Jazz Networks

Jazz Platform

Feature overview of version 7.1, released November 2019.

Insider threat detection & response

Complete visibility and deep behavioral context

into user activity and workstation, server, and cloud events

Cyber passport

Know who your users are, where they've been, and what they've been doing.

Individual employee visibility from multiple LDAP directories

Summary of alarms, triggered sensors, and policies

Exact Wi-Fi connection and Geo-IP location

Activity feed displays all user actions and alarms in logical sequence

incl. print, browser, file, and integration events, as well as connections, logins, DNS lookups, USB events, applications, and more

Pseudonymization

Identify a suspicious or problematic situation and make an initial incident analysis without violating users' privacy, in accordance with legislation, e.g. GDPR articles 6, 25, 32, and 89.

Control whether operators can see users' actual or pseudonymized profiles with multi-level monitoring.

In this view, information is either pseudonymized (replaced with realistic fictional data) or anonymized (hidden).

High-risk actors

Identify which threats pose the greatest risk to your organization and determine how to best allocate your time to threat response.

- Prioritize risks important to your organization by configurating the policy and machine learning severity scores.

Powerful user activity detection coupled with immediate response

RULE-BASED POLICIES

Detect & respond:

- Searching the web using blacklisted term
- Sending files over SFTP
- Conducting network scans
- Creating, modifying or deleting an account
- Sharing files though the web browser

MACHINE LEARNING

Detect & respond:

- Surge in print volume/jobs
- Login outside normal work pattern
- Application run for the first time
- Concurrent login to multiple machines
- Network traffic outside normal work pattern

Windows Security integration

Red flags for sabotage attempts to use forbidden software or access suspicious websites, careless users, or malware. Be alerted when your security might be weakened.

Windows Defender:

- Detects when Windows Defender finds malware.
- Detects when a user, malware, or third-party application tries to modify, disable, or delete settings.

Windows Firewall:

- Detects when a user, malware, or third-party application tries to change settings, including add, modify, disable, or remove rules.

Microsoft Office security:

- Detects when Microsoft Office security is compromised due to registry changes.

Keystroke analytics New

Automate your defense against keystroke injection attacks, unauthorized access, and more. Improve workplace security.

Unauthorized access:

- Detects when users' typing patterns deviate from the norm.

Keystroke injection attacks:

- Detects non-human typing patterns.

Blacklisted keywords:

- Detects use of harmful language in any application–for example, “gun”, “kill”, or “suicide”.

Continous and comprehensive training

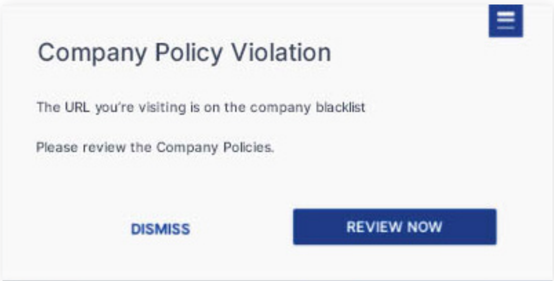
Incident-based training

Immediate feedback is the most effective training.

- Reinforce corporate security policies
- Immediately connects an individual's action with an explanation of company violation
- Improves behavior over time
- On-screen messages are customizable and link to company policies

Cyber hygiene:

- Unsecure or open Wi-Fi connections
- USB storage device use
- BitTorrent or P2P sharing tool use
- File uploads to Dropbox, OneDrive, and more
- File uploads with blacklisted keywords
- HTTP connections



Company Policy Violation

The URL you're visiting is on the company blacklist

Please review the Company Policies.

Insights and security for the remote workforce

IT productivity

See if IT applications, software, cloud applications, web services are being used without company approval.

- Track shadow IT
- Identify corporate assets misuse

Breach detection & response

Combine the power of two detection methods

Policy templates

Allow you to control threat detection and automate threat response from day 1.

- Define rules for specific user activities and the actions that are taken if these rules are breached
- Apply policies to individuals or flexible groups
- Out-of-the-box, customizable, or create your own
- Automated response using one or more actions
- Sensor and alarm events sent to webhooks to Slack, Splunk, and more

Covering a wide range of threats:

- Advanced content inspection on files using regex, New monitor activity when users access files containing U.S. social security numbers, credit card numbers, or smiliar.
- Additional templates: browser, connection, file, mail, printing, Rsync, SCP, indicators of attack (EDR), risk of leaving, USB, Wi-Fi, Windows security integration, Keystroke analytics, DLP

40+ new policies, including: New

- External threat
- File downloaded from IP address
- TCP connection with high bandwidth
- Share folder access exceeded
- File transferred over RDP
- Screenshot taken
- Blacklisted folder accessed

Machine learning

Identifies abnormal activity, allowing operators to more efficiently investigate events and remediate threats. Quickly identify threats such as:

Malicious or abnormal activity

- Login (time & # of New machines)
- Keyboard typing pattern New
- New location pattern
- Outbound connection
- Machine-generated DNS
- Binary file execution
- Port scanners
- Spoofed Wi-Fi networks
- Failed login attempts
- Connections to unsecure networks

Data exfiltration

- USB usage
- Printing amount
- DNS exfiltration
- DNS server change
- Unusual networks (phone tethering)
- Inbound/outbound bytes sent & received

RULE-BASED POLICIES AND MACHINE LEARNING:

Indicators of attack:

- Logins using local machine credentials
- SSH and Telnet connections
- Windows Firewall modifications
- Hacking or scanning tools use
- Restricted file access

Data exfiltration:

- Excessive printing
- Remote connections using SFTP
- File copying using rsync
- Backup application use
- File uploads matching content inspection
- USB storage device use

Real-time actions

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

Lock
a computer if malicious intent is identified

Display message
to prompt end users with customized text

Take screenshot
to capture an image of a user's desktop

Actions page New

The new Actions page centralizes action information. The page eases oversight and management of servers and workstations on which actions have been executed.

Alarms page New

The Alarms page shows key details for each alarm, such as the severity score, the time and date the alarm was raised, and motion screenshots corresponding to policy violations.

Cases

Uncover and remediate threats with ease using cases. Designed to simplify threat hunting and forensic analysis, cases enable operators to identify suspicious events requiring investigation, and then collaborate on investigations for more informed decision-making and rapid response.

Build a case over time
by proactively adding events requiring investigation.

Collaborate across team
individuals can add alarms, sensors, events, comments, links, photos, and screenshots.

Threat hunting & forensics

Get the full picture, even without policy violation.

Power search

Forensics and threat hunting made easy. Ensure you comply with government and industry regulations, e.g. GDPR article 55, to notify the supervisory authority within 72 hours of a personal data breach.

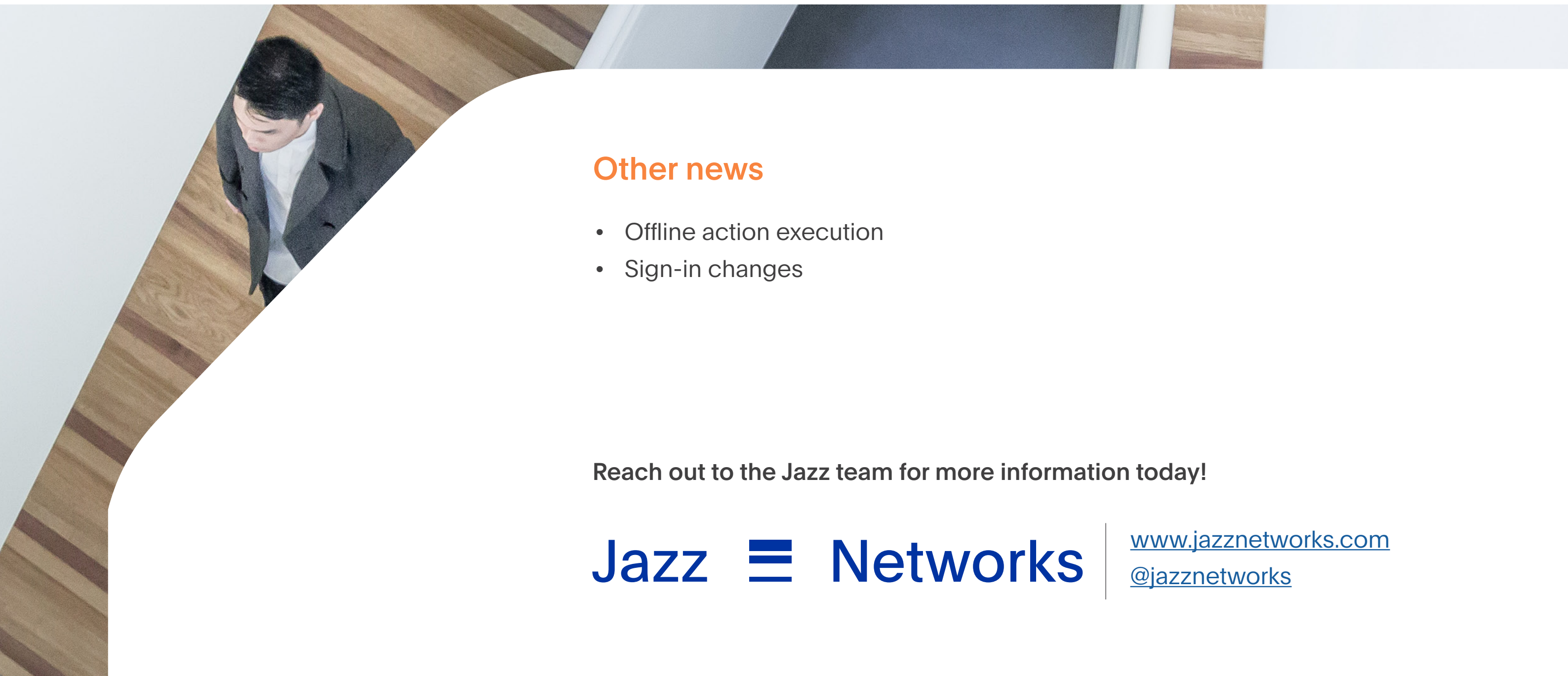
Uncover user details in seconds
such as file names, frequency of use, data movement, applications, and processes connections.

No query language knowledge needed
to search for specific historical context.

Cybersecurity data recorder

A full paper trail during an incident investigation–even if data is deleted or evidence is destroyed during an attack. All the data available in one place.

Legacy products only do visibility on policy violations.



Other news

- Offline action execution
- Sign-in changes

Reach out to the Jazz team for more information today!

Jazz ☰ Networks

www.jazznetworks.com
@jazznetworks