THE ESSENTIAL GUIDE TO
NETWORK ANALYTICS
What's ahead?

1. What is network analytics?
2. How it all works
3. Who benefits and why
4. Why you need network analytics, right now.
5. About Nyansa
Unlike conventional network and infrastructure management tools, network analytics goes several steps beyond simply identifying who, what, when, and where network issues happen, but rather, answers the more complex questions of 'Why is this occurring?' and 'How can I fix it?'.

Most existing infrastructure management tools view the network from the inside out, looking at problems and anomalies within the network infrastructure such as switch or server configurations.

Network analytics takes a radically different approach: it views all network behavior from the perspective of its impact on client device performance as they connect to the network and access applications.

Network analytics has three essential tenants. Like any "analytics", it should:

1. Efficiently answer complex questions
2. Proactively recommend real actions
3. Verify results and provide feedback

When people think about analytics, applications such as Google's Waze, Amazon, Uber, or Netflix immediately jump to mind.

They draw our attention because they make something like a movie recommendation or route guidance seem deceptively simple. These applications constantly stare at different types of data and user behavior, analyzing it all to answer a simple problem littered with complexity.

Data sources include raw packet data, network management plane information (e.g. SNMP), system logs, application APIs and traffic flows.
Waze, for example, consumes and analyzes a variety of data sources to suggest the best route to a given destination. It doesn’t show the user the algorithms used to synthesize crowdsourced data about traffic patterns.

The app knows users just want an answer to the question “How long will it take me to get to the Wharf and what’s the best way to get there?” It then provides step-by-step directions and uses your driving experience to verify their estimate.

Analytics should seamlessly and simply answer the user’s inquiries and even [...] questions the user didn't think to ask.

This is what any true analytics system should do for the user. Analytics should seamlessly and simply answer the user’s inquiries and even recommend answers to questions the user didn't think to ask.

Finding answers to complicated questions should be that easy for networking questions — but it isn’t.

To date, many networking professionals have been content with using a combination of legacy monitoring tools, elbow grease, and manual deduction with command line interfaces to answer issues arising on the network. But, as networks evolve, the range of issues impacting user performance and productivity are becoming larger and more complex than ever before.

This hasn’t always been the case. The influx of smart mobile phones, IoT systems, and other devices is changing the way we access the network; they are complex devices carrying volumes of data that can’t be easily or efficiently analyzed by humans.

A decade ago, enterprise networks were largely comprised of company laptops or desktop computers wired by ethernet to on-premise application servers – all sanctioned by the company for employee use.

All the major nuts and bolts were under the control of the IT team because users literally plugged in an Ethernet cable to their device. Their experience on the network didn’t generate any questions and wasn't particularly significant.

With fewer variables, troubleshooting usually consisted of straightforward fixes, like adding more bandwidth, upgrading switches, and network drivers. But in today’s modern enterprise access network, everything has radically changed.
DEVICES
The device ecosystem is now large, mobile, and diverse. Employees are bringing in their own devices and operating systems are introducing, all at once, a bevy of different operating systems, models, and configurations previously unseen in the workplace.

Each new device and operating system operates uniquely on different parts of the network. It’s become nearly impossible for IT teams to keep pace with the rate of new devices being brought onto the network.

Meanwhile the Internet of Things (IoT) has introduced an influx of headless (i.e. robotic or autonomous) specialized devices that need 24/7 connectivity.

These devices, often wireless connected, are dedicated to line of business operations with unique protocols and behavior unfamiliar to networking staff. If the network performance of these devices falters, there is a direct business impact.

ACCESS MEDIUM
Today, nearly everything done within enterprises is performed through a wireless (Wi-Fi) network connection. In fact, most IoT or BYoD devices can’t be wired.

As any network professional will attest, maintaining and troubleshooting wireless connectivity, stability, and performance is much more complicated than a wired ethernet connection with no easy fixes. Issues like noise, roaming, coverage, RF interference and channel planning require constant attention.

Beyond the enterprise access network, WAN networks have also experienced profound changes. WANs used to send all branch traffic via data centers over private links. Now software-defined wide area networks (SD-WAN) dynamically send application traffic over many different types of links.

As the trend toward SD access networks continues, the network is becoming increasingly opaque, making it much more difficult to pinpoint where user network performance problems are hiding.
APPLICATION LANDSCAPE

Applications are moving to the cloud and beyond IT’s purview. Networks now provide access to a wide variety of mission critical applications that range from cloud/web-based to on-premise and UC (unified communications) which need to work on the new device and access landscape.

With all these changes to enterprise infrastructure, IT teams simply can’t continue to use traditional monitoring tools, elbow grease, and deduction to tackle problems on larger, more complex networks.

Today’s modern enterprise networks are less predictable than their predecessors. They venture into the unknown by speedily adopting new technologies. They are large and diverse.

Tending to network issues manually using traditional tools drains time, budget, and personnel.

Volumes of data must be captured, analyzed and compared across different parts of the network to find and fix problems.

Traditional tools were never designed for this purpose, and if used, result in persistent blind spots with virtually no holistic understanding of how the user is really experiencing the network from a performance perspective.

It’s no secret that industries are trending toward increasing digitization and that there is an acute competitive advantage in being a successful early adopter of game-changing technologies.

Consequently, companies can no longer afford to let inefficient, lagging networks be a roadblock to growth as the network is now viewed as a strategic and imperative asset to any enterprise.

Enter big data network analytics.
How it all works

Recent technical advances in big data analysis, cloud computing, and Web 2.0 tools have given birth to sophisticated network analytics that can help enterprises capitalize on network evolution.

New network analytics platforms have been designed to gather data from as many sources as possible, which are then fed through a powerful cloud-based, back-end analytics engine.

This engine correlates the incoming data from all different sources to identify anomalies, trends, patterns and create a detailed end-to-end view of the user network experience that can be used to predict behavioral outcomes as they relate to device performance on the network.

Because these systems are constantly staring at every client network transaction, they are able to baseline application and service behavior over time to understand what’s “normal” and what is not.

When activity deviates from this norm, the system is able to automatically recognize it, rank it’s importance and provide who, what, when, where and why details that might take hours, days or months to figure out using conventional tools.

THE TECHNOLOGY

Next generation analytics platforms typically use small software extractors (within a physical appliance or virtual form) to ingest various data sources, as well as summarize and compress traffic from devices accessing the network.

These traffic extractors are easily deployed, residing out-of-line from network traffic flows – collecting, but not capturing, all network packets sent to them from network switch SPAN, monitor or taps ports.

These same extractors talk directly to different infrastructure elements including: wireless LAN (WLAN) controllers; RADIUS, DNS and DHCP servers; clients and WAN routers using SNMP, SYSLOG, NetFlow, and other standard IP protocols.

In addition, extractors use APIs to gather more detailed data from specialized systems such as unified communications (UC), Microsoft’s SKYPE for Business, and virtual desktop infrastructure like Citrix XenDesktop and XenApps.

Below: Next gen big data network analytic platform architecture

COMPREHENSIVE CROSS DATA CORRELATION AND ANALYSIS

- Massive data ingestion/analysis/correlation/processing/search engine
- Data models built/augmented for UX/UI & APIs
- Visibility & root cause / remediation, data visualizations
- Algorithmic / ML framework (recommendation engine, predictive analysis, etc.)
- Inter and intra site industry benchmarking
- Private cloud deployments
- Public or private cloud deployments
As gigabytes of data are collected from these extractors about every device transaction on the network, this data is summarized and securely transmitted over encrypted connection to massive, back-end cloud analytics engine for processing and display to the user.

Instead of analyzing a small portion or layer of the network, these next generation analytics platforms measure every transaction of every client across the full network stack – correlating how the device is performing on the network from the moment of access all the way through to any application usage.

This provides a complete picture of the user experience and alerts staff to potential problems negatively impacting any aspect of user network performance.

From a client device accessing the network over a Wi-Fi connection, to the user/device authenticating, receiving an IP address, and traversing the WAN to access an application in the cloud. Each of these transactions, for thousands of client devices, are analyzed in real time.

By doing this, IT teams now have the ability to automatically identify issues, remediate problems and quantify infrastructure performance without costly and cumbersome manual data analysis.

Left: Multiple data sources are analyzed and correlated using packet, application, network service, client and WAN data.

Using streaming and batch analytics, machine learning techniques, and cloudsourcing methods, these new analytics systems:

- Reveal the root cause of any problem on the network, from problematic clients to misconfigurations
- Baseline the historical behavior of network services and applications to determine “normal” behavior
- Scale visibility from a global to micro-level analysis of all sites, infrastructure, and devices
- Identify, objectively, how to achieve “good” performance on your network
- Benchmark performance metrics against similar enterprises
- Recommend concrete measures for improving user experience, down to the device level
- Assess the severity and importance of network incidents by their deviation from baselines

Most IT teams are used to relying on vendor-provided tools that focus on one aspect or layer of the network, like Wi-Fi connectivity, or monitor vendor-specific infrastructure, like switches or routers.

Modern network analytics technology takes a vendor-agnostic approach infrastructure management, scrutinizing every bit of the network and all gaps in between to provide the most complete view of the network across the entire infrastructure.

Above: Next generation enterprise analytics detail all incident root causes and suggest remediation

Left: Vendor-agnostic network analytics platforms provide an end-to-end view of the network based on the impact to client performance
Who benefits and why?

Because full-stack network analytics platforms span the entire infrastructure, they provide a single source of truth for the entire IT team. This helps eliminate ambiguities and discrepancies caused by individual teams using specific tools to address just a segment of the network.

Since network analytics scales from a macro-level overview down to granular details, the range and scope of use cases is wider than most monitoring tools. Here's a sample of how teams are using network analytics:

**EXECUTIVE-LEVEL (DIRECTOR OF IT/VP OF TECHNOLOGY)**
- Global overview, compare performance across sites
- Easily assess the quality of network performance without requiring a report or sifting through spreadsheets
- See industry averages, rank performance against similar organizations
- Reduce costly downtime
- Improve productivity by reducing work hours lost to network issues

**SENIOR IT/NETWORK OPERATIONS**
- Receive alerts for critical problems
- See root-cause identification immediately
- Learn the normal baseline performance for your network
- Proactively correct deviations from the norm
- See concrete recommendations to improve performance in problem areas
- Less frequent escalation from Helpdesk - able to focus on critical issues
- Reduce operational costs (i.e. WAN links) by seeing accurate picture of usage

**ENGINEERS/ARCHITECTS/ADMINISTRATORS**
- Immediately answer the question “Where are my worst problems happening?”
- Receive practical suggestions for configuration changes, hardware upgrades, and capacity planning that will improve user experience
- Identify which changes will have the most impact
- Confirm the value of planned upgrades
- Reduced escalation from Helpdesk - able to focus on critical issues

**HELPDESK/SUPPORT**
- Easily receive root-cause identification and steps to remediation, reducing time to resolution
- Reduce escalation to senior IT staff
- Adopt a proactive rather than reactive approach
- Identify problematic devices or applications before an issue is reported
Why you need network analytics, right now.

The quality of network performance is no longer a negotiable for enterprises. Network-connected technologies are used more often for critical business operations than ever before and the trend is not slowing: enterprises leveraging network analytics are growing top-line revenues, cutting bottom-line IT costs, and improving the overall productivity of users on the network.

Most industries are seeking a competitive advantage by turning to digitization in a world where technology is moving at light speed. Network analytics gives IT teams the tools to not only keep pace with transformations in technology, but more importantly, to actively encourage the growth of digitization in the workplace.

Here’s a breakdown of the benefits of big data network analytics across a variety of major industries:

MANUFACTURING

In ‘smart’ factories, everything from RFID-tagged tools to assembly robots relies on consistently perfect network access and performance. Even a minute of downtime can be costly on the manufacturing line. As manufacturers invest more heavily in IoT technology, stakeholders need a way to assess both device performance and the value of that investment.

NETWORK ANALYTICS:

• helps reduce disruption to manufacturing lines caused by dropped connections and misconfigurations
• provides visibility into the performance of IoT tools and devices (scanners, etc.)
• monitors custom applications
• tracks the impact on lost revenue due to downtime
• provides insight into “headless devices” on the network
From telemetry monitors, smart phones for voice communication, and custom EHR applications to lighting/heating controls, healthcare providers are turning to network-based technologies to improve care and streamline operations. In order for these investments to actually work, however, healthcare providers require consistently good network performance in order to avoid potentially critical errors.

**NETWORK ANALYTICS:**
- Manages the performance of IoT devices
- Monitors custom application performance
- Securely transmits data (HIPAA compliant)
- Improves clinician productivity by reducing downtime due to network issues
- Seamlessly integrates with ticketing systems
- Assists with proactive network capacity planning
- Faster remediation of client/network incidents

IT teams in higher education are dealing with an influx of diverse, mobile devices on campus, increasingly digital classrooms, and an increase in overall network usage (blame Netflix and YouTube) spread over thousands of students.

**NETWORK ANALYTICS:**
- Analyzes the behavior of unique student devices (like gaming systems)
- Assesses the performance of integral Unified Communication (UC) devices and apps
- Looks beyond Wi-Fi to the broader network configuration
- Confirms the value of network changes
- Assists in capacity planning
- Reduces Helpdesk ticket escalation
Digitization is transforming retail from the supply chain to the store-level. Digital signage, network-connected devices, and IoT-driven supply chains all rely on excellent network performance.

**NETWORK ANALYTICS:**
- Analyzes the performance of all connected devices
- Retrieves customer and app user behavior
- Proactively assesses the network health at all sites (distribution, store, etc.)
- See the impact of device load on network capacity
- Confirm the value of network changes
- Significantly improve customer experience in-store by reducing service disruptions

Network connectivity is key in the user experience for large public venues. Whether it’s ensuring seamless Wi-Fi access for thousands of visitors in an airport or an excellent fan experience at the stadium, the quality of network performance matters.

**NETWORK ANALYTICS:**
- Scales to analyze the performance of hundreds of thousands of devices
- Provide reliable, uninterrupted user experience
- Provides real-time and historical insight into key devices (digital signage, video monitoring, etc.)
- Quantify and assess the value of infrastructure changes
- Isolate problematic areas inside a venue that require focused IT resources
- See trends in device usage and identify event-specific issues
- Delivers visibility into how customers experience network as part of your brand
Credited with developing the industry’s first cloud-based enterprise network analytics platform, **Nyansa** is a fast-growing innovator of advanced IT analytics software technology and operates the world’s largest and the only vendor-agnostic public analytics service – observing and analyzing traffic across hundreds of production sites with more than 10 million client devices around the world.

Focused on quantifying end user network performance, **Voyance** is the only analytics platform that uniquely analyzes and correlates every client network transaction across the full network stack. Nyansa’s Voyance product is available as a public SaaS service or as a pre-configured private cloud solution.

Customers range across a variety of industries including companies such as MuleSoft, Stanford University, Uber, Tesla, Mission Healthcare System, San Francisco International Airport and American Eagle Outfitters. With Voyance, organizations can now proactively predict problems, optimize their network and justify infrastructure changes based on actual data, radically reducing the time and expense related to optimizing IT network operations from the client to the cloud.

Voyance is available for proof of concept demonstrations at no cost. The system is typically deployed and operational in under one hour.

To request a demo, trial or more information, visit: [https://www.nyansa.com/demo](https://www.nyansa.com/demo).