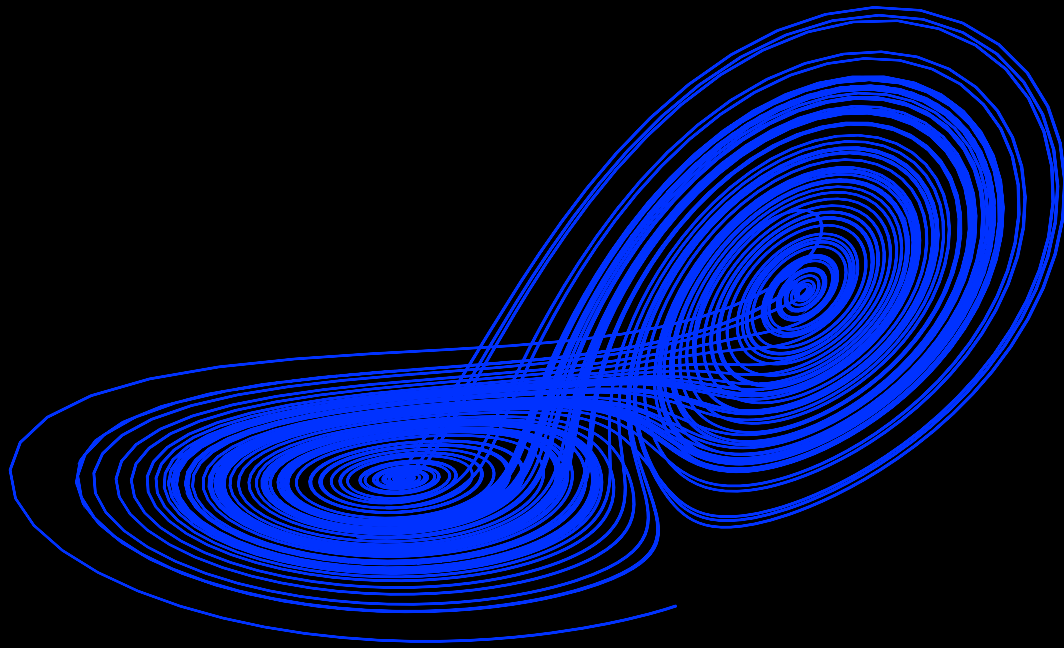
OPSCURA



Get Cloaked. Frictionless Protection for Industrial Networks.

Increase OT Cyber without Disrupting the Operations

Legacy Asset Cloaking

Protect legacy (unsupported or discontinued), long lifetime and mission critical assets in manufacturing plants.

Guarantee business continuity with our drop-in solution that cloaks industrial assets delivered in just a micro-cut downtime and without changes in the network

Protect Disparate Networks

Securly connect disparate automation systems and collate usage information into an analytics application.

Highly scalable solution with low-learning curve that minimize maintenance costs

Simplify Cybersecurity Together

Cybersecurity solutions used to be niche focused solving highly specific problems.

Opscura supports partners and customers along all cybersecurity roadmap, simplifying the overall design, integration, operation and maintenance

Unbiased Solutions Empowerment

CLAROTY
ARMIS
NOZOMI NETWORKS
FORTINET
DARKTRACE
nunsys
DRAGOS
tenable

Gathering data for visibility and detection tools requires to products from vendors that will lock-down specs.

Opscura brings a fair framework to compare visibility tools, avoiding vendor lock-in, expediting and de-risking deployments in OT environments

Quick Asset Inventory

Asset inventory tools used to be invasive and complex to deploy in OT environments.

Opscura lights up the blind spots in the OT network by delivering a simple and network transparent solution.

Discover your assets and their communications in 90 minutes

Increased Security with Minimum Time or Impact

Securing the main plant in Spain for one of the largest speciality chemicals companies in the world.

System integrator implements advanced security mechanisms such as encryption, data integrity, segmentation, firewalling in a transparent ways.

Deployment in 3 sites in 2 hours. No specific configuration or reengineering is required.

Empowering Integrators

The United Nations is an intergovernmental organization that aims to maintain international peace and security.

Opscura secures the infrastructure that brings services to the field missions.

UN' field technicians have been empowered to deploy and manage Opscura in field missions worldwide.

Protecting Legacy Critical Infrastructures

Together with Ferrovial, Opscura secured a wastewater plants that services more than 2.5 million inhabitants.

Opscura technology protects legacy SCADA systems while securely sends information to a IoT detection solution.

The deployment and configurations was done in less than 3 hours.

Assets Discovery in Market Leader

World leader in Water and Wastewater management.

Inventory done in largest European desalination plant. It takes 90 minutes to discover all devices in the network and 15 minutes to deploy and decommission.

After the successful pilot, customer plans to scale the solution to 200 plants.

Secure Monitorization

Monitorization of the electrical analyzer in charge of a telco’s back-up systems. Integration of the logs with its corporate SIEM.

Providing a complete offer for cybersecurity services, filling the OT gap in the portfolio.

Opscura was used to monitor and protect Telco’s electric analyzers managing Data Centers’ backup systems.

Remote and Secure Connection

State-owned company which operates freight and passenger trains with more than 7.000 km and 1.000 stations

Securly connect disparate building automation systems and collate usage information into an analytics application.

500 train stations. 1 person is able to deploy 8 stations per day.

Securing Decentralized Network Distribution

World leader in renewable energy production and the 4th largest utility by market capitalisation worldwide.

Microgrids face new cybersecurity challenges arising from:

- Complex interoperability between different technologies and actors
- Increase of attack-surface

Opscura's solution is vendor and protocol agnostic and reduces the attack-surface by obfuscating the network, making impossible to an attacker getting network information to exploit their vulnerabilities.

Avoid network reconfiguration (and save >90%)

Requirement:
A 150K ton per year pulp & paper plant wanted to enhance visibility and implement segmentation within their plant.

Problem:
A first estimation was $1M just for the network reengineering, retrofitting projects, software changes in the PLCs, etc.

The planned and unplanned downtime, labor and hardware, and IT/OT friction would increases costs even more – creating an unacceptable burden for implementation.

Result:
Opscura increased the cybersecurity level of the plant with…

- zero downtime
- no reengineering the network
- total cost of less than $40,000/year

Visibility and Protection at Scale

State-owned company which operates freight and passenger trains with more than 7.000 km and 1.000 stations

Problem:

Securly connect disparate building automation systems and collate usage information into an analytics application. Costs on deployment and vendor lock.

Opscura's solution:

- 1 person is able to deploy 8 stations per day.
- Simplifies the architecture and the amount of HW.
- Enables visibility and protection at same time, minimizing costs.

Extending the OpEx Value of Legacy Machinery

Requirement:
A manufacturer of industrial appliances was caught in the dilemma of not being able to secure a critical machine, but were unable to operate without it.

Problem:
The OS is WindowsXP and the machine tool manufacturer discontinued the cybersecurity support.

They could not segment these machines from the rest of the network.

The solution had to be easy and cost-efficient to implement and maintain.

Result:
Opscura's 'drop in' solution enabled the needed cybersecurity to allow the continued usage of the tool, with...

- zero operational downtime
- no network reengineering

Internal Network Security Monitoring (INSM)

Requirement:
FERC order 887 instructed NERC to update the CIP standards to address internal network security monitoring (INSM)

Problem:
Legacy network environments lack the ability to capture “east-west” traffic. IEDs, PLCs, RTUs and other equipment within the ESP of a transmission substation, control center, or generation plant typically use hard-coded addresses, making network changes expensive, and are unable to run security agents.

Result:
Opscura’s ‘drop in’ solution allows internal network security monitoring without agents and without network changes:

- Zero operational downtime
- No network reengineering


OPSCURA