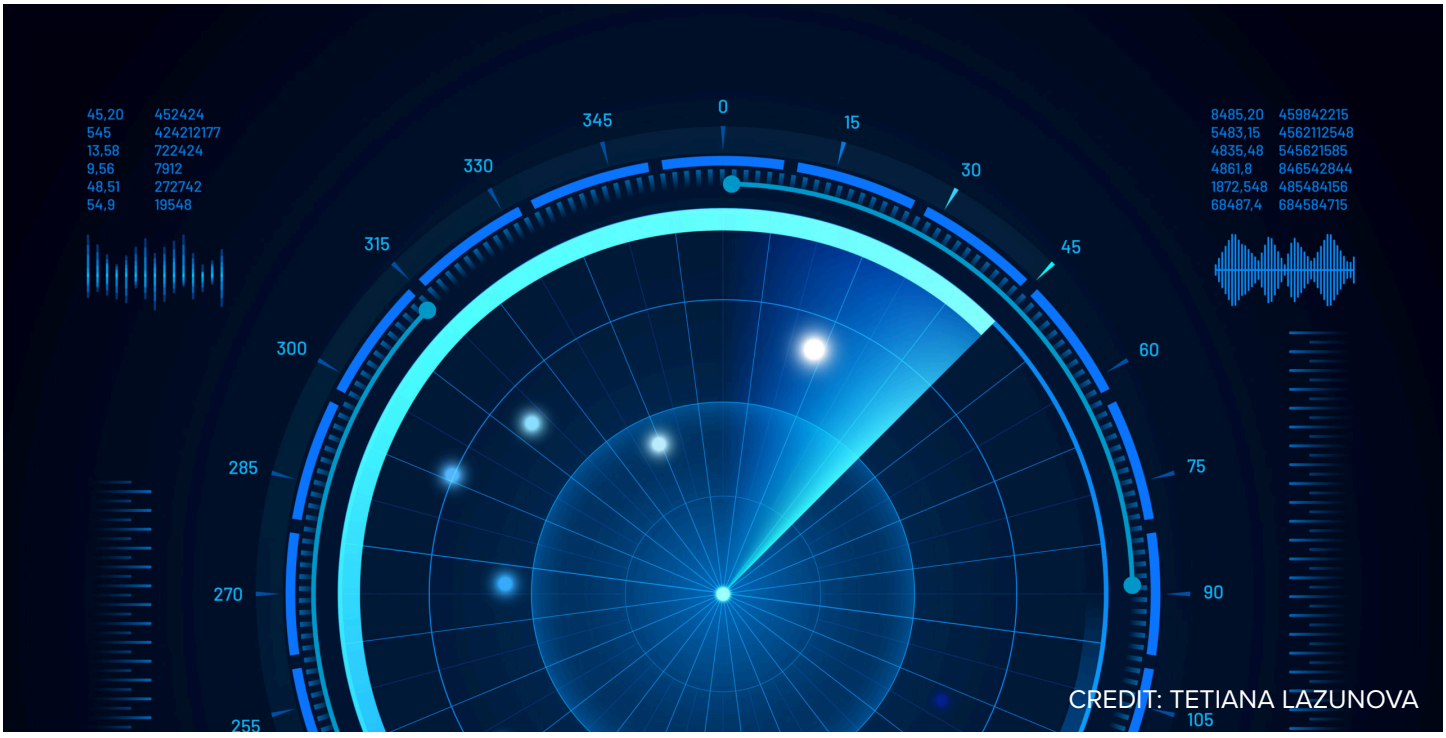
GIGAOM

MARKET RADAR

GigaOm Radar for Network Observability v1.0

CHRIS GRUNDEMANN | JAN 22, 2021 - 11:35 AM CST

TOPIC: NETWORKING



CREDIT: TETIANA LAZUNOVA

GIGAOM

GigaOm Radar for Network Observability

TABLE OF CONTENTS

1. Summary

Network observability is a category of platforms and tools that go beyond device-centric network monitoring to provide truly relevant, end-to-end visibility and intelligence for all the traffic in your network, no matter whether on-premises, in the cloud, or anywhere else. A step beyond network performance monitoring, network observability guarantees visibility and distinguishes itself with actionable insights. These insights shift many low-level decision-making activities—such as troubleshooting or capacity planning—from engineers to the network observability tool.

Observability tools are less about specialization and more about consolidating a comprehensive experience in a single tool. This brings numerous advantages, including a better user experience, lower costs than those faced when deploying multiple tools, adaptability for complex IT environments, future-proofing, and cohesiveness across IT departments. Network observability is perhaps the only way to ensure that modern critical infrastructure achieves the required uptime and availability.

While businesses of all sizes can benefit from the end-to-end visibility offered by network observability tools, the ones likely to see the most improvement are those with large, complex networks. These can be either companies with proprietary networks, where IT plays a supporting role-—such as retail or manufacturing—or businesses that sell network services, such as communication service providers. We explore these categories in more depth in the following section.

This report looks at key vendors in the emerging network observability space and aims to equip IT decision-makers with the required information to select suitable providers according to their specific needs. We analyze the vendors on a set of key criteria and evaluation metrics, which are described in depth in the Key Criteria Report for Network Observability.

HOW TO READ THIS REPORT

This GigaOm report is one of a series of documents that helps IT organizations assess competing solutions in the context of well-defined features and criteria. For a fuller understanding consider reviewing the following reports:

Key Criteria report: A detailed market sector analysis that assesses the impact that key product features and criteria have on top-line solution characteristics—such as scalability, performance, and TCO—that drive purchase decisions.

GigaOm Radar report: A forward-looking analysis that plots the relative value and progression of vendor solutions along multiple axes based on strategy and execution. The Radar report includes a breakdown of each vendor's offering in the sector.

Vendor Profile: An in-depth vendor analysis that builds on the framework developed in the Key Criteria and Radar reports to assess a company's engagement within a technology sector. This analysis includes forward-looking guidance around both strategy and product.

2. Market Categories and Deployment Types

Network observability tools are necessary and effective across all types of networks, but they are particularly important in complex IT environments. By taking into consideration the size of the network, its geographical spread, the security requirements, and whether IT is a supporting or a central function, we identified the following market categories that can benefit from network observability:

- **Small-medium enterprise**: Solutions in this category are those that meet the needs of very small businesses but can grow up to address those of medium-sized infrastructures. These solutions also can serve large enterprises for departmental use cases.
- **Large enterprise:** Usually adopted for large or business critical projects, solutions in this category have a strong focus on flexibility, performance, data services, and features that improve security and data protection. Scalability is another big differentiator, as is the ability to use the same service in different environments.
- **Public Sector**: These types of networks have comprehensive security requirements and can span countries (government, parliament, health services) or nations (such as the European Council).
- **Communication Service Providers**: CSPs are carriers, Internet service providers (ISPs), and network service providers (NSPs) that offer network services and often have a very complex national and international infrastructure serving both enterprise and consumer customers.
- **Managed Service Providers**: MSPs are enablers that take over a customer's network operations and deal with maintenance, upgrades, and other day-to-day activities. Their needs can align with any of those mentioned in the above categories, depending on the MSP's customer base, and include strict multi-tenancy requirements as well.

Network observability tools can be delivered using three deployment models:

- **SaaS**: The tool can be accessed directly through a web portal with no additional installation. This is often the simplest and easiest way to leverage network observability. The downside is that it may not meet the security requirements or complex customization needs of some customers.
- **Virtual Appliance**: This is a software tool that can be deployed in public clouds, private clouds, or other on-premises infrastructure. This gives you greater control, while still allowing solid deployment flexibility. The tool's performance, however, depends on whatever infrastructure the software is running on, as well as connectivity to the rest of the network.
- **Physical Appliance**: The tool requires one or more specialized hardware units to be installed on the customer's network. This approach typically offers the least deployment flexibility (you must physically attach the appliance to your infrastructure), but the highest degree of control and security.

Tables 1 and **2** provide insight into vendor support for these market segments and deployment models.

Table 1: Vendor Positioning

	MARKET SEGMENT				
	Small-Medium Business	Enterprise	Public Sector	Communication Service Provider	Managed Service Provider
Accedian	++	+++	++	+++	++
Broadcom	++	+++	++	+++	++
Kentik	++	+++	++	+++	+++
LiveAction	+++	+++	++	+++	+++
LogicMonitor	++	+++	++	++	+++
ManageEngine	++	++	++	++	++
Motadata	++	++	+++	+++	++
NetScout	++	+++	+++	+++	+++
Paessler	++	++	+++	++	++
Park Place Tech	++	+++	++	+++	+++
Plixer	++	+++	++	++	++
Progress	+++	++	+++	++	++
SolarWinds	++	+++	+++	++	+++
Zabbix	+++	+++	++	+++	++

+++: strong focus and perfect fit of the solution
++: The solution is good in this area, but there is still room for improvement
+: The solution has limitations and a narrow set of use cases
-: Not applicable or absent.

Source: GigaOm 2020

Table 2: Deployment Models

	DEPLOYMENT MODELS		
	SaaS	Virtual Appliance	Physical Appliance
Accedian	++	++	++
Broadcom	++	-	-
Kentik	+++	++	++
LiveAction	-	+++	++
LogicMonitor	++	++	++
ManageEngine	-	++	++
Motadata	-	++	++
NetScout	-	++	-
Paessler	-	++	++
Park Place Tech	-	+++	+++
Plixer	++	++	++
Progress	-	-	+++
SolarWinds	-	++	++
Zabbix	-	+++	++

+++: strong focus and perfect fit of the solution
++: The solution is good in this area, but there is still room for improvement
+: The solution has limitations and a narrow set of use cases
-: Not applicable or absent.

Source: GigaOm 2020

3. Key Criteria Comparison

Following the general indications introduced with the "Key Criteria for Network Observability," **Table 3** and **Table 4** summarize how each vendor included in this research performs in the areas we consider differentiating and critical for network observability. The objective is to give the reader a snapshot of the technical capabilities of different solutions and define the perimeter of the market landscape.

In the Key Criteria report for network observability, **Table 1** describes how much each key criterion weighs in the assessment of the Evaluation Metrics. To create a more accurate assessment of each vendor's capability, we used additional information to calibrate the vendor's rating for some metrics.

Table 3. Key Criteria Comparison

	KEY CRITERIA							
	Discovery	Visibility	Visualization	Validation	Trouble-Shooting	Security Observability	Planning	Wireless
Accedian	++	+++	+++	-	++	++	+	++
Broadcom	++	+++	++	++	+++	+++	+++	+++
Kentik	-	++	+++	+	++	+++	+++	-
LiveAction	++	++	+++	++	++	+++	++	++
LogicMonitor	+++	++	++	+++	+++	+	+++	++
ManageEngine	+++	++	+++	++	+++	+++	+++	++
Motadata	++	+++	++	+	++	++	++	++
NetScout	++	+++	++	+	+++	++	++	+++
Paessler	++	+++	++	+	+	++	++	++
Park Place Tech	++	++	++	+++	+++	++	++	++
Plixer	++	++	+++	-	+	+++	+++	++
Progress	++	+++	++	++	+++	++	+	+++
SolarWinds	++	++	+++	+++	++	++	+	++
Zabbix	+	+++	++	+	+	+	++	+

+++: strong focus and perfect fit of the solution
++: The solution is good in this area, but there is still room for improvement
+: The solution has limitations and a narrow set of use cases
-: Not applicable or absent.

Source: GigaOm 2020

Table 4. Evaluation Metrics Comparison

	EVALUATION METRICS					
	Scalability	Flexibility	Feature Set	Ease of Use	TCO and ROI	Solution and Partner Ecosystem
Accedian	+++	+++	++	++	+++	++
Broadcom	+++	+++	+++	++	++	+++
Kentik	+++	++	+	+++	+++	+++
LiveAction	++	++	++	++	+++	+++
LogicMonitor	+++	+++	++	+++	++	+++
ManageEngine	+++	+++	+++	++	+++	++
Motadata	++	++	++	++	++	+++
NetScout	+++	++	++	++	+	+++
Paessler	++	+++	++	++	++	++
Park Place Tech	++	++	+++	++	++	+++
Plixer	++	+++	++	+++	+++	++
Progress	++	+++	++	++	++	+
SolarWinds	+++	++	++	+	++	+++
Zabbix	+++	+++	+	+	+++	+++

+++: strong focus and perfect fit of the solution
++: The solution is good in this area, but there is still room for improvement
+: The solution has limitations and a narrow set of use cases
-: Not applicable or absent.

Source: GigaOm 2020

4. GigaOm Radar

This report synthesizes the analysis of key criteria and their impact on evaluation metrics to inform the GigaOm Radar graphic in **Figure 1**. The resulting chart is a forward-looking perspective on all the vendors in this report, based on their products' technical capabilities and feature sets.

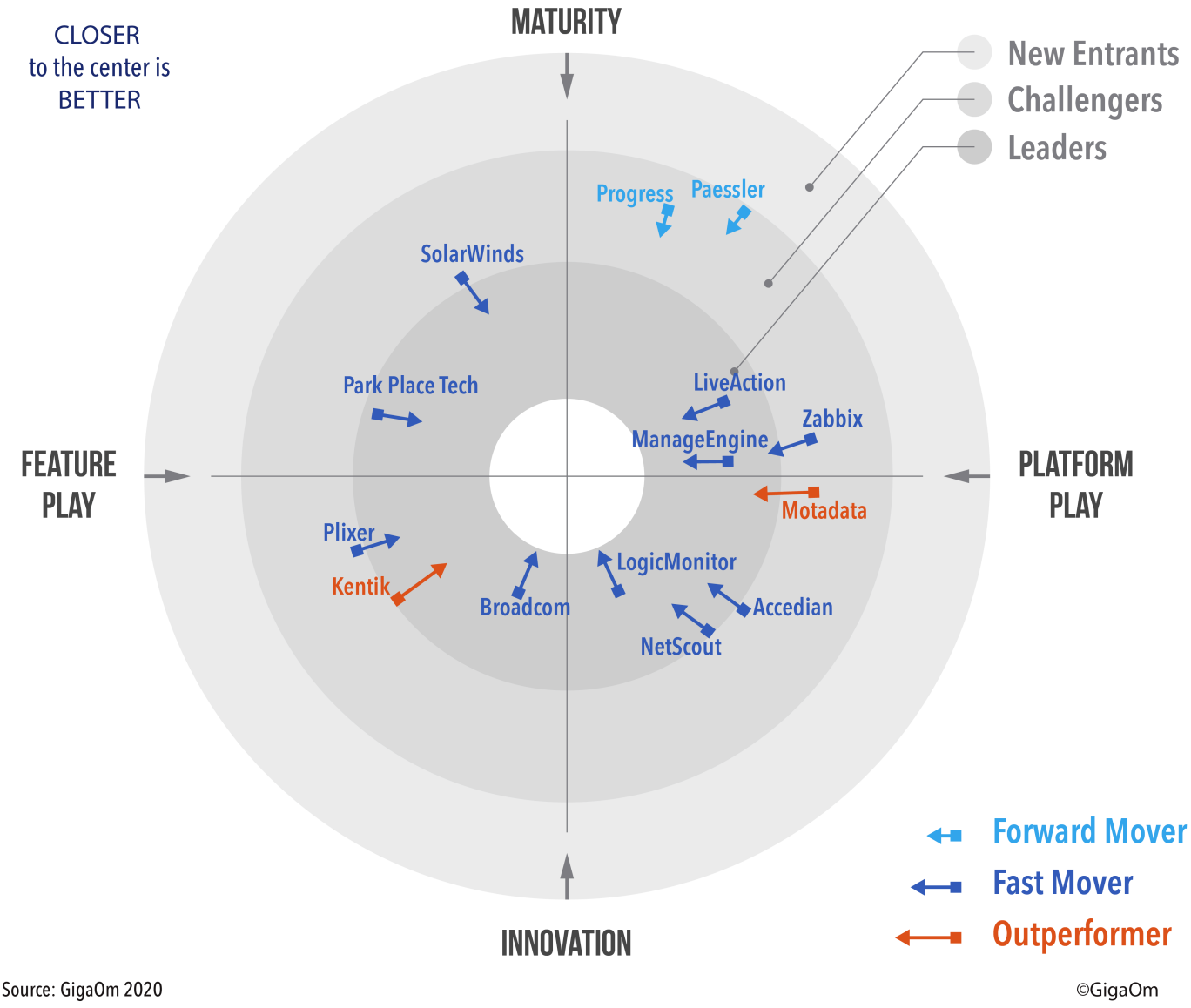


Figure 1: GigaOm Radar for Network Observability

The GigaOm Radar plots vendor solutions across a series of concentric rings, with those set closer to center judged to be of higher overall value. The chart characterizes each vendor on two axes—Maturity versus Innovation, and Feature Play versus Platform Play—while providing an arrow that projects each solution's evolution over the coming 12 to 18 months.

As you can see in the Radar chart in **Figure 1**, the companies in this report are distributed fairly evenly across the radar, with at least one Leader present in each of the four quadrants.

The Feature Play versus Platform Play spectrum is primarily determined by the scope of the specific product or suite of products required to achieve network observability. Feature play products are focused solely on the network, while a platform play product supports additional IT stack visibility and control; although this additional functionality was not incorporated into the scoring.

The Maturity versus Innovation spectrum was largely determined by the inclusion (or not) of AIOps and other automated troubleshooting and predictive analysis features, with those including such automation falling on the innovation side of the Radar.

Two vendors were deemed Outperformers in this report. Kentik is a relatively young provider, having been founded in 2014, while Motadata is working hard to develop AI and ML capabilities. Additionally, Zabbix is worth mentioning as the only fully free and open source solution included in this report.

INSIDE THE GIGAOM RADAR

The GigaOm Radar weighs each vendor's execution, roadmap, and ability to innovate to plot solutions along two axes, each set as opposing pairs. On the Y axis, **Maturity** recognizes solution stability, strength of ecosystem, and a conservative stance, while **Innovation** highlights technical innovation and a more aggressive approach. On the X axis, **Feature Play** connotes a narrow focus on niche or cutting-edge functionality, while **Platform Play** displays a broader platform focus and commitment to a comprehensive feature set.

The closer to center a solution sits, the better its execution and value, with top performers occupying the inner Leaders circle. The centermost circle is almost always empty, reserved for highly mature and consolidated markets that lack space for further innovation.
The GigaOm Radar offers a forward-looking assessment, plotting the current and projected position of each solution over a 12- to 18-month window. Arrows indicate travel based on strategy and pace of innovation, with vendors designated as Forward Movers, Fast Movers, or Outperformers based on their rate of progression.

Note that the Radar excludes vendor market share as a metric. The focus is on forward-looking analysis that emphasizes the value of innovation and differentiation over incumbent market position.

5. Vendor Insights

Accedian

Accedian's network observability offering uses orchestration to scale, making it suitable for CSPs or businesses with highly distributed networks. The platform's excellent visualization capabilities make the tool a good fit for complex networks that use hybrid solutions and legacy equipment.

On the other hand, the tool does not support validation, which has a negative impact on the efficacy of the platform in select cases. The solution lacks built-in troubleshooting capabilities, but does use AI/ML to perform root cause analysis. And it provides APIs that can be leveraged to send actions to third-party devices or services.

Compared to other vendors, Accedian provides basic capabilities for capacity planning, giving administrators the data they require but lacking more advanced capabilities like predictive analysis.

Accedian's offerings include good security capabilities, with behavior-based intrusion detection and investigation, threat hunting, and forensics. The company is also improving its security capabilities by implementing 5G monitoring, and further developing the AI/ML technology for its Skylight sensor solution to enhance its network traffic analysis features.

Accedian network observability is achieved with the following products:

- Skylight Performance Analytics (SaaS deployment), the main tool for viewing and analyzing network performance data
- Skylight Orchestrator (physical and virtual deployment), Accedian's deployment-management solution
- Skylight Cloud and on-premises sensors (physical and virtual deployment) for capturing all network traffic between users and infrastructure (North-South) and between virtualized infrastructure resources (East-West)

Strengths: Accedian's offerings can deliver excellent scalability using its orchestration tool, good security visibility, and continuing development of AI/ML integration.

Challenges: Validation is missing. Planning and troubleshooting features could be more robust.

Broadcom

Broadcom achieves network observability with its DX NetOps and AIOps solutions following the company's acquisition of CA technologies. Its main network performance solution, DX NetOps, provides end-to-end network monitoring with excellent visibility and good visualization capabilities. The complementary solution, AIOps, leverages artificial intelligence and machine learning for full stack correlations, predictions, and algorithmic analysis of alarms, metrics, logs, and topologies.

Broadcom's extensive visibility capabilities include Wi-Fi, radio networks, SD-WAN, chip-level monitoring, and backhaul networks. This makes Broadcom's network observability offering a very good candidate for carriers, system integrators, managed service providers, and large enterprises. Broadcom's DX NetOps and AIOps solutions benefit from an excellent partner ecosystem, leveraging industry-leading vendors for comprehensive visibility across all network segments.

A benefit of DX NetOps and AIOps is the SaaS deployment model, which can mean easier installation, lower costs, and easy off-site accessibility. Both products are available under Broadcom's portfolio license agreement (PLA), through which customers are licensed to use the entire enterprise software portfolio, or a subset by segment. A cap is contractually agreed upon to provide customers with price predictability.

Strengths: Broadcom's use of AI makes it a stand out in delivering troubleshooting, planning, and validation. Its visibility and security observations are also highly developed.

Challenges: The capabilities offered by DX NetOps are very limited without the addition of the AIOps product.

Kentik

Kentik's network intelligence platform supports observability for very large networks. It includes excellent security monitoring capabilities from its broad partner ecosystem, as well as built-in threat intelligence data that can interoperate with customer-supplied data. The company tailors its approach to the customer, whether enterprise or CSP, for example, providing over-the-top (OTT) traffic attribution to CSPs.

Kentik provides advanced insights with autodetection of anomalies and emerging issues, using built-in diagnosis and potential root-cause analysis with a combination of semantically enriched algorithmic learning. The platform also provides very good capacity planning capabilities, continuously gathering data and alerting when additional capacity is required.

One considerable drawback: The solution lacks support for network discovery. We are told that Kentik will be adding auto discovery in 2021. Today, it supplies or assists many customers with scripts that not only set up, but sync through lifecycle management so that provisioning winds up automated for

customers that have authoritative sources for listing devices, clouds, and the like. The network intelligence platform also has limited network configuration capabilities, which limits the control engineers have from a single platform. Moreover, there is no ability to monitor wireless networks, including Wi-Fi or radio networks.

The network intelligence platform does offer cost analytics, identifying how applications and internal departments are using high-cost resources, which adds visibility to network spend drivers. With the recent release of Kentik Synthetic Monitoring, the company improves the way customers can monitor their digital experience across hybrid networks. Synthetic monitoring continually looks at network traffic, picks the highest value targets to test, and automatically provisions and executes these tests.

Kentik's deployment model is mainly based around a SaaS architecture. Customers with compliance requirements to keep data on-premises can deploy the Kentik platform in their own app-hosting infrastructure. In this case, the solution is physically deployed within the customer's control, but it is still a Kentik-managed SaaS service.

Strengths: Kentik is easy to use and delivers very good visualization, planning tools, and security observability. It also offers tailored experiences for different market categories.

Challenges: Kentik is the only vendor featured in this report that lacks the ability to conduct network discovery. Configuration management capabilities are also limited.

LiveAction

LiveAction offers multiple products for network observability. LiveNX is the main monitoring tool targeting the enterprise, while LiveSP is a product dedicated to service providers. Both platforms are complemented by LiveNCA, the network configuration automation tool that automates such service management activities as configuration, change, and inventory management. Omnipeek is another complementary platform, offering in-depth data analysis and visualization.

LiveAction has an excellent partner ecosystem, leveraging relationships with many specialized vendors in areas such as WLAN, VoIP, Wi-Fi, load balancing, forensics, and troubleshooting. Via these partnerships, LiveAction offers very good security observability, which includes network forensics, packet intelligence, and SIEM.

LiveAction seems to achieve true network observability only through the use of multiple products, which can significantly impact the total cost of ownership. For instance, you would need to use Omnipeek, LiveCapture, LiveNA, and LiveNCA to achieve network observability.

LiveNX supports a Server Node architecture. Each Node supports 1,000 Devices and 150K flows/second. One can add multiple Nodes to scale horizontally. Same design is possible with physical appliances. A combination of physical and virtual also can be used. LiveSP follows a similar model, supporting up to 500 routers with a virtual appliance, up to 3,000 routers with a standard physical

appliance, and over 3,000 routers with custom sizing options.

Strengths: LiveAction's offerings have superior visualization capabilities, and its strong partner ecosystem helps achieve excellent security observability.

Challenges: While LiveAction products are tailored to specific market categories, its reliance on complementary products such as LiveNCA, LiveNA, LiveCapture, and Omnipeek make it harder to achieve network observability with a single product.

LogicMonitor

LogicMonitor offers end-to-end network visibility to IT departments in medium and large enterprises, and caters as well to managed service providers. The LogicMonitor solution features a well-developed network discovery function in which collectors use its NetScan feature to discover network devices. NetScans can be executed via ICMP. Native algorithms provide automatic tech-stack discovery via protocols such as WMI, Perfmon, SNMP/SSH, JDBC, HTTP/S, PowerShell, and Groovy APIs for virtual infrastructure.

Planning is a strongpoint in LogicMonitor's solution, resulting from its use of AIOps forecasting algorithms to predict metric usages, as well as threshold algorithms that help users understand the rate of change for certain metrics. Accurate forecasting is achieved via LogicMonitor's time series database, which can hold data at full granularity for up to two years.

Another strength of the LogicMonitor solution is its ability to perform network validation. The platform can detect configuration changes and automatically identify the associated impact on network performance metrics.

LogicMonitor has room to improve around its support for security observability. Security monitoring is not built into the platform, though users can ingest security insights from other platforms and route them through LogicMonitor's alerting system. We are told that LogicMonitor plans to add security capabilities by the end of 2021.

LogicMonitor is an agentless product fully deployed as SaaS, using collectors that can be installed on-premises or hosted in cloud environments via APIs.

Strengths: The platform provides very robust validation and troubleshooting capabilities as well as advanced capacity planning features.

Challenges: LogicMonitor's main drawback is its lack of built-in security observability.

ManageEngine

ManageEngine is a key player in the network observability space due to the innovative and comprehensive feature set of its OpManager Plus product. A distinguishing aspect of the ManageEngine solution is its visualization capabilities. The platform goes beyond topological and geographical maps to provide 3D server room and virtual device views.

OpManager Plus offers real-time change management, automatic configuration task execution, performance and bandwidth forecasts, validation, and API integration. Some of these functions are also available in the solution's security observability elements, including: firewall policy management, change management, network security management, user internet activity monitoring, real-time VPN and proxy monitoring, compliance management, network forensic audits, log analysis, and network traffic and bandwidth monitoring, among other features, to enable end users to secure their IT infrastructure from external and internal threats.

The ManageEngine solution implements a number of other differentiating capabilities, such as compliance auditing, user activity tracking, and billing monitoring for third-party services such as AWS's EC2, RDS, Lambda and the like.

One downside compared to other network observability tools on the market is that the probe-based deployment model might be less attractive when SaaS solutions are available. Also, the solution is based on Java, which can be seen as a weakness by some users, especially when it comes to upgrades.

ManageEngine continues to develop new functions, improving its AI capabilities to analyze synthetic data for better network diagnostics and more accurate forecasting regarding bandwidth usage.

Strengths: ManageEngine offers unique visualization capabilities and delivers great troubleshooting, planning, and security visibility.

Challenges: ManageEngine's OpManager Plus is based on Java, which can lead to issues when upgrading. There is no SaaS option available.

Motadata

Motadata offers a compelling network observability solution via its Infrastructure Intelligence and Data Analytics platforms, which, together, offer excellent visibility and validation. The Infrastructure Intelligence Platform (IIP) gathers data from a multitude of sources, offering complete visibility over all kinds of modern networks, applications, web servers, and middleware. Unfortunately, that excellent visibility does not include radio networks, making it unsuitable for some carriers.

IIP automates network configuration management for configuration changes, backups, and restores.

These are mature features that provide the capabilities of asset management software. However, the platform is not able to achieve validation, which entails correlating configuration with network performance impact and offering automated remediation.

Motadata is working on developing AI and ML technologies to strengthen its platform. In version 8.0, the company expects to integrate AI to enable predictive analysis and enhance troubleshooting and intelligent alerting. If the AI solution is mature and is integrated strategically, Motadata can enhance its network observability solution considerably.

The solution can be deployed as a virtual appliance using either on-premises or cloud-based infrastructure. Users can select whether the solution can be deployed as a standalone or distributed model, with a high-availability option for either model.

Strengths: Motadata offers great visibility to provide insights across complex networks, as well as a wide range of third-party integrations.

Challenges: The tool does not yet offer comprehensive validation capabilities. There is no SaaS option.

NetScout

NetScout is a key player in the network observability space, with established solutions developed over three decades of working with some of the largest network operators in the world. nGenius, NetScout's network observability suite, is a mature and well-rounded solution. NetScout tailors its solution based on varied industry requirements—for carriers, public sector, finance, healthcare, or MSPs.

In addition to its ability to deliver network observability across any market segment, nGenius is highly scalable and supports a good selection of data sources, making it a versatile tool for large enterprises with complex networks and for communication service providers.

While NetScout has broad capabilities, its comprehensive portfolio of products can make it difficult for engineers to get network observability up and running. For example, it uses vSTREAM, a product that complements other Adaptive Session Intelligence-based solutions (such as nGeniusONE) to provide smart data visibility for virtualized and cloud infrastructures. Other solutions within the network observability space are able to deliver this capability with only one product.

A key aspect of NetScout's solutions is its patented Adaptive Session Intelligence (ASI) technology, which performs real-time data mining of user and application traffic at the network source. The ASI metadata includes key traffic and performance indicators and Layer 4 through 7 problem indicators for the discovered applications and servers, without installing device agents or complex provisioning.

In terms of deployment, NetScout offers its flagship product, nGeniusONE, as an on-premises solution featuring the nGeniusONE server unit. NetScout also provides network visibility as a managed service with its nGeniusVaaS (visibility as a service) offering.

Strengths: NetScout offers mature, industry-specific solutions that were developed over decades. These solutions have excellent scalability, visibility, and troubleshooting capabilities.

Challenges: The nGeniusOne platform has very limited validation capabilities, which may make it more difficult to manage intent-based networking configurations. Its reliance on multiple products can lead to deployment complexity.

Paessler

Paessler's network observability solution is called PRTG, and it ranks highly in the visibility and visualization key criteria. The platform enables customers to monitor a multitude of data sources and offers good insights over most metrics available for physical and virtual appliances. PRTG can visualize data in several different modes, including its signature sunburst map. The platform also ranks well in flexibility, due to its highly customizable sensors, dashboards, licensing models, and available APIs.

While PRTG offers very good visualization over network operations, it falls short at providing true observability because of its approach to troubleshooting and validation. The tool presents all the information required to diagnose and identify issues, but relies on the engineer's expertise for remediation rather than providing actionable insights and intelligent suggestions.

In terms of deployment, PRTG can be installed either as a virtual appliance, using a physical probe, or as a web-hosted application. As a virtual appliance, PRTG can be installed in a cloud environment. A physical PRTG probe requires a local machine on-premises. The hosted version simply requires a user to log into the web portal while Paessler manages the PRTG server.

Strengths: PRTG offers excellent visibility over network data sources and has great flexibility in terms of APIs, customizable sensors, and licensing models.

Challenges: While it supplies good information about the network, its troubleshooting and validation capabilities are not as strong as other vendors featured in the report.

Park Place Technologies

Park Place Technologies' Entuity Network Analytics is a comprehensive network observability platform that provides end-to-end network visibility by combining its event and configuration management systems with third-party integrations.

Event Management System actions are based on defined conditions and specific workflows, configured either by network administrators or out of the box. Multiple events can be combined into incidents, which are raised in response to one or more events that identify situations that need attention.

The Configuration Management and Monitoring System allows users to create and automatically push configuration settings to thousands of monitored devices and ports. This system provides automatic validation and can work in conjunction with the Event Management System to streamline workflows because configuration management tasks can be executed as EMS actions. For example, the two features can work together to detect and automatically shut down a port that has been flapping for more than a defined amount of time, or to enable back-up circuits for a period of high utilization on a WAN.

Entuity Network Analytics also features excellent third-party integrations, such as integrating with BMC TrueSight to leverage AIOps capability, which brings intelligent data to the platform. A comprehensive set of add-on modules provides specific management capabilities from solutions such as IBM BladeCenters and Cisco Unified Communications Manager.

Entuity can be installed on virtual or physical servers. For installation, Park Place Technologies provides ISO images of the Entuity server to be installed on a virtual machine, creating a virtual network management appliance. For a full installation, Entuity requires certain IP addresses, configuring basic security, and running network discovery. Once deployed, users have access to the fully instrumented solution via a web browser portal. While there is no SaaS version available, a hosted option is available through the services team.

Strengths: By combining its event and configuration management systems, Entuity achieves excellent troubleshooting and validation capabilities.

Challenges: There is no SaaS option available.

Plixer

The Plixer Scrutinizer network observability platform supports most of the key criteria in this Radar report. Scrutinizer takes advantage of two AI-based solutions, Network Intelligence and Security Intelligence, to enhance its capabilities. The Plixer solution is straightforward, and customers can easily select the features they need for maximum ROI with no redundant capabilities.

Scrutinizer, especially when used with Security Intelligence, provides excellent visibility into all security concerns. It is augmented by AI/ML technology and includes the ability to automate workflows to reduce the impact of security incidents. Scrutinizer also boasts superior visualization capabilities, with geographical and topological map views and highly descriptive and customizable graphs.

While Plixer's solutions offer mature features, network validation and troubleshooting are limited. The platform equips administrators with all the information needed to run diagnostics, but falls short in providing light-touch/no-touch network management. Scrutinizer does offer ServiceNow integration for automated ticket creation, which reduces the engineering team's investigative efforts.

Network Intelligence also offers excellent capacity planning, fully leveraging AI/ML for accurate

capacity forecasting, which enables customers to achieve a very good return-on-investment ratio.

Plixer offers a flexible deployment model, with Scrutinizer available either as a SaaS offering or as a virtual or hardware appliance. Customers can buy the SaaS version of the platform or a subscription license that covers the virtual and physical deployments.

Strengths: Plixer has a straightforward solution with excellent visualization, security observation, and AI-based capacity planning capabilities.

Challenges: The solution does not provide validation capabilities, and its troubleshooting features require investigative efforts by an operator. Full observability as we've defined it here requires three products.

Progress

Progress' WhatsUp Gold has become a distinguished name in the network observability arena, providing a mature solution that features an advanced interactive mapping interface. The solution boasts easy implementation, usability, and customization.

WhatsUp Gold has excellent visibility capabilities and is able to source data from physical and virtual infrastructure, cloud, third-party services, and wireless networks including radio and Wi-Fi.

WhatsUp Gold performs well in troubleshooting, providing smart alerts, self-healing capabilities, and automated configuration management. It also features a fully fleshed-out hardware asset management system with inventory, warranty, and licensing reports. However, the lack of any AI/ML implementation in WhatsUp Gold makes its capacity planning abilities less attractive compared to other players in the market.

WhatsUp Gold can be deployed only as an on-premises solution, but it has a lot of flexibility in terms of licensing with options based on subscriptions, devices, or points.

Strengths: WhatsUp Gold tops the list in terms of providing visibility across available data sources. It also has great troubleshooting features and APIs.

Challenges: The Progress partner ecosystem for WhatsUp Gold is not as developed as other vendors featured in this report. Their solution does not yet implement AI/ML and has limited planning capabilities.

SolarWinds

SolarWinds is a household name in network performance management, and its Network Automation Manager platform provides a great network observability experience. The solution offers a wide range

of capabilities, including monitoring hardware health, packet analysis, flow monitoring, bandwidth analysis, configuration and change management, switch port and end-user monitoring and tracking, WAN performance monitoring, and IP address management.

SolarWinds continues to enhance its proprietary AI/ML technology while partnering with other leaders in the AIOps sector to develop comprehensive capabilities for intelligent anomaly detection, automation, and troubleshooting.

The solution is able to deliver validation using SolarWinds' Orion Maps, Network Insight features, network automation, and configuration comparisons. This makes Network Automation Manager one of the few solutions in this report to provide truly comprehensive validation capabilities.

Compared with other solutions in the network observability space, Network Automation Manager works with fewer data sources and provides slightly less visibility. For example, it lacks visualisation over virtual appliances, such as containers or virtual infrastructure, and it does not monitor application data. Network Automation Manager's capacity planning does not yet use AI/ML for enhanced forecasting, but it does feature usage trends and peak calculations based on existing data. Network Automation Manager also lacks an API for exporting its data into different platforms.

Network Automation Manager and its associated modules can be deployed on physical or virtual servers on-premises or in the cloud, as well as via the Azure or AWS marketplaces.

Strengths: Network Automation Manager lives up to its name and provides great automation features that gives it a high score for validation. SolarWinds also has a good AIOps implementation and a well-developed partner ecosystem.

Challenges: The solution lacks visibility over some technologies, such as containers or virtual infrastructures. The capacity planning feature does not yet implement AI, so the forecasting ability is limited to simple predictions.

Zabbix

Zabbix stands out in the network observability space due to its open source, free-to-use model. Zabbix provides end-to-end network monitoring for free to any customer who installs its platform, with paid support models available in five tiers. The company also offers various professional services such as consulting, integrations, and development.

The Zabbix architecture and its unlimited scalability make it suitable for any kind of business, from small operations that can employ the free platform to multinationals spread across the world that will adopt one of the paid support tiers.

Zabbix's ability to deliver troubleshooting, validation, wireless monitoring, and security observability is fully reliant on its integrations. Depending on customer requirements, this can be both positive and

negative. If you're looking for an out-of-the-box, fully comprehensive solution, the platform might not be suitable (although we note that Zabbix 5.2, released in October 2020, is a lot more usable without any custom integrations). If, on the other hand, you want maximum flexibility or are already using multiple monitoring solutions, Zabbix can help bring everything under a single roof for increased efficiency. As such, Zabbix ranks low on ease of use, but high on flexibility and partner ecosystem.

Zabbix does not support NetFlow or packet capture as data sources. The solution offers network discovery, but not discovery of network topology. However, infrastructure maps can be created manually.

Zabbix is supported both on-premises and as a virtual appliance, with easy installation for containers, VMs, and cloud deployments. In addition to the Zabbix application service, the only other prerequisites are a back-end database and a web front end.

Strengths: If configured correctly, Zabbix has excellent scalability and offers the potential to reach superior ROI. Its flexibility can make Zabbix a bespoke tool for handling any kind of network.

Challenges: While the Zabbix model, with its support for third-party integrations, makes for a flexible solution, it can also be difficult to use and implement.

6. Analyst's Take

The network observability space is seeing rapid development and heavy investment in next-generation technologies. Vendors are extending their capabilities to offer innovative observability tools including:

- **Data visualization:** Data is no longer just available, but presented in a way that makes it easy for network administrators to identify challenges and opportunities without having to spend time extracting useful information out of raw data.
- **AI implementations:** Vendors that have started implementing AI into their solution have either developed their solutions in-house, tailoring the features for their customers' needs, or have leveraged specialist third-party vendors that offer more advanced AI solutions.
- **APIs and integrations:** All vendors are working toward creating a more integration-friendly solution, either by offering advanced APIs or by creating partnerships with vendors in the networking industry.
- **Actionable insights:** Solutions are moving further toward providing actionable insights for highlighting issues and optimization opportunities.
- **Automation:** In order to reduce downtime and MTTR, network observability solutions are relying on automation, achieved through rules and workflows, thereby reducing the need for human involvement in the handling of common occurrences.

For IT decisions-makers to select a network observability platform, we recommend the following:

- The solution must meet all the key criteria required for your network. For example, if you require visibility over security infrastructure, you must consider only vendors that either provide the feature or integrate a third-party provider's capability to do so.
- The solution is easy to deploy, integrate, and support. If you require a solution that can be deployed in a public cloud environment with integrations for help desk ticketing and 24/7 support, the vendor you choose must provide all of these.
- The vendor must understand your industry's requirements. For example, solutions that offer a federated architecture might be more suitable for MSPs that handle multiple client networks.
- The solution must complement your team's capabilities. If your network has complex configurations, validation is critical. If you have few administrators, automated troubleshooting is important to provide assistance. For growing networks, visualization and discovery can equip your engineers to make more informed decisions.

We expect vendors in this report to provide a high-quality observability experience and to improve network efficiency. However, small differences in the key criteria can yield a significant impact on a platform's ability to maximize return on investment and provide optimal network observability.

7. About Chris Grundemann

Chris Grundemann is a passionate, creative technologist and a strong believer in technology's power to aid in the betterment of humankind. In his current role as VP, Strategy at Myriad360 he is expressing that passion by helping clients build bigger, faster, more efficient technology infrastructure that is both more secure and easier to operate and scale. Chris has well over a decade of experience as both a network engineer and solution architect designing, building, securing, and operating large IP, Ethernet, and Wireless Ethernet networks. His specialties include infrastructure design, protocol design, consensus building, technology evangelism, research and development (R&D), leading collaborative groups, communicating abstract ideas to diverse audiences, and generally getting stuff done!

Chris has given presentations in 34 countries and is often sought out to speak at conferences, NOGs, and NOFs the world over. He holds 8 patents in network technology and has written two books: *Day One: Exploring IPv6* and *Day One: Advanced IPv6 Configuration*; as well as an IETF RFC, various industry papers, a personal weblog, and several other publications, including contributions to GestaltIT, CircleID, Packet Pushers, and Forbes.

Chris is also a co-founder and Vice President of IX-Denver and Chair of the Open-IX BCOP committee. He has held previous positions with Markley Group, Internet Society, CableLabs, tw telecom, CO ISOC, ISOC-NY, ARIN, NANOG, AfPIF, CEA, UPnP, DLNA, RMv6TF, and several others.

Chris is currently based in Brooklyn, NY.

8. About GigaOm

GigaOm provides technical, operational, and business advice for IT's strategic digital enterprise and business initiatives. Enterprise business leaders, CIOs, and technology organizations partner with GigaOm for practical, actionable, strategic, and visionary advice for modernizing and transforming their business. GigaOm's advice empowers enterprises to successfully compete in an increasingly complicated business atmosphere that requires a solid understanding of constantly changing customer demands.

GigaOm works directly with enterprises both inside and outside of the IT organization to apply proven research and methodologies designed to avoid pitfalls and roadblocks while balancing risk and innovation. Research methodologies include but are not limited to adoption and benchmarking surveys, use cases, interviews, ROI/TCO, market landscapes, strategic trends, and technical benchmarks. Our analysts possess 20+ years of experience advising a spectrum of clients from early adopters to mainstream enterprises.

GigaOm's perspective is that of the unbiased enterprise practitioner. Through this perspective, GigaOm connects with engaged and loyal subscribers on a deep and meaningful level.

9. Copyright