Splicecloud enables

rapid visibility of cyber-physical exposures in Operational Technology networks

Splicecloud enables rapid visibility into cyber-physical exposures on Operational Technology networks. The zero-touch version of this service requires no hardware deployment and is enabled by forwarding metadata of communications using built in switch capabilities to Splicecloud for analysis and profiling. Alternatively, if the OT network underlay infrastructure does not support metadata export, a no-cost light virtual probe, or full featured hardware or deep deep probe can be used to extract the required data from a network tap.

Rapid visibility

Splicecloud acts as a flight recorder for OT communications, bringing visibility down to the infrastructure level.

Behavioural profiling

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

Forensic audit trail

Splicecloud keeps a record of OT nodes and behaviours, the backbone for a timely incident response capability.

Network Visualizations

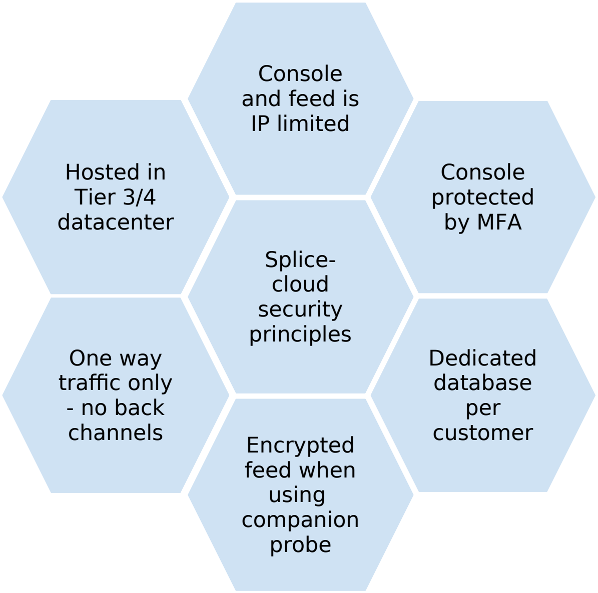
Visualize and understand OT network traffic using our Untangle engine.

Outlier detection

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

Three steps to get started

Follow simple guided three step setup instructions to get going.



Splice-cloud security principles

Console and feed is IP limited

Hosted in Tier 3/4 datacenter

Console protected by MFA

One way traffic only - no back channels

Dedicated database per customer

Encrypted feed when using companion probe

Step 1	Step 2	Step 3
Subscribe at https://subscriptions.cybersplice.com and follow the tenant setup instructions. Provide us with the required contact details and IP address from which Splicecloud will accept the metadata and allow connections to the console.	Forward your flow records from the OT infrastructure systems (switches) through to Splicecloud (remember to allow this one way outgoing traffic through your corporate and/or infrastructure firewalls).	Log in to Splicecloud and tag subnets and OT devices as they are discovered by the passive metadata feed. Visualize and monitor your OT network. Splicecloud automatically identifies behaviours, outliers, assets and services.

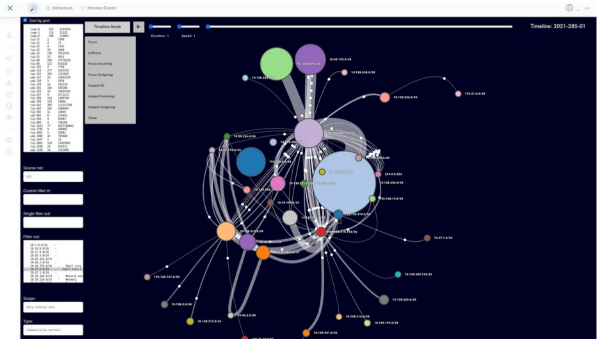
* For the deep hardware probe option, there is an additional step to ship, commission and activate the feed.

Cybersplice and our partners can advise on how to enable export of flow records. We also offer an initial feedback session to assist customers with queries and advise on mitigations for avoidable exposures.

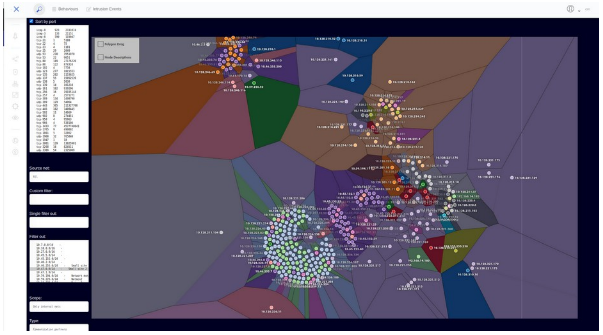
Deep visibility into OT networks, the good, the bad and the ugly

The screenshots below show some of the Cybersplice advanced visualizations and insights available from the rapid visibility offering:

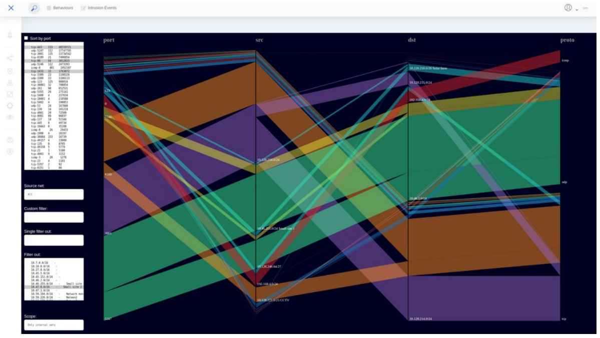
Cybersplice timeline replay of OT comms



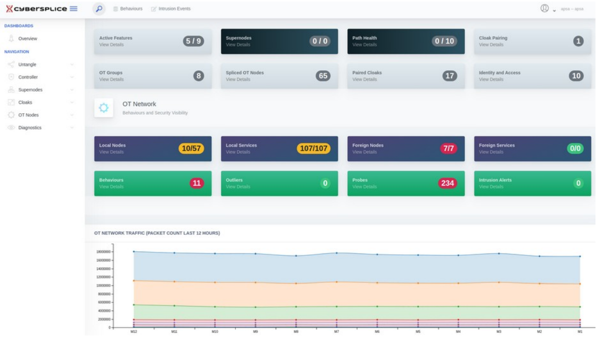
Clustering of communication partners



Who's talking to who: flow summary



Cybersplice dashboard birds eye view



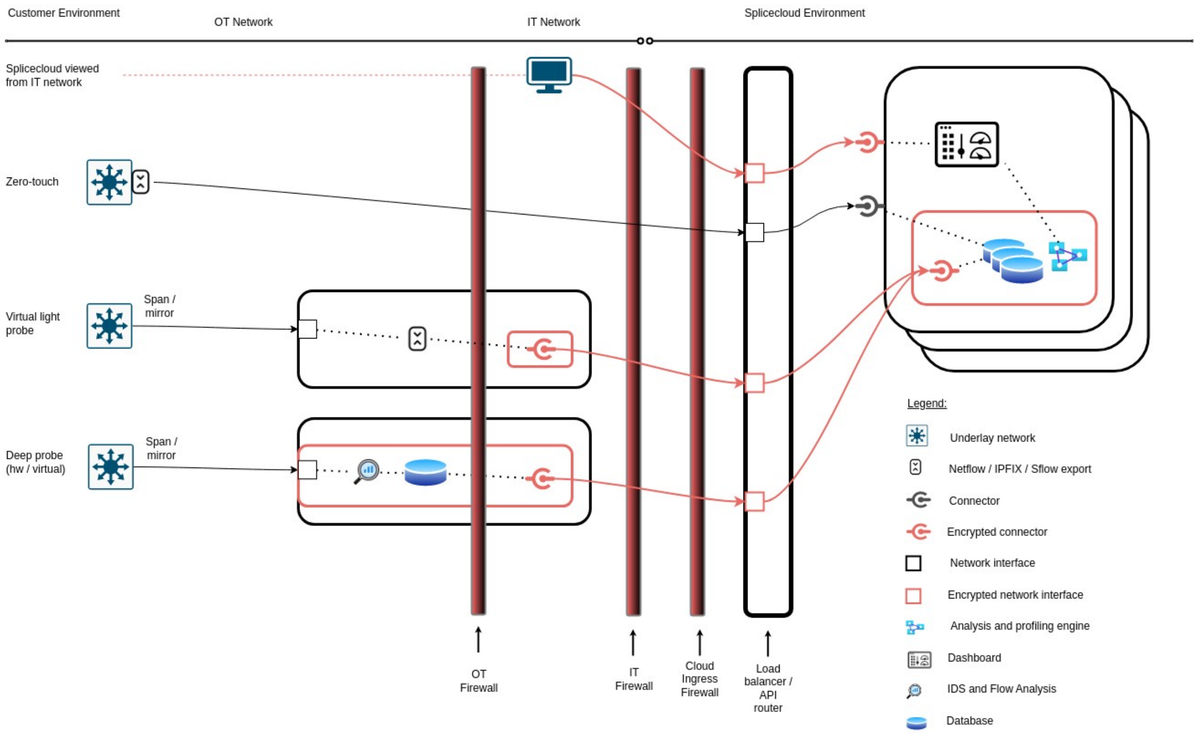
Eligibility

Cybersplice rapid visibility (ie. Splicecloud) is available to customers in select regions. Splicecloud does not include the active protect features available in Cybersplice OT Secure Access Edge, such as vulnerability shielding, overlay encryption, identity shielding, secure remote access, in-core isolation and intrusion detection. Please contact us at splice-ng@cybersplice.com or your nearest Cybersplice partner for a no obligation demonstration.

Simple options for a **rapid start**

Various options are available depending on customer infrastructure capability and visibility requirements. These are depicted below:

Rapid visibility deployment architecture options



The capability and requirements for of each of the options are shown below:

Option	Features	Requirements
Zero-touch	• No hardware requirement • Node and services detection • Probe triage required to convert into behaviours • Behavioural analysis • Outlier detection • One way channel, no back channel to OT network • Node identification through companion agent	• Underlay infrastructure must support netflow/sflow export • OT Network infrastructure must be able to reach Splicecloud servers • Customer to configure netflow/sflow exports and firewall rules required to reach Splicecloud

Option	Features	Requirements
Virtual light probe	• No hardware requirement • Node and services detection • Behavioural analysis • Outlier detection • Visibility where underlay infrastructure does not support Netflow/Sflow • One way channel, no back channel to OT network • Probe triage required to convert into behaviours • Metadata transfer is encrypted through to Splicecloud • Node identification through companion agent	• VMWare, HyperV or KVM infrastructure required • Probe IT facing port must be able to reach Splicecloud • Customer to commission probe once on-site, including flow export or port mirror / span port and required firewall rules
Virtual deep probe	• No hardware requirement • Node and services detection • Behavioural analysis • Outlier detection • Automatic node identification as well as through the companion agent • Automatic probe triage • Visibility where underlay infrastructure does not support Netflow/Sflow • One way channel, no back channel to OT network • Metadata transfer is encrypted through to Splicecloud	• VMWare, HyperV or KVM infrastructure required • Customer to provide configuration details for virtual deep probe preparation • Probe IT facing port must be able to reach Splicecloud • Customer to commission probe once on-site, including port mirror / span port and required firewall rules
Deep probe	• Node and services detection • Behavioural analysis • Outlier detection • Automatic node identification as well as through the companion agent • Automatic probe triage • Visibility where underlay infrastructure does not support Netflow/Sflow • One way channel, no back channel to OT network • Metadata transfer is encrypted through to Splicecloud	• Customer to provide configuration details for deep hardware probe preparation • Probe IT facing port must be able to reach Splicecloud • Customer to commission probe once on-site, including port mirror / span port and required firewall rules

The visibility provided through Splicecloud 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 Splicecloud, 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.