

FAQ



1. WHO IS NYANSA?

Nyansa is a fast-growing innovator of advanced IT analytics software technology based in Palo Alto, California. Founded in September 2013 by technology professionals from MIT, Meraki, Aruba Networks, and Google, Nyansa is credited with developing the first cloud-sourced network analytics system, called Voyance.

2. WHAT IS VOYANCE?

Voyance is a new, vendor-agnostic IT network analytics service purpose-built for CIOs, network operations, and help desk personnel managing heterogeneous enterprise environments. Voyance is focused on the end user experience by helping IT staff gain new insights into client access conditions, network service behavior, and enterprise applications issues that impact user performance. Voyance automatically baselines issues in the IT environment, establishes an objective benchmark for good performance, pinpoints specific problems, and suggests their root causes and remediation.

3. WHY WAS VOYANCE DEVELOPED?

Voyance was developed to address new problems being faced by network operations staff driven by the explosion of smart mobile and IoT devices, the mission criticality of wireless connectivity, and the usage of cloud applications out of the control of enterprise IT. In this environment, traditional tools such as CLI and network management and monitoring tools are unable to analyze and correlate all of the data related to tens of thousands of client experience issues, and thus predict, pinpoint, and remediate problems faster and more cost effectively.

4. HOW DOES VOYANCE WORK?

Voyance works by inspecting, analyzing, and correlating every client device's user experience across the entire network application stack. It does this by extracting performance data from real user traffic, and simultaneously collecting metrics from wireless controllers and other on-premise systems. Voyance employs big data analytics to yield actionable information that gives IT staff the ability to quickly pinpoint problems, symptoms, and root causes of connectivity issues while proactively suggesting remediation of user issues. Additionally, using cloud-based analytics techniques applied to network infrastructure data; Voyance opens the door to a revolutionary new IT analytics concept called "cloudsourcing."

5. WHAT IS CLOUDSOURCING?

Cloudsourcing is a new approach to IT network analytics that allows network information, infrastructure service metrics, application behavior, key performance indicators, and trending information to be anonymously shared and compared between different companies. This allows organizations to gain a deeper understanding of network operation best practices and predictive insights into the user experience.

6. HOW IS VOYANCE DEPLOYED?

One or more small software extractors (known as a Voyance crawlers) are deployed off a span, monitor, or tap port set up on one or more switches, pushing data to the crawler(s). The Voyance crawler gathers and inspects packet data from real user traffic, fusing it with wireless LAN metrics obtained from WLAN controllers. Voyance crawlers securely transmit only performance metric summaries of the data to the Voyance cloud based analytics engine for analysis. Software crawlers are available as a VM software download (EXSI v. 5.5 or higher) or within a small physical appliance.

7. WHAT TYPE OF DATA DOES VOYANCE COLLECT AND INSPECT?

Voyance analyzes every packet that it sees on the wire as well as wireless metrics collected from WLAN controllers. This includes a broad range of protocol, flow, network, WLAN, and device statistics as well as information such as client device type / vendor / capabilities, OS version, DHCP issued IP addresses, DNS, DHCP, HTTP response times, packet loss, transmission error rates, Wi-Fi channel utilization, signal-to-noise ratios, application performance, WLAN controller configuration and much more.

8. HOW MUCH DATA IS SENT UP TO THE CLOUD?

For every 1Gbps of real user traffic that goes to the crawler, approximately 500kbps is sent securely to the cloud.

9. HOW SECURE IS THE VOYANCE SERVICE?

Voyance provides hardened security across a number of dimensions including user, backend, and application security. No packets or payload are stored or leave the customer premise. Anonymization options for classifier metrics (e.g. IP hostnames, ports, etc.) are also available. Strong encryption of in-transit data from onsite crawlers to the Voyance cloud analytics engine is achieved using SSL (TLS) communications. Backend secure access controls provide two-factor authentication and audit trails. Logical isolation of the Voyance service within the AWS virtual private cloud delivers state-of-the-art security supporting SOC1, attestation standards. Application-level security is achieved through third-party penetration and vulnerability testing with protection against SQL injections and cross-site scripting, weekly nmap scans are also performed.

10. HOW MUCH HISTORICAL DATA IS STORED ON THE VOYANCE SYSTEM?

While there is no real limit to how long historical analytics and data can be stored, Voyance provides up to 6 months for historical trending data at no charge and 15 days for real-time (by minute) client transaction data.

11. HOW LONG DOES IT TAKE TO DEPLOY VOYANCE?

The configuration and deployment of the Voyance services typically takes under one hour and can be installed in less than 30 minutes depending on the environment.

12. WHAT WI-FI SYSTEMS ARE COMPATIBLE WITH VOYANCE?

Nyansa currently integrates with Aruba, Cisco, and Ruckus wireless LAN controller systems.

13. HOW IS NYANSA DIFFERENT FROM TRADITIONAL NETWORK MANAGEMENT AND EMERGING IT ANALYTICS SOLUTIONS?

Voyance differs significantly from conventional NMS and emerging IT analytics alternatives solutions that merely provide mountains of raw data that IT staff must manually analyze and correlate into meaningful,

understandable information that can be used to take action. Voyance does this by aggregating a collection of unique capabilities not found in any other solution today. These include but are not limited to:

- full-stack analysis of wired and wireless data analysis for every client network transaction in real-time and over time,
- automatic root cause analysis and remediation "next steps,"
- automatic baselining of client incidents and network services,
- anonymized cross-company sharing and comparison of network key performance indicators and infrastructure metrics,
- vendor-agnostic big data analytic system, purpose built for enterprise environments.

14. HOW DOES NYANSA MAKE IT EASIER TO SOLVE PROBLEMS?

By translating the analysis and correlation of network, client, and application data into plain English summaries, the system helps IT staff identify and remediate user experience problems faster and more cost effectively. Finally, by incorporating anonymous data from other environments, Voyance can provide objective benchmarks for good performance, and predict issues based on knowledge obtained from from other organizations' experiences..

15. HOW MUCH DOES VOYANCE COST?

Available immediately, Voyance comes in small, medium, large, extra large, and custom pricing options on a one-year, three-year, or five-year subscription basis with no additional hardware, licensing, or support costs. Flexible pricing options for the enterprise and education markets give customers the choice between the pricing for Voyance based on number of users or network nodes (i.e. access points and switches) that are supported.