication: IP address & user account & role
- Permission Level: Based on role (Role Based Access Control - RBAC)
- Frequency of authentication: Upon accessing resource (network/data). Renewal not enforced.
- Perimeter Type/Trust Boundary: Network and Data
- Resource location: On premise and some remote
- Data Access: Role based
- Authentication Time frame: Persistent
- Level of Trust: Implicit based on role



Role Based Access (RBAC)

- Authentication: User, MFA, Device validation
- Permission Level: Least permissions granted
- Frequency of authentication: Dynamic, granular, continual, and context driven
- Perimeter Type/Trust Boundary: Micro perimeter, layered, and granular
- Resource location: On premise and remote
- Data Access: Very granular (just-enough)
- Authentication Time frame: Dynamically assessed, time bound (just-in-time)
- Level of Trust: Explicitly granted based on policies. No implicit trust



Tenets of Zero Trust

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

Tenets of Zero Trust - Simplified

1. Everything is unique and needs access control.
2. Traffic is from point A to point B, and only be visible by point A and point B.
3. “Trust but Verify” turns into “Never trust, always verify”
4. Dynamic access based on a set of attributes.
5. The security posture of assets is not static, and must be monitored
6. Building off earlier tenets, access is granted and reviewed continuously.
7. Zero trust does not have an end state, and collecting and analyzing information allows for continuous improvement.