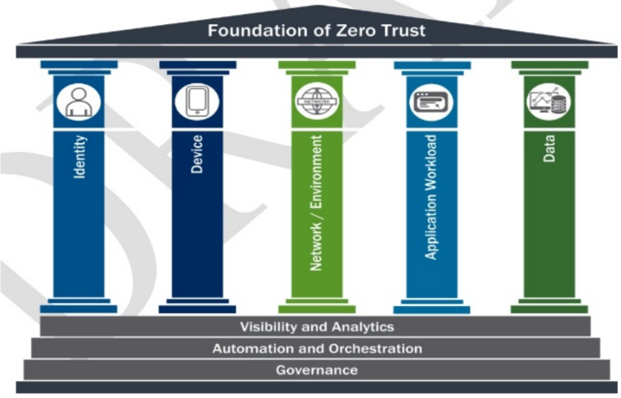
The Case for a Data Stewardship-First Approach to Zero Trust



The CISA draft Zero Trust Maturity Model[1] depicts five enterprise pillars, each requiring their own set of capabilities for achieving optimal maturity. (DoD's ZT Framework has seven pillars.[2]) Optimizing an enterprise's Zero Trust posture has been described as a journey; it is not a technology quick fix, and it will take time.

Zero Trust is not only a "journey", it is also a program. Like any good program Zero Trust requires executive, or mission, sponsorship, and it requires measures and metrics to determine if the program milestones and goals are being met. The key metrics that executives will demand are: 1) how well did the program protect what is most important to the mission (relative data protection "bang for the buck"), and 2) how much did it cost to get that level of protection. In other words … **what is the ROI for this program and its individual projects?**

Cost/Benefit	Identity	Device	Network	Application	Data
Relative Cost	$$	$$$	$$$$$	$$$$	$$
Mission Criticality	****	***	**	****	*****
Time to Achieve Benefits	tt	ttt	ttttt	tttt	t
Impact on Users	→	→	↓	↓	↑

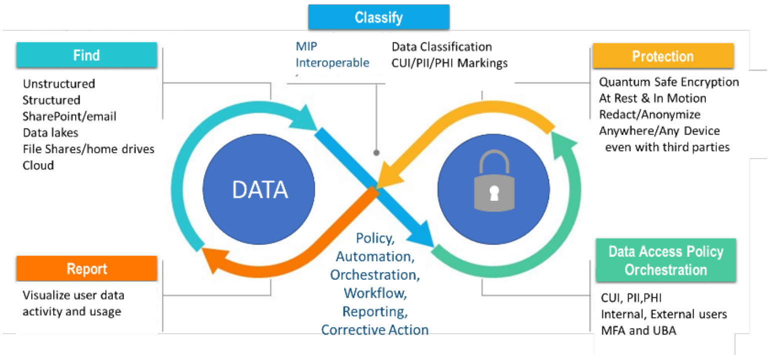
A "notional" ROI Analysis for the Zero Trust Pillars shows comparative benefits, costs, and returns achieved by a focus on the data pillar! -Emery/Connor

Data Stewardship and Zero Trust

Our premise—based upon years of executing programs that protect enterprise operations—is that the program execution plan for Zero Trust must start with the data. Data is the lifeblood of the mission… mission data protection has the highest ROI for any ZT pillar project. Data is what the "bad guys" are ultimately after… hence it is the "first" ZT pillar among equals. Data Stewardship, simply defined, are the measures taken by the responsible leaders in an organization to ensure critical mission data is ALWAYS available to support mission functions … and is NEVER compromised or NEVER falls into the wrong hands. The designated Data Stewards are responsible/ accountable for:

- **Data Ownership and Control** – they "own" the data (based on mission function), and they control who has (or doesn't have) access to that data
- **Data Protection** – they ensure the data is always protected (at rest, in transit, wherever the data is and whenever the data is being used)
- **Data Usage** – they understand how data is used (for their given mission functions) and they adjust access/permissions based on the ever-changing mission usage needs

Continuous Data Stewardship Model



Open the aperture on data visibility; Close the aperture on Risk!

The data steward, partnered with the IT team, can then implement these data policies. They can use the OODA Loop model to identify, classify, and protect the data according to its sensitivity. They can monitor and manage the use of the data on a continuous basis. Having precision insights into mission data flows/usage is a key ingredient for effective Data Stewardship. Continuous monitoring enables ongoing "mission/data ops analysis", essential for deciding data protection, data access and data usage. The Data Stewardship operating model can be up and running in as little as 90 days. We have seen this to be true in the largest financial institutions, and in small government implementations like DARPA.

[1] https://www.cisa.gov/publication/zero-trust-maturity-model

[2] Automation/Orchestration and Visibility/Analytics are pillars 6 and 7 in the DoD ZT Framework

[3] Data Breaches dominate public discussions; other "pillar failures" lead to data breach "headlines"

THE EMERY GROUP

The Case for a Data Stewardship-First Approach to Zero Trust

Benefits of Starting the Zero Trust Program with the Data Pillar

" You know how you always say innovation creates uncertainty... well I'm not certain where our data is."

1. It unifies the IT department's efforts with the mission owners.
2. It discovers, classifies, and protects the data in the least amount of time.
3. It is a low-cost project within the program as this pillar enables the others to be more effective:
   - the data owner sets policy for data access based on user identity,
   - data is protected on any device,
   - data location can be used as input to any network micro-segmentation efforts, and
   - data policy is set for the appropriate use by enterprise applications—regardless of where the workload is hosted.
4. Data use is continuously monitored and log data about who, what, when, and where is available to the orchestration layers for behavior analysis.
5. It allows the security team to focus on the other pillars ***knowing that enterprise data is secured***.

Zero Trust Quick Wins

A data stewardship approach has many quick win opportunities. Our favorite, and probably the easiest to implement, is a "data rights management" rollout. Data rights management, done right, is DLP on steroids. Every document created, or ingested, by an organization can be wrapped and protected for use by only those users on an approved access list. In a Microsoft 365 environment this wrapper is simply integrated with the Microsoft DRM suite to enforce copy, print, edit functions policies for each user. Automating these functions by policy makes them transparent to users and it enforces enterprise encryption policies while not allowing ad hoc encryption that stifles DLP inspections.

But wait... there's more!

Automated data encryption by policy protects an organization against ransomware. Even if a bad actor gets by all other Zero Trust controls, the stolen data is encrypted with quantum-generated keys. The organization cannot be blackmailed by the risk of sensitive data exposure.

Data rights management plays a key role in supply chain risk management. Sensitive data can be securely shared with third parties (other companies, agencies, vendors, coalition, or business partners). The enterprise maintains control over every individual with access to the data. The protection follows the data, wherever it goes. The data cannot be used without the enterprise data steward's permission.

Data Stewardship Summary

Data Stewardship combines accountability (data owner) with mission/organization policy automation (enabled by technology), to ensure the right data is used at the right time by the right people/applications for the mission.

- Data is protected for its entire lifecycle, from creation to archival.
- Data owners can visualize data use, and thus tailor data access to only those who require it.
- When other Zero Trust pillars are breached, the enterprise data remains protected behind encryption enabled by quantum-resistant encryption keys.

About the Authors

Mark Emery is the managing partner of The Emery Group. He serves as a strategic advisor to systems integrators, government executives, and innovative technology companies. Formerly, the Deputy CIO for the Department of Homeland Security, he has managed business portfolios at Nortel Government Solutions and CSC (now GDIT). He volunteers with the AFCEA Homeland Security Committee, GTSC, and is on the board of TiE-DC, an entrepreneurship mentoring association.

Brig. Gen. Gary Connor (USAF retired) is an independent Aerospace and Defense consultant. He specializes in "systems thinking" and strategies for complex systems. He had a 31-year Air Force career as program management and senior executive leader, and he served as a warfighting CIO (J6) with Multi-National Force Iraq.

THE EMERY GROUP