DATA NOTARISATION

DETECTING DATA TAMPERING AND HIJACKING

ENDIDA

NEXT GENERATION CYBER DEFENCE

WHY WOULD SOMEONE WANT TO TAMPER WITH YOUR DATA?

Data tampering attacks can come from both within and from outside of your organisation and can cause substantial damage with minimal effort. Malicious tampering of data is used to influence applications, data services, AI/ML models, and decision-making.

Its impact is considered to be worse than other cyber attacks at it is hard to detect and intended to cause long term harm to your business.

COMMON TYPES OF DATA TAMPERING ATTACKS

MAN-IN-THE-MIDDLE ATTACKS

Interception and alteration of communication between two parties, including eavesdropping, stealing data, or impersonating one or both parties

FALSE DATA INJECTION

Manipulating or inserting false data into a system or network to cause disruption or gain unauthorised access

DATA SABOTAGE

Intentional destruction, alteration, or manipulation of data with the intent to cause harm or disrupt normal operations

SPOOFING

Impersonating a legitimate entity to deceive the victim into revealing sensitive information

GET IN TOUCH TO FIND OUT HOW WE CAN HELP YOU TODAY

endida.com | 0238 2180 428 | info@endida.com

OTHER USES FOR DATA NOTARISATION

System failures

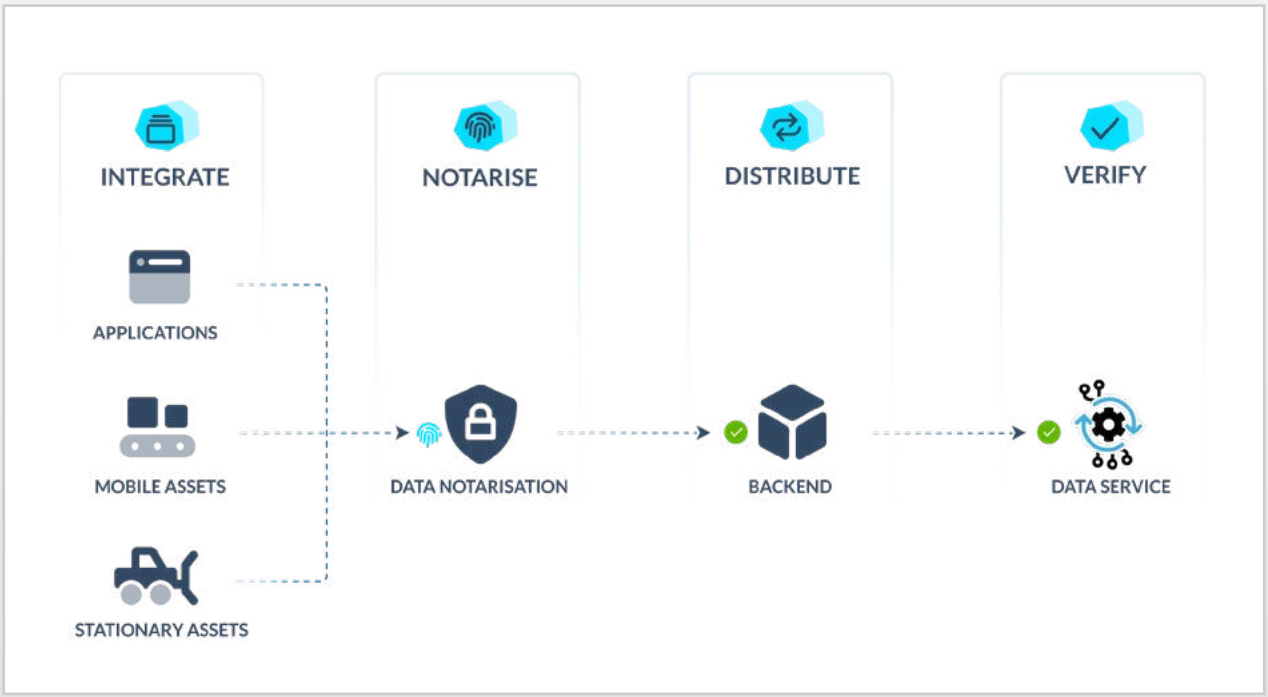
Long term data integrity protection

Establish provenance of resources

Mitigation of human error

Restore trust in your data supply chain

Cut time to market for new products



HOW DOES IT WORK?

1. Integrate log data, documents, critical files, sensor or application data from any IT/OT/IoT source
2. The patented data notarisation creates a unique fingerprint for every data point at source
3. Distribute the data to any application or back end system within the organisation, across applications and infrastructures
4. Verify integrity and authenticity of log data, documents, critical files, sensor or application data before using it

GET IN TOUCH TO FIND OUT HOW WE CAN HELP YOU TODAY

endida.com | 0238 2180 428 | info@endida.com