JITSUIN

Archivist

Operators of Essential Services face continual supply chain risks from connected Things.

Regulatory burdens, strengthening threats, thinning air gaps and complex deep technology supply chains compound the challenge for CISOs to manage risk with fewer resources. A solution needs to integrate with corporate risk governance, enable automated collaboration, connect with existing platforms and deliver combined insight and action, not more contextless alerts!

Move fast and fix Things.

Archivist permanently records when who did what to a Thing. All supply chain stakeholders responsible for cybersecurity can contribute to shared service histories of Things.

Archivist logs events, automates corrective actions and enables a collaborative framework across the cyber security supply chain; security increases with assured intelligence and compliance is proven with distributed ledgers.
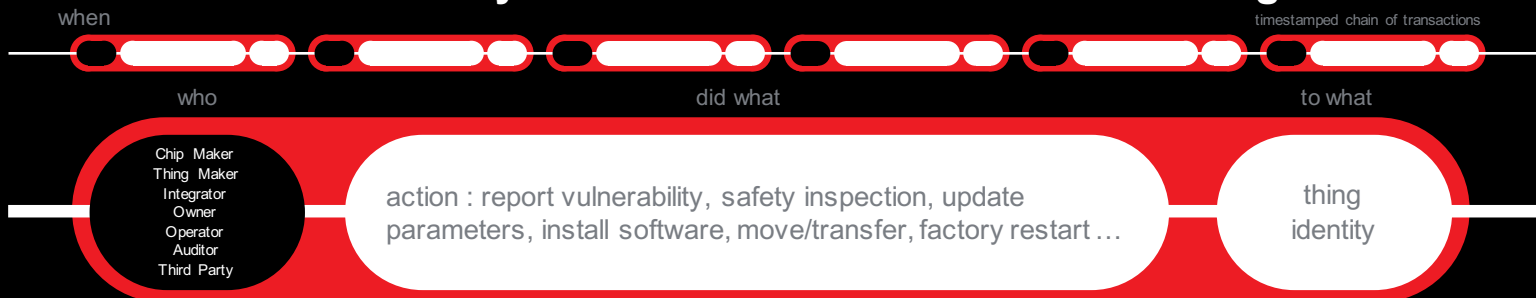
Archivist is a cloud-native SaaS that is data first, protected by industry standard identity and access management, built on open source distributed ledger technology and integrates with any system or application through REST APIs.

Customers use Archivist to:

• Increase transparency with regulators to show continual compliance, clearly communicate risks to supply chain partners and collaborate on fixes.

• Reduce costs through automated compliance reporting and streamline labour intensive audits.

• Lower risk by fixing of cybersecurity issues with supply chain partners before vulnerabilities impact business.

Permanently record when who did what to a Thing

when   timestamped chain of transactions

who   did what   to what

Chip Maker
Thing Maker
Integrator
Owner
Operator
Auditor
Third Party

action : report vulnerability, safety inspection, update parameters, install software, move/transfer, factory restart …

thing identity

Visibility

No need for all to agree on a trusted Third Party

Incorruptible shared record of events

Proof of who claimed what when

A single version of history

Collaboration

Coordinate who needs to do what in the event of an incident

Coordinate partner response to an event in near-real time

Ensure the right stakeholders take the right action at near-real time

Continuity

Distributed records introduce no single point of failure

Irrefutable proof of who knew what when

Ambient accountability built in by design

No back-dating records

Automation

Encode SLAs in smart contracts and monitor supply chain performance

Remove lossy, error prone paperwork and labour-intensive processes

Automate reporting

Easily Integrated   **Single Source of Truth**   **Highly Available**   **Efficient and Accurate**

Archivist shared service histories deliver Truth in Things

JITSUIN

Archivist

Markets

Energy & Utilities

Electricity
Water
Oil & gas
EV infrastructure
Renewables
Energy storage

Transportation

Airports
Aircraft manufacturers
Railway operators
Train manufacturers
Automakers
Maritime

Buildings & Infrastructure

Smart city
Road infrastructure
Buildings automation
Heating and cooling
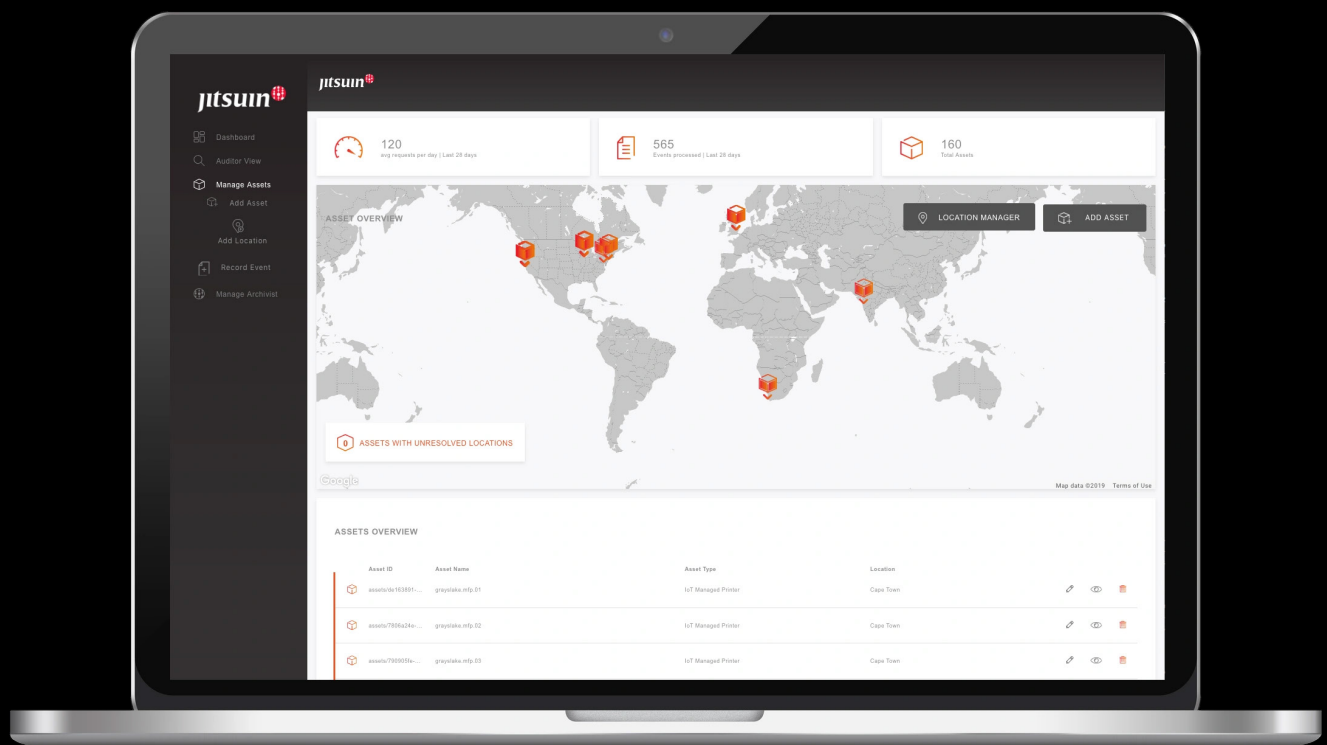Street lighting
Environment monitoring

Healthcare

Hospital equipment
Medical electronics
Telemedicine
Pharmaceutical manufacture

Finance & Insurance

Cyber-risk insurance
Healthcare insurance
Automotive insurance
Home insurance

Platforms & Digital Services

Cloud computing
Edge computing
5G networks
Marketplaces

Users and Uses

CISO
Risk governance of IoT
SLA visibility and accounting
Security exception sign off

Audit / QA
IoT calibration records
Safety inspections
Supplier collaboration

Compliance
Incident alerts and reporting
Network Information System Directive
Continuous compliance

Sensitive Supply Chain
Device and data provenance
Operation within parameters

Line of Business
Maintenance scheduling
Business continuity

Product Lifecycle Managers
Enhanced warranty service
Product recall notification