EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Prepared for:

BLUECAT™

The Network Observability Maturity Model:

How to Plan for NetOps Excellence

September 2025 EMA Research Report
By **Shamus McGillicuddy**, VP of Research
Network Infrastructure and Operations

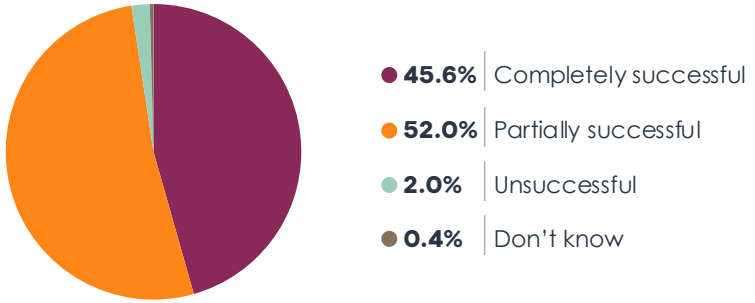
Table of Contents

NetOps Teams Need Better Tools

Network observability tools are essential to network operations. They enable enterprise IT organizations to monitor, troubleshoot, optimize, and audit their networks. These tools also help network teams collaborate with other groups, including cybersecurity, cloud, and DevOps. Additionally, CIOs require dashboards and reports that assure them the network is supporting service-level and business objectives.

Given the critical role that network observability tools play in IT organizations, network infrastructure and operations teams must strive for best-in-class solutions. Unfortunately, Enterprise Management Associates (EMA) research consistently finds that IT organizations struggle to establish and maintain an effective network observability toolset. For this paper, EMA surveyed 252 IT stakeholders who are directly engaged with network observability tools. That research found that only 46% believe they are fully successful with network observability tools (see **Figure 1**).

Figure 1. To what extent do you think your organization is successful with its network observability tools?



Why do network teams to often struggle with these tools? IT professionals have seven top complaints about them.[1]

1. Limited scope. They cannot monitor certain aspects of their network, such as the public cloud or secure access service edge architect.
2. Too expensive. The prices tool vendors charge limit how many devices and how much traffic they can afford to monitor.
3. Lack of customization. The inability to build custom dashboards, reports, alerting, and data collection limits the overall value of their tools.
4. Difficult to implement and maintain. The overhead of adopting a tool and maintaining it strains internal resources.
5. Insufficient scale. Networks are growing, and the amount of data collected from them is spiking. Many tools can't keep pace.
6. Poor data quality. Errors, formatting issues, packet drops, and other problems undermine data quality, which leaves network teams struggling to get an accurate picture of their networks.
7. Alert noise. Network teams struggle to tune alerts on their tools to minimize noise. This prevents them from focusing on alerts and events that require immediate attention.

Figure 2. Which of the following are your biggest complaints about your network observability tools?

Given the challenges that network teams continue to face with their network observability tools, they need a path to follow toward success. A maturity model can help organizations find that path. By defining multiple stages of maturity, such a model can help IT stakeholders understand where they are with a given technology today and how they can improve their approach through both incremental and fundamental changes.

[1] EMA, "Network Observability: Managing Performance Across Hybrid Networks," January 2025.

The Network Observability Maturity Model

BlueCat and EMA collaborated on a network observability maturity model. This model will help network teams understand the gaps in their existing network observability capabilities and chart a path for optimizing their toolsets.

EMA validated this maturity model by surveying 252 enterprise IT professionals who select, implement, and use network observability tools. This survey revealed that enterprises experience more success with network observability as they advance along this maturity model.

Today, very few organizations fall into the immature "Ad Hoc and Reactive" stage of network observability. Instead, resource-constrained IT organizations that lack the budget and personnel to advance maturity will tend to fall into the "Fragmented and Opportunistic" stage. Organizations that have the resources to invest in network observability are typically in stage 3 ("Integrated and Centrally Managed") or stage 4 "Intelligent and Automated." Best-in-class organizations are edging into the "Optimized and AI-Driven" stage as the technology that powers this final phase of maturity becomes more widely available from tool vendors.

This report highlights the changes that network teams can make to advance along this maturity model. EMA used market research data, highlighted in the following pages, to validate these recommendations. By following this path toward network observability maturity, IT organizations can establish a best-in-class network operations practice.

The Network Observability Maturity Model

Maturity Level	1. Ad Hoc and Reactive	2. Fragmented and Opportunistic	3. Integrated and Centrally Managed	4. Intelligent and Automated	5. Optimized and AI-Driven
Technologies Used	Basic monitoring of some hardware (SNMP, ICMP, simple scripts) Little to no traffic visibility	Basic monitoring of most hardware complemented by flow visibility (NetFlow, IPFIX) Tools are siloed Ad hoc packet captures (PCAPs and Wireshark) for forensic analysis of incidents	Comprehensive SNMP and flow monitoring Insights into health and behavior of network resources Tools are integrated Extensive packet capture is integrated into standard processes Basic monitoring of new environments like SD-WAN, cloud, branch offices, and remote workers	Real-time performance monitoring and correlation across metrics, flows Raw packet data is correlated with performance metrics Deep monitoring of software environments (SD-WAN, cloud)	Real-time performance monitoring across metrics, flows, and deep packet inspection AI and advanced analytics drive anomaly detection, predictive management, network optimization, and security insights
Operational Posture	Limited overall visibility Monitoring is usually ad hoc, reactive to issues and complaints	Good monitoring coverage, but operations are still reactive Tools are fragmented, correlations across tools are manual Lack of dashboard and report customization limits insights and usability	NetOps tools are defined and standardized to ensure consistent operations NetOps establishes KPIs/SLAs and monitors against them Higher levels of tool integration provide more insights and better correlation across tools	NetOps proactively monitors the network Issues are addressed promptly Increased automation accelerates mean time to resolution and reduces operational overhead	Proactive problem prevention is enabled Rapid resolution of network trouble via automated remediation NetOps and SecOps partner on unified observability platforms Organizations use AI assistants and stream observability data into security tools Observability drives continuous improvement, security integration, and business agility

The Path to Network Observability Maturity

Reduce Tool Sprawl Through Integration

IT organizations can mature network observability by addressing tool sprawl. EMA has long found that organizations use multiple tools for network monitoring and troubleshooting, and this report agrees. **Figure 3** reveals that 87% of network operations teams use multiple network observability tools.

Tool sprawl can feel inevitable because IT organizations adopt specialized tools to address emerging requirements. For example, they use the native observability capabilities of software-defined WAN (SD-WAN) to get visibility into their WAN overlays, and they use synthetic network monitoring tools to get better visibility into internet connectivity and cloud applications. These new solutions add sprawl to existing toolsets.

Figure 3. How many network observability tools does your IT organization use?

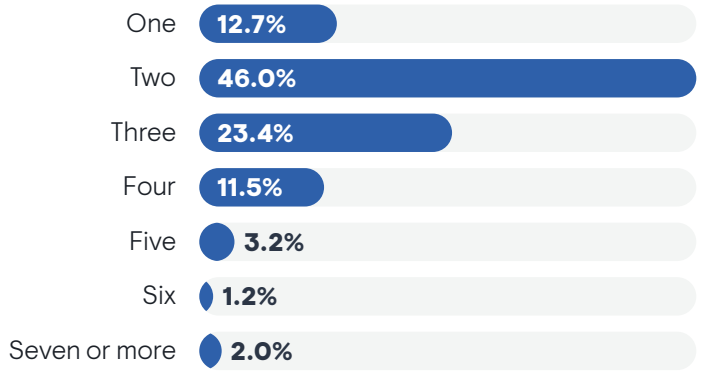
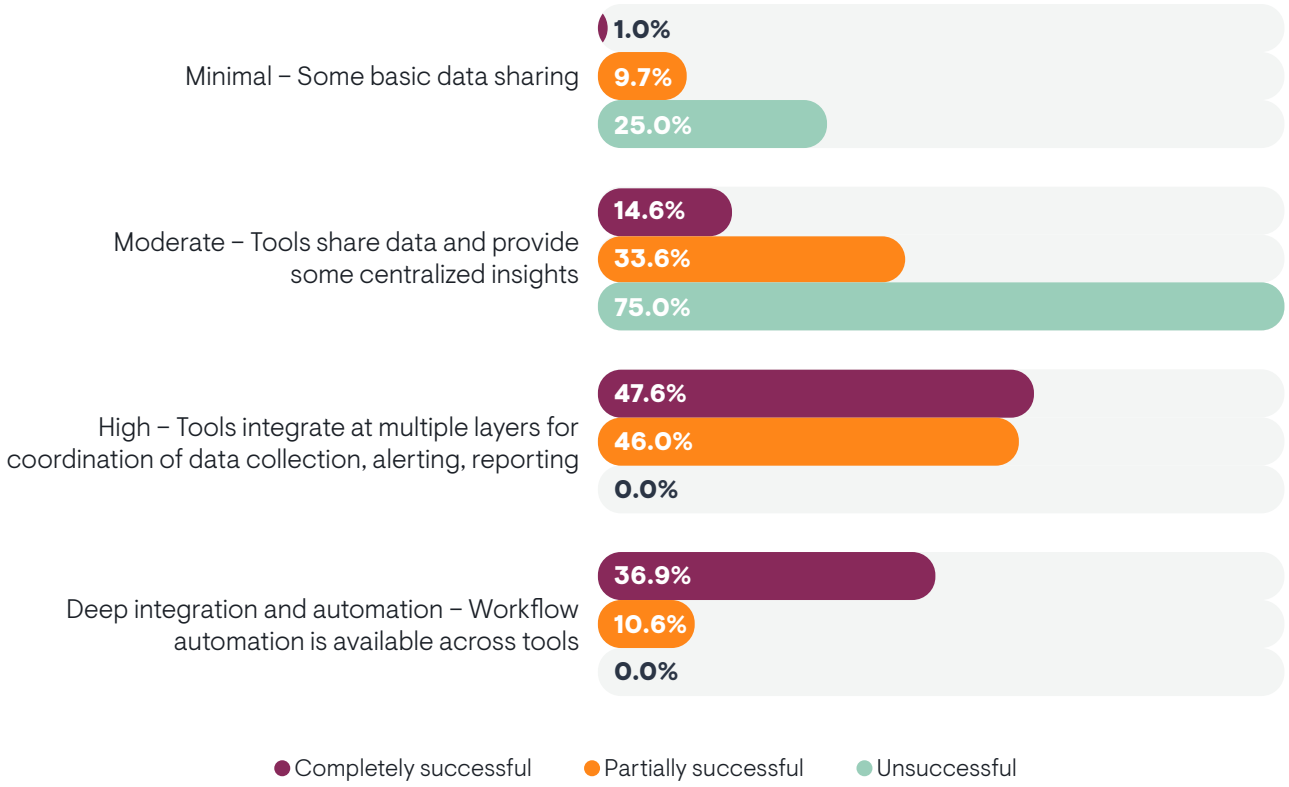


Figure 4 demonstrates that deep integration of tool sprawl is essential to network maturity. Basic data sharing between tools isn't enough. Unsuccessful network teams stop there. More successful organizations go further, with integrations at multiple layers for coordination of data collection, alerting, and reporting. Best-in-class organizations deepen integration even more, enabling automated workflows across tools.

Figure 4. To what extent are these network observability tools integrated? correlated with Overall success with network observability tools



Ensure Comprehensive Network Data Collection

A second pillar of network observability maturity is data. A mature toolset must have automated network data collection mechanisms that are extensive, granular, and scalable. Fundamentally, network teams must mature their ability to collect both network infrastructure data and network traffic data.

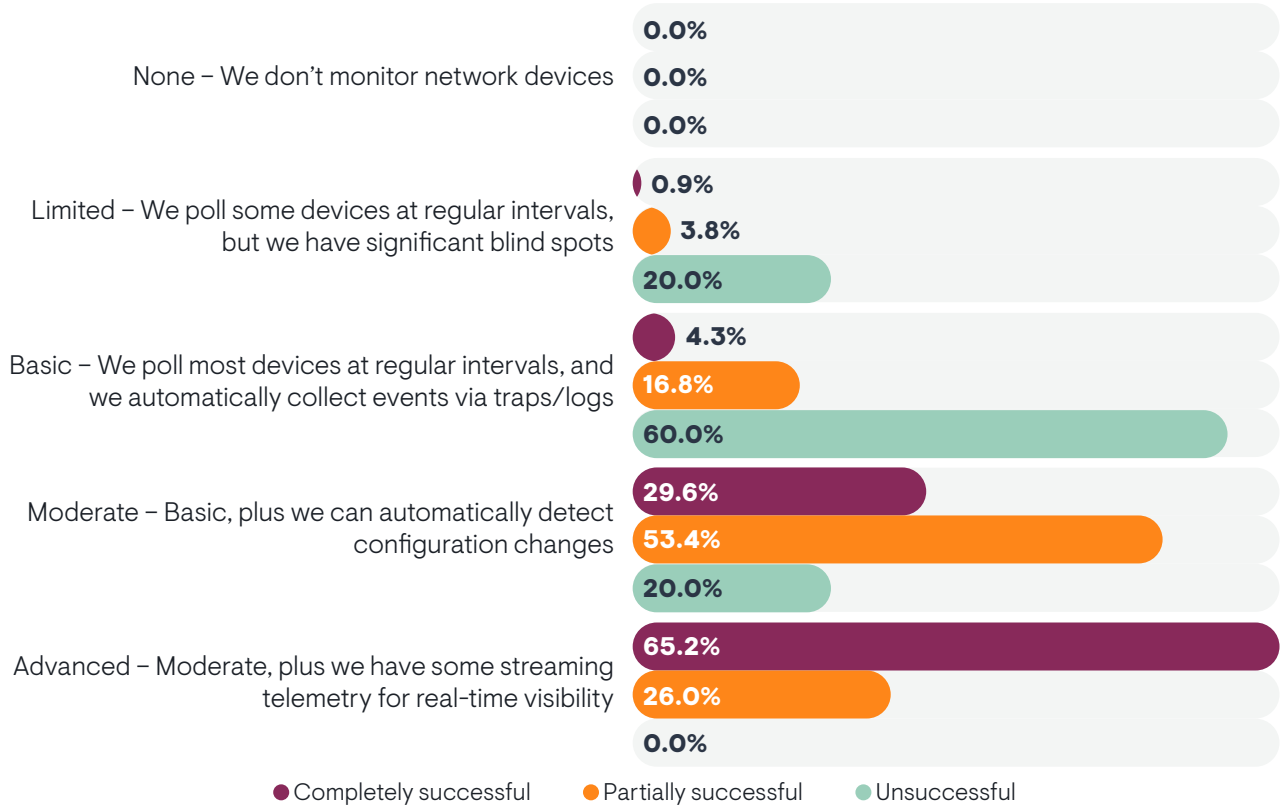
Collecting Data from Network Infrastructure

Network observability tools must collect telemetry from a maximum amount of network infrastructure. Traditionally, tools collect this data via SNMP MIBs (for metrics) and traps (for events). **Figure 5** reveals that this data collection must be extensive. Network teams with significant blind spots are very like to fail with their tools.

However, extensive polling and trap collection are not good enough, either. Network teams that augment this visibility with automated network configuration change detection start to experience more success. This allows them to correlate network faults with configuration changes, but even this isn't the final step to maturing this aspect of network observability.

Best-in-class network observability includes real-time data collection. Most SNMP polling intervals are five minutes. Shorter intervals can overload infrastructure with excessive SNMP-based management traffic. These intervals leave gaps in visibility and delay response times. The most mature network teams add streaming network telemetry to their network observability tools. These real-time data collection methods push data to tools, rather than rely on polling. The data usually flows to the tool only when conditions change, minimizing load but ensuring real-time granular insights. Industry support for streaming telemetry is limited, but many network operations teams are deploying it at strategic points on the network when possible.

Figure 5. Which of the following describes the level of visibility into network devices that your network observability toolset provides? correlated with Overall success with network observability tools



Collecting Network Traffic Data

Network traffic is also essential network observability data. It reveals how data flows across the network, providing insight into performance, user experience, capacity, security, and more.

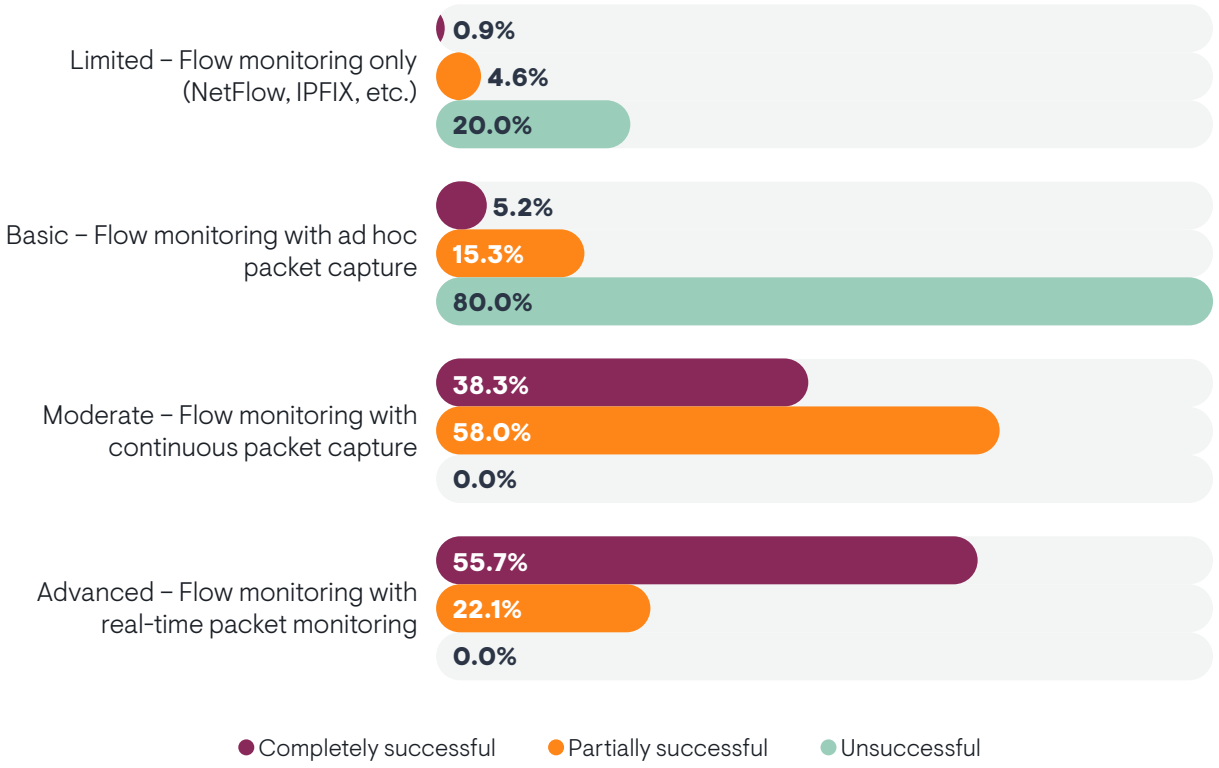
Network observability tools typically collect two types of network traffic data. Flow records, based on standards like NetFlow and IPFIX, offer a partial summary of the traffic that flowed across a network interface. This data is cheaper to collect, but it is less granular.

Network packets are the actual data that is transmitted across the network. It is more expensive to collect, but expensive packet capture can provide a full record of data that passed through a given interface, including source and designation information.

Figure 6 reveals that immature IT organizations start with flow monitoring and perhaps some ad hoc, reactive packet captures. This approach to traffic monitoring offers limited observability and network teams tend to experience less success with their tools.

As organizations complement flow monitoring with more sophisticated approaches to packet monitoring, they do better. Moderately mature organizations have continuous packet capture in place, which ensures that they have a full record of what happened on the network. With time, they can discover the root cause of whatever issue they are troubleshooting. However, the key to full maturity is real-time packet monitoring. These organizations have tools that derive metadata from packets and analyze them in real time to proactive detect issues and resolve them quickly.

Figure 6. Which of the following best describes the level of visibility into network traffic that your network observability toolset provides? correlated with Overall success with network observability tools



Extend Data Collection and Analysis to Software-Defined and Cloud Networks

New technologies like SD-WAN and the public cloud often drive network operations teams to adopt new tools. However, many organizations also look for ways to extend their traditional toolsets to these environments to ensure a more integrated, end-to-end view of the network.

For example, SD-WAN vendors offer uneven support of traditional observability data collection methods like SNMP. Network observably vendors will work with an SD-WAN vendor's APIs to extract comparable data. Cloud providers have proprietary observability data, such as VPC flow logs, and observability tools must adapt to this data to ensure cloud traffic observability.

Figures 7 and **8** reveal that network operations teams have better success with their tools when those tools offer excellent visibility into SD-WAN and the cloud. These are important signs of network observability maturity.

Figure 7. To what extent does your network observability toolset provide visibility into public cloud networks? correlated with Overall success with network observability tools

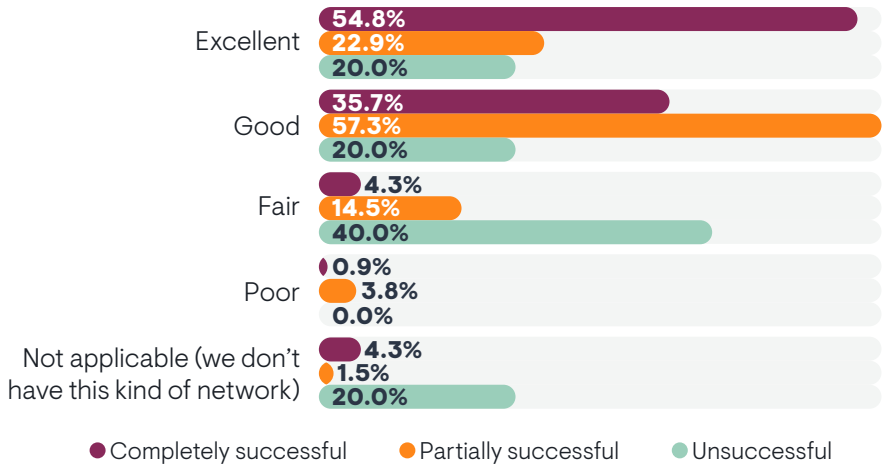
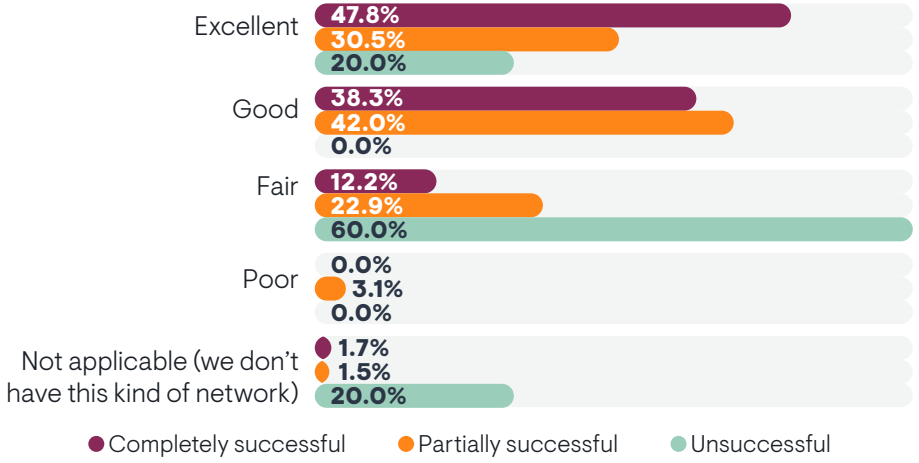


Figure 8. To what extent does your network observability toolset provide visibility into software-defined WAN (SD-WAN) and secure access service edge (SASE)? correlated with Overall success with network observability tools



Optimize NetOps Responses with Intelligent Alerting

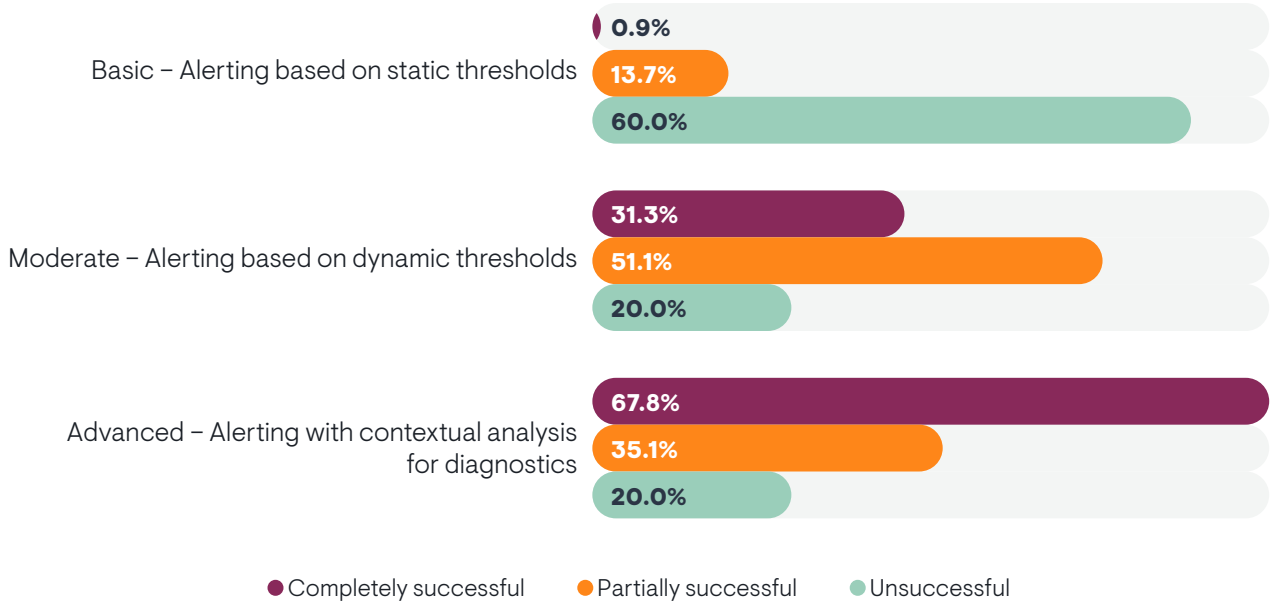
Nearly all network observability tools have alerting capabilities. When data collected from the network falls out of expected parameters, a tool will generate an alert. Network operations personnel use these alerts to detect and respond to problems.

However, not all alerts are indicative of a problem that must be solved. Immature tools rely on static thresholds that aren't a good measure of whether something is a problem. Immature tools also lack correlation and are unable to identify that a dozen or more alerts are related to one single instance, such as a device failure causing other devices to report data transmission errors.

EMA research found that only 29% of alerts from network observability tools are actionable.[2] This lack of precise alerting leads to excessive noise, and this noise is hard to sort through. Network teams spend too much time triaging alerts and not enough time solving the problems buried in the noise.

Figure 9 reveals that network observability tools are more mature when they advance beyond static thresholds. Dynamic thresholds that are tied to actual service performance are more helpful. However, network teams need more than dynamic thresholds. The alerts themselves must be enriched with contextual analysis so that network teams can act more quickly.

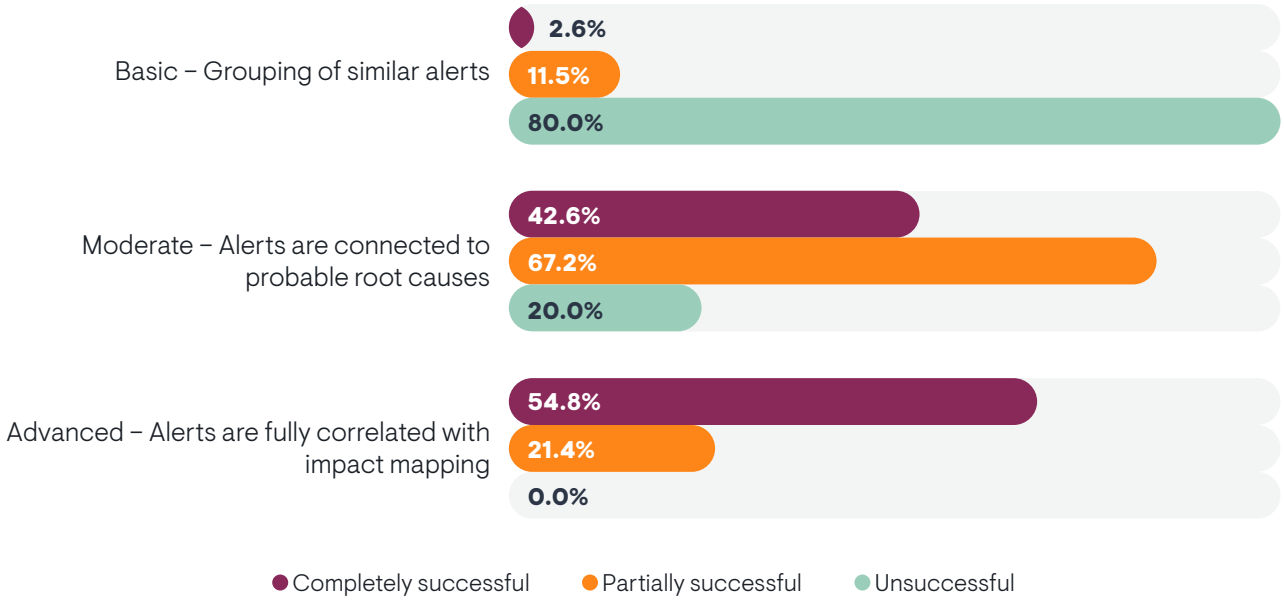
Figure 9. Which of the following describes the alerting capabilities of your network observability toolset? correlated with Overall success with network observability tools



[2] EMA, "Network Management Megatrends 2024," May 2024.

Figure 10 reveals the importance of alert correlation and impact mapping. Network teams whose tools can only group alerts by type tend to fail. Tools that can group alerts by connecting them to a probable root cause are more mature. However, the tools that drive the most success go beyond that. The most mature tools can fully correlate alerts and provide impact mapping.

Figure 10. To what extent is your network observability toolset able to correlate alerts? correlated with Overall success with network observability tools



Streamline Operations with Customizable and Integrated Dashboards and Reports

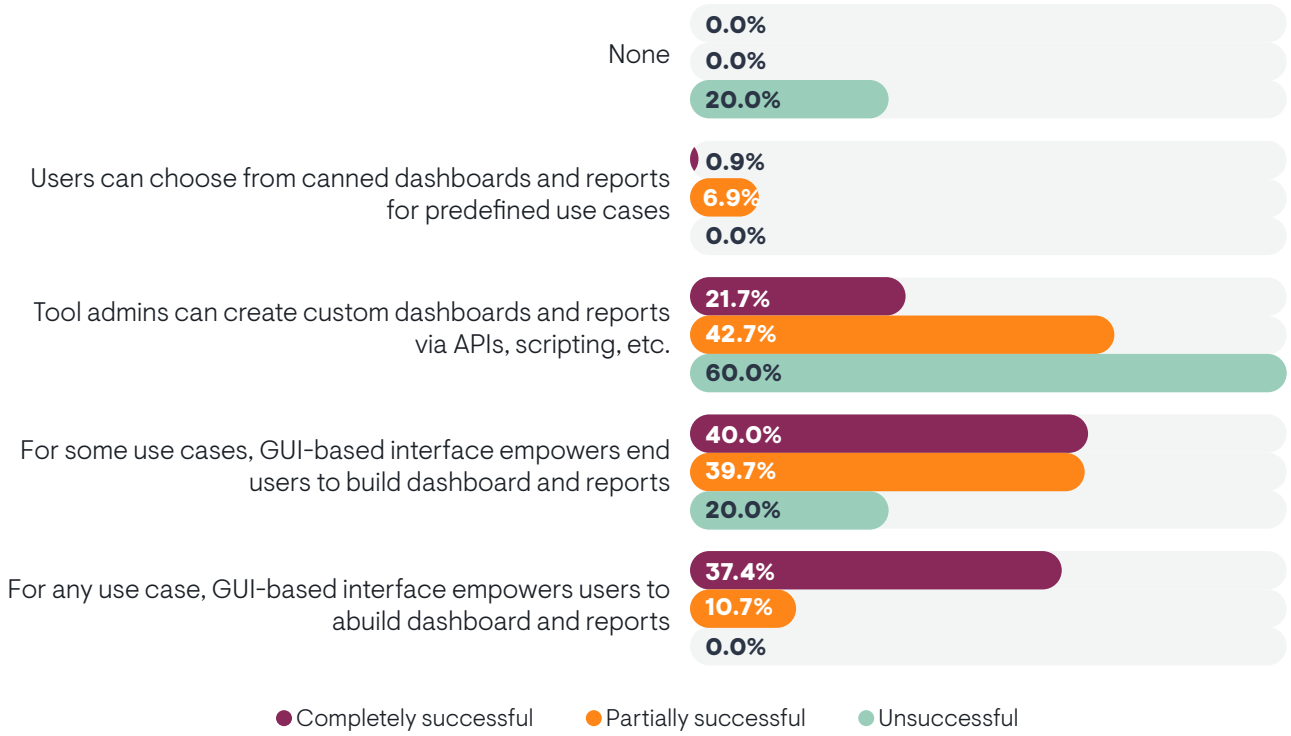
Dashboards and reports are essential components of network observability. At a basic level, they tell a story to users, such as what they should focus on, what's wrong on the network, and how they can get insight into a given issue. These stories are often specific to users, roles, and business units. Thus, customization and integration are key to assembling stories that are meaningful to these personas.

"One of the main problems with our vendor tools is the customization of dashboards. A lot of things are hard-coded. It doesn't allow you to customize its dashboards enough," said a network tool architect with a Fortune 500 retailer.

"I want to use different visualizations. I want more flexibility in visualization engines. As a system architect, I can't predict everything that users will need. So, tools need customization features that will personalize user experience," said a monitoring tool architect at a Fortune 500 media company.

This research shows that the more customization a tool offers, the more successful network teams are with that tool. **Figure 11** maps customization to maturity. Network teams with no dashboard and reporting customization are failing. Network teams that can customize with APIs and scripting tools do a little better. The most mature and successful toolsets have GUI interfaces that enable all users to build dashboards and reports for any use case without using APIs and scripts.

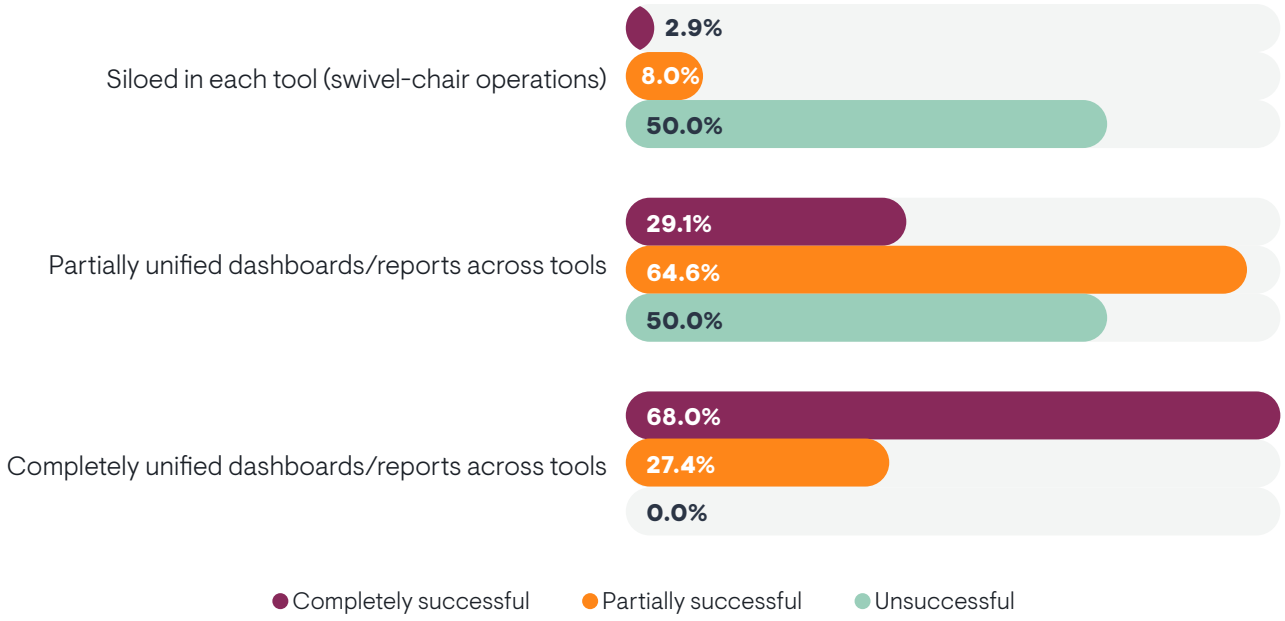
Figure 11. To what extent are your network observability tool's dashboards and reports customizable? correlated with Overall success with network observability tools



Given the state of network observability tool sprawl, dashboards and reports must also provide integrated insights across tools. This integration allows engineers to see more information in one place and correlate information across tools without having to pivot from one tool's console to another.

Figure 12 reveals that network teams without any dashboard and reporting integration fail. Many had partial integration, in which dashboard elements from one tool might be embedded as a widget within the dashboard of another tool. This integration offers some value, but is inflexible. Network teams who have full integration of dashboards and reports across tools experienced the best results.

Figure 12. To what extent are reports and dashboards unified across your organization's network observability tools? correlated with Overall success with network observability tools



AI-Driven Automation Advances NetOps to Ultimate Observability Maturity

Automation is a major priority for network operations teams, since they seek to accelerate response times and problem resolution and improve overall operational efficiency. Immature tools have primitive automations, such as basic correlations, manually-defined scripts and runbooks triggered by events, and static forecasting based on manually-defined thresholds.

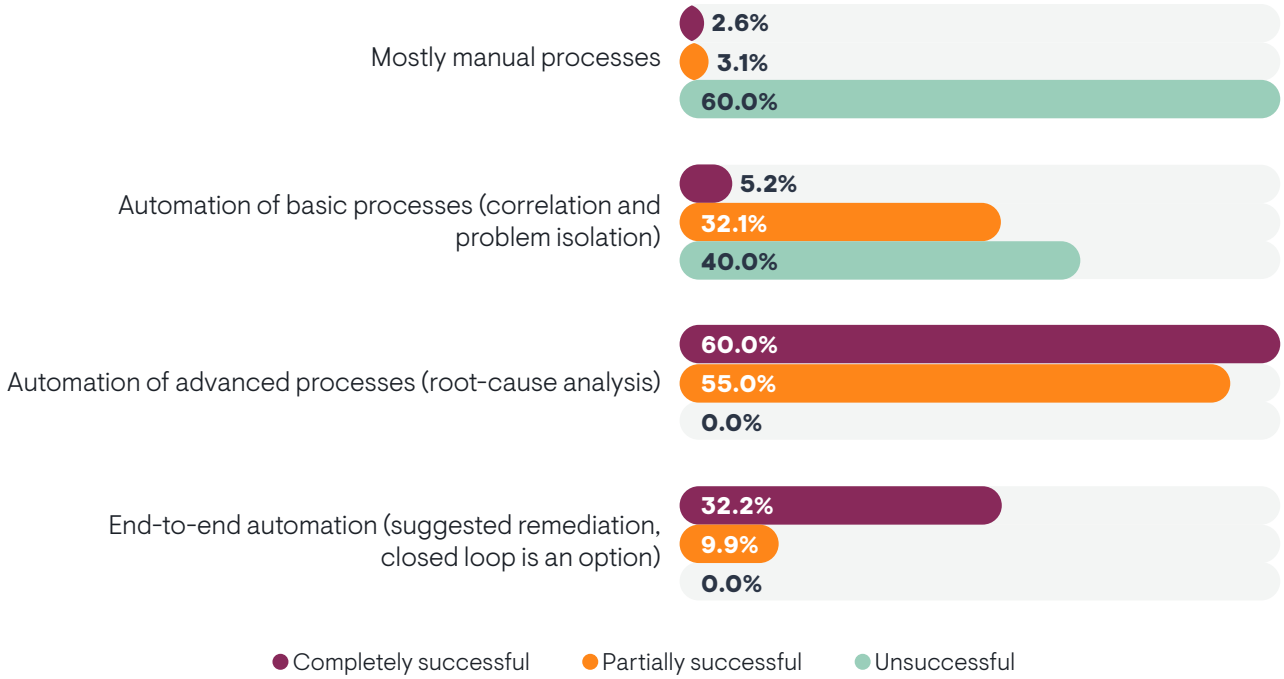
This research found that this level of automation returns only middling results. AI and analytically-driven automation lead to more success and ultimately network observability maturity.

Troubleshooting Automation

Figure 13 revealed that network teams without any ability to automate troubleshooting are struggling. Automation of simple processes based on simple correlations and groupings offers some incremental improvements.

Automation of more advanced processes, such as root-cause analysis, drives more network observability success. However, the most mature organizations leverage advanced AI that can provide end-to-end troubleshooting automation with suggestions for fixing problems.

Figure 13. To what extent does your network observability toolset help automate troubleshooting of complex issues? correlated with Overall success with network observability tools

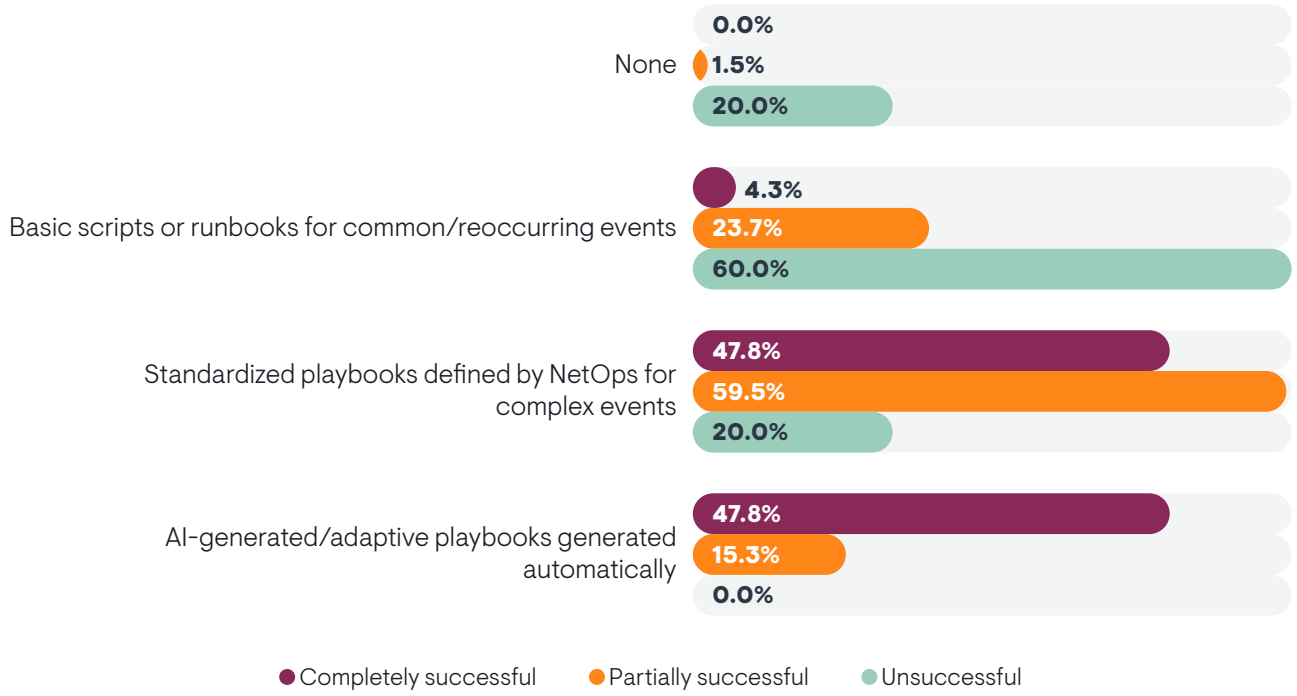


Automated Remediation Triggered by Incidents

Network teams often strive to streamline operations by configuring their tools to trigger automated actions in response to incidents and events. **Figure 14** reveals that advanced, AI-driven techniques yield more maturity.

Network teams that build basic script runbooks for common, reoccurring problems to trigger do little to move the needle on success and maturity. Instead, network teams see better results when they establish standard playbooks for complex network events. However, AI-generated playbooks that are produced automatically and are adaptive to variability in network operations drive the most success.

Figure 14. To what extent are your network observability tools able to trigger automation in response to network incidents? correlated with Overall success with network observability tools



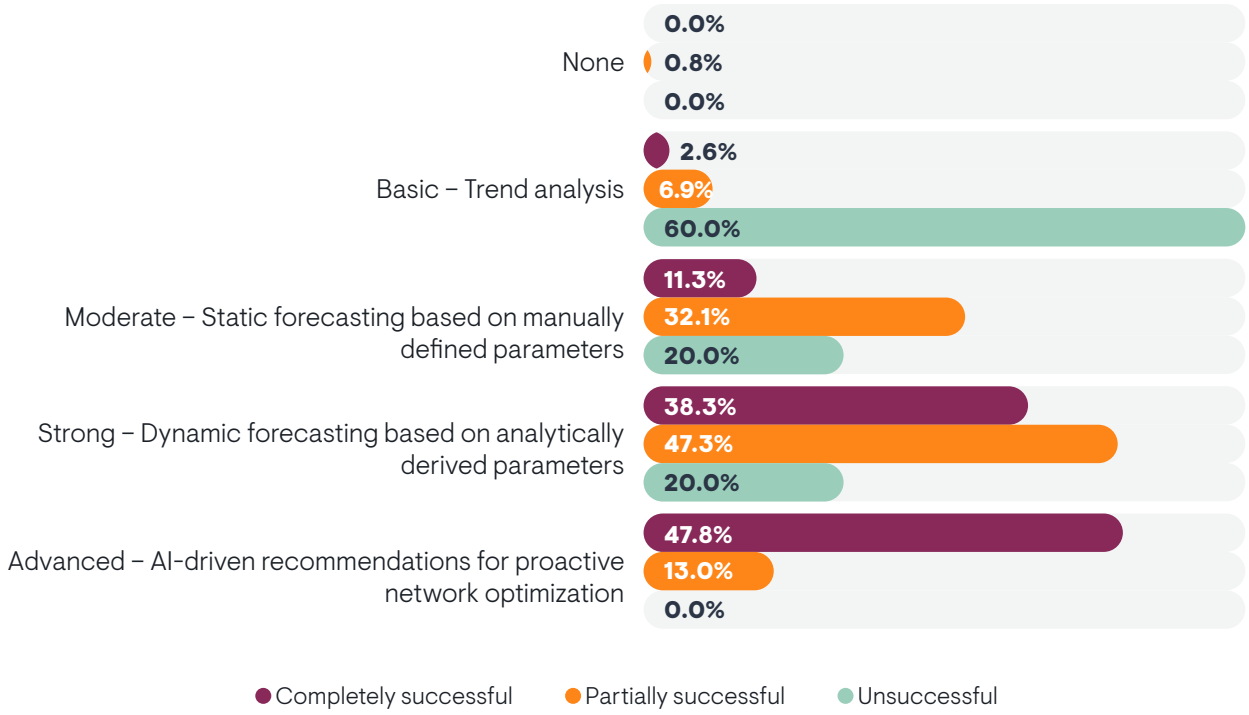
Predictive Optimization and Capacity Management

The ultimate sign of maturity is predictive network operations. These network teams can anticipate future needs and adjust the network to meet those needs. Most network teams try to achieve this, but they often rely on manual and static tools and processes. **Figure 15** shows that basic manual trend analysis is ineffective.

Tools that offer static forecasting based on manually-defined parameters lead to better results. However, automation is key. Dynamic forecasting based on analytically-derived parameters leads to more maturity. Ultimately, the most mature organizations are using AI-driven recommendations for proactive network optimization.

NetOps teams that try to do basic manual trend analysis or static forecasting based on manually-defined parameters tend to lack success.

Figure 15. To what extent do your network observability tools provide predictive analytics? correlated with Overall success with network observability tools



EMA Perspective

It has been more than thirty years since the modern internet kicked off mainstream adoption of information technology, and network operations teams are still struggling with their tools. This research found that only 46% of research participants believe they are fully successful with network observability. They need a better approach.

The stakes are high. As organizations adopt SD-WAN and secure access service edge, the public cloud, and artificial intelligence, complexity will increase and service expectations will rise.

The maturity model specified in this report provides a framework for transformation. IT stakeholders can use this instrument to understand where they are today and chart a path toward improvement. Organizations can mature network observability by reducing tool sprawl through integration and establishing comprehensive and scalable data collection. At a feature level, stakeholders should seek tools that offer analytically-driven alerting, customizable dashboards and reports, and AI-driven automation. EMA's research proved that IT organizations are more successful with network observability when they follow these steps. In other words, this network maturity model provides a roadmap toward best-in-class network operations.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading IT research and consulting firm dedicated to delivering actionable insights across the evolving technology landscape. Through independent research, market analysis, and vendor evaluations, we empower organizations to make well-informed technology decisions. Our team of analysts combines practical experience with a deep understanding of industry best practices and emerging vendor solutions to help clients achieve their strategic objectives. Learn more about EMA research, analysis, and consulting services at **www.enterprisemanagement.com** or follow EMA on **X** or **LinkedIn**.

2770 Arapahoe Road, Ste 132 - 544, Lafayette, CO 80026 +1 303.543.9500 **www.enterprisemanagement.com**

4588.082725