A Zero Trust Module for Cybersecurity Education

CISSE 2024

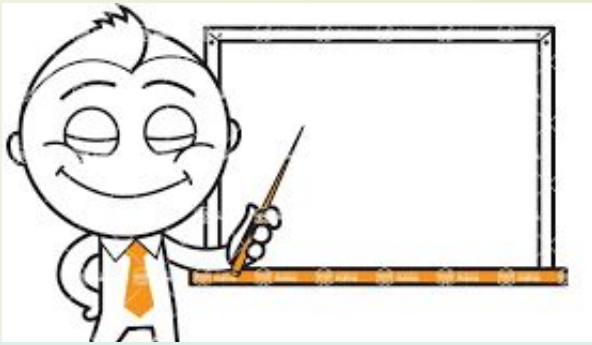
Xinli Wang, Vijay Bhuse, and Yuan Cheng

College of Computing
Grand Valley State University

CISSE 2024

Outline

- Motivation
- Zero trust
  - What is it?
  - Problems it tries to resolve
  - How these problems are mitigated
  - Issues – is it perfect?
- Conclusion and discussion



The teaching module includes:

1) A lecture to introduce zero trust.
2) Homework assignment.
3) Test questions.

Our Teaching Module

- Our teaching module includes:
  - A lecture to introduce zero trust – principles, architectures, and challenges.
  - Homework assignment – gain more in-depth understanding of zero trust through self-study.
  - Test questions.
- Introduction to zero trust is focused for this presentation.

Motivation – We need to introduce zero trust in cybersecurity education.

- Many companies have joined and produced their frameworks and products.
- In May 2021, the Biden administration announced a new Executive Order on Improving the Nation's Cybersecurity
  - "the federal government must adopt security best practices [and] advance toward zero trust architecture."
- In March 2023, the Biden administration – National Cybersecurity Strategy, -- "… implement a zero-trust architecture strategy and …"
- Recent survey shows 94% of responded organizations are in the process of implementing zero trust strategies.

But ….

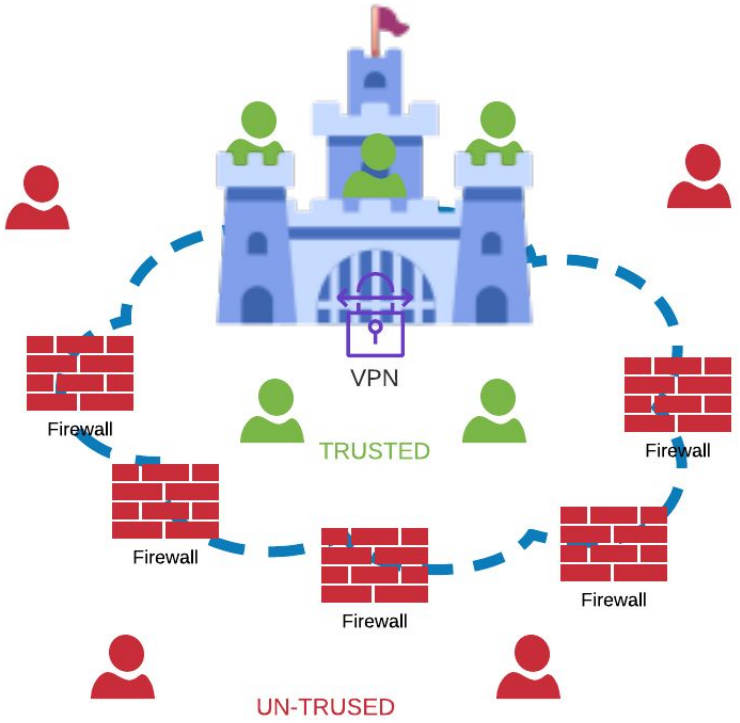
CISSE 2024

- Why do we need zero trust, and what does it mean?

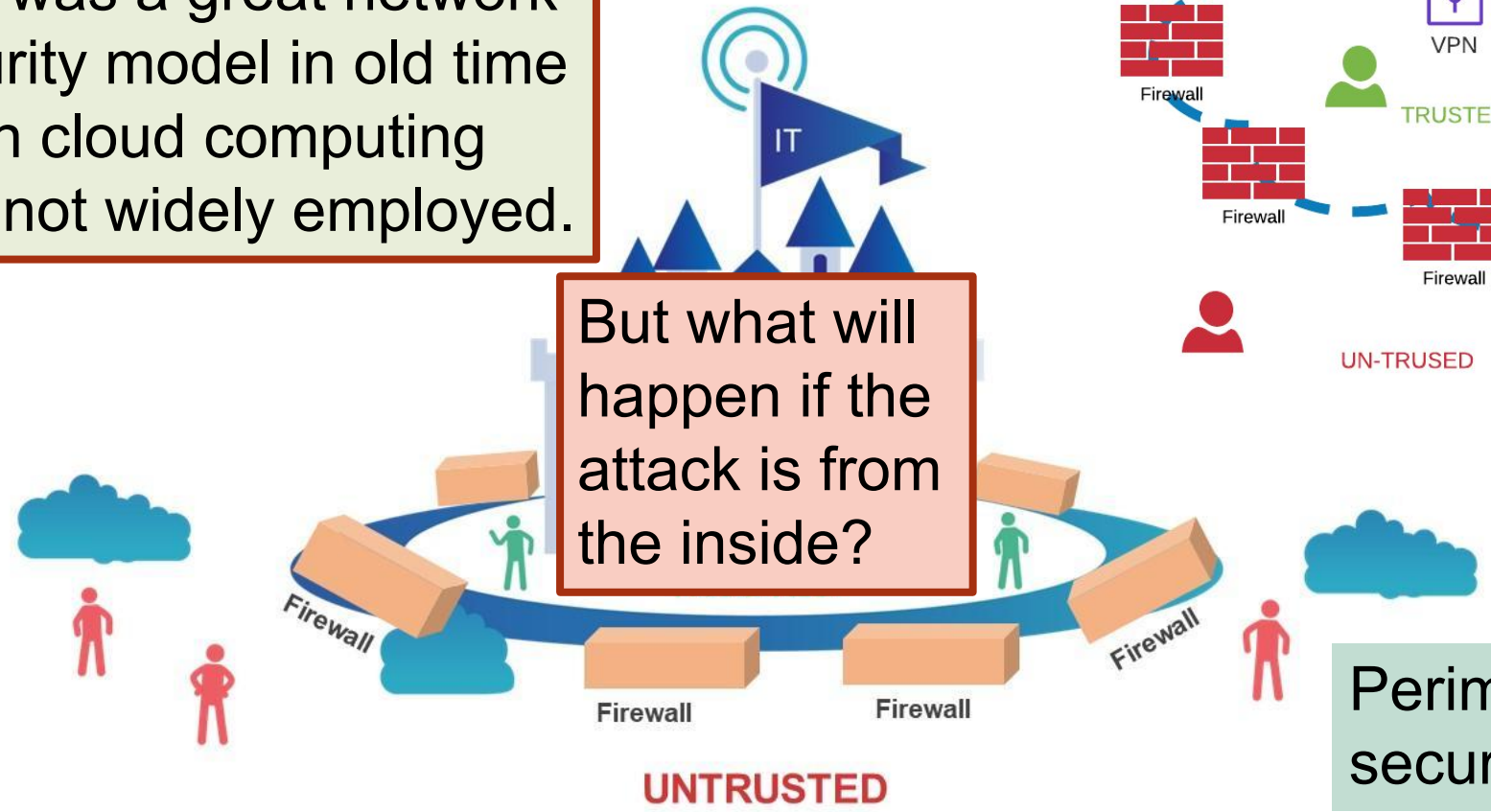
CISSE 2024

Traditional Network Secu

This was a great network security model in old time when cloud computing was not widely employed.

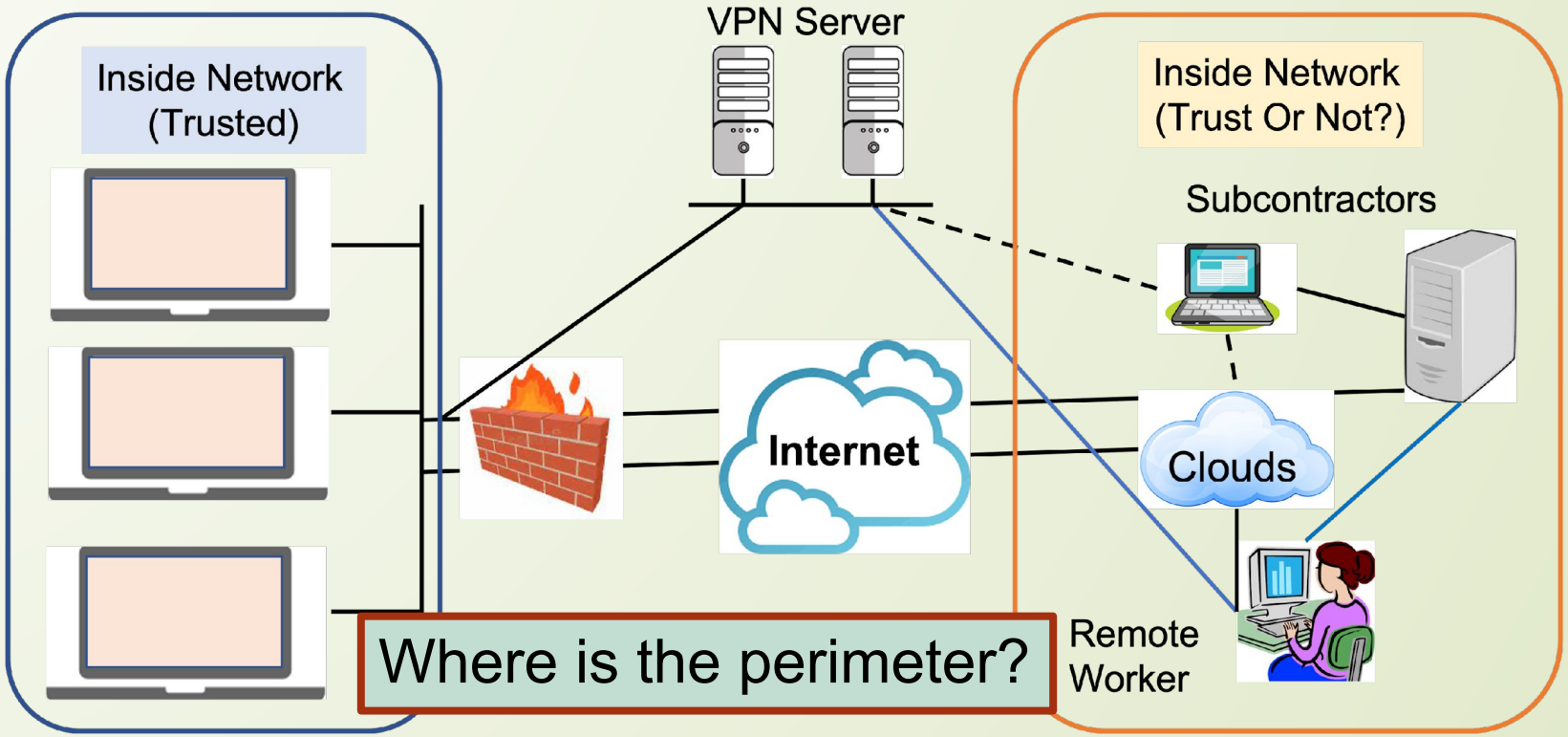


But what will happen if the attack is from the inside?



Perimeter-based security model

Main Components in Modern IT Infrastructure



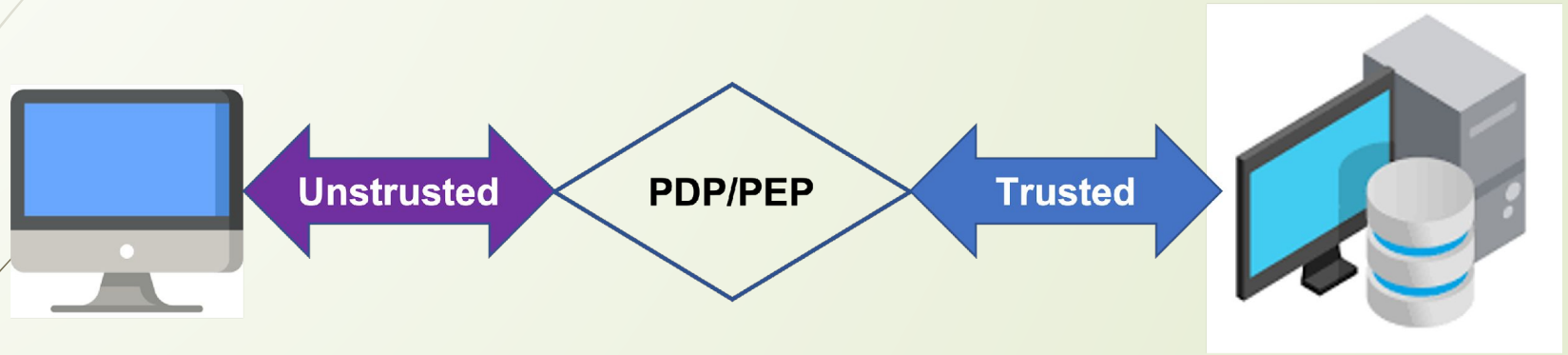
Issues in Perimeter-Based Security Model

- Where is the perimeter? No physical perimeter exists!
- Attacks from inside

In all the cases, the succeeded attacks will be easily spread on the internal network into other systems due the fact that access from the internal network is trusted by default.

This is recognized as “lateral movement”.

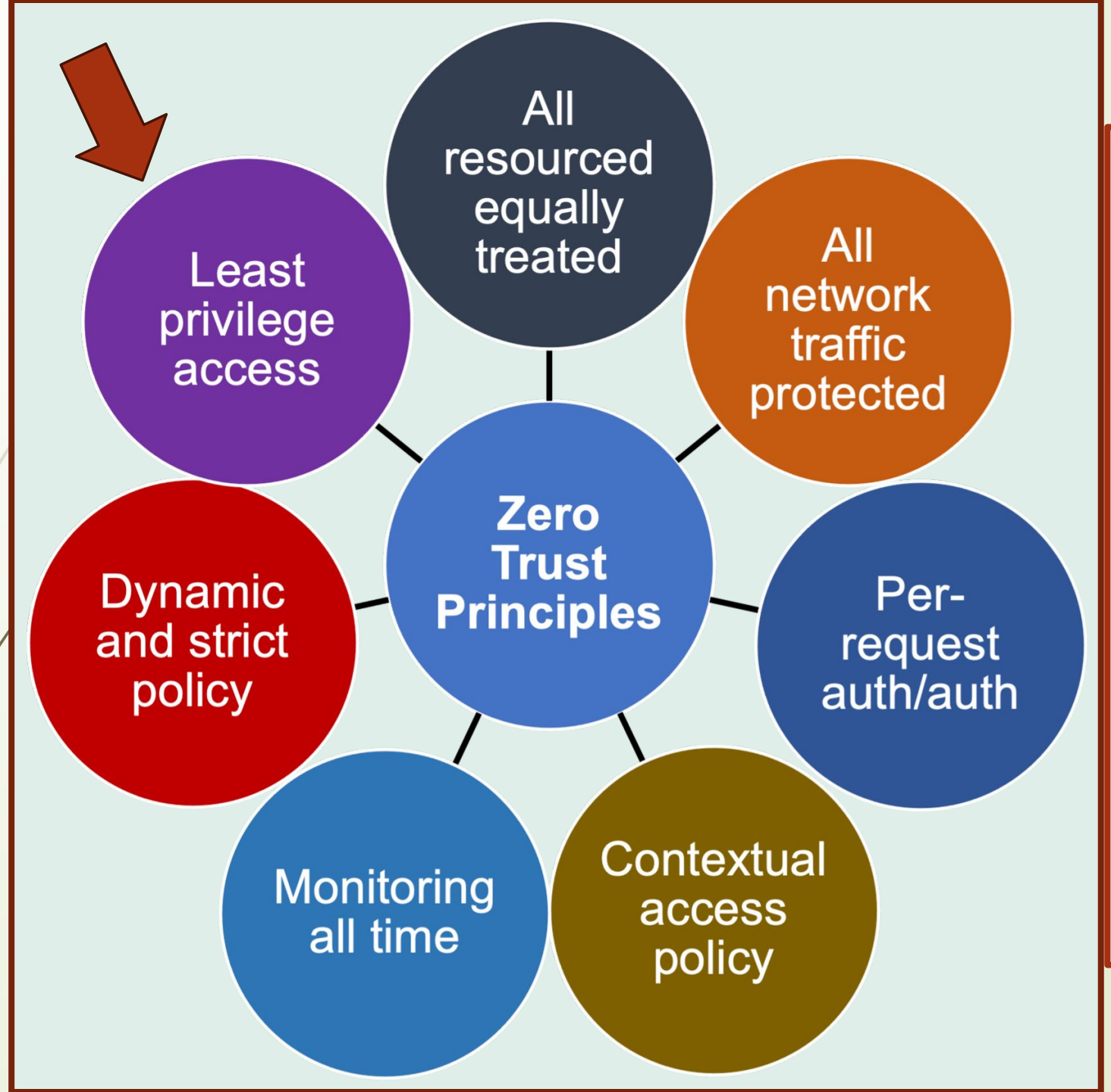
How Can the Issues Be Mitigated?



Philosophy of Zero Trust:

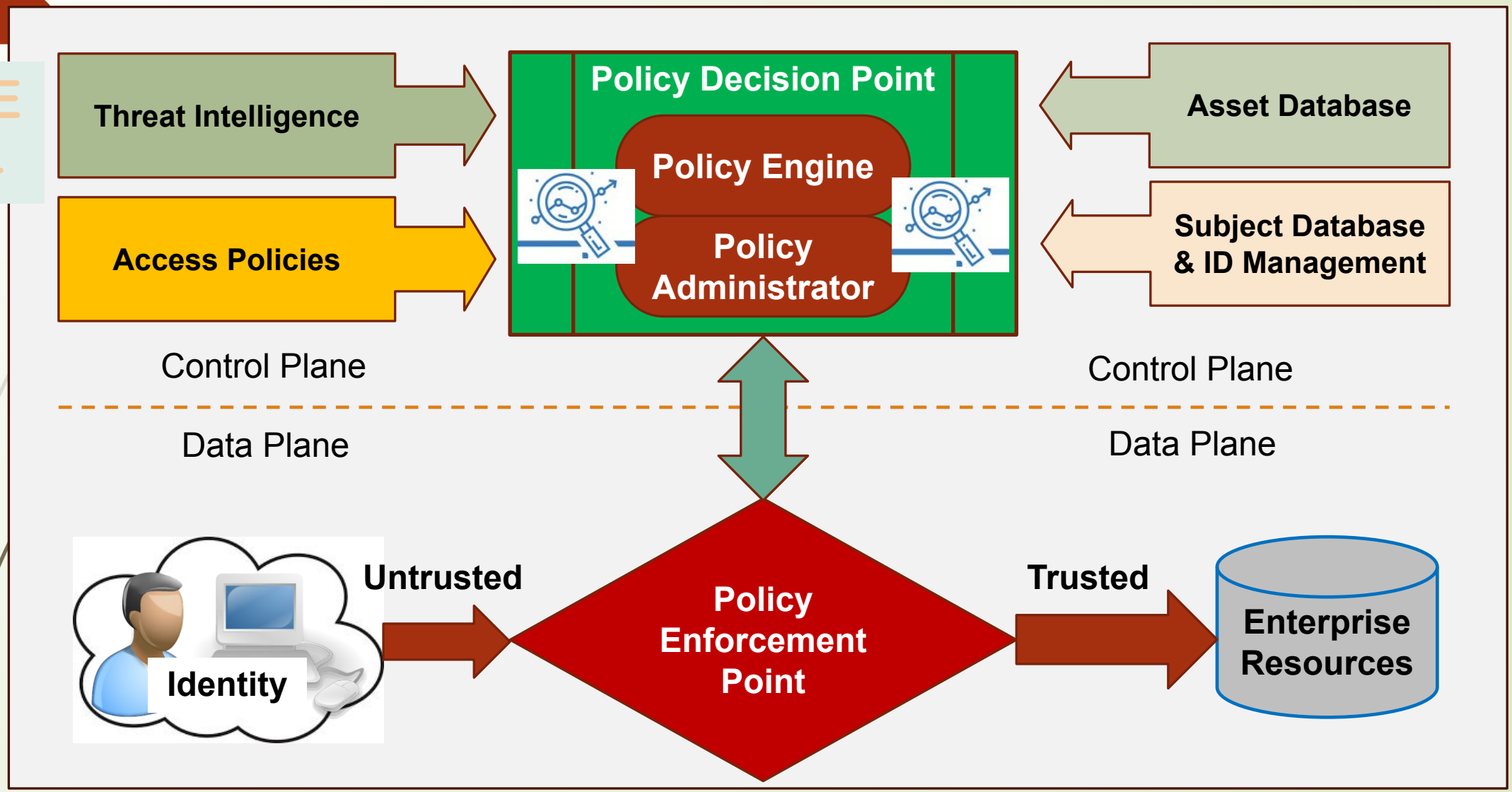
"Never trust, always verify."

The only perimeter on networks is identity – users and devices.



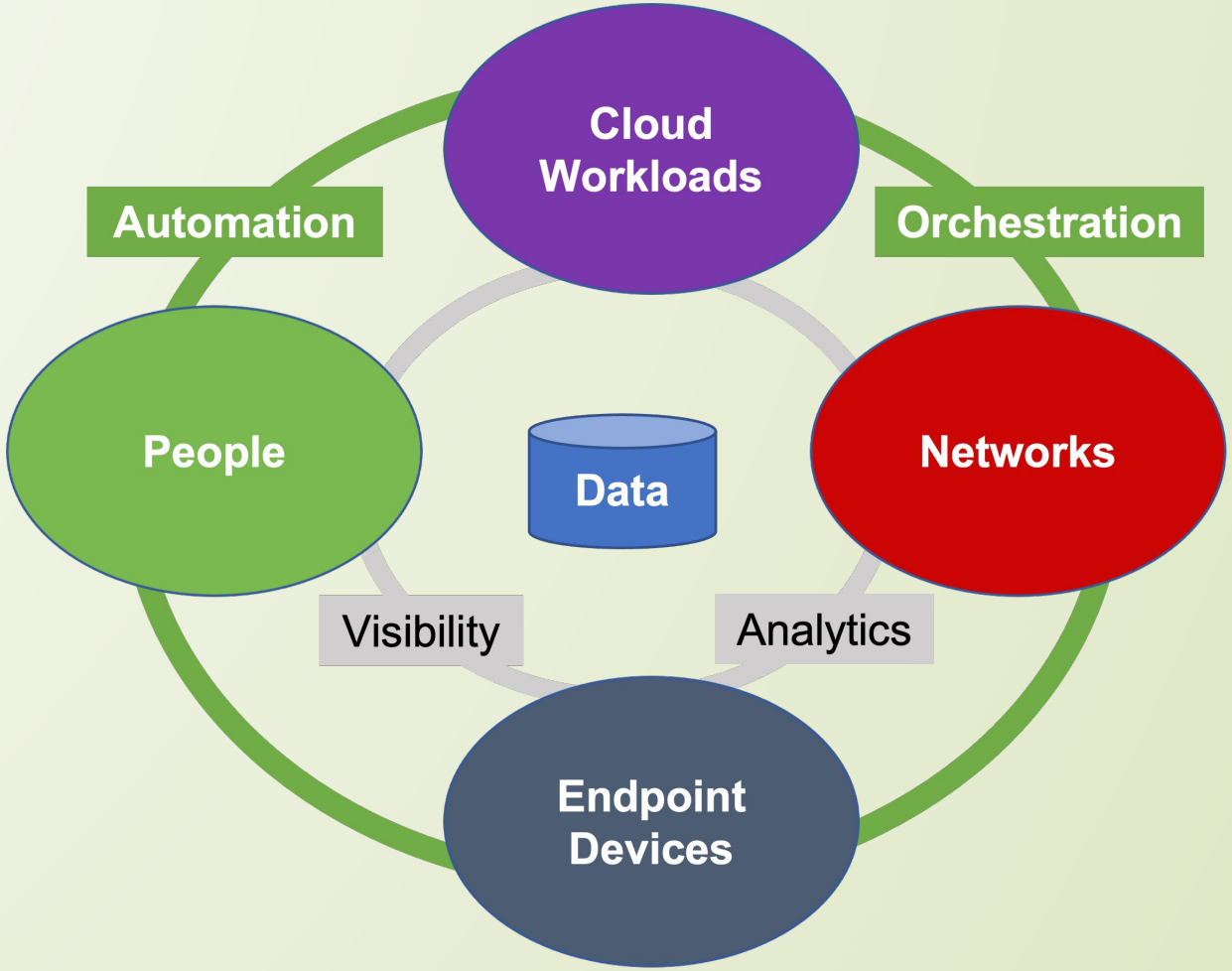
ZT is a collection of guiding principles for workflow, system design, and operation that can be employed to improve the security posture of a system to enforce "least privilege".

Both NIST and Forrester Research give a similar list of principles.


Threat Intelligence
Access Policies
Policy Decision Point
Policy Engine
Policy Administrator
Asset Database
Subject Database & ID Management
Control Plane
Data Plane
Control Plane
Data Plane
Identity
Untrusted
Policy Enforcement Point
Trusted
Enterprise Resources

Zero Trust Architectures – the Forrester ZTX Framework

Forrester Zero Trust Extended (ZTX) ecosystem framework extends data flows across local networks, cloud computing infrastructure, external applications and websites, and a wide range of endpoint devices, including IoT devices.



Benefits of Zero Trust:
-- Does It Resolve the Problems? How? (1 of 3)

- Removal of network perimeter in the design
  - As shown in previous slides, a physical perimeter is effectively removed in the design of zero-trust architecture.
  - All access requests, no matter whether from outside or inside, must be authenticated and authorized based on the identify of a subject at the PDP and enforced at PEP.
  - In other words, the effective perimeter in a zero-trust architecture is identity.

Benefits of Zero Trust:
-- Does It Resolve the Problems? How? (2 of 3)

- Effective mitigation of lateral movement
  - In a fully featured implementation of ZTA, it is highly unlikely that an adversary or malware program will be able to spread through a network starting from a comprised endpoint device.
  - This is because ZTA provides end-to-end protection, continuous monitoring and evaluation, and per session verification, especially the integration of Threat Intelligence and its use at the PDP.

Benefits of Zero Trust:
-- Does It Resolve the Problems? How? (3 of 3)

- Quick detection of compromised devices and data breaches
  - With ZTA, the integrated subsystems are watching, and the status of the system is analyzed continuously with SIEM, continuous diagnostics and mitigation subsystem, along with system and security logging systems and threat intelligence system.
  - This ability to inspect all network traffic and packets through the application layer provides the security operation teams with visibility.

Technical Challenges to Practice Zero Trust

- Huge number of complicated policies
  - Huge number of policies are expected, may be dynamic
- Effective integration of various sub systems
  - SIEM, threat intelligence, PKI, ID management, etc., not easy even to implement each of them
- Lack of standardization
  - Need standardization to avoid “lock-in” problem

Potential Cyber Threats

- Subversion of ZTA decision processes
- Denial-of-service attack
- Stolen credential and insider threat
- Monitoring techniques and tools
- Use of non-person entities in ZTA administration

Takeaways

CISSE 2024

- Zero trust has been there for more than a decode. It has been attracted high interest due to the explosion of the use of cloud computing.
- A physical perimeter is effectively removed from the design of a zero-trust architecture. All accesses are verified before being granted.
- With the integration of continuous monitoring and threat intelligence systems, lateral movement of attacks can be effectively mitigated. Data breaches can be detected shortly.

End of the Lecture

CISSE 2024