Alvarium

As a Stage 1 project in LF Edge, Project Alvarium aims to build a framework and SDK for trust fabrics that deliver data from devices to applications with measurable confidence.

See the vision at: https://youtu.be/88KbYmIkFdw

Project Alvarium at a Glance

- New LF project forming to focus on system-level trust and data confidence
- Differentiated in its comprehensive view and in delivering data to applications with measurable confidence
- Unifying, not reinventing trust insertion technologies
- Relevant to all markets and solution stacks
- Seeded by Dell Technologies code

<u>Project Mission:</u>

- Create the framework and open APIs that bind together existing open source and commercial value-add for trust insertion, develop confidence score algorithms
- Collaborate with other LF projects and industry efforts (OSS, SDO) to unify existing and emerging trust insertion technologies and refine scoring algorithms

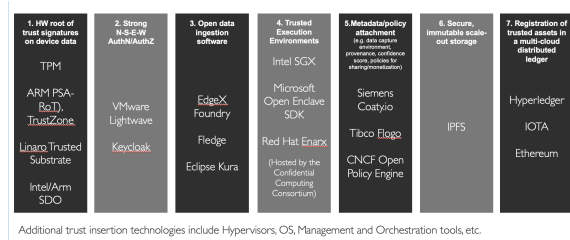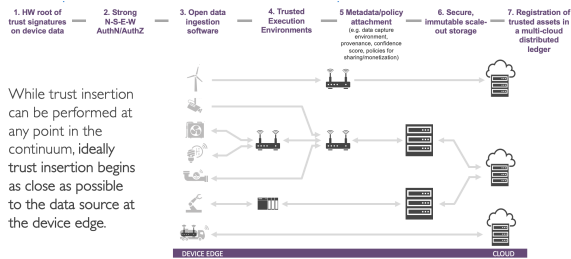## What is a Data Confidence Fabric (DCF), or "trust fabric"?

- A Data Confidence Fabric (DCF), or more generally-speaking trust fabric, is a virtual overlay that aids in the delivery of data from devices to applications with <u>measurable</u> trust characteristics.
- A DCF is a loosely-coupled collection of various trust insertion technologies, bound together with an open framework
    - Example technologies include tools for silicon-based Root of Trust (RoT), open authentication and data ingestion APIs, metadata handling, immutable storage and blockchain/ledger
- The Alvarium framework features open APIs and integrated algorithms to generate confidence scores for data based on the trust insertion technologies used and overall context
- There is no single DCF, rather each entity/organization can build their own fabric with preferred technologies using the Alvarium framework
    - A trust fabric built with widely trusted ingredients will naturally produce the highest data confidence scores
    - Confidence scores normalize across systems of systems as data flows through intersecting trust fabrics
- Key differentiation from other efforts focused on security, privacy and trust:
    - Holistic, system-level focus
    - Confidence scores to enable organizations to act with measured risk based on policy appropriate for the use case / context, working across heterogenous systems of systems

Why we need to collaborate on a **global trust fabric**

- Pervasive sharing and monetization of data, resources and services across heterogenous systems of systems spanning public and private boundaries
    - Can also include trusted sharing/exchange of data sets for training AI model
    - The common "zero trust" model isn't scalable, access policy needs to be attached to trustworthy data

- Consolidating workloads on common infrastructure in a trusted fashion
    - Enable sharing of data/services based on policy while protecting privacy and IP
    - Address common debates on data ownership

- Meeting compliance requirements (e.g. GDPR) at scale
    - Enables organizations to trigger deletion of distributed data in place when a user requests to revokes privacy consent

Example end-to-end trust insertion points

Example OSS trust insertion technologies

| 1. HW root of trust signatures on device data | 2. Strong N-S-E-W AuthN/AuthZ | 3. Open data ingestion software | 4. Trusted Execution Environments | 5 Metadata/policy attachment (e.g. data capture environment, provenance, confidence score, policies for sharing/monetization) | 6. Secure, immutable scale-out storage | 7. Registration of trusted assets in a multi-cloud distributed ledger |

While trust insertion can be performed at any point in the continuum, ideally trust insertion begins as close as possible to the data source at the device edge.

DEVICE EDGE — CLOUD

1. HW root of trust signatures on device data	2. Strong N-S-E-W AuthN/AuthZ	3. Open data ingestion software	4. Trusted Execution Environments	5.Metadata/policy attachment (e.g. data capture environment, provenance, confidence score, policies for sharing/monetization)	6. Secure, immutable scale-out storage	7. Registration of trusted assets in a multi-cloud distributed ledger
TPM			Intel SGX			
ARM PSA-RoT), TrustZone	VMware Lightwave	EdgeX Foundry	Microsoft Open Enclave SDK	Siemens Coatyio		Hyperledger
Linaro Trusted Substrate	Keycloak	Fledge	Red Hat Enarx	Tibco Flogo	IPFS	IOTA
Intel/Arm SDO		Eclipse Kura	(Hosted by the Confidential Computing Consortium)	CNCF Open Policy Engine		Ethereum

Additional trust insertion technologies include Hypervisors, OS, Management and Orchestration tools, etc.

Initial DCF prototype

- Dell Technologies' initial Data Confidence Fabric (DCF) prototype (completed in August 2019) demonstrated a trust fabric comprised of a mix of open source and commercial technologies
- Prototype was deployed entirely on one edge system to locate policy insertion for data monetization/compliance as close as possible to the data source
- **Alvarium framework unifies the various loosely-coupled trust insertion elements**
- **Solution could just as well be deployed in a distributed fashion**
- Next steps in prototyping – demonstrating technology swapability, for example exchanging Project Concord ledger for Hyperledger or IOTA
- Dell will contribute the Alvarium framework code to seed the project
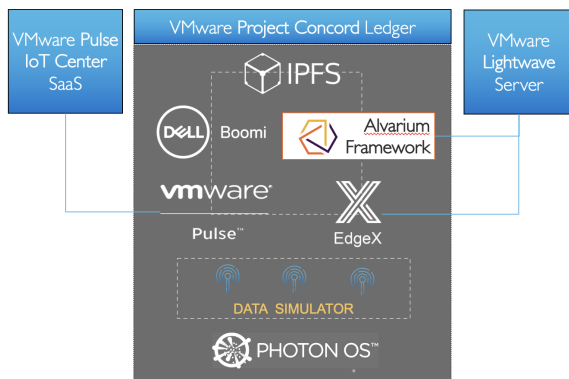
Example Confidence Scoring

- Scoring creates a weighted confidence depending on trust insertion technologies implemented in a given trust fabric
- Dell's initial DCF prototype leveraged a simple linear scale for simplicity
- Scoring algorithms will require industry collaboration to develop
- Initially via OSS but may require some standards work
- Likely to make sense for weighted scoring, some factors that zero out confidence