Zero Trust security model

CANADIAN CENTRE FOR CYBER SECURITY

November 2022 | ITSAP.10.008

The traditional security model used by organizations to protect information systems focused on perimeter defense and implicitly trusted anyone inside the corporate network, therefore granting them access to resources. As more governments and enterprises undergo digital transformation, adopt cloud-based technologies, and embrace remote/hybrid work, the traditional perimeter-focused defenses are no longer sufficient to protect internal networks and data. This document provides information on Zero Trust (ZT) as a model to address the modern challenges of securing remote workers, protecting hybrid cloud environments, and defending against cyber security threats.

What is 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. The degree of access provided is dynamically adjusted based on the level of trust established with the subject. ZT involves adopting a new mindset to security by always assuming a breach and focusing on resource protection (e.g. services and data). With an ever changing technology landscape and more sophisticated and persistent cyber threats, the ZT security model can help organizations to significantly improve their cyber defenses.

The Government of Canada (GC) is working on developing a ZT Security Framework that is based on the CISA model and the National Institute of Standards and Technology's (NIST) special publication. The framework includes ZT concepts and components that can be leveraged by departments and agencies to improve the GC's overall security posture.

> "Never trust, always verify"

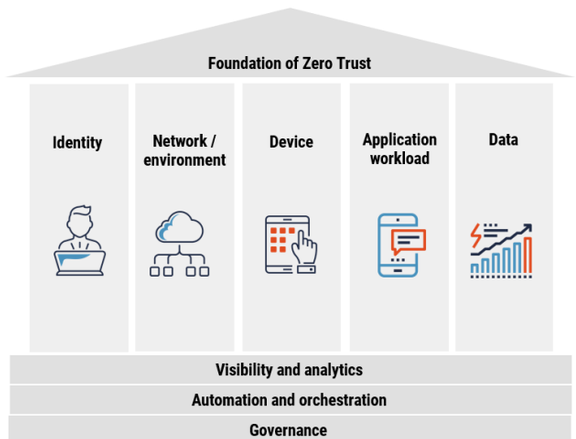
CISA Zero Trust Maturity Model

The U.S. Cyber security and Infrastructure Security Agency (CISA) proposes a ZT model that consists of five pillars and three capabilities. This model is designed to provide organizations with a roadmap and resources to achieve an optimal zero trust environment over time.

Identity. Use phishing-resistant multifactor authentication (MFA) and continuously validate users and entities throughout their interactions with services or data. Use enterprise-managed identities for both on-premises and cloud environments. Implement least privilege access.

Network/Environment. Utilize micro-segmentation to isolate critical data from other data. Control privileged network access, manage data flows (internal and external) and encrypt all traffic and connections.

Device. Establish baseline device security protections. Continuously monitor and validate device security. Use machine learning analytics to make access control decisions for services and data. Conduct regular inventory of devices.



Application workload. Continuously authorize access to applications. Strongly integrate threat protections into application workflows. Integrate application security testing throughout the development and deployment process.

Data. Protect data on devices, in applications and in networks. Inventory, categorize and label data, and deploy mechanisms to detect data exfiltration. Encrypt all data at rest or in transit (in cloud or remote environments).

Visibility and analytics. Utilize tools like advanced security analytics platforms and security user behaviour analytics to observe and analyze real-time user behaviour, service and device health. Log and analyze all access events for suspicious behaviours.

Automation and orchestration. Automate security and network operational processes by managing functions between all the security systems and applications. Implement just-in-time and just-enough access controls. Automatically enforce strict access controls for high-value data.

Governance. Automate enforcement of data protections required by policy. Use automated discovery of networks, devices, and services with manual or dynamic authorization and automated remediation of unauthorized entities.

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada

Zero Trust security model

CANADIAN CENTRE FOR CYBER SECURITY

November 2022 | ITSAP.10.008

What are the benefits with ZT?

While there is no perfect security strategy and some form of cyber threats will always exist, ZT is an effective approach to increase an organization's cyber security posture for today's digital transformation. Some of the benefits of ZT includes:

- **Increases network security.** Every digital interaction (e.g user connecting to an application) is verified and authorized continuously to ensure conditional requirements of an organization's security policies are met. Coupled with network segmentation and strong user and device authentication, this will improve overall network security.
- **Reduces impact from data breach.** Smaller trust zones mean cyber threat actors need to be authenticated and authorized to a new security boundary each time they access a different resource. This would limit their lateral movement across the network and reduce potential harm from a data breach.
- **Improves data protection.** ZT leverages technologies such as strong encryption, VPNs and data loss prevention capabilities to protect all data at rest or in motion.
- **Achieves continuous compliance.** By improving visibility of who, what, and where, ZT enables network operators to more closely log behavior and activities to verify compliance to policies.
- **Improves visibility, detection and response.** Automatic logging and monitoring of cyber related events from user devices and services gives an overall real-time view of the environment. Analytics improves visibility for network operators to develop proactive security measures before incidents occur or to quickly respond to threats.
- **Enables modernization of the workforce with a secure solution.** ZT enables new ways of working, by securely connecting users, devices, applications, and services over any network (on-premises, public cloud or hybrid environment) using identity-based validation policies.

Learn more about ZT architecture, frameworks and guidelines:

- NIST SP 800-207: Zero Trust Architecture
- NIST SP 1800-35: Implementing a Zero Trust Architecture (Preliminary Draft)
- CISA's Zero Trust Maturity Model
- National Cyber Security Centre—UK, "Zero trust architecture design principles"
- Australian Cyber Security Centre Australia - Essential Eight Maturity Model

What are the challenges with ZT?

Organizations looking to improve their security posture with ZT will need to consider some challenges they may face which include:

- **Increased time and effort** to strongly authenticate every user and device using two factor authentication. Significant technical and administrative work across organizations is needed to define and implement detailed attributes of every user and resource to support trust/access decisions.
- **Increased organizational focus and commitment** will be needed over multiple years which could make ZT difficult to achieve. ZT affects multiple levels of infrastructure and operations - all of which require tight coordination to succeed.
- **Increased chance of being locked into a long-term commitment with cloud providers' proprietary systems.** Organizations with multi-cloud solutions may encounter such challenges since ZT is a framework and not an industry standard. Partnership with commercial cloud providers is key to properly understand the organization's business and security objectives in order to select the appropriate solution.

How to transition to a ZT security model?

To improve your organization's cyber security posture consider implementing the following steps as a starting point in your transition towards ZT:

Enforce strong MFA. Aim for Level of Assurance (LoA) 3. Check out our publication for more details on "*User authentication guidance for information technology systems (ITSP.30.031 v3)*".

Employ just-in-time (JIT) and just-enough access (JEA) risk-based adaptive policies to implement least privilege access.

Grant access based on user and device information and not only logical location. Use multiple data points (e.g identity, location, device health, resource, data classification, and anomalies) to make security decisions.

Use dedicated devices, Privileged Access Workstations (PAW) and Secured Admin Workstations (SAW) to separate sensitive tasks and accounts from non-administrative computer uses, such as email and web browsing.

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada