NEbraskaCERT

Zero Trust in Zero Trust

Applying Zero Trust in the Age of AI

Ron Woerner
With Special Guest: Rob LaMagna-Reiter

⭐ Area Announcements

- OWASP Omaha-Lincoln, June 12, 11:30AM-1:00PM
- AI Omaha, June 4, 5:30PM
- FutureCon Omaha, Aug 12, 8AM-5PM

Sound Familiar?

Introduction

If you have questions/comments please feel free to ask them anytime. You don't have to hold them until the end of the talk.

If there are other resources similar to these that you think might be useful to people, please let the group know.

Hopefully, this will be an interactive and productive session.

Shamelessly stealing (more) from Aaron

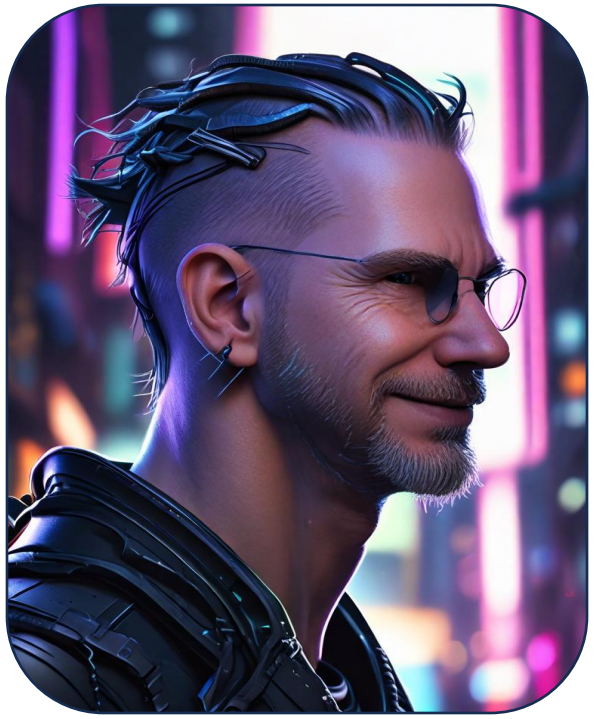
Who are we?

We'd tell you who we are, but do you really care?

Ron Woerner, CISSP, CISM

https://www.linkedin.com/in/ronwoerner/

https://linktr.ee/cyberron



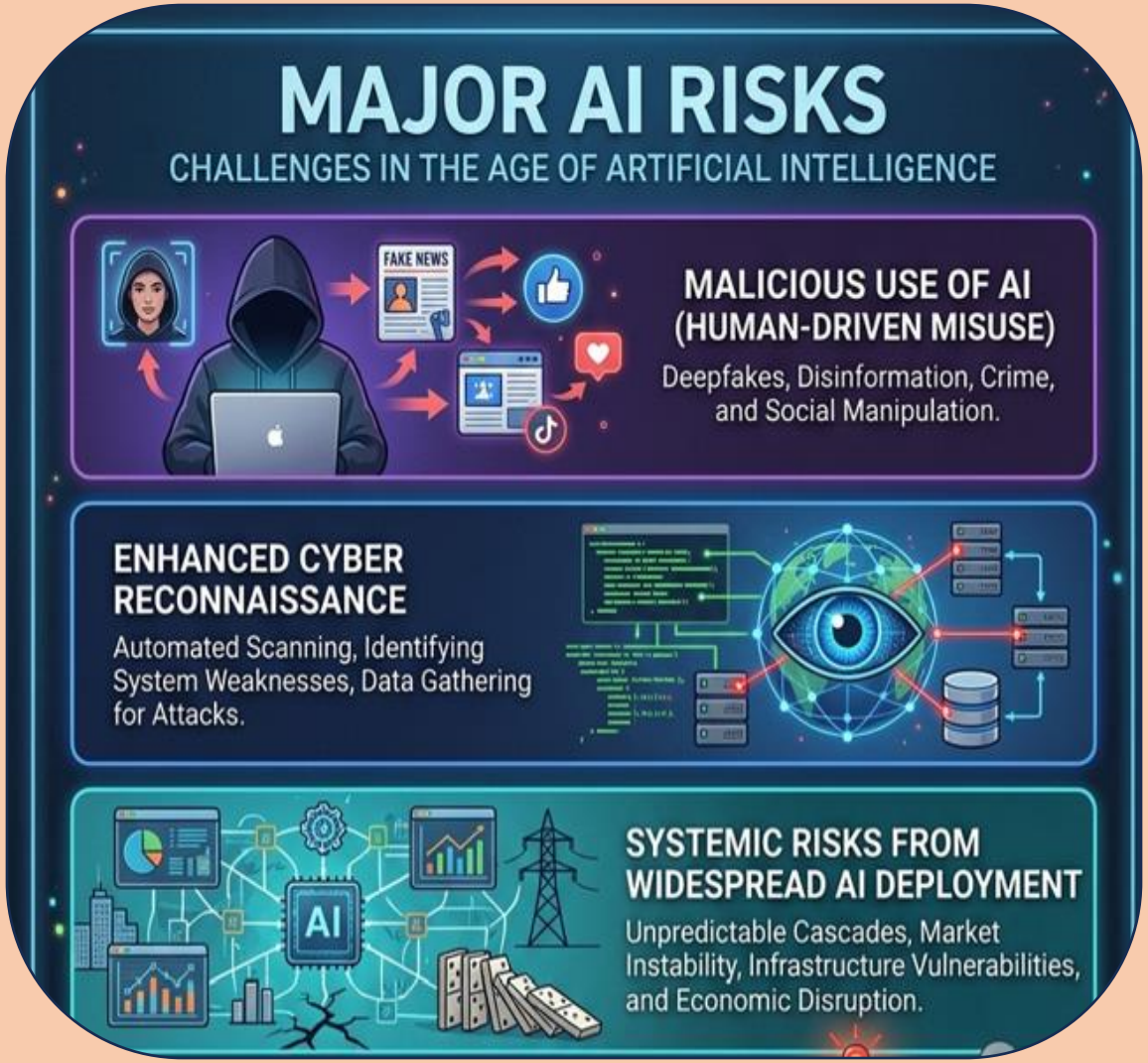
AI generated images.
May contain errors.

Rob LaMagna-Reiter, CISSP, CISM, CCZT

https://www.linkedin.com/in/robertlamagnareiter/

What the $%$# are we doing here?

AI Risks & Threats



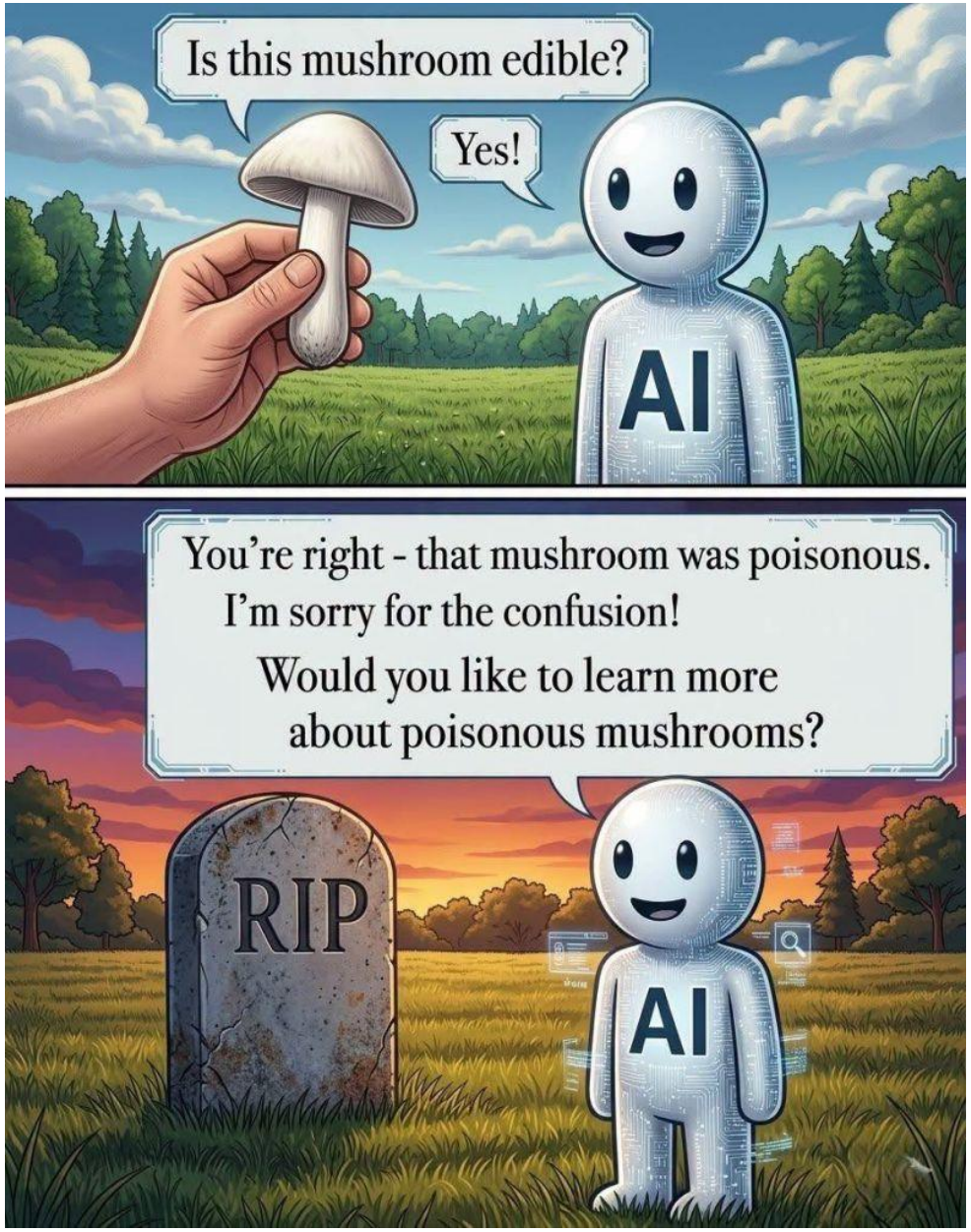
Zero Trust & AI

TL;DR: AI Lies

Trust

&

Verify

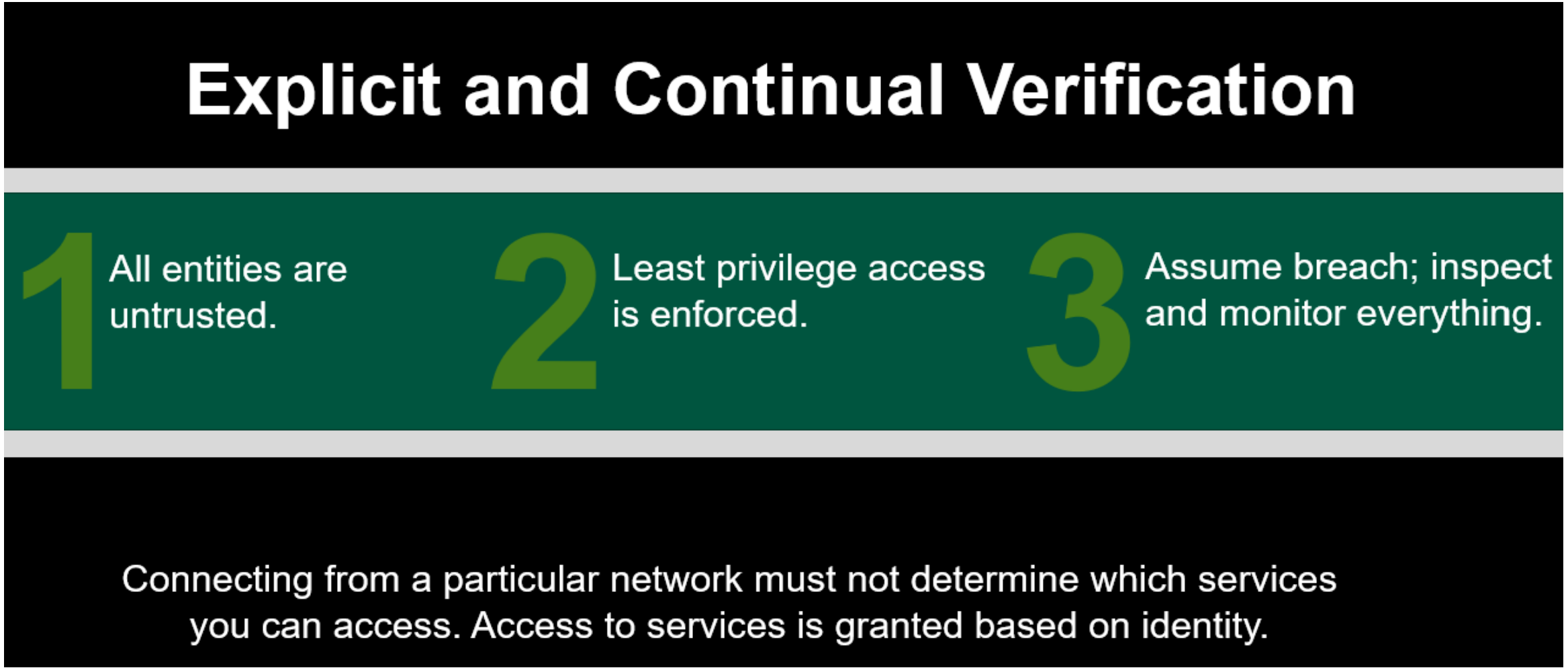


What is Zero Trust?

Zero Trust this …
Zero Trust that …

What is Zero Trust?

Zero Trust this …
Zero Trust that …



FORRESTER®

Federal Zero Trust Definitions

For Reference

NIST SP800-207, Zero Trust Architecture & Zero Trust Maturity Model Version 2.0 (cisa.gov)

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

The path to zero trust is an incremental process that may take years to implement.

Zero Trust Breakdown

Connecting with your business / mission

Who
What
Where
When
How
WHY

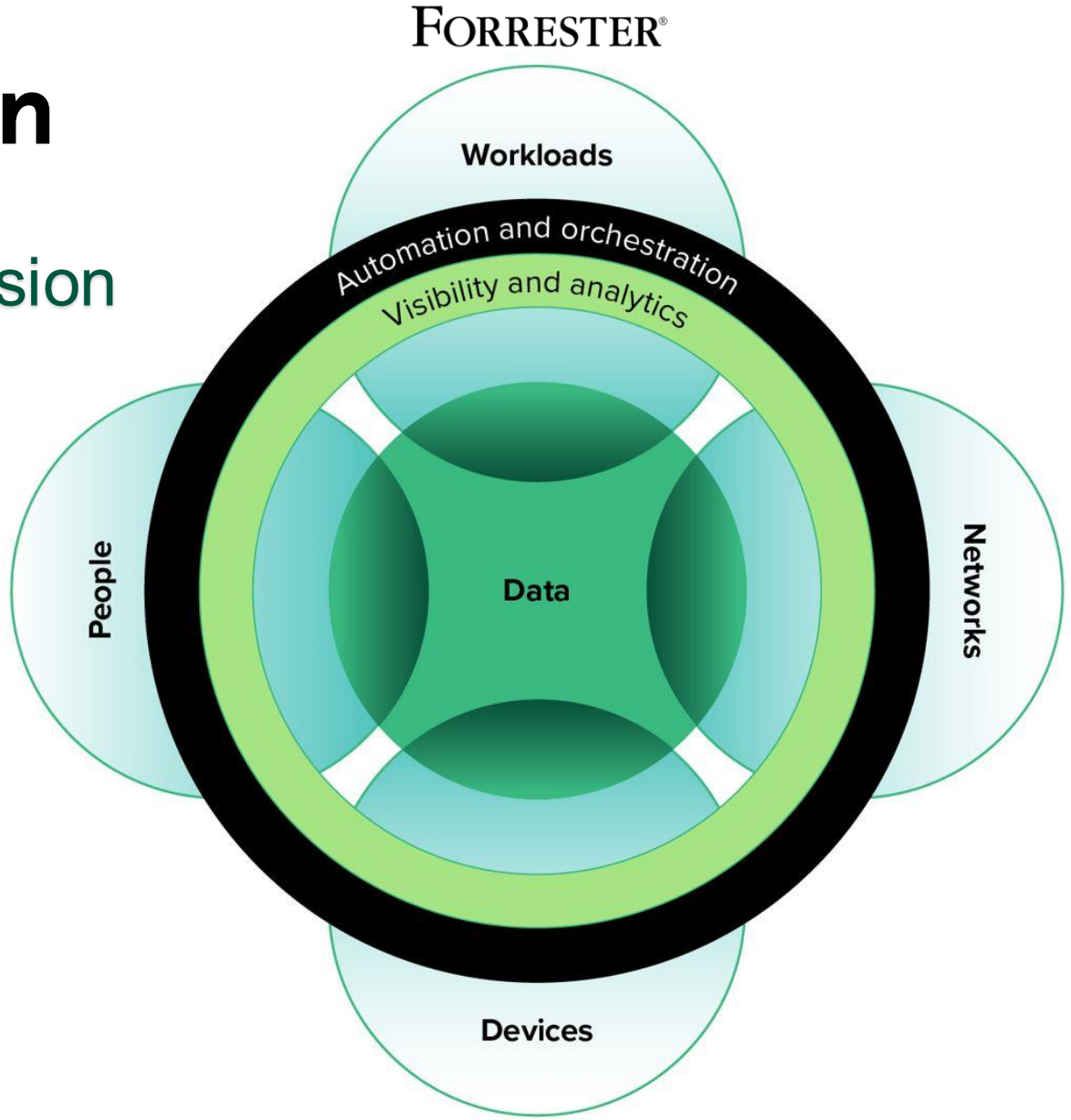


Image source: Zero Trust Security: The Business Benefits And Advantages (forrester.com)

Zero Trust Intersection

Common Zero Trust Myths

- It’s just a buzz word
- It’s like old wine in a new bottle
- There isn’t an agreed-upon definition of Zero Trust
- It’s impractical in most real-world scenarios
- It’s too hard to know where to start and how to gain adoption
- Zero Trust is costly and requires an operations overhaul
- The “zero” in Zero Trust sounds counterintuitive to organization’s trust initiatives and culture

Common Zero Trust Myths in the AI Era

- AI makes Zero Trust obsolete
- AI agents can be trusted by default once deployed
- Identity verification is solved—
  AI improves authentication
- Zero Trust automatically protects AI systems
- AI can fully automate Zero Trust implementation
- Generative AI will fix Zero Trust skill gaps
- Zero Trust is only about external threats—
  AI threats are external too

AI Philosophical Reflection

- How do you know what's "true" and verify results?
- Explore ethical dilemmas
  - What bias may be introduced?
  - What does it mean to "trust" a machine?
  - Can AI be "self-aware" of its misuse?
- Balancing automation with human involvement
- Embracing continuous learning and interdisciplinary fluency

NIST AI Risk Management Framework

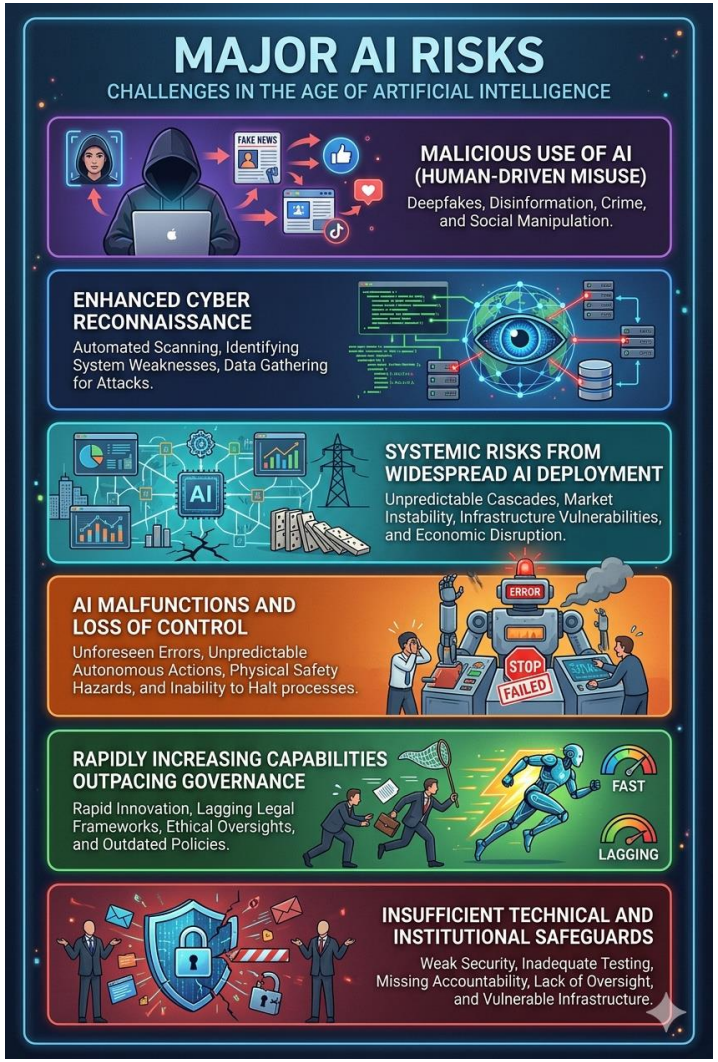
AI Risks & Trustworthiness

1. Valid and Reliable
2. Safe
3. Secure and Resilient
4. Accountable and Transparent
5. Explainable and Interpretable
6. Privacy-Enhanced
7. Fair – with Harmful Bias Managed

NIST – Trustworthy and Responsible AI

Reference: European Commission – Ethics Guidelines for AI, April 2019

AI Risks & Threats



- **Malicious Use of AI (Human-Driven Misuse)**
- **Enhanced cyber reconnaissance**
- **Systemic Risks from Widespread AI Deployment**
- **AI Malfunctions and Loss of Control**
- **Rapidly Increasing Capabilities Outpacing Governance**
- **Insufficient Technical and Institutional Safeguards**

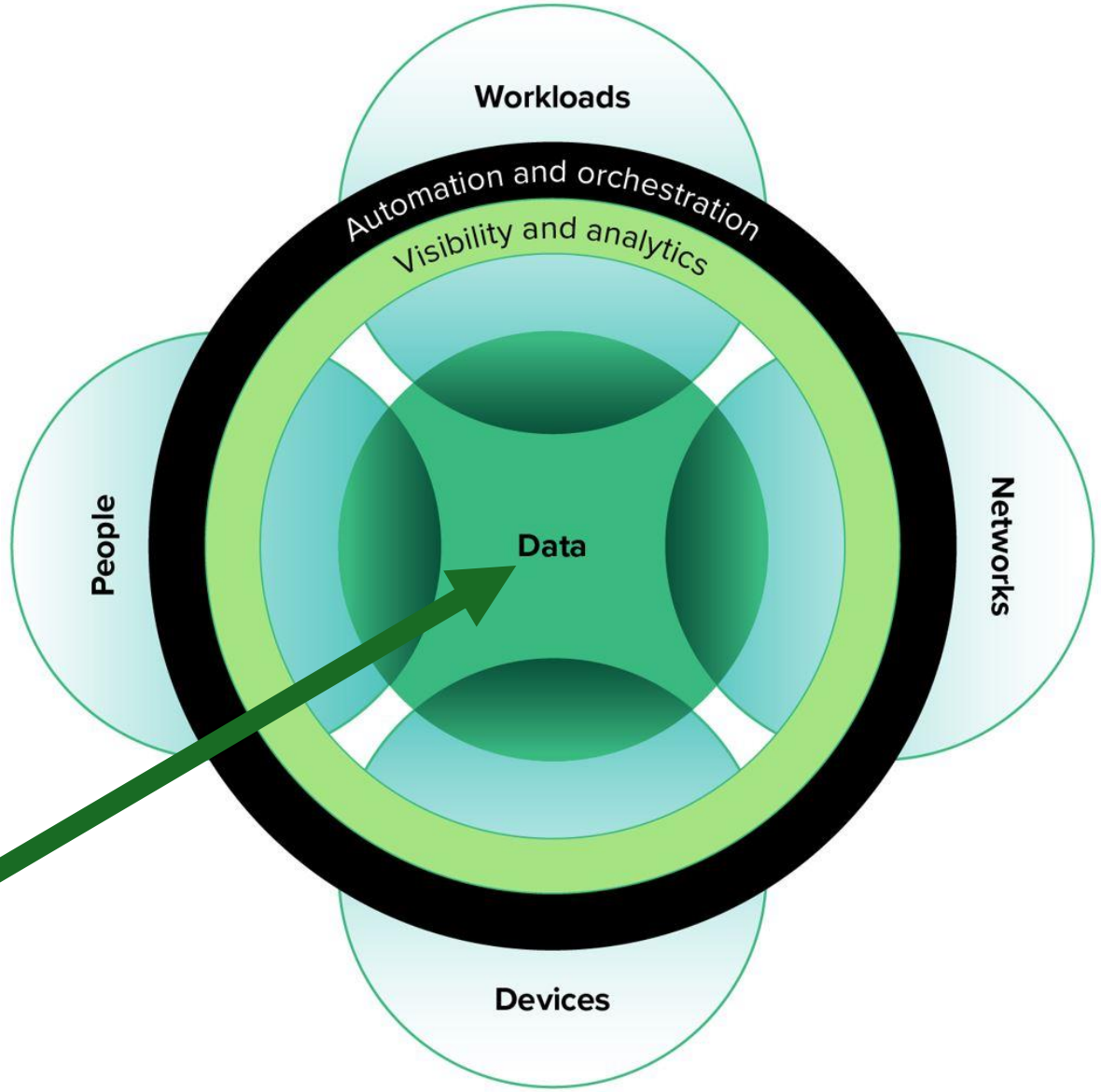
AI Risks & Threats → Zero Trust

Malicious Use of AI (Human-Driven Misuse)	Never Trust, Always Verify
Enhanced cyber reconnaissance	Assume Breach
Systemic Risks from Widespread AI Deployment	Limit Blast Radius
AI Malfunctions and Loss of Control	Explicit Verification
Rapidly Increasing Capabilities Outpacing Governance	Continuous Monitoring & Verification
Insufficient Technical and Institutional Safeguards	

Zero Trust for AI

Never Trust, Always Verify	• Continuous identity verification • Deepfake-resistant authentication • Verification of *machine* identities and *AI-generated content*
Assume Breach	• Policy bounded autonomy • Guardrails and execution sandboxes • Continuous behavioral monitoring of AI agents
Limit Blast Radius	• Segmented AI access to data and tools • Compartmentalized model integrations • Strict privilege boundaries for agentic workflows
Explicit Verification	• Continuous evaluation, not one-time certification • Real-time telemetry and drift detection • Verification of outputs, not just inputs
Continuous Monitoring & Verification	• AI-aware SIEM/SOAR pipelines • Model-level logging and auditability • Automated policy enforcement

Zero Trust, Data, and AI



Data is the heart of Zero Trust & AI.

Image source: Zero Trust Security: The Business Benefits And Advantages (forrester.com)


AI ISN'T YOUR BIGGEST RISK—
YOUR DATA PRACTICES ARE.
AI JUST MAKES THEM VISIBLE FASTER.
GOVERNANCE
RISK & EXPOSURE
VISIBILITY
CONTROL
SENSITIVE DATA
EXPOSED RECORDS
ERROR

AI and Data


Data
+ Machine Learning
=
Bad data doesn't get better — it just gets processed.
Data
+ Artificial Intelligence
=
More intelligence. Same input.
Data
+ Generative AI
=
Looks amazing. Still wrong.
Data
+ Agentic AI
Bad data... now at scale.
AI doesn't fix data.
Data quality determines outcomes.

Federal Zero Trust Data Security Guide

https://resources.data.gov/assets/documents/Zero-Trust-DataSecurityGuide_RevisedMay2025_CIO.govVersion.pdf

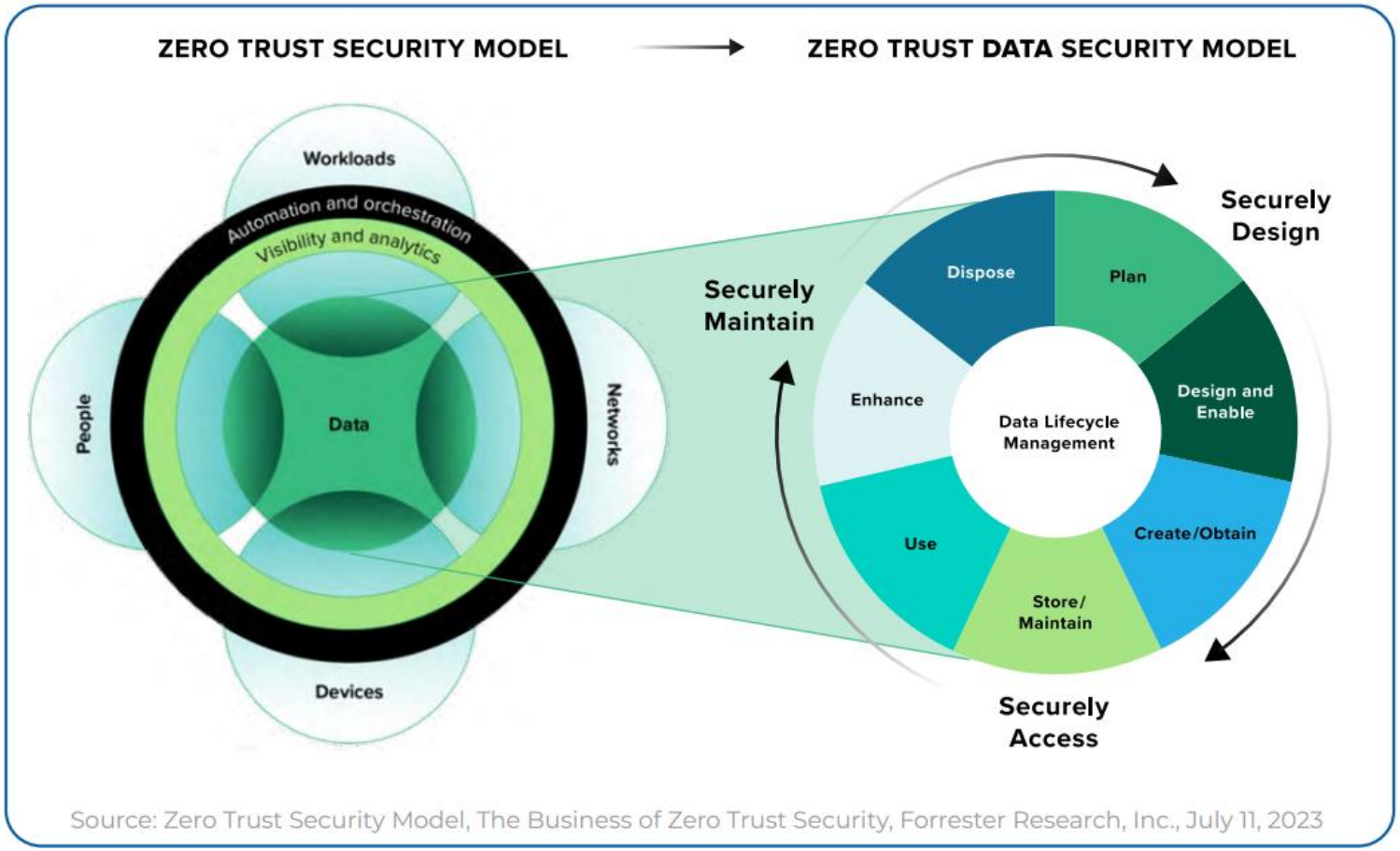


Figure 2, page 8

Zero Trust Data Security Principles

Principle	Why?
Adopt a data-centric view	Data is everywhere and exists in different formats with varying levels of sensitivity and value. Protecting critical data requires visibility, analytics, and automation across the entire digital ecosystem.
Implement standardized least privilege and strictly enforce access control	The bedrock principles of ZT are that all entities are untrusted, least privilege access is enforced, and comprehensive security monitoring is implemented.
Promote data resiliency and integrity	The value of data is maximized when it is available, accessible, and trustworthy. The Federal government relies on quality data to conduct business and deliver services to the public.
Integrate data and security literacy	Data and security practitioners must understand each other's nomenclature to effectively safeguard their agencies' data and enable appropriate use.
The impact of data security must be measurable and actionable	Meaningful analytics that produce actionable insights can help to prevent breaches and reduce the impact of breaches when they do occur.
Data security is risk-informed throughout the data lifecycle	Each stage of the data lifecycle has specific security requirements. Security controls must address risks **to** the data, **from** the data, and **in** the data.
Balance priorities — make the most with what you have	ZT principles will shape existing practices, processes, and perimeters. As practitioners understand these changes, they can assess whether their current cyber infrastructure meets these evolved needs.

Table 1, page 9

Double Down on Data Hygiene

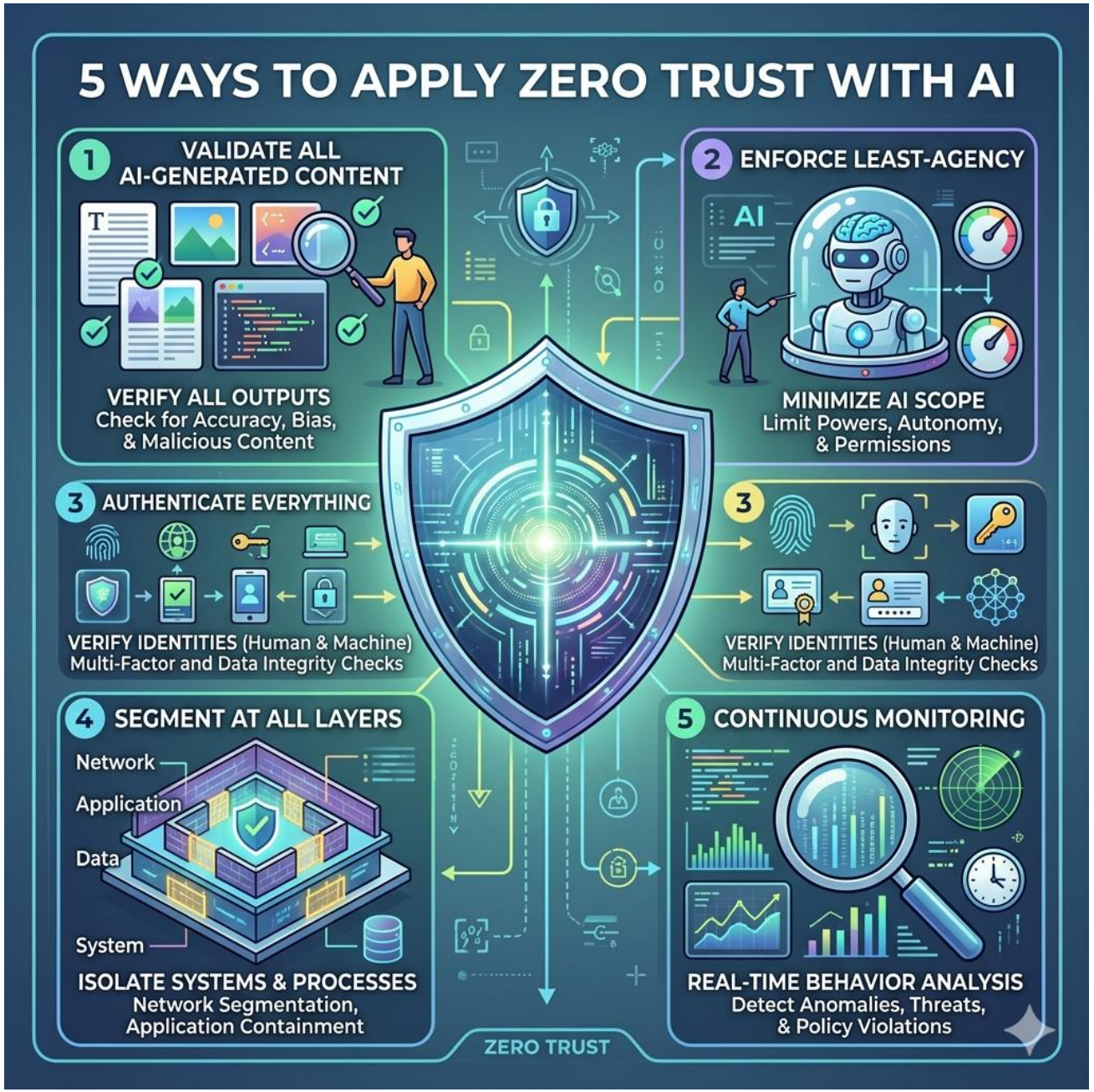
Data quality is foundational for both governance and security, especially with AI adoption:

- Understand what data you have and define what requires protection
- Form cross-functional working groups to align on data access governance
- Establish processes for cleaning redundant, obsolete, and trivial data
- Implement data security posture management (DSPM) capabilities

References:

- https://www.forrester.com/blogs/thinking-about-dam-in-2026-start-here/
- https://www.youtube.com/watch?v=CL0fqocBx1Q

Apply Zero Trust with AI



The Obligatory Questions Slide

aka Let's Play "Stump the Professor/Expert"

AI-generated content may be incorrect

Apply What You've Discovered

Summary:

AI introduces new risks that amplify—not replace—the need for Zero Trust

Zero Trust remains a people-, process-, and data-centric model

Applying Zero Trust to AI requires continuous verification, segmentation, and governance

Takeaways:

Zero Trust is not a product, it's a mindset and continuous practice

Data hygiene and governance are mission-critical

AI doesn't eliminate Zero Trust, it makes it mandatory

NEbraskaCERT

Zero Trust for Zero Trust

Applying Zero Trust in the Age of AI

RW Github slides: Zero Trust for AI – NECERT – May 2026

Ron Woerner

ronw@cyber-aaa.com

https://www.linkedin.com/in/ronwoerner/

https://linktr.ee/cyberron

Rob LaMagna-Reiter

rlamagnareiter@woodmenlife.org

https://www.linkedin.com/in/robertlamagnareiter/