Informatica

Zero Trust Architecture realized with AI-enabled Data Governance & Protection

Michael R. Anderson, Chief Strategist, Public Sector

June 25, 2025

Where data & AI come to LIFE

What is Zero Trust Architecture?

- Bottom Line: ***Trust nothing and no one*** on your network(s)
  - Trust is never granted implicitly - continually evaluated when accessing data, applications, compute, etc. even after initial network access granted
  - Assumes an adversary is present in the environment
  - Must continually analyze & evaluate risks to assets and business functions and then enact protections to mitigate these risks
  - **There is no single vendor solution**
  - Inherent joining of CIO, CISO, CDO personas to achieve

Zero Trust Architecture

Why *Now* for Agencies?

- **Policy & Mandate Driven**

  WH EXORD 14028 on Cybersecurity, May 2021

  OMB ZT Memo M22-09, Jan 2022

- **Adversary “Mandate”**

  No image of hacker in dark room necessary …

Zero Trust Architecture

States are adopting too …

- NASCIO Survey: 67% of state CIOs plan to introduce/expand ZTA in 2-3 yrs
- Federal Gov't is pushing cybersecurity responsibility to States
- Gartner predicts 60% of enterprises embracing ZTA as starting point for security in 2025
- Several states are actively moving w/legislation or guidance
    - OK, WA, MA, FL, TN and expanding

Zero Trust Architecture

Plenty of Help …

- **Guidance**

  Federal Data ZT Security Guide, Oct 2024

  NIST SP 800-207, Aug 2020

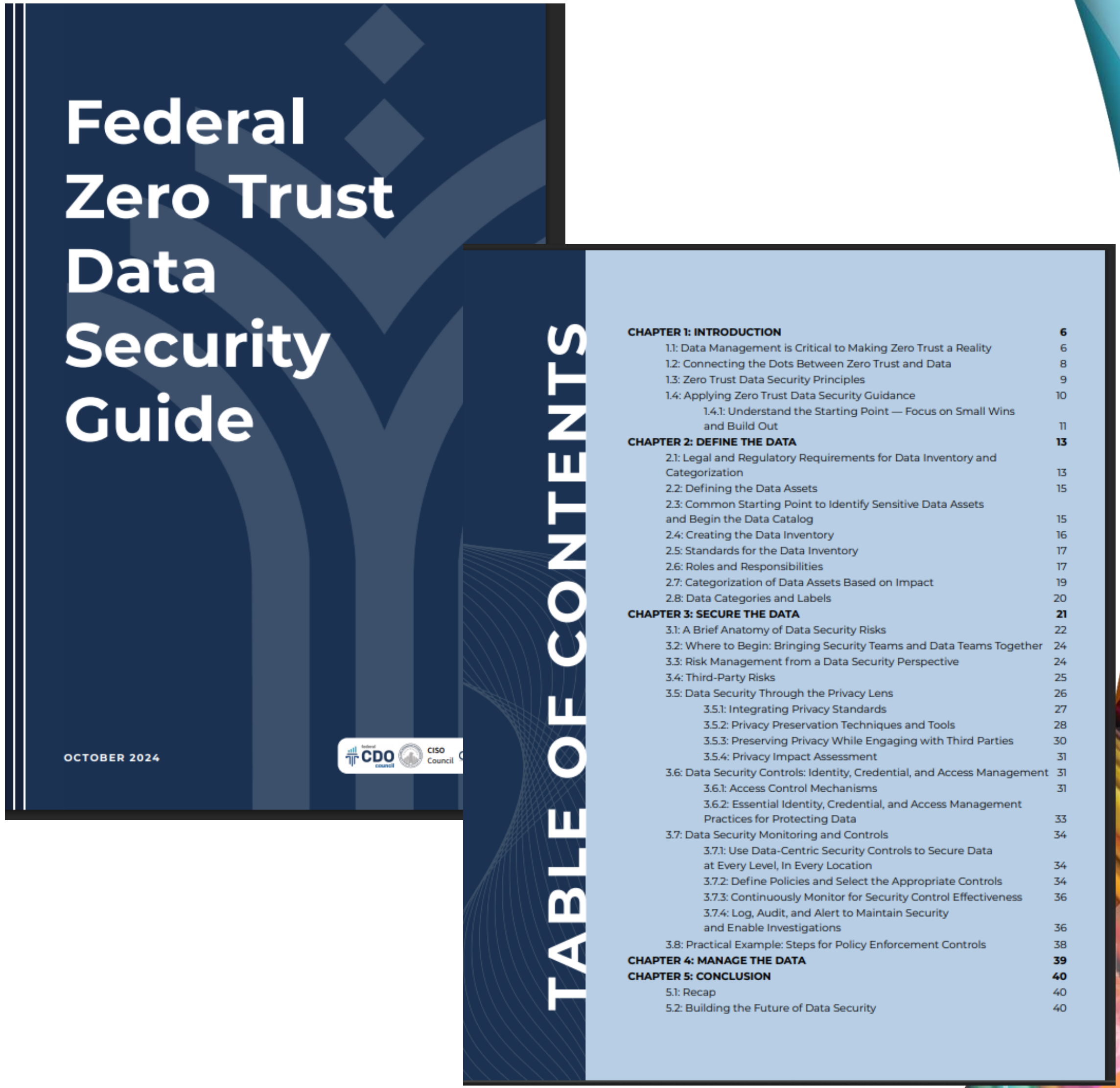
  NIST SP 800-207A, Sep 2023

  NIST CSF 2.0, Feb 2024

  DHS CISA ZT Maturity Model

  DoD ZT Ref Architecture, 2027 target

  DoD ZT OT Guidance, ~2025



Federal Zero Trust Data Security Guide

OCTOBER 2024

TABLE OF CONTENTS

Zero Trust Architecture

Barriers …

- Costs and budgetary constraints
- Complexity – performance impact
- Minimal data foundation
- Outdated technology and legacy systems
- User experience, training, education
- Lack of urgency and behavioral friction

How do we *Fund* Zero Trust Initiatives?

- Federal Agencies: ~$12B
- DoD ~$977M in FY25 NDAA
- $1B cyber grant money for State Gov't within the 21-22 Infrastructure & Investment Jobs Act (expires Sep 2025)

Leverage other budgets: data management, AI

Zero Trust: Point of View

Heard on “the street”

- “… technology is not the answ … need t hange the culture …”
- “… Zero Trust is not just a tech problen
- “… is not a framework … need to cha e the culture … you need leadership …”

“… the time to make the change is now”

Finally … “ZT needs to use policy-based access control with identity, roles and attributes”

Informatica

Zero Trust Foundational Pillars

Identity

Enforce MFA and least privilege access to systems

Devices

Prevent unauthorized device access to resources

Networks

Encrypt and manage networks for internal and external data flows

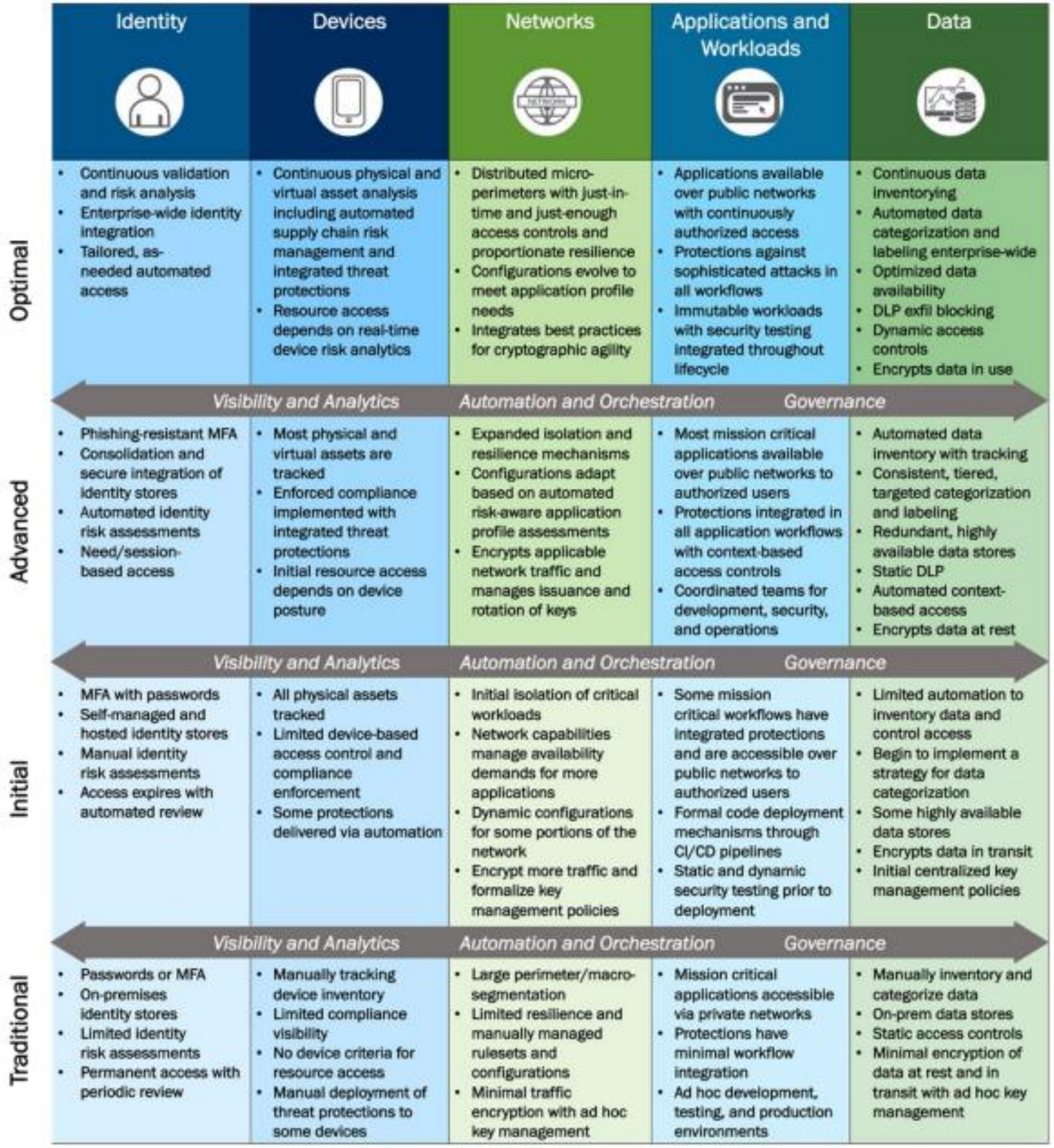
Applications & Workloads

Continuous vulnerability testing, monitoring, and management of applications

Data

Protect data through categorization and creating an inventory of all assets

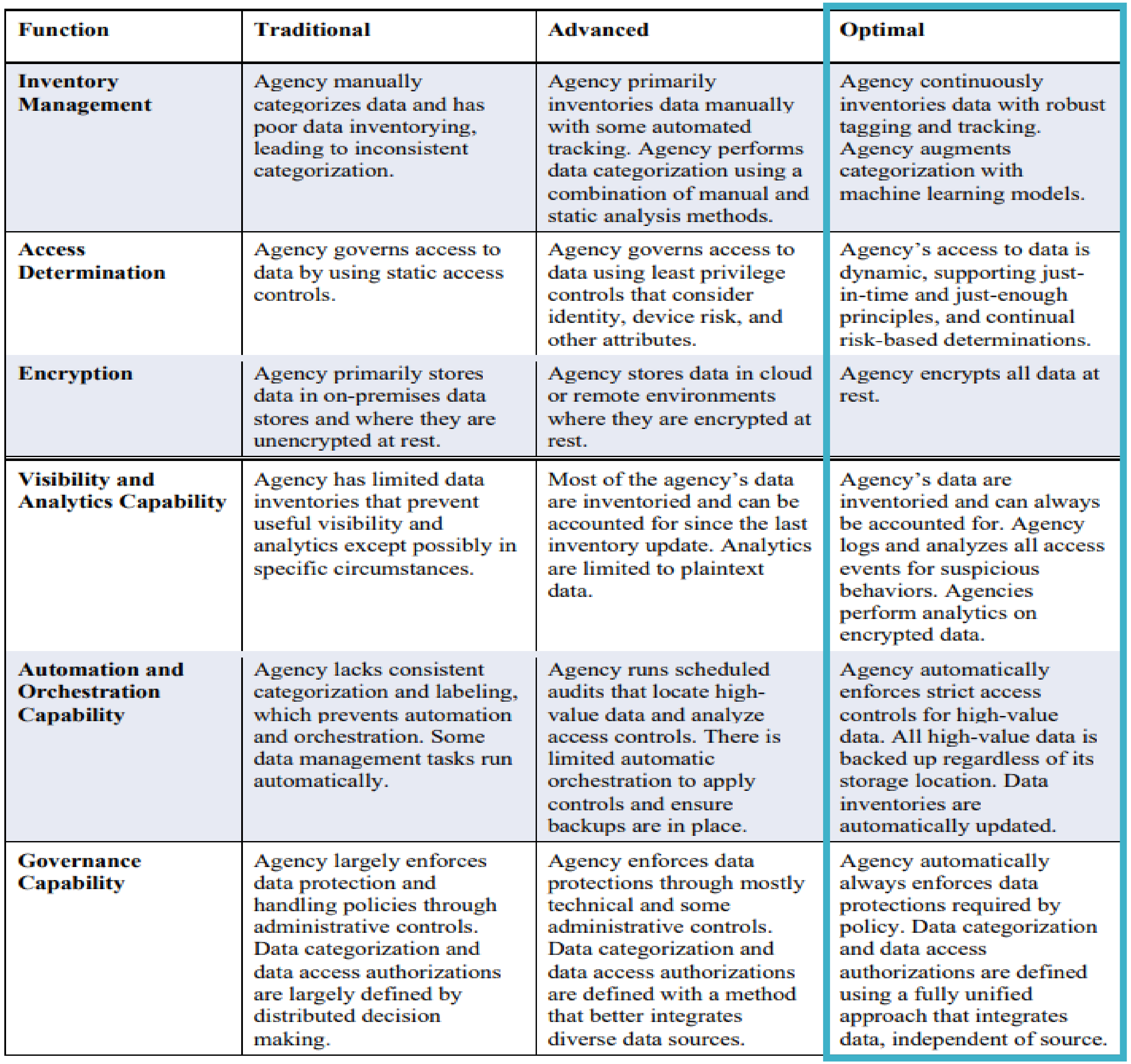
DHS CISA ZTA Maturity Model - Categories



	Identity	Devices	Networks	Applications and Workloads	Data
Optimal	• Continuous validation and risk analysis • Enterprise-wide identity integration • Tailored, as-needed automated access	• Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat protections • Resource access depends on real-time device risk analytics	• Distributed micro-perimeters with just-in-time and just-enough access controls and proportionate resilience • Configurations evolve to meet application profile needs • Integrates best practices for cryptographic agility	• Applications available over public networks with continuously authorized access • Protections against sophisticated attacks in all workflows • Immutable workloads with security testing integrated throughout lifecycle	• Continuous data inventorying • Automated data categorization and labeling enterprise-wide • Optimized data availability • DLP exfil blocking • Dynamic access controls • Encrypts data in use
		Visibility and Analytics	Automation and Orchestration	Governance	
Advanced	• Phishing-resistant MFA • Consolidation and secure integration of identity stores • Automated identity risk assessments • Need/session-based access	• Most physical and virtual assets are tracked • Enforced compliance implemented with integrated threat protections • Initial resource access depends on device posture	• Expanded isolation and resilience mechanisms • Configurations adapt based on automated risk-aware application profile assessments • Encrypts applicable network traffic and manages issuance and rotation of keys	• Most mission critical applications available over public networks to authorized users • Protections integrated in all application workflows with context-based access controls • Coordinated teams for development, security, and operations	• Automated data inventory with tracking • Consistent, tiered, targeted categorization and labeling • Redundant, highly available data stores • Static DLP • Automated context-based access • Encrypts data at rest
		Visibility and Analytics	Automation and Orchestration	Governance	
Initial	• MFA with passwords • Self-managed and hosted identity stores • Manual identity risk assessments • Access expires with automated review	• All physical assets tracked • Limited device-based access control and compliance enforcement • Some protections delivered via automation	• Initial isolation of critical workloads • Network capabilities manage availability demands for more applications • Dynamic configurations for some portions of the network • Encrypt more traffic and formalize key management policies	• Some mission critical workflows have integrated protections and are accessible over public networks to authorized users • Formal code deployment mechanisms through CI/CD pipelines • Static and dynamic security testing prior to deployment	• Limited automation to inventory data and control access • Begin to implement a strategy for data categorization • Some highly available data stores • Encrypts data in transit • Initial centralized key management policies
		Visibility and Analytics	Automation and Orchestration	Governance	
Traditional	• Passwords or MFA • On-premises identity stores • Limited identity risk assessments • Permanent access with periodic review	• Manually tracking device inventory • Limited compliance visibility • No device criteria for resource access • Manual deployment of threat protections to some devices	• Large perimeter/macro-segmentation • Limited resilience and manually managed rulesets and configurations • Minimal traffic encryption with ad hoc key management	• Mission critical applications accessible via private networks • Protections have minimal workflow integration • Ad hoc development, testing, and production environments	• Manually inventory and categorize data • On-prem data stores • Static access controls • Minimal encryption of data at rest and in transit with ad hoc key management

Figure 4: High-Level Zero Trust Maturity Model Overview

DHS CISA’s Zero Trust Maturity Model – Data Pillar



Function	Traditional	Advanced	Optimal
Inventory Management	Agency manually categorizes data and has poor data inventorying, leading to inconsistent categorization.	Agency primarily inventories data manually with some automated tracking. Agency performs data categorization using a combination of manual and static analysis methods.	Agency continuously inventories data with robust tagging and tracking. Agency augments categorization with machine learning models.
Access Determination	Agency governs access to data by using static access controls.	Agency governs access to data using least privilege controls that consider identity, device risk, and other attributes.	Agency’s access to data is dynamic, supporting just-in-time and just-enough principles, and continual risk-based determinations.
Encryption	Agency primarily stores data in on-premises data stores and where they are unencrypted at rest.	Agency stores data in cloud or remote environments where they are encrypted at rest.	Agency encrypts all data at rest.
Visibility and Analytics Capability	Agency has limited data inventories that prevent useful visibility and analytics except possibly in specific circumstances.	Most of the agency’s data are inventoried and can be accounted for since the last inventory update. Analytics are limited to plaintext data.	Agency’s data are inventoried and can always be accounted for. Agency logs and analyzes all access events for suspicious behaviors. Agencies perform analytics on encrypted data.
Automation and Orchestration Capability	Agency lacks consistent categorization and labeling, which prevents automation and orchestration. Some data management tasks run automatically.	Agency runs scheduled audits that locate high-value data and analyze access controls. There is limited automatic orchestration to apply controls and ensure backups are in place.	Agency automatically enforces strict access controls for high-value data. All high-value data is backed up regardless of its storage location. Data inventories are automatically updated.
Governance Capability	Agency largely enforces data protection and handling policies through administrative controls. Data categorization and data access authorizations are largely defined by distributed decision making.	Agency enforces data protections through mostly technical and some administrative controls. Data categorization and data access authorizations are defined with a method that better integrates diverse data sources.	Agency automatically always enforces data protections required by policy. Data categorization and data access authorizations are defined using a fully unified approach that integrates data, independent of source.

- Reaching the optimal level within each function is an iterative process
- Choose wisely – comprehensive solutions assist with **implementing and automating** these functions

✓ Inventory Management

✓ Applying Governance Capabilities

Data Management Pitfalls - Categories

Current limitations support the need for Zero Trust Frameworks

Automation & Orchestration

- Meet data needs at scale
- Hybrid environments
- Metadata ingestion
- Manual tasks and processes
- AI/ML capabilities for automation

Governance

- Create inventory of data assets
- Understand business relevancy
- Take ownership of data
- Leverage data as a product
- Cleanse and standardize

Visibility and Analytics

- Access Auditing
- Anomaly detection
- Classify and control sensitive data
- Ensure compliance
- Data Lineage

Achieve optimal Data Pillar ZTA with an all-in, data management platform

Automate & Orchestrate

- Integrated capabilities to share metadata-driven intelligence for sensitive classifications & improve cross-team collaboration for policy-driven decision making
- Connect data to data owners/users for reporting on data subjects and determining risk exposure
- Automated risk remediation such as DSAR reporting, along with data masking help protect data for consumption

Govern

- Enable Sharing of Trusted Data
- Identify Risks and Remediations Involving Sensitive Data
- Connect Confidential Data to Data Owners
- Reduce Exposure of Sensitive Data

Visibility & Analytics

- Data cataloging automates data discovery, inventory & lineage to enable data transparency
- Data governance tools align stakeholders with policies for data use
- Data privacy connects data to users to help identify and report on anomalies
- With data masking, confidential data can be redacted (anonymized) while still leaving non-sensitive data open for safe analytics

Achieve optimal Data Pillar ZTA with an all-in, data management platform

Inventory Management

- Continuously maintain an updated inventory of assets
- Reduce Manual Data Discovery and Curation with AI/ML
- Deliver Trustworthy Data
- Ensure Responsible Data Sharing

Access Determination

- Enable Sharing of Trusted Data
- Identify Risks and Remediations Involving Sensitive Data
- Connect Confidential Data to Data Owners
- Reduce Exposure of Sensitive Data

Encryption

- Data is Encrypted throughout the pipeline.
- Tagging automation for sensitive data
- Protect Sensitive Data by Masking

Informatica Overview & Public Sector

OUR MISSION

- Informatica brings data and AI to life by empowering higher education to **unlock the transformative power** of their most valuable asset, their data

WHO WE ARE

- Founded in 1993
- Headquartered in Redwood City, California
- **5000+** employees
- **5000+** active customers
- Where data & AI come to LIFE

WHY INFORMATICA

- The **data management choice** government and public sector
- Serving 600 public sector customers
- "Switzerland of data"
  - Multi-cloud, hybrid, and on-premises
- Cloud, on-prem & FedRAMP capabilities available
- Third-party **validated market leadership**
- Consumption-based for cloud & subscription for on-prem pricing models

Informatica

Technology Challenges

- Data is difficult to find and understand
- Poor data quality, not trusted
- Can’t scale for volume and variety
- Data and applications siloed and fragmented
- Difficult to share data and not governed or protected

Business Challenges

- Balancing cost and risk of data privacy and protection
- Driving to better decision making by improving data quality and governance
- Empowering employees through legacy IT modernization
- Democratizing data for non-tech users to streamline processes, data, and technologies to include AI
- Leveraging analytics with trusted data for actionable insights to improve societal challenges
- Improving digital gov’t/digital services for residents

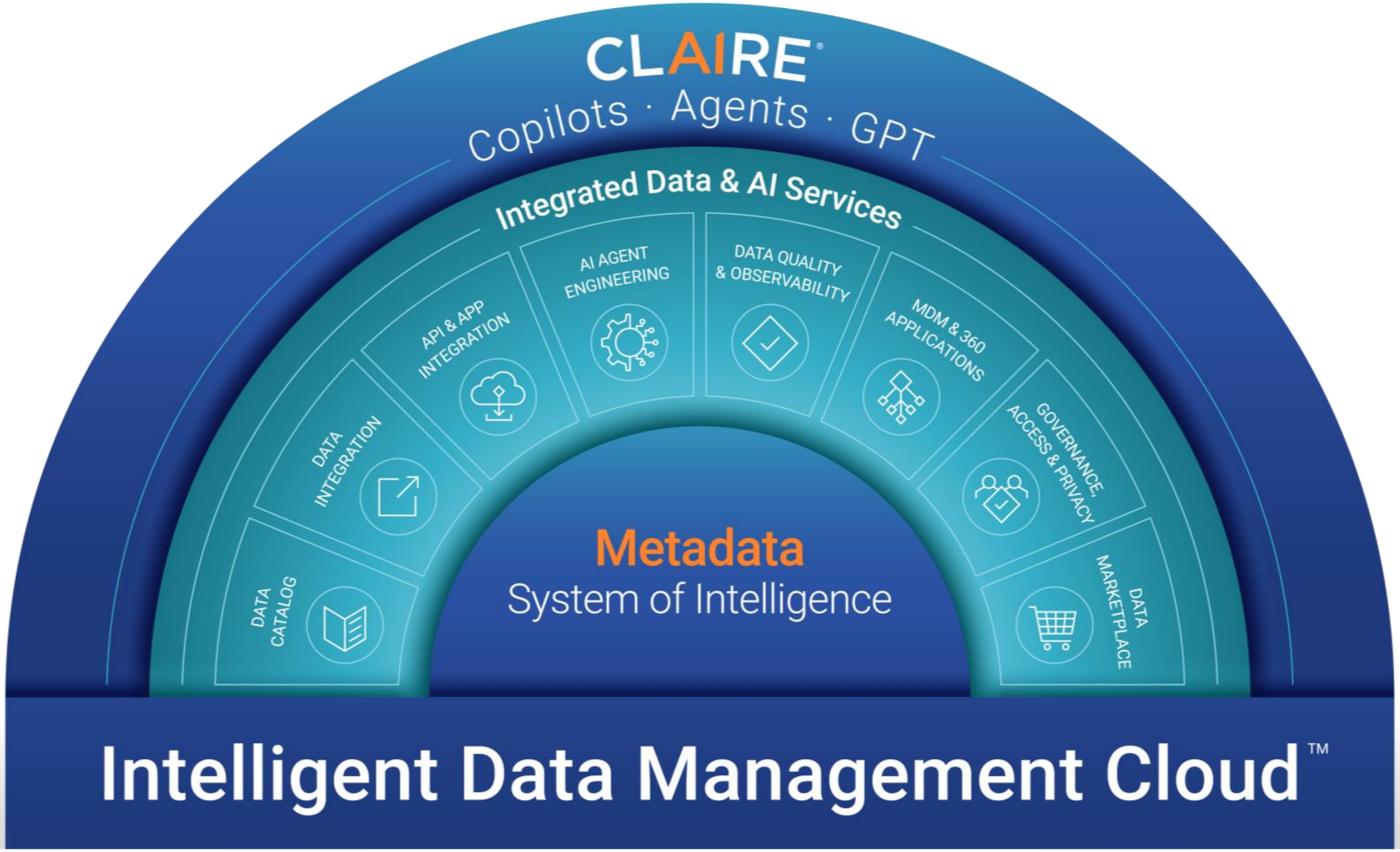
Government success IS DATA INTENSIVE!

Intelligent Data Management Cloud (IDMC) 2025

Trust your data and automate processes, enabling AI and analytics

Streamline business processes, analytics, and AI across multiple applications

Connect data silos for a single view of people, places and other critical data



Multi-Cloud & Hybrid	50,000+ Metadata-Aware Connections	Global Scale	Security & Compliance	Flexible Pricing

Provide a flexible roadmap for one AI-powered data management platform

Invest in one use case and leverage same investment for multiple use cases

Enables building, connecting, and managing AI agent workflows

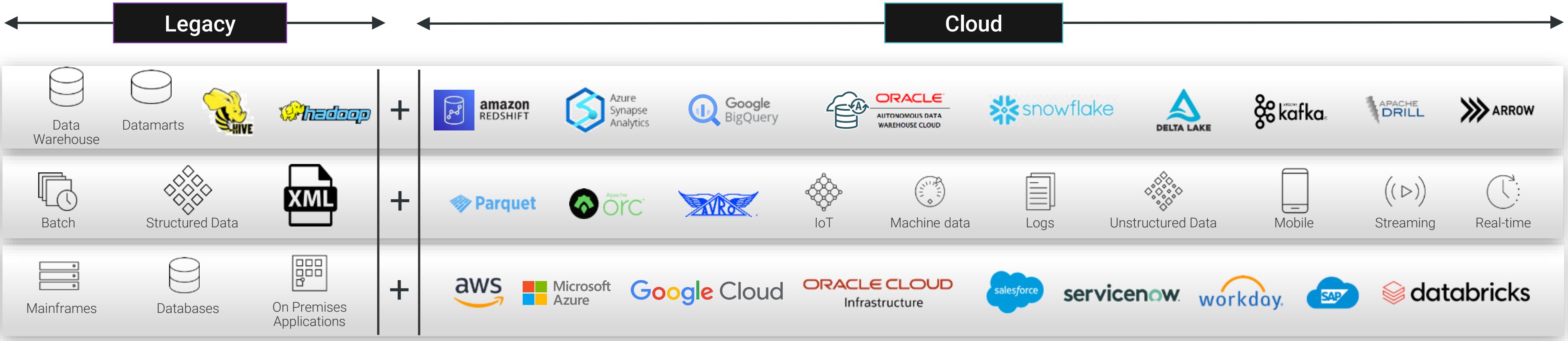
Informatica

Data Management Is Strategic and Complex

Cloud

Legacy

DATA CATALOG	DATA INTEGRATION & ENGINEERING	API & APP INTEGRATION	DATA QUALITY & OBSERVABILITY	MDM & 360 APPLICATIONS	GOVERNANCE, ACCESS & PRIVACY	DATA MARKETPLACE
38+ Vendors[1]	**195+ Vendors[2]**	**134+ Vendors[3]**	**128+ Vendors[4]**	**96+ Vendors[5]**	**165+ Vendors[6]**	**55+ Vendors[7]**



Legacy

Cloud

Data Warehouse

Datamarts

HIVE

hadoop

+

amazon REDSHIFT

Azure Synapse Analytics

Google BigQuery

ORACLE AUTONOMOUS DATA WAREHOUSE CLOUD

snowflake

DELTA LAKE

kafka

APACHE DRILL

ARROW

Batch

Structured Data

XML

+

Parquet

Apache orc

AVRO

IoT

Machine data

Logs

Unstructured Data

Mobile

Streaming

Real-time

Mainframes

Databases

On Premises Applications

+

aws

Microsoft Azure

Google Cloud

ORACLE CLOUD Infrastructure

salesforce

servicenow

workday

SAP

databricks

[1] Trust Radius, Data Catalog Software, May 2023
[2] Trust Radius, Data Integration Tools Software, May 2023
[3] Trust Radius, API Management Tools, May 2023
[4] Trust Radius, Data Quality Software, May 2023
[5] Trust Radius Master Data Management (MDM) Tools, May 2023
[6] Trust Radius, Data Governance Software, May 2023
[7] Trust Radius, Data Collaboration Tools, May 2023

Informatica

Data Management Landscape is Fragmented

CATALOG

Discover, catalog, and curate all enterprise data

- Informatica
- Alation
- Alex
- collibra
- data.world
- erwin
- WATERLINE DATA
- aws Glue
- Azure

INGEST

Multi-latency data ingestion and edge computing

- Informatica
- Azure Data Factory
- AWS Glue ETL Service
- Fivetran
- MATILLION
- alooma
- StreamSets

INTEGRATE

Integrate all types of data

- Informatica
- Azure Data Factory
- ORACLE
- snapLogic
- talend
- MATILLION
- SAP
- boomi

CLEANSE

Make data fit for purpose

- Informatica
- IBM
- ataccama
- SAP
- sas
- talend

RELATE

Match and relate identities and entities

- Informatica
- SAP
- IBM
- riversand
- Orchestra Networks
- ataccama
- STIBO SYSTEMS Master Data Management
- Reltio
- TIBCO
- Profisee

GOVERN

Define and verify data governance policies

- Informatica
- collibra
- precisely
- IBM
- OvalEdge
- erwin

PROTECT

Detect and protect sensitive data

- Informatica
- DATAGUISE
- protegrity
- hp
- Voltage security
- Vormetric
- BigID

PREPARE

For analytics and collaborate on projects

- Informatica
- tamr
- Datameer
- TRIFACTA
- Paxata
- alteryx
- snapLogic

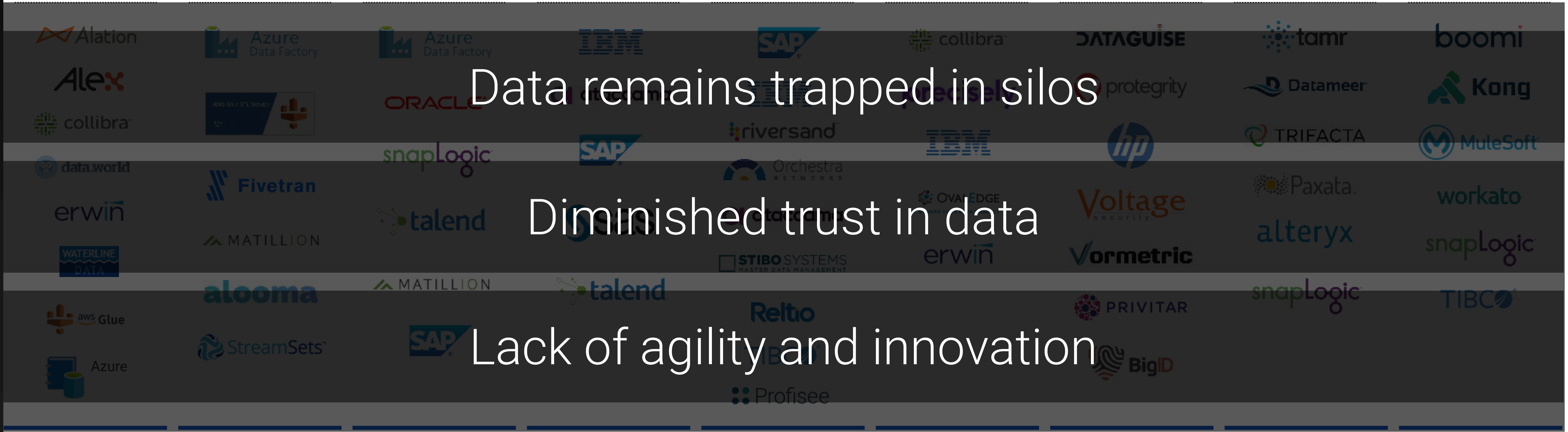
SHARE & DELIVER

Publish and manage APIs and Data Services

- Informatica
- boomi
- Kong
- MuleSoft
- workato
- snapLogic
- TIBCO

Data Management Landscape is Fragmented

CATALOG	INGEST	INTEGRATE	CLEANSE	RELATE	GOVERN	PROTECT	PREPARE	SHARE & DELIVER
Discover, catalog, and curate all enterprise data	Multi-latency data ingestion and edge computing	Integrate all types of data	Make data fit for purpose	Match and relate identities and entities	Define and verify data governance policies	Detect and protect sensitive data	For analytics and collaborate on projects	Publish and manage APIs and Data Services



Data remains trapped in silos

Diminished trust in data

Lack of agility and innovation

Informatica

IDMC Delivers Best-of-Breed Products in a Single Platform

CATALOG
Discover, catalog, and curate all enterprise data

INGEST
Multi-latency data ingestion and edge computing

INTEGRATE
Integrate all types of data

CLEANSE
Make data fit for purpose

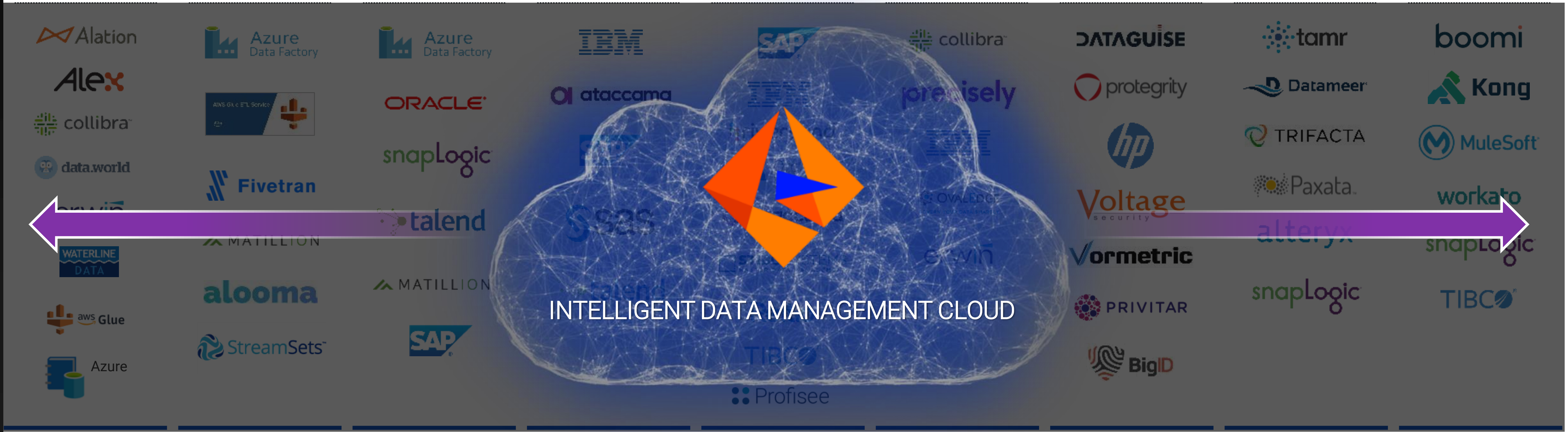
RELATE
Match and relate identities and entities

GOVERN
Define and verify data governance policies

PROTECT
Detect and protect sensitive data

PREPARE
For analytics and collaborate on projects

SHARE & DELIVER
Publish and manage APIs and Data Services



Key Take Aways

- **Data Vision**: Agencies deploy protections that make use of thorough data labeling & categorization

- Informatica covers the ZTA data pillar by inventorying and monitoring…
  - How data is labeled, consumed, protected and complies with policies and regulations
  - Data Governance, Data Usage, Data Protection, Data Privacy, Data Sharing, Data KPIs and Metrics

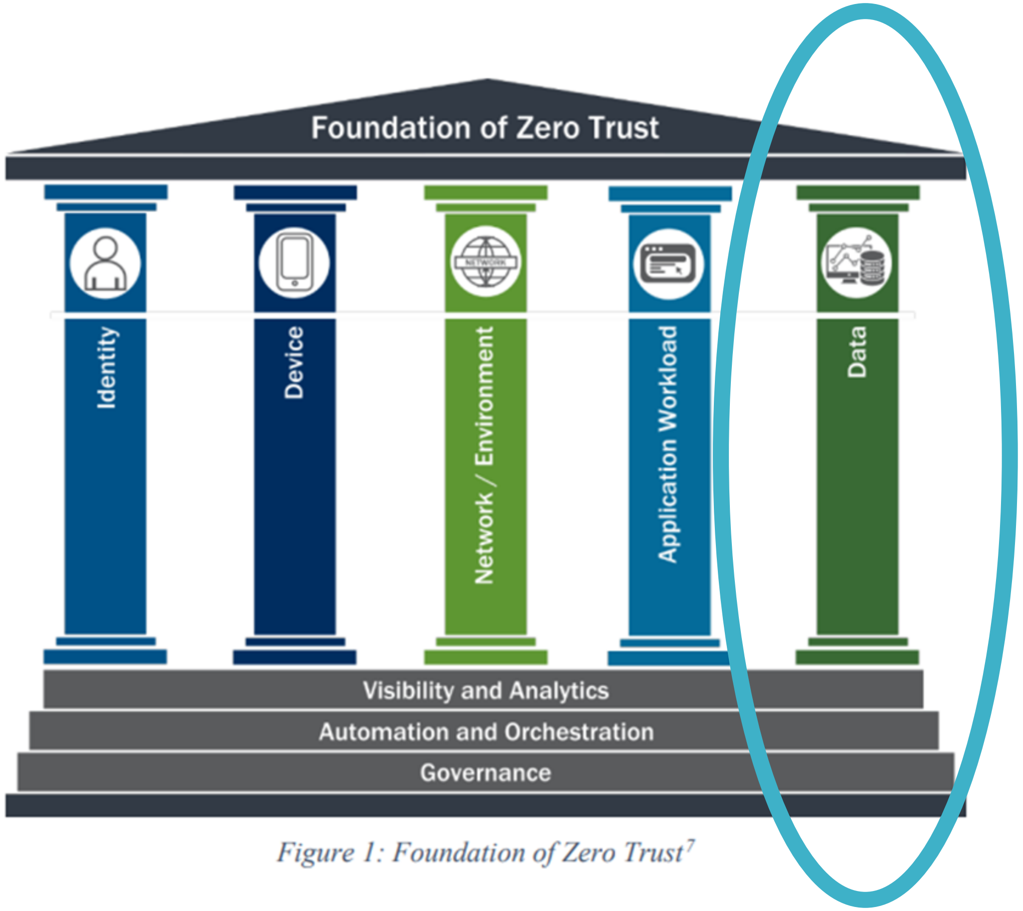


Figure 1: Foundation of Zero Trust[7]

Informatica

Michael R. Anderson, mianderson@informatica.com

Thank You

Learn more about Informatica Public Sector:

https://www.informatica.com/solutions/industry-solutions/public-sector.html

Where data & AI come to LIFE