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 low cost light probe, or full featured 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.

Network Visualizations

Visualize and understand OT network traffic using our Untangle engine.

Behavioural profiling

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

Outlier detection

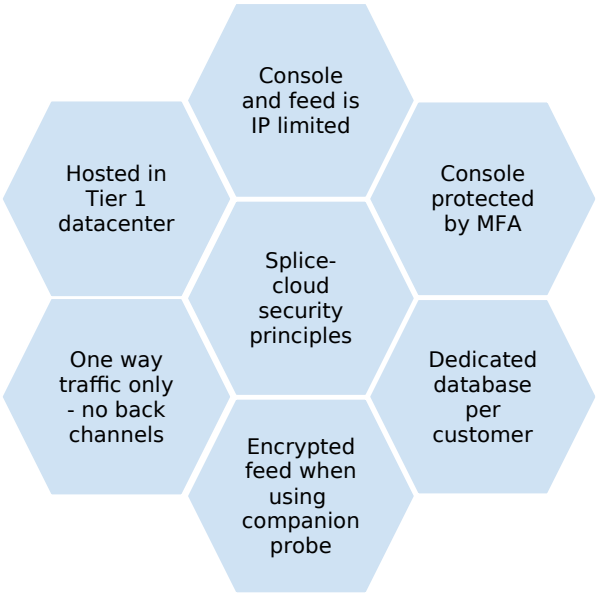
Splicecloud uses AI to identify anomalies in device to device communication, and to detect compromised devices and command-and-control back channels.

Forensic audit trail

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

Three steps to get started

Follow simple guided three step setup instructions to get going.



Step 1

Contact Cybersplice or one of our partners to confirm eligibility. Provide us with the required contact details and IP address from which Splicecloud will accept the metadata and allow connections to the console.

Step 2

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).

Step 3

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.

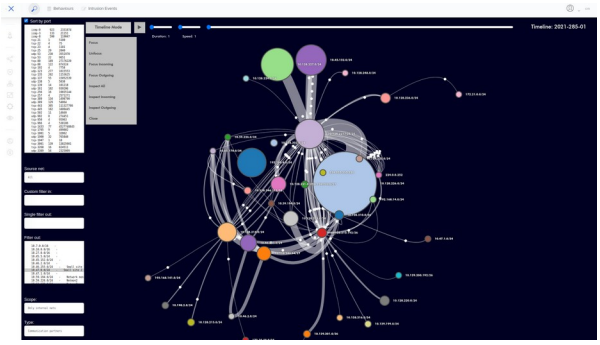
* For the companion probe option, there is an additional step to ship, drop and activate the feed.

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

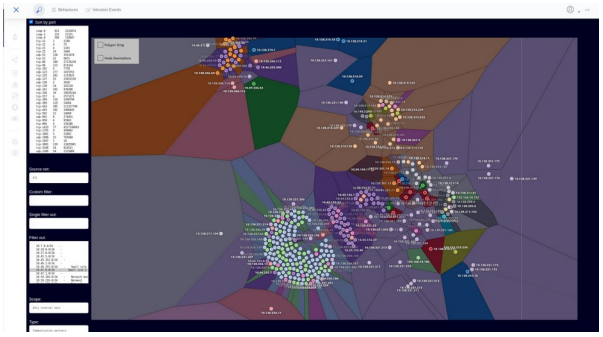
Deep visibility into OT networks, the good, the bad and the ugly

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

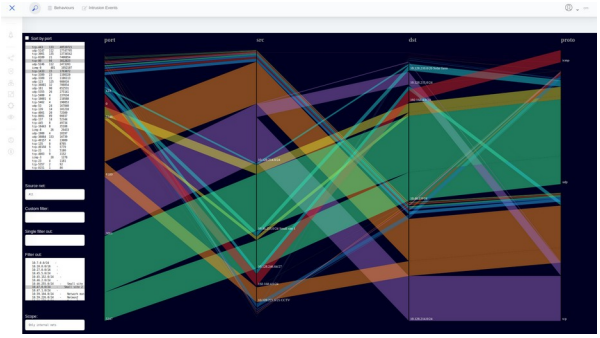
Cybersplice timeline replay of OT comms



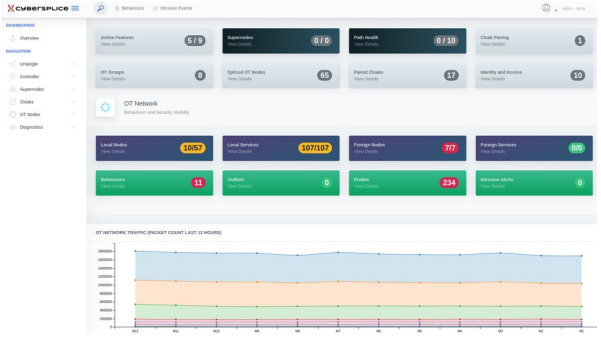
Clustering of communication partners



Who's talking to who: flow summary



Cybersplice dashboard birds eye view



Eligibility

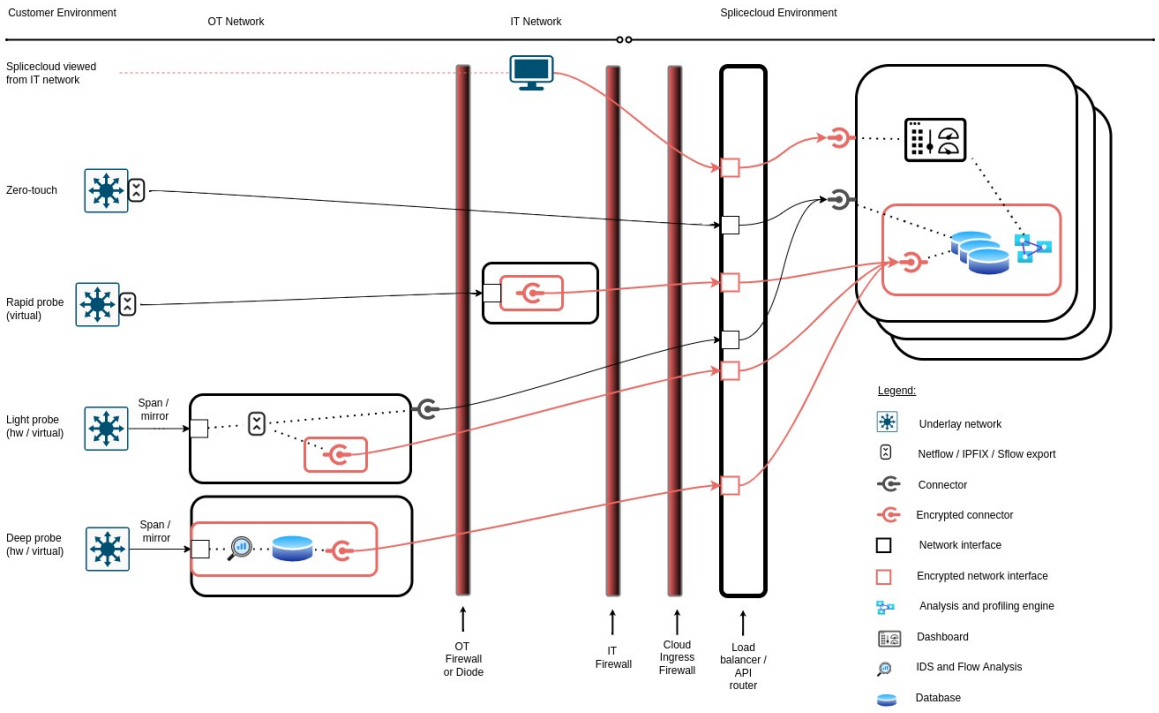
Cybersplice rapid visibility (ie. Splicecloud) is available to customers in select regions. Splicecloud does not include the active protect features available in Cybersplice OT Secure Access Edge, such as vulnerability shielding, overlay encryption, identity shielding, secure remote access, in-core isolation and intrusion detection. Please contact us at splice-ng@cybersplice.com or your nearest Cybersplice partner to see if you qualify.

Simple options for a **rapid start**

Options and pricing

Various options are available depending on customer infrastructure capability and visibility requirements. These are depicted in Figure 2 below:

Figure 2: Rapid visibility deployment architecture options



The capability, requirements and pricing for of each of the options are show below:

Option	Features	Requirements	Hardware cost (once off) and Subscription month to month	Subscription 12-months
Zero-touch	• Node and services detection • Behavioural analysis • Outlier detection • One way channel, no back channel to OT network • Cannot provide node identification	• 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	No hardware requirement Once off setup fee: none Monthly subscription: USD1,100/m	No hardware requirement Once off setup fee: non Annual subscription: USD 11,000/a

Option	Features	Requirements	Hardware cost (once off) and Subscription month to month *	Subscription 12-months **
Rapid probe	• 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 • Cannot provide node identification	• Underlay infrastructure must support netflow/sflow export • VMWare, HyperV or KVM infrastructure required on the IT network • OT Network infrastructure must be able to reach the virtual Rapid probe deployed on the IT network • Customer to configure netflow/sflow exports and firewall rules required to reach • Customer to configure IT firewall rules in order for the Rapid probe to reach Splicecloud	No hardware requirement Once off setup fee: USD 550 Monthly subscription: USD1,100/m	No hardware requirement Once off setup fee: USD 550 Annual subscription: USD 11,000/a
Light probe	• Node and services detection • Behavioural analysis • Outlier detection • Visibility where underlay infrastructure does not support Netflow/Sflow • Probe triage required to convert into behaviours • Metadata transfer may optionally be encrypted through to Splicecloud • Cannot provide node identification	• Customer to provide configuration details for light 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	Hardware once off cost: USD 825 Once off setup fee: USD 550 Monthly subscription: USD1,100/m	Hardware once off cost: USD 825 Once off setup fee: USD 550 Annual subscription: USD 11,000/a
Deep probe	• Node and services detection • Behavioural analysis • Outlier detection • Node identification • Automatic probe triage • Visibility where underlay infrastructure does not support Netflow/Sflow • Metadata transfer is encrypted through to Splicecloud	• Customer to provide configuration details for light 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	Hardware once off cost: USD 1,950 Once off setup fee: USD 1,200 Monthly subscription: USD1,950/m	Hardware once off cost: USD 1,950 Once off setup fee: USD 1,200 Annual subscription: USD 19,500/a

* Billed monthly in advance
** Billed annually in advance

The visibility provided through Splicecloud may be supplemented with a cyber-physical exposure assessment. Please contact for pricing.

Cybersplice **prevents**

death and destruction caused by cyber-physical attacks

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 mirror mode, edge mode, and in-path protection at your own pace, or deploy Cybersplice in mirror mode with in-path available as a contingency when under attack.