Ingredients

Cloud Native Shift
Service Mesh Architecture
Key Ingredients to Enabling ZTA
Operationalizing
Cloud Native Shift

- Attack Surface Area
- All Resources Networked Attached
- New Paradigm For Identity, Trust, and Verification

All Shifted to App Teams
Mesh Architecture Protects You

The Unwanted Ingredients

[ Weak] Leaked Credentials
Unpatched or Misconfigured Software
Time
Implicit Trust
What is a Service Mesh?

A Service Mesh is a dedicated & transparent infrastructure layer placed between the application and the network that enables *Reliable, Fast, and Secure* service communication.
Service Identity

A service mesh will issue cryptographically-verifiable workload identity for all services this is not tied to infrastructure.

SPIFFE is widely adopted identity framework most commonly utilizing short very lived X.509 certificates.
mTLS

X.509-based identities are utilized in a full stack solution for transport authentication and encryption of data in transit.

Mesh sidecars serve as Policy Enforcement Points (PEPs) guarantee policy conformance with zero application changes.
End User Credential & Identity

Fine-grained control over end user and/or external upstream service requests

Control end user AuthN/Z based on identity expressed in JWT credential or layer 7 request attributes
Network Policy

A Service Mesh provides centralized policy management with distributed runtime enforcement.

Whitelisting/Blacklisting or shape traffic based on service, IP, layer 4/7 request attributes, or logical environment.

Usually a combination of many.
Operationalize Mesh With DevSecOps

As complexity increases:
- Multi-Cluster
- Multi-Cloud
- Hybrid Cloud
- Integration with Legacy

ZTA must be built into automation toolchains
Thank You

Contact

@tetrateio  Tetrate  www.tetrate.io

For any further queries, feel free to contact us at info@tetrate.io