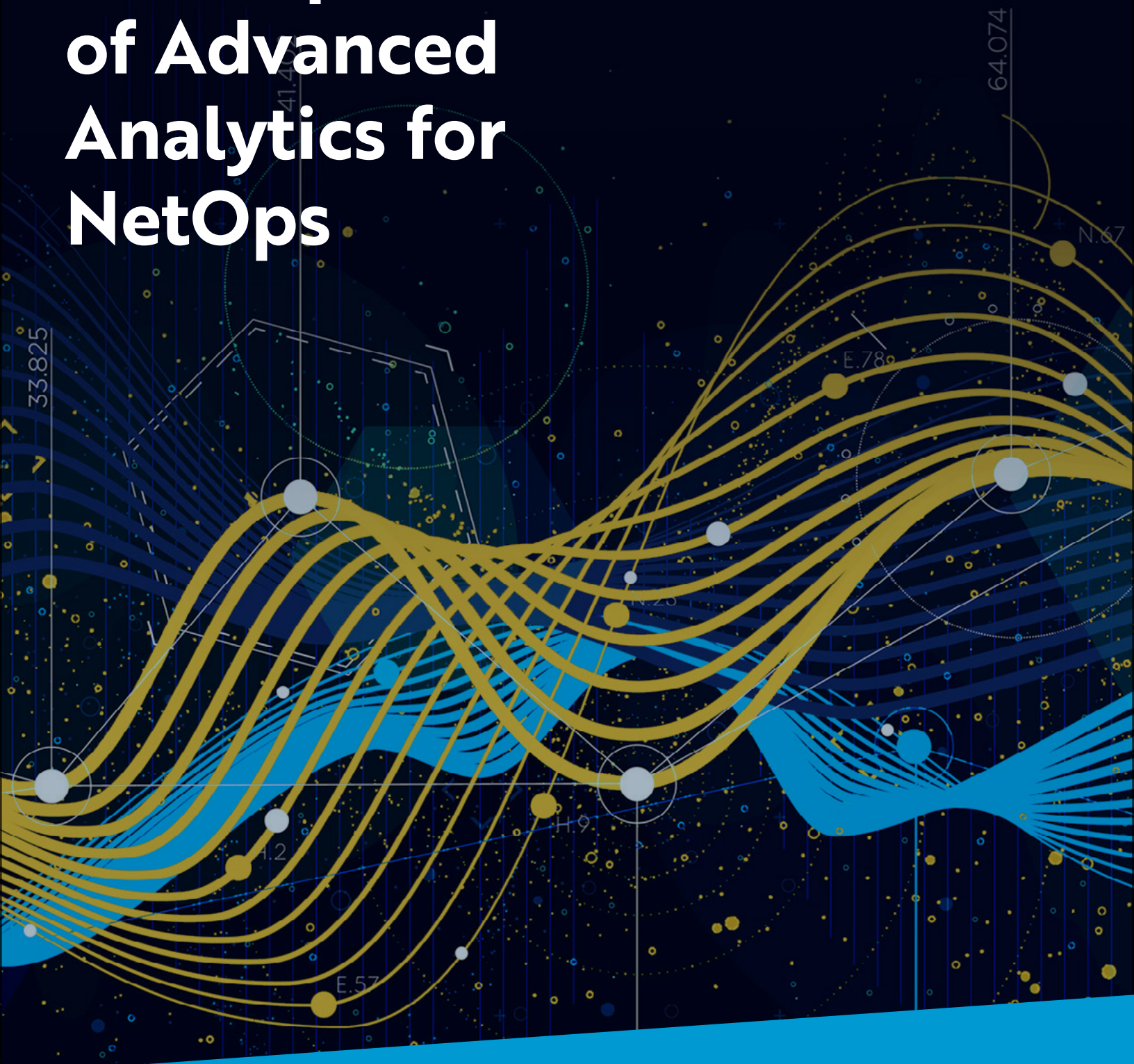
The Importance of Advanced Analytics for NetOps



LiveAction®

Table of Contents

How Advanced Network Analytics Impacts NetOps Teams

Network analytics and monitoring procedures that once were considered standard are quickly becoming inadequate in today's rapidly changing IT network landscape, but advanced networking analytics leveraging Artificial Intelligence (AI) and Machine Learning (ML) exist with features that can overcome new challenges to maintain network performance and future-proof NetOps teams.

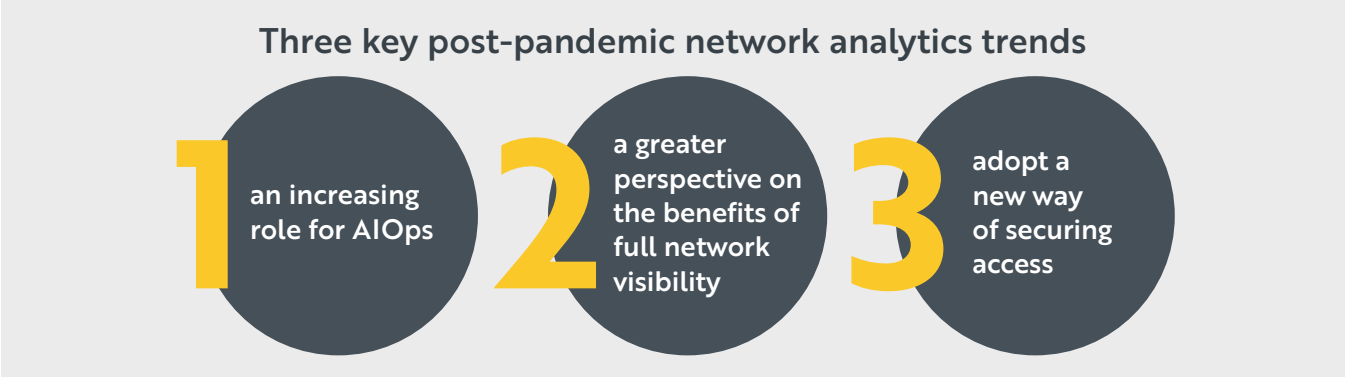
The future network landscape envisioned in pre-pandemic forecasts predicted that IP traffic would multiply exponentially in the coming years, estimates that professionals will now need to expand following the sudden normalization of remote work, IoT, Edge computing, and a reliance on VoIP and video in business life.

By 2023, leading industry professionals expect that 66% of the world population will be connected to the internet, machine-to-machine (M2M) connections will have surpassed half of the total globally connected devices, mobile connectivity will move beyond 2G and 3G networks in favor of 4G and cutting-edge 5G networks, and total IP traffic will exceed 443.5 Exabytes (EB) per month, more than double 2020's total traffic of 194.4 EB.

As a result, more and more enterprise network traffic will traverse public networks, exposed to security risks, and at the mercy of its latency, forcing businesses of all sizes to explore new techniques, specifically AI/ML, and powerful network analytics and performance platforms that offer full visibility of network assets even across the public cloud in order to remain relevant.

Future Network Analytics Trends

Technology choices during this period of accelerated Internet growth will focus in part on managing the new normal faced by IT teams. Three key post-pandemic network analytics trends to watch are, one, an increasing role for AIOps, two, a greater perspective on the benefits of full network visibility, and finally, a need to adopt a new way of securing access regardless of where users are.



AIOps will play an integral role for NetOps. Between 70% - 80% of IT teams have explored options and use cases to integrate AIOps into their operations, but only 3% identify that their AI adoption is at a "high-level", that is by achieving a single-pane of network visibility, consolidated monitoring, fully implemented AIOps, use case models, and automated event resolution. Adoption does exist at lower levels, some AIOps tools can already be found in IT operations, nearly 47% describe their AI adoption as mid-level, incorporating forms of intelligent alerting, root-cause analysis, anomaly/threat detection, capacity optimization, and incident auto-remediation. The remaining 50% use minor forms of digital transformation, but rely on manual management of their networks. These organizations should consider how significant their network supports their business operations, if 24-hours of downtime impacts business operations then it is significant; adopting a network performance platform offers a game changing tool.

Enterprises will seek greater network visibility in a cloud world, as cloud applications are accessed by more devices, and more small and medium sized businesses digitally transform by integrating cloud technology with on-premises networks. These new network configurations present sizable challenges for NetOps teams responsible for monitoring and securing business traffic both in and outside the local network, not to mention what new security threats must be considered.

For the near future, many enterprises will begin to reevaluate and shorten their Secure Access Service Edge (SASE) adoption timelines, a technology adoption that will allow IT teams to apply security access regardless of where their users, applications, or devices are located. Useful since today workers are more reliant on mobile technology and on accessing cloud applications and platforms from remote locations.

For each of these trends, network analytics provides a base that AI/ML technologies use to create intelligent automated networks.

What is Network Analytics?

Network analytics applies data analytic techniques to network data in order to monitor complete network behavior. With the addition of AI/ML technologies, deeper insights on application and network performance can be drawn on network data. These insights help NetOps teams troubleshoot networks and make goal-based improvements more efficiently, while helping organizations effectively make intelligent business decisions.

Network analytics collects and utilizes network data from various sources to visualize the entire network, including using NetFlow data, packet capture, simple network management protocol (SNMP), WiFI data, and API data. Once collected, the analytics engine will aggregate network data with non-network data (cloud data, user data, ITSM, etc.) into a contextual representation of the network, ready for analysis or visualization.

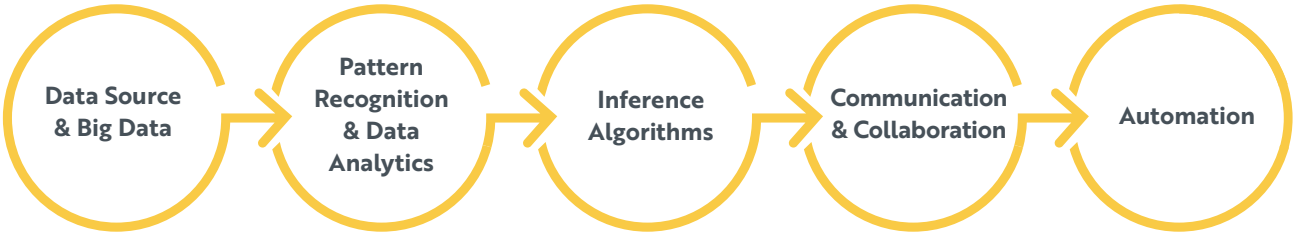
Producing insights at the heart of a network analytics software is the analytics engine, which processes data gathered from network resources using various software and hardware devices. Analytics engines broadly fall into two categories, real-time streaming analyzers, and historic analyzers that rely on processing stored network data. Using these large stores of device information, flow data, server logs, telemetry and more, AIOps can use heuristic learning to draw out patterns and extract insights for many applications:

- **Anomaly Detection** — Send alerts when network performance deviates from expected historic pattern.
- **Forecasting** — Predict where a metric is headed in the future.
- **Outlier Detection** — Identify groups that behave differently than their peers.
- **Predictive Analytics** — Harvest patterns from Big Data sets to predict useful insights and optimizations.
- **Utilization and Application Baselining** — Baseline performance metrics at the device level and on a per direction basis.

In many cases, these analytics engines are migrating to cloud platforms, overcoming many NetOps pain points, such as maintainability and scalability, while offering flexibility and future-proofed capacity.

The AIOps Workflow Supporting Advanced Network Analytics

The current state of AIOps thinking is polarized on the idea that networks are far too complex for fully closed-loop automation, however, automating general tasks is routine and trusted when impacts are thought to be minimal. To outline the complexity of automating IT networking operations, the five dimensions of AIOps represent sophisticated algorithms along layering the artificial cognitive process, each performing an advancing step towards automated management of networks.



1. Data Source & Big Data
The fundamental issue at this level is the massive influx of seemingly unrelated data. Much of this data is redundant and corrupt. Therefore, data set selection algorithms must clean up much of the noise. The main problem is that implementing these algorithms requires complex and specialized mathematics, making it challenging for vendors who run the risk of underestimating or not recognizing the significance of the noise.

2. Pattern Recognition & Data Analytics
The popular pattern discovery algorithms is template discovery, an approach, though vital, that more or less highlights patterns already in the data, rather than discovering deeper insights. High excitement surrounds deeper insights, using deterministic or statistical approaches is a way to go beyond the content and expand what is actually known about the data, and deliver actionable insights.

3. Inference Algorithms
Pattern discovery is just a beginning; more statistics and logic can be applied to draw out deeper insight. At this stage applying inference such as "what-if" experiments can establish causal links between different events, as well.

4. Communication & Collaboration
After deep insights are found, they are translated into many forms to be visualized, expressed in natural language, or machine-readable language. The idea is to formulate findings and propagate insightful action.

5. Automation
Automation is the cap stone of the AIOps workflow; however, it is also the trickiest due to complex networks that may not easily be modified while operating.

Operational Benefits

By implementing a single unified network monitoring solution that utilizes AI/ML advanced network analytics and automation, organizations gain benefits that contribute to reduced costs and greater operational standard.

- **Full Network Visibility** — Granular monitoring of network traffic opens the door to a completely visible network, information from NetFlow provides a broad picture of traffic, while packet capture information allows admins to drill down to understand the details.
- **Efficient Proactive Troubleshooting** — NetOps teams can reclaim a significant amount of time lost by leveraging AI/ML in combination with automation to proactively monitor security threats, discover network bottlenecks, and troubleshooting network issues.
- **Insightful Business Intelligence** — Business teams can discover richness in application traffic previously undetectable, which can be used to honor SLA contracts, plan for network capacity needs, and understand user behavior insights.
- **Security Issues Detection** — Network analytics can monitor endpoint activity and discover anomalies that indicate that it's compromised. If security is compromised, historical analytic data can be used in forensic analysis of breaches to uncover technical and legal evidence against culprits.

Dashboards and Visualizations

Organizations benefit greatly from the sophisticated analytics engine and AI features. But in addition to these under-the-hood aspects, daily NetOps benefits tremendously from the network data visualizations created by network monitoring software, allowing teams to understand at-a-glance the health of their public and private network traffic, and with interactive capabilities to drill down into the details of flows and devices. Two important visualizations monitor network performance, and application performance.

- **Flow Visualization** — By integrating flow and packet level analysis, network traffic can be analyzed in real-time and historically, providing a top level view as well as forensic views at-a-glance. Flows can be visualized across multiple network fabrics, devices, remote sites, VPNs, and service provider transports, easily bringing to the forefront problems and affected areas of the network.
- **QoS Monitoring** — QoS can be monitored on a per-class basis, easily visualizing the impact QoS policy changes have on network and application performance. Alerts can automatically indicate when QoS drops below a specific standard, and AI can remediate the issues so that the company never breaches their SLA contracts.

Making a Case for Advanced Analytics

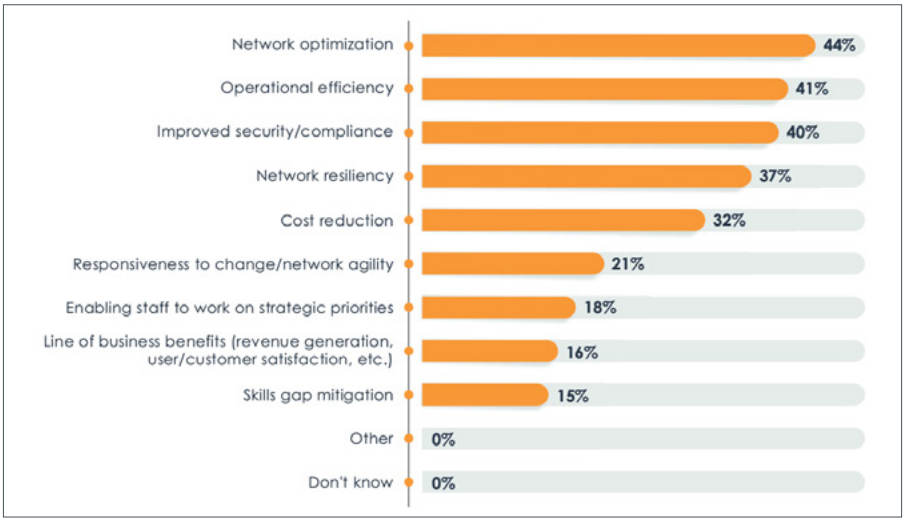
Advanced Reporting for Baseline and Trend Analytics
Baselining is a common strategy to stave off downtime and capacity problems that lead to performance issues. Network monitoring software can easily report on baselines as well as trends, the best of class packages will use AI and machine learning to predict when to add capacity and alert teams when the network or network segment is deviating from the typical baseline, even responding to incidents automatically.

Real-world Security Investigations with Network Analytics
As the internet's capacity increases so do cybersecurity threat vectors. Recognizing and stopping breaches as they occur is priority number one, but if attacks should go undiscovered until it is too late, the weakness may never be corrected. Fortunately, a solution is at hand. Network analytics and forensics–the recording, storage, and analysis–of traffic gives IT organization and security experts the comprehensive data they need for finding proof of attacks.

Root Cause Analysis with Packet Data
While incidents may abound indicating problems affecting performance of the network, discovering the root-cause requires investigating deeper into the details. Network monitoring software can access in-depth analytics on network activity such as bandwidth utilization, application response times, flow volume, packet types, expert events, security events, and VoIP calls.

Managing a Smarter Network

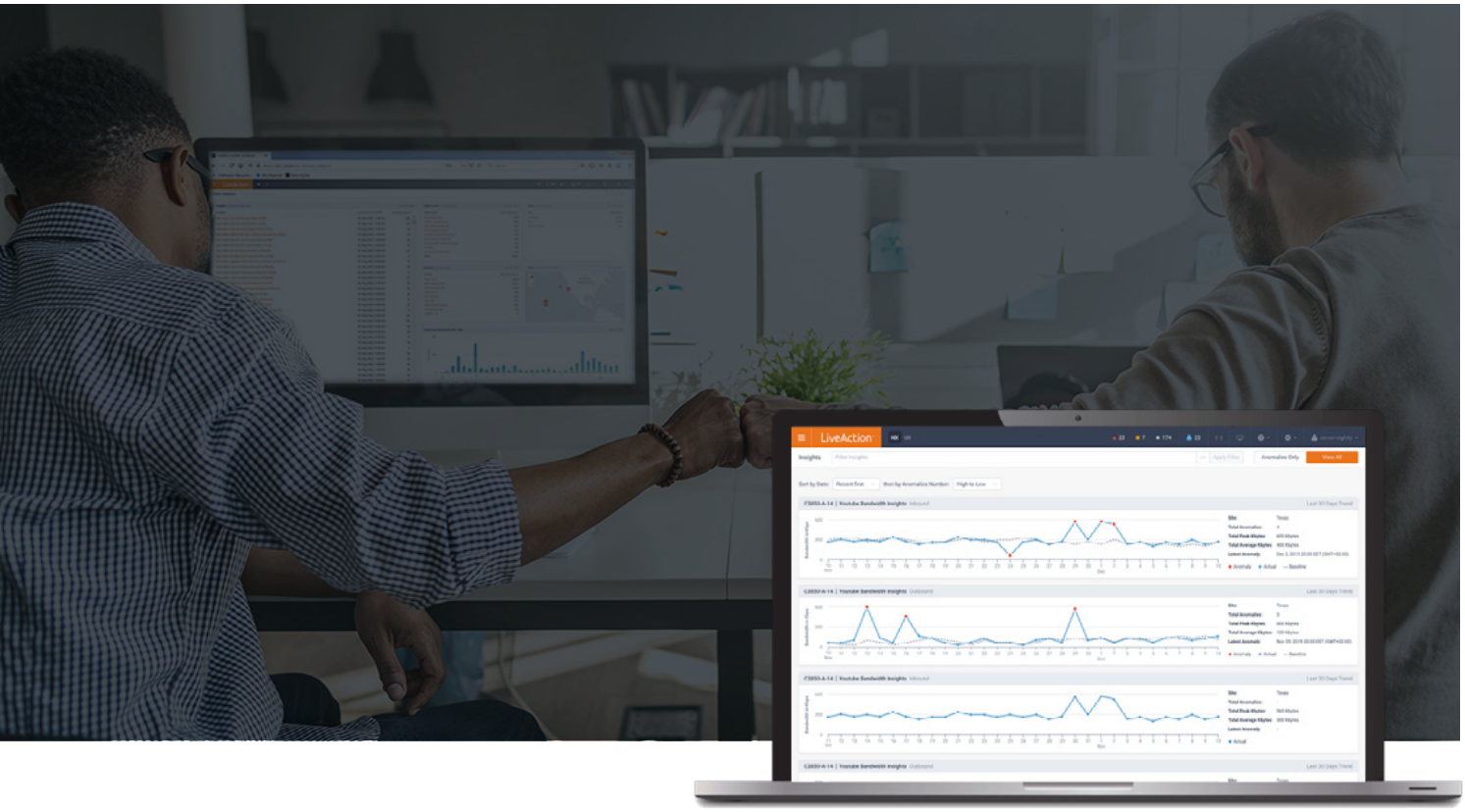
For those still unsure of role that advanced analytics could play for your ITOps teams, consider how quickly these technologies have transformed other industries such as the financial services and healthcare sectors. It's a safe bet that AIOps has the potential to be a truly revolutionary technology in the coming years.



The most important potential benefits of applying AIOps to network management

IT departments are in desperate need of modernization, while minimizing time and resource constraints. AIOps can be the missing key piece to a more automated, streamlined and optimized approach to IT management that can help your team more quickly and effectively identify and resolve network issues.

Enterprise Management Associates, "Revolutionizing Network Management with AIOps", April 2021.



Where LiveAction Comes In

LiveAction solutions deliver the network performance your organization demands. LiveAction has the enterprise scalability that can consume the millions of performance data points sent every second by your network. Our unmatched data fidelity and the finest level of granularity gives you end-to-end visibility at the global level but lets you drill down to a location, a single hop, or packet. LiveAction gives you all of this with both real-time access to this data as well as historic playback, without compromise.

To continue delivering next-generation technologies to our customers and partners, we developed LiveNA which uses Artificial Intelligence and Machine Learning to provide expert insights to application and network performance. LiveNA is an AIOps solution that delivers intelligent insights to applications and network performance. Unlike typical monitoring solutions that require users to identify issues, LiveNA automatically identifies anomalies and surfaces the most critical for users to act on.

About LiveAction

LiveAction provides end-to-end visibility of network and application performance from a single pane of glass. This gives enterprises confidence that the network is meeting business objectives offers IT administrators full visibility for better decision making and reduces the overall cost of operations. By unifying and simplifying the collection, correlation and presentation of application and network data, LiveAction empowers network professionals to proactively identify, troubleshoot and resolve issues across increasingly large and complex networks proactively and quickly. To learn more and see how LiveAction delivers unmatched network visibility, visit www.liveaction.com

LiveAction®

3500 West Bayshore Road Palo Alto, CA 94303, USA · +1 (888) 881-1116