Splice-net Industrial Cloud extends OT Network reach across hostile carriers and Corporate IT networks

Splice-net builds a dedicated encrypted overlay network on top of existing carrier infrastructure, for a secure private OT and sensor network. Splice-net is carrier independent, allowing OT networks and sensor networks to expand across multiple carrier footprints, and allowing for high availability by rerouting overlay traffic through alternate carriers. Customers remain in full control of encryption keys and therefore fully in charge of their OT networks, even where traffic traverses hostile or untrustworthy carriers.

Secure Remote Access

Facilitate seamless and secure remote access for partners, operators and engineers.

Role based access

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

Identity shielding

Strengthen fragmented and weak identities across the OT landscape through authentication offloading and multi-factor injection.

Intrusion detection

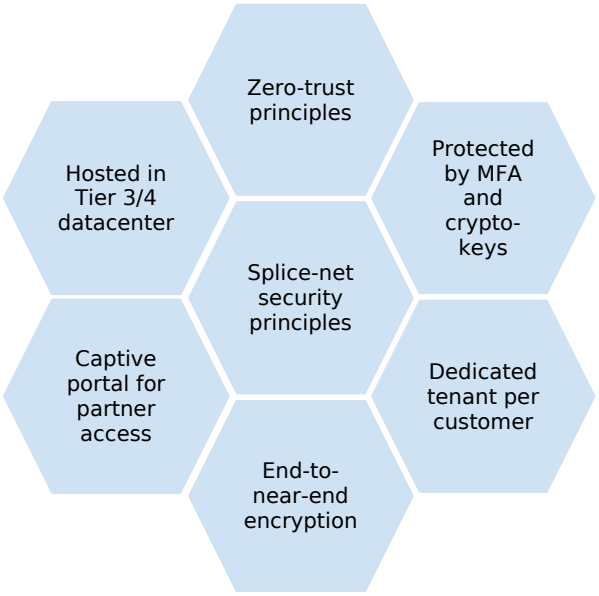
Detect common attack signatures with IDS in the overlay network core.

Increased resilience

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

Behavioural monitoring

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



Step 1

Request a demo or quote at https://cybersplice.com/splice-net

Subscribe to initiate tenant setup, order hardware cloaks or download virtual cloaks and agents to cover the OT Network.

Step 2

Deploy software agents or hardware cloaks at remote sites.

Create user accounts for operators, partners and engineers.

Step 3

Log in to Splice-net and configure subnets and OT devices reachable over the encrypted overlay network.

Remotely access your OT Network without compromising security.

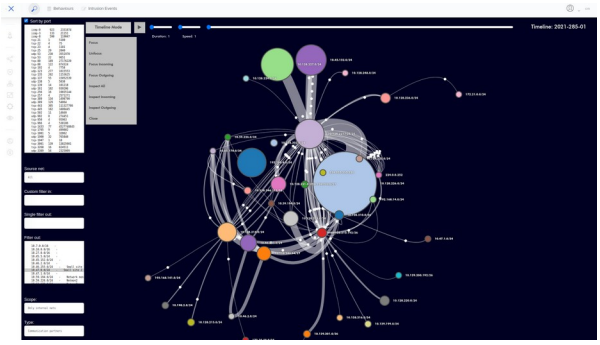
Visualize and monitor your OT network.

Cybersplice and our partners can advise on architecture options to cover your OT Network. We also offer an initial feedback session to assist customers with queries and advise on mitigations for avoidable exposures.

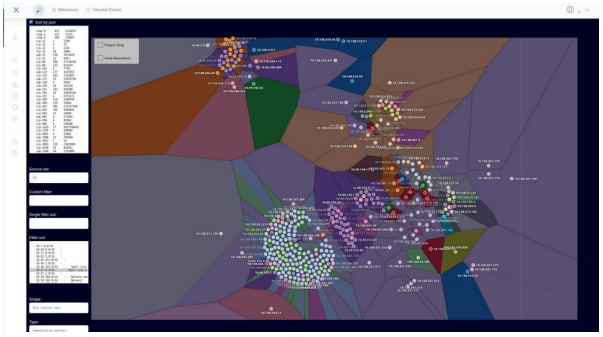
Deep visibility into OT networks, the good, the bad and the ugly

The screenshots below show some of the advanced visualizations and insights available when using Splice-net Industrial Connectivity Cloud:

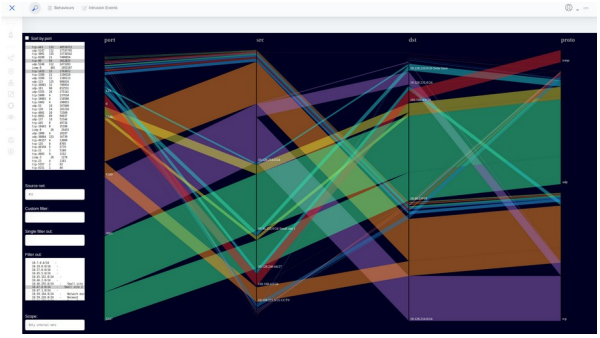
Cybersplice timeline replay of OT comms



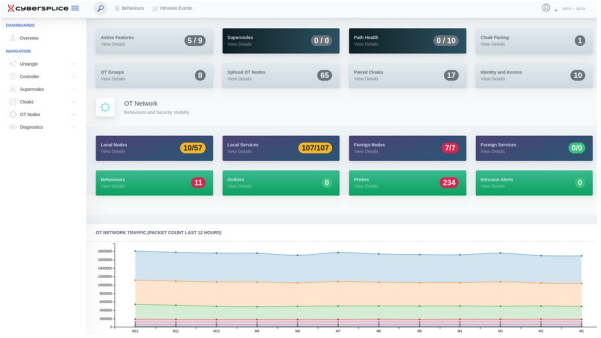
Clustering of communication partners



Who's talking to who: flow summary



Cybersplice dashboard birds eye view



Eligibility

Splice-net Industrial Connectivity Cloud is available to customers in select regions. Please contact us at splice-ng@cybersplice.com or your nearest Cybersplice partner for a no obligation demonstration.

Splice-net may be supplemented with a cyber-physical exposure assessment. Please contact for pricing.

Cybersplice **prevents**

destructive cyber-physical attacks

when Splice is deployed in edge and in-path mode by shielding vulnerable equipment inside an encrypted overlay network

Insecure protocol wrapping

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

In-core isolation

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

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.

Behavioural monitoring

Leverage the near-deterministic nature of OT traffic to identify attacker behaviour and unauthorized 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.

Secure remote access

Facilitate seamless and secure remote access for partners, operators and engineers.

Untangle

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

Identity shielding

Strengthen fragmented and weak identities across the OT landscape through authentication offloading and multi-factor injection.

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.

Eliminate bridges

Eliminate unauthorized and unintentional bridges between IT and OT networks through edge mode deployments.

Autopilot

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

Secure access edge

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

Intrusion detection

Detect common attack signatures with IDS in the network core.

Transition from Splice-net, to on-site mirror mode, edge mode, and in-path protection at your own pace, or deploy Cybersplice on-site in mirror mode with in-path available as a contingency when under attack.