IDC ANALYZE THE FUTURE

IDC TECHNOLOGY SPOTLIGHT

Sponsored by: NetScout

Visibility and monitoring have become essential for the secure and efficient operation of enterprise networks, but the modern cloud era has introduced significant complexities in gaining tangible insights into increasingly complex environments. Network packet data is a rich and valuable source for gleaning this strategic information with analytics.

Network Visibility and Analytics: The New Currency of a Modern Digital Enterprise

July 2019

Written by: Brandon Butler, Senior Research Analyst, Enterprise Networks

Introduction

In today's modern enterprises, data is the new currency of business. Insights into modern digital technologies are used to fuel operational decision making, ensure secure and efficient use of IT equipment, and guarantee high-quality service levels for internal and external users. Gaining visibility into IT operations has never been more critical, but it has also never been more complex.

AT A GLANCE

KEY STATS

69% of organizations expect to make "major" investments in their network performance management systems in the coming years, while another **30%** expect to make only minor investments.

IT's footprint has expanded from being solely in the datacenter to now being an amalgamation of multiple on- and off-premises services. Applications are increasingly diverse: They are made up of a polyglot of programming languages and microservices-based architectures running in ephemeral containers with a range of dependencies service chained together. Insights into operations are invaluable for the secure and efficient operation of a modern digital enterprise. Of the handful of primary methods for collecting performance monitoring data, the most common are flows, agents, logs, and packet data. This paper examines all of these methods, including their pros and cons, and shows how network packet data provides comprehensive visibility into and service assurance of any application running on any infrastructure.

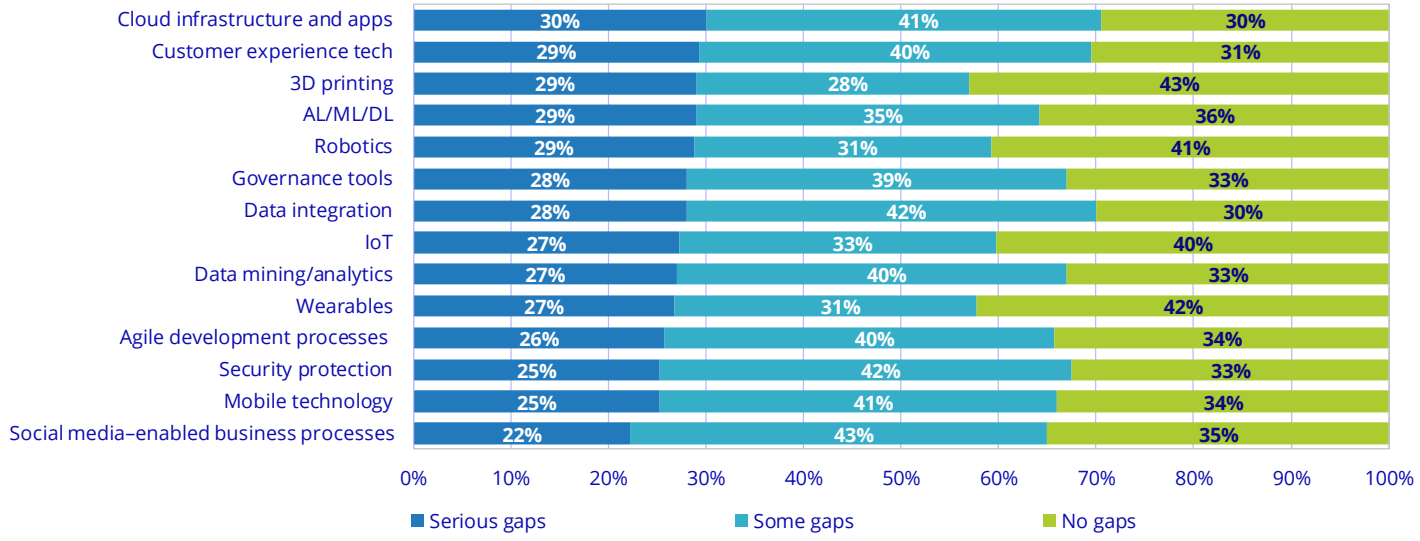
As Digital Transformation Accelerates, Complexity Increases

The past decade-plus has seen the rise and mainstream adoption of a variety of technologies that have fundamentally reshaped the function of IT. The growing reliance on cloud-based applications for mission-critical tasks has created not only enormous new opportunity but also new challenges in terms of efficient and secure management of these resources. Meanwhile, the growing interdependency of IT systems across the compute, storage, and networking domains has created a mix of both exciting opportunity and management complexity.

As enterprises around the globe look to embrace these digital transformation trends, they are realizing the shortfalls in the skills their workers have to deploy and manage these technologies. Figure 1 shows the top skills gaps that enterprises report as they look to meet the digital needs of their organization.

FIGURE 1: ***Skills Gaps in IT Organizations***

Q How would you describe your organization's skills gaps in the following areas of digital expertise over the next five years to meet your organization's business goals?



n = 400

Source: IDC's Cloud and Artificial Intelligence Perceptions Survey, January 2018

This skills gap is a critical issue in monitoring and analytics. Organizations need to comprehensively monitor and analyze all aspects of the network — on-premises and cloud as well as both traditional and newly developed applications — but this has become an enormous challenge given the variety of technologies relied on today and the many different ways they are architected. It's a significant advantage if enterprises can use existing tools they are comfortable with and have invested in as opposed to managing multiple niche solutions. Having a monitoring and analytics platform that is flexible and extensible and works across a variety of environments is increasingly becoming a critical decision factor for enterprises.

IT Monitoring and Performance Collection Methods

The need for monitoring and performance analytics has crystallized in recent years. A recent IDC survey of enterprise network performance managers found that 68.8% of U.S. organizations expect to make major investments in network performance management (NPM) technology in the coming year, while 30.4% expect to make minor investments; less than 1% have no plans to change their spending. This healthy level of investment has given rise to a wide variety of methods for collecting and analyzing performance data. The following sections discuss the top methods used in enterprises today.

Flows

Flow-based monitoring tools derive data from network infrastructure, which can be programmed to automatically record and export system operations. These flows require a network operator to configure a destination — a collection platform known as a flow manager, which must be set up and managed to expose these network flows to operators. Netflow, which is generated from Cisco networking equipment, is a common example of a flow technology.

Flow data is volumetric, which means it does a good job of describing the "who," "what," and "when" of network activity. However, flow data lacks the granularity needed for meaningful insights into user experience and troubleshooting. Flows can create a bandwidth strain for the infrastructure equipment that generates flow data, taxing the equipment and draining the infrastructure of the resources that it needs to perform its core task. Another challenge with flows is that as the size of the environment scales up, the amount of flow data scales linearly, creating an increasingly difficult management problem. Flows are therefore commonly deployed in small or medium-sized enterprises or in organizations that do not have a need or a budget for deep granular insights into IT operations.

Flows, agents, logs, and packet data each have unique characteristics for collecting and analyzing performance data in the modern digital enterprise.

Agents

Agent-based monitoring platforms are most typically used in application development and testing to provide detailed visibility into code performance of specific operating system (OS) or application development environments. Agents are typically focused on specific programming languages, making them difficult to use in polyglot environments, and they do not inherently provide performance metrics of the infrastructure layer. This means they are typically used for application-specific monitoring, particularly in development and quality assurance.

Logs

Logs are the written diagnostics records produced by various infrastructure and applications. Infrastructure logs are typically specific to the OS and the vendor, but there is no single log standard. For example, Windows and Linux have separate log formats. Syslog, commonly mistaken for a standard, is for log transport, but not log content. As a result, logs are typically "noisy," meaning they are voluminous in size with low-fidelity data that requires extensive supporting architectures for storing, indexing, and analyzing them. Logs are commonly used in security information and event management (SIEM) scenarios.

Packet Data

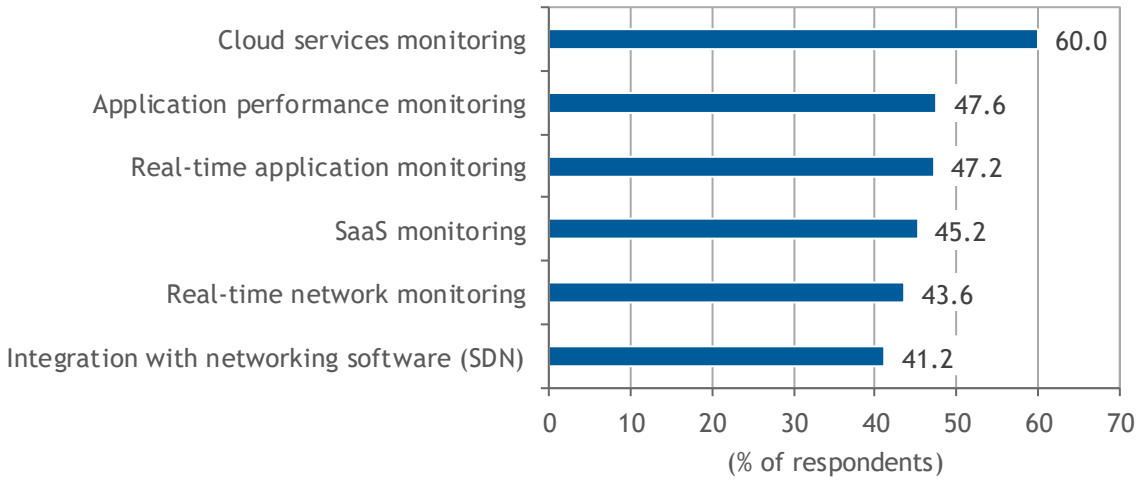
Packet data derives from monitoring the connections between digital points. These packets can be analyzed in real time to provide insights into any communication across the network, including the performance of components at both the application layer and the infrastructure layer; packet data is also able to capture end-user experience metrics.
The entirety of the packet, including layers of embedded protocols and payloads, is processed and transformed into real-time metadata insights, which makes for a highly scalable architecture. At the same time, some commercial packet data solutions also store the packets for after-the-fact forensic investigations. While storing packets is not necessary, having the ability to quickly go from metadata to packet forensics creates significant automation that can be leveraged by operations and security teams. Because all network traffic uses packets to transit data, the method can be deployed on-premises or in the cloud, and no interaction can escape it.

Analysis Engines Are Only as Good as the Data They Have to Work With

Choosing the right monitoring method is a critical decision for enterprises. Given how each method has its own strengths, it's important that enterprises choose a collection method that fits their use cases. Typically, data collected by the monitoring system feeds an analysis engine that surfaces meaningful insights to the network or IT operators. These analysis engines are only as good as the data they have to work with though. If a low-fidelity data source is used that does not provide a comprehensive view into the entire IT operation (both on- and off-premises), then the engine will not be able to provide relevant analysis. Furthermore, if a "noisy" type of data collection method is used, then it's more difficult for the analysis engine to find germane insights.

Enterprises are looking for performance management platforms that meet the needs of their business, as evidenced by the top investment priorities for performance management systems shown in Figure 2. A key priority is for the system to be able to monitor both on- and off-premises resources, including SaaS and IaaS. Data should be available across a range of metrics, from application to infrastructure and user experience. Packet data is in a unique position to be able to satisfy all of these requirements because it is network based, meaning it sees every transaction in the enterprise. Other forms of performance monitoring may be able to only partially cover each of these points.

FIGURE 2: ***Top Priorities as Organizations Invest in Network Visibility and Analytics***



n = 250

Source: IDC's NPM Survey of Network Managers, 2017

The Value of Performance Analytics

Gaining visibility and insights into the performance of the IT environment has never been more critical. Enterprises across the globe have a strong desire for a powerful, pervasive, and detailed performance management platform that can provide relevant insights into all aspects of the ever-expanding enterprise IT footprint. The performance insights and analysis are used in a variety of ways:

- To monitor, improve, and ensure the performance and user experience of infrastructure and applications
- To provide detailed analysis of ongoing operations, including the types of applications and services on the network, identification of bottlenecks, historical trend analysis, and future performance prediction
- To optimize the environment, including to automate the provisioning and management of additional capacity where and when needed
- To recognize anomalous activity and flag it to identify potential security issues or performance degradations

Considering NetScout's Adaptive Service Intelligence

NetScout's Adaptive Service Intelligence (ASI) platform uses packet data to capture and produce relevant, real-time, granular details about the operations of the enterprise applications, infrastructure, and network. Because the system sources its insights from passive monitoring of IP communications, it can be deployed anywhere — on-premises or in the cloud, in physical or virtual environments — meaning it can see everything happening across the entire enterprise. It analyzes the metadata of packets traversing any two points in the network while efficiently storing the packets as a forensic investigative tool. Combined with analytics capabilities, ASI flags the important events it captures, including known and learned security incidents as well as performance degradations experienced by equipment or end users. Because it sees all communications, it can map service- and application-specific infrastructure in real time. Key abilities of NetScout ASI include the following:

Visibility into what is happening in the network is a foundational component of automating and securing the IT environment.

- Produces actionable insights based on end-to-end, pervasive visibility
- Provides insight and analysis on a range of management domains, including infrastructure, application, and end-user experience
- Analyzes data in real time to provide insights into the performance of the network and broader IT environment
- Extends from on-premises to the cloud as well as virtual or physical environments
- Is not tied to a single programming language or flow standard

The extensible nature of ASI is a key point: As enterprises look to digitally expand their organizations, opportunity abounds, but so does management complexity. Any new cloud service that is spun up, any new application that is onboarded, or any new user on the network should not require a reconfiguration and rollout of new performance and security monitoring and analytics tools. The ability for packet data to provide actionable insights across any range of environments and application types means it is extensible as the use cases and needs of the business evolve into the future.

Challenges

NetScout has built the next-generation IT performance monitoring method using packet-based data and a powerful analytics engine in ASI. A key challenge for NetScout will be to prove to customers the value-added differentiation of packet-based data versus other data collection forms. Enterprises may have relied on other types of monitoring platforms in the past, but the complexity of the modern IT environment will force organizations to consider more holistic solutions.

Conclusion

Organizations are looking for ways to get pervasive visibility into what's happening in their IT environments, even as the enterprise footprint expands from the traditional on-premises physical world to an increasingly diverse cloud-based environment. Enterprises should consider a visibility and analytics platform that is able to provide real-time actionable insights into the broad array of technologies that make up today's modern digital business.

About the Analyst

Brandon Butler, *Senior Research Analyst, Enterprise Networks*

Brandon Butler is a Senior Research Analyst with IDC's Network Infrastructure group covering Enterprise Networks. He is responsible for market and technology trends, forecasts, and competitive analysis in Ethernet switching, routing, wireless LAN, as well as network management software. He also assists in end-user surveys, interviews, and advisory services and is a frequent speaker at industry events.

MESSAGE FROM THE SPONSOR

It is widely accepted that visibility into the performance of IT is critical to success of digital enterprise. Yet with every wave of technology adoption existing domain- and silo-based management approaches bring us an ever more complex tool glut, which are hard to use, hard to manage, and have high costs. Broad adoption of Hybrid Multi-Cloud (HMC) architectures provides an opportunity to reexamine and streamline fractured monitoring strategies and their associated high administrative resource requirements at a time of historic skilled staff shortage. The universality of packet data makes it the ideal tool for pervasive visibility into the health and performance of all applications and infrastructure regardless of location, while rapid access to packet forensics automates otherwise cumbersome workflows by operations and security teams for troubleshooting and incident response respectively.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Corporate USA

5 Speen Street
Framingham, MA 01701, USA

T 508.872.8200

F 508.935.4015

Twitter @IDC

idc-insights-community.com

www.idc.com