Protect what really matters.

Your people, data, and reputation.

Jazz Networks is helping companies protect what matters most–their people, data and reputation. Jazz Networks' cybersecurity platform helps organizations gain deep visibility into all actions made by users and servers and stop data breaches, regardless of physical location.

With the deepest endpoint visibility, Jazz strengthens the organizational security posture with:

- a policy reinforcement tool, which educates employees and reduces human error before an attack,
- machine learning and real-time actions, which protect data during an attack, and
- easy forensics to investigate, respond, and reduce reputational damage if an attack does occur.

BEFORE THE ATTACK

Protect your people

Train your weakest link to be part of your defense.

How do we shift from humans being the weakest link in company security to them being the first line of defense?

Companies that only offer periodic security training are suffering from a lack of traction within their organization. In 2018, a Norwegian chemical shipping company conducted an internal test with a fake phishing link, resulting in 87% of employees clicking through. Three months after a security consultancy training, another test was conducted where 62% of employees still clicked through. Benefit from a direct action-to-impact feedback to ensure something will resonate long-term.

Employee training

On the spot training
that explains the violation to the end user, correlating their action to an outcome.

Enforce company policy
and track policy violations.

Cyber Passport

Protecting your people requires knowing who they are, where they've been, and what they've been doing.

Employee details sync
from the active directory - online status, location, network name, and foreground application.

Exact current location & Wi-Fi connection

Summary of alarms & triggered sensors

Activity feed displays all user events in logical sequence

- Print events
- Browser events
- Integration events
- Connections
- File events
- DNS lookups
- USB events
- Logins
- Applications

DURING THE ATTACK

Protect your data

Identify and block breaches or policy violations.

Machine learning

Filters abnormal activity based on user, application, and operating system:

Corporate security policy violations
- Using cloud storage
- USBs
- Connecting to unsecure networks

External attack attempts
- Port scanners
- Spoofed WiFi networks
- Failed login attempts

Malicious or abnormal activity
- Outbound connection
- Machine generated DNS
- Binary file execution

Data exfiltration
- Inbound/ outbound bytes sent & received
- DNS exfiltration
- Web uploads
- Printing

Real-time action

Soft:

Display message
to prompt end users with a customized pop-up notification.

Take screenshot
to capture end users desktop: visible through activity feed.

Multi-factor authentication
to confirm an employee's identity, if they're behaving abnormally.

Hard:

Lock
a computer if malicious intent is identified.

Isolate
an infected computer or server to prevent malicious software from spreading.

AFTER THE ATTACK

Protect your reputation

Investigate, respond and gain control.

Power search

No query language knowledge needed
to search for users, servers, or events.

Built like a search engine, the Jazz Power Search enables operators to find a detail amongst the millions of data records collected.

Uncover user event details in seconds
like file names, frequency of use, data movement, applications, processes, connections, and more.

Quickly create a hypothesis
in response to an alarm, or research situations arising from other tools.

Connections view

A clear visualisation of an employee's data flow between different hosts.

See netflows of traffic & applications
that initiated the user or server's connections.

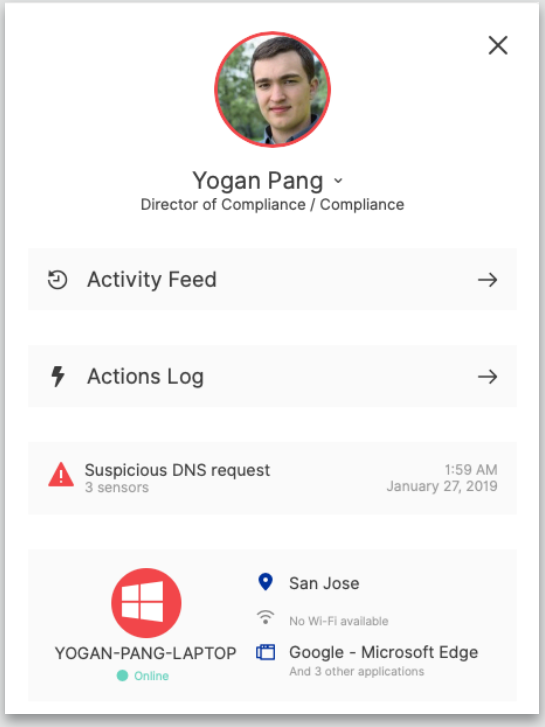
Expand details
to see other users connected to the same host.

See bandwidth volume

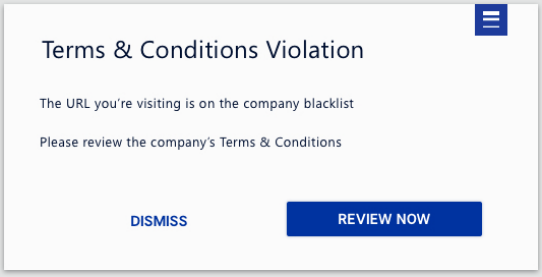
See process-to-process communication
between any Jazz agent endpoints.

The view enables you to virtually walk across the network, viewing a node's connections and related processes

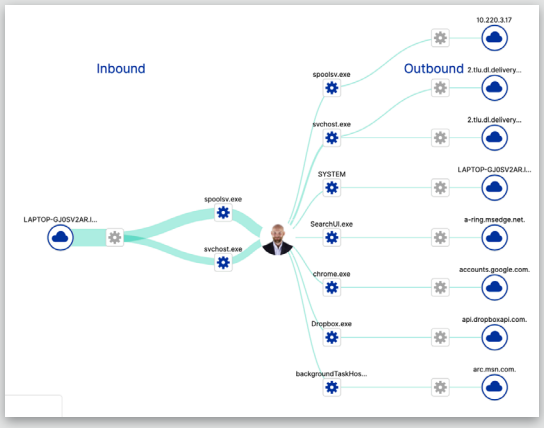
Cybersecurity data recorder
During an incident investigation, the data recorder provides a full paper trail – even if data is deleted or evidence is destroyed during an attack.



The Cyber Passport provides a significant amount of information for every user and associated managed nodes.



The customizable company policy pop-up notifications explain violations to the end user.



The connections view provides a clear visualization of an employee or server's network traffic.

Next steps

Contact us at sales@jazznetworks.com to get a free 45-day trial.