The End of Point Solutions: Modern NetOps Requires Pervasive and Integrated Network Monitoring

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for Kentik

February 2016

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

The End of Point Solutions: Modern NetOps Requires Pervasive and Integrated Network Monitoring

Table of Contents

The End of Point Solutions: Modern NetOps Requires Pervasive and Integrated Network Monitoring

Executive Summary

Network operations teams typically rely on a fragmented set of monitoring and troubleshooting tools, a situation that leads to ineffective management and network instability. IT organizations must adopt a new tool strategy that emphasizes integration, consolidation, and advanced analytics including big data. This strategy should not only focus on improved network operations. Given that network data can provide insight into security operations and business operations as well, network managers should explore how a new tool strategy can contribute to their IT organization as a whole and the business it serves.

Network Operations Has a Fragmentation Problem

Fragmentation of visibility has long plagued the world of network operations. IT organizations have no shortage of tools that provide them with glimpses of what is happening with network infrastructure, but these tools often provide very narrow views. Some tools present insights gleaned from the collection of device metrics while others use network flows. Other tools gain insight through analysis of packet data, and so on. In many cases, multiple, separate tools receive the same set of source network data but retain different data subsets. While a network operations team can assemble a good understanding of the health and performance of a network with these tools, it is not easy. In fact, as Enterprise Management Associates (EMA) research has shown, a lack of end-to-end network visibility is the top challenge to enterprise network operations today.[1]

Network operators struggle with visibility because they use a fragmented set of tools to monitor and troubleshoot their networks. This fragmentation leads to visibility gaps, inefficient workflows, and time wasted on data correlation. Many IT organizations rely on highly skilled network engineers to fill in the gaps among these fragmented tools, which is not an efficient use of technical resources. Moreover, when IT organizations are hobbled by this kind of management tool problem they miss the opportunity to use network data for other use cases. Network data can provide critical insight to groups outside of the networking team, particularly to security operations and business operations. If network operators struggle to establish their own visibility into the network, they have little hope of providing insight to other constituencies.

Given that networks are becoming more complex and more critical to the success of many enterprises, IT organizations need integrated network operations tools that provide deep, end-to-end visibility. They will also benefit from tools that can apply advanced analytics technology, such as big data, to provide network insights more quickly. These tools will be even more valuable if they can support cross-domain operations since network data can provide important insight to security operations and business operations.

Today's Network Operators Need an Integrated Toolset

Over the years, EMA research has consistently found that network managers use too many tools to monitor and troubleshoot their networks. Some IT organizations admit to using dozens of network monitoring tools on a daily basis. This situation is untenable. Enterprises should adopt a strategy to develop an integrated or consolidated toolset.

When pursuing this tool integration, network operators should look for ways to correlate data across tools, eliminate visibility gaps between standalone tools, and facilitate workflows from one tool to the next. They should explore how this integration can promote collaboration both within network operations and across other IT management domains, by providing either deep reporting from the

[1] All data cited in this paper is from EMA research and was originally published in the report "Network Management Megatrends 2016: Managing Networks in the Era of the Internet of Things, Hybrid Clouds, and Advanced Network Analytics" (April 2016).

tools or customized views directly into the tools themselves. According to a recent EMA survey of IT professionals, the two groups identified as most likely to use these custom views were IT executives (67% of respondents indicated that their IT leadership used these custom views) and security operations (58%).

EMA argues that this consolidation and integration is essential because network operations teams are more effective when they use a smaller set of tools. For instance, our research found that IT organizations using fewer network management tools reported more effective network problem detection than organizations that were using more tools. The typical network operations team reported detecting 60% of network problems before end users experience and report these issues. However, organizations using 11 or more network monitoring and troubleshooting tools detect only 48% of problems before end users, and organizations using only one to three tools catch 71% of problems before they affect end users.

Network stability also correlates with the size of a management toolkit. Among organizations that use 11 or more tools, 34% experience several network outages a day and another 28% experience network outages several times a month. Meanwhile, just 6% of organizations using one to three tools experience several outages a day. Instead, 21% of them experience just one or two outages per year, and 18% said they almost never have an outage.

Network operations should take a strategic approach to tool acquisition and look for opportunities to consolidate and integrate wherever possible. A question about existing tool acquisition policies showed that network operators are already aware of this need. Sixty percent (60%) of organizations using 11 or more network management tools said they do consolidate tools whenever possible. Fifty-two percent (52%) of organizations using one to three tools follow a policy of maintaining their current number of tools.

Network Operators Can Support Cross-Domain Integration

A valuable source of data for other domains in IT and the business, the network can deliver value to security operations in particular. For instance, the same network flow data that can provide insight into network health and availability can also be used to detect a distributed-denial-of-service (DDoS) attack. In many ways, DDoS detection is actually advanced network availability monitoring. A network interface that is congested with traffic may indicate organic traffic growth, or it may be point to a DDoS attack. In either case, the performance of applications will be impacted by degraded network availability. The relevance of network data to security monitoring is so widely recognized that 47% of organizations require their network monitoring tools to integrate with security monitoring systems.

Many enterprises are aware that network data can be valuable to cross-domain operations. EMA research has found that 26% of enterprises primarily conduct network operations from within a cross-domain operations center. Even organizations that don't use cross-domain operations centers recognize both the value of cross-domain visibility and the ability of network monitoring tools to support that visibility. Of the enterprises not using cross-domain operations centers, 48% were integrating their network monitoring tools into a cross-domain operations console and another 42% planned to do such an integration in the future.

The Rise of Advanced Network Analytics

Networks generate tremendous volumes of data, and network monitoring tools often specialize in collecting and providing insight from specific subsets of data, including packets, flows, routing, device metrics, logs, and many other data types. And analysis across these different data sets can deliver valuable insights. Many enterprises are exploring the potential of advanced analytics technologies that leverage big data to provide deeper insight into network availability, performance, and security. Analytics tools that can perform this analysis in real time and in an ad-hoc fashion, rather than just forensically are especially valuable since they can help network operators understand events as they are happening.

EMA research shows that many enterprises have launched advanced network analytics initiatives for improved IT and business operations. Network flow data (used in 49% of initiatives) and network security data (used in 48%) were the data types most frequently used. A majority of these enterprises (51%) assimilates network data for advanced analytics in the cloud. The top five use cases for advanced network analytics point to just how valuable these initiatives can be.

1. Network security monitoring (38%)
2. Network optimization (30%)
3. Business process optimization (27%)
4. Predictive network analysis (25%)
5. Predictive security analysis (24%)

Network security monitoring appears to be a low-hanging fruit for network analytics. When such an initiative contributes to business process optimization, the IT organization is able to establish itself as a true partner to the business. And predictive network and security analysis enables the IT organization to prevent problems before they occur, putting these technologies at the cutting edge of the IT industry.

EMA Perspective

The days of network operators relying on point tools for network monitoring and troubleshooting are over, even if network managers aren't yet aware of this change. The time has come for them to put away their point solutions, spreadsheets, and open source tools. EMA research shows that network operations teams are more effective when they use an integrated, consolidated toolset.

Enterprises can derive even more value when their tool strategies are integrated into a cross-domain approach to IT operations. This integration is especially an opportunity for network operations to support and enhance security operations. When this tool integration and consolidation is supplemented with advanced big data analytics techniques, network operators can become the MVPs of their IT organizations. With the right tool strategy, network managers can provide real-time insight not only to network operations, but also to security operations and business operations.

About Kentik

Kentik is the network intelligence company, offering a big data platform that's purpose-built for turning network data – NetFlow, sFlow, IPFIX, BGP, performance metrics, geolocation and more – into valuable real-time intelligence for digital operations. Unbounded ad-hoc analytics and anomaly detection help you improve operations, optimize capacity, resolve anomalies, orchestrate DDoS defense and protect your applications and service performance. Kentik gives you the visibility to deliver an optimal network experience and achieve your digital business and cloud IT goals.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

3509.011917