Cybersplice enables and secures Operational Technology for advanced Building Automation

Building automation is often built on geographically dispersed operations with localised OT connected to the IT network in the form of Building Management Systems, Access Control, Surveillance systems, Generators, Environmental Sensors and the like. Although some form of separation may be in place, bridges between the IT and OT networks abound.

Attackers target OT both as entry point to the IT network and also as a prize in itself. Due to the number of different vendor products involved and limited security capability of devices, the application of traditional IT security practices and controls (like patching, configuration hardening and segregation) is unrealistic.

Splice secures these environments through logically relocating OT into an encrypted overlay network, and provides vulnerability shielding within this network, allowing customers to continue normal operations even with vulnerable equipment connected.

Splice provides **security visibility** into OT networks and enables **connectivity and convergence** through secure integration inside an encrypted overlay network. Splice capabilities specifically applicable to Building Automation include:

Standardised and secure remote access

Facilitate standardised, seamless and secure remote access for all partners, operators and facilities managers. Remote Access Users connect into the overlay network

Identity shielding

Strengthen fragmented and weak identities across the OT landscape through authentication offloading and multifactor injection.

OT network traffic profiling

Profile OT network traffic at key points with out-of-band mirror mode, or the entire network using in-path mode.

Behavioral monitoring

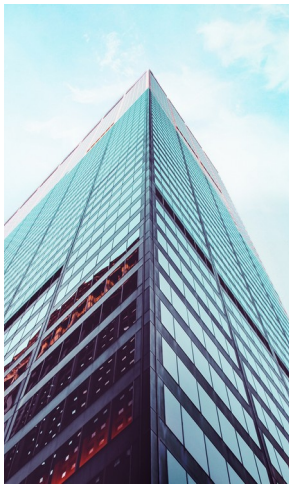
Leverage the near-deterministic nature of OT traffic to identify attacker behavior and unauthorised changes to the network or nodes.

Outlier detection

Cybersplice uses AI to identify anomalies in device to device communication, and to detect compromised devices and command-and-control back channels.

In-core isolation

Prevent cross talk between OT disciplines across the entire network, at the edge as well as right inside the overlay network core.



Secure access edge

Cybersplice provides a secure access edge across the entire OT environment, mediating cryptokeys for all nodes using Splice cloaks, including limited spec legacy devices.

Role based access control

Build role based access controls into legacy systems without touching the code.

Increased resilience

Scale Splice Supernodes to increase resilience, leveraging underlay redundancy, and building parallel paths across the overlay network.

Untangle

Cybersplice acts as a flight recorder for OT communications, bringing visibility down to the infrastructure level. Visualise and understand OT network traffic, perform threat hunting and forensic analysis going back a full year.

Insecure protocol wrapping

Cybersplice draws OT communications into an encrypted overlay network, shielding unauthenticated and vulnerable ICS protocols from adversaries.

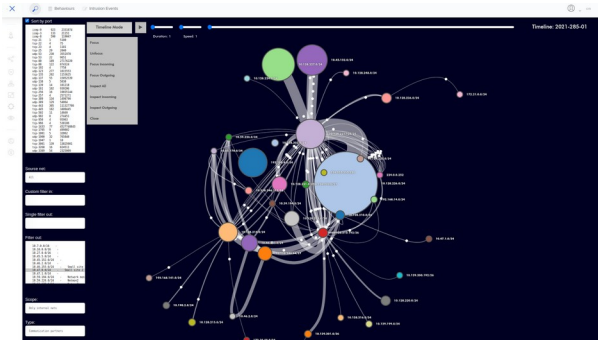
Autopilot

Automatically triage newly detected behaviors for rapid on-boarding or in noisy converged networks.

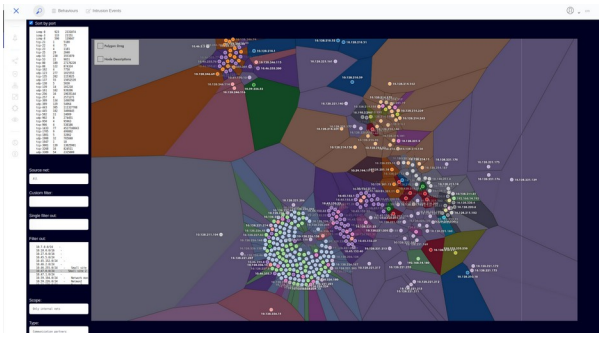
Deep visibility in Operational Technology networks, the good, the bad and the ugly

The screenshots below show some of the Cybersplice advanced visualisations and behavioural tracking:

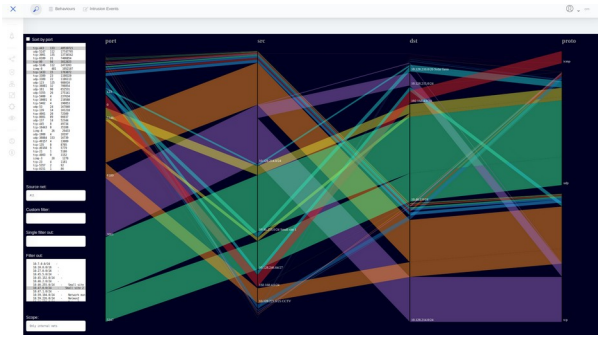
Cybersplice timeline replay of OT comms



Clustering of communication partners



Who's talking to who: flow summary



Cybersplice dashboard birds eye view