Driving Business with Continuous Operational Intelligence

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

October 2014

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

Table of Contents

Executive Summary

The role of Information Technology (IT) is changing. Gone are the days when IT can be viewed as a necessary evil or as simply a "cost center." Today, IT is widely recognized as a valuable business-enabling necessity. In some cases, whole businesses have been built around information technologies and simply could not exist without them. Such dramatic changes require more than just new business strategies – they demand rethinking the very ways in which IT is oriented and operated. One imperative strategy involves the shift from reactive, introverted, break-fix to data-driven, business-aware operations. For IT organizations to successfully make such a transition, they must find and leverage operational information via live real-time monitoring systems that provide sufficient depth and granularity to not only reveal what is happening inside the IT realm, but also expose a range of powerful new insights directly into how the business itself is running. This Enterprise Management Associates® (EMA™) whitepaper examines the concept of operational intelligence – what it is, which data types/sets can be used as a basis for it, and how to use it – and introduces an innovative approach offered by ExtraHop for producing continuous operational intelligence.

The Connection between Business and IT

Most commercial and governmental organizations today rely on IT infrastructures and functions in order to keep up with day-to-day business operations and processes. IT-enabled workers are the norm, and their ability to be continuously productive is heavily, if not entirely, based on the efficiency and efficacy of IT. And at the frontline – the touch point between IT and the business – are the applications which IT infrastructure is designed to host and deliver. While IT end users and customers use a wide (and growing) range of endpoint technologies, their collective engagement experience revolves around the applications and data they access and operate on a daily, hourly, and even minute-to-minute basis.

This application-centric net value that IT delivers must drive the ways IT leaders plan, operate, and manage their organizations. Enterprise Management Associates has long been tracking IT management tools, technologies, and practices as they converge upon application awareness and service centricity. Recent EMA research has even shown that the majority of enterprise network managers and operators, who are often the last to join service management initiatives, are now concerned with issues such as application performance, end-user experience, and service quality (see Figure 1).

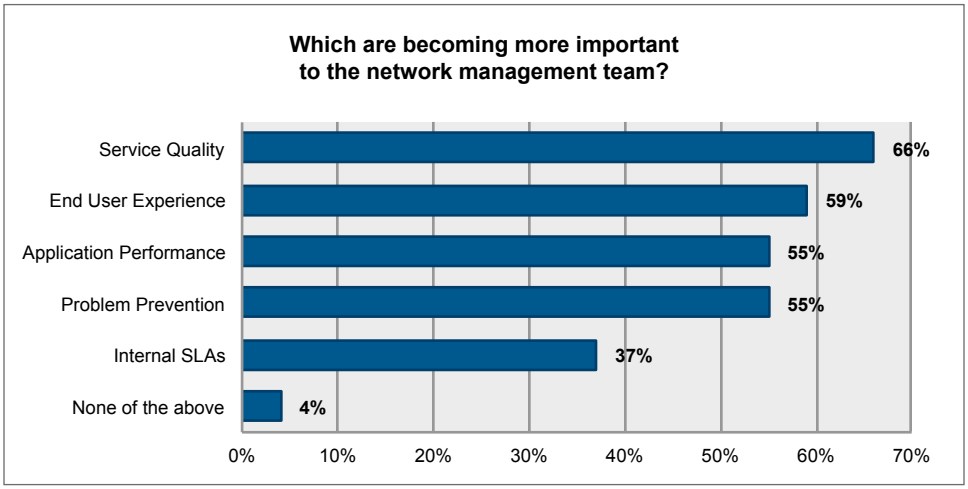

Figure 1. Increased importance of service quality and related objectives, from *Managing Networks in the Age of Cloud, SDN, and Big Data: Network Management Megatrends 2014*, EMA, April 2014 (Sample Size = 246)

This transition to application awareness is manifesting itself in a number of ways, from evolving management tools requirements to newly emerging organizational structures, visions, and objectives. From a management tools and practices perspective, IT organizations need to rally around and focus on how successfully applications and services, particularly the most mission-critical ones, are being accessed and used. This prioritization process, by its very nature, brings IT into alignment with the demands of the business/organization as a whole.

Moving Toward Application & Data-Centric IT Operations

Such a shift in IT strategy sounds logical enough, but successfully making the change is not as simple as one might think. It requires examining and revising fundamental goals and objectives, many of which will be specific to each individual organization, while others are shared industry-wide. At the core of enlightened application-aware monitoring and management lies the challenge of finding and reconciling accurate sources of data. Management systems offer the ability to gather data of all types, sizes, volumes, and depths, but not all such systems are complete, and few can truly serve as the basis of application-centric operations.

Management systems offer the ability to gather data of all types, sizes, volumes, and depths, but not all such systems are complete, and few can truly serve as the basis of application-centric operations.

Historical approaches to providing comprehensive monitoring coverage have focused on collecting all available data and attempting to correlate and reconcile that data with a central configuration and services model. This is the approach of traditional top-down Business Service Management (BSM). While BSM has been demonstrated to function successfully, it is significantly challenged to keep pace and remain accurate in the face of highly dynamic, virtualized, multi-sourced application and delivery infrastructures.

Another approach has involved data science, sifting through and reviewing all of the monitoring data that is gathered and looking for significant or noteworthy patterns and trends, typically in an off-line, post-collection manner. This is the traditional space of Business Intelligence (BI) approaches. BI techniques have regularly delivered vital results, yet most are challenged to deliver operational intelligence in the same way applications and services are delivered and consumed – in true real time.

If IT organizations hope to position themselves as something more than an inhibitor to the organizations they serve, they must consider new approaches to improving operations. Such approaches will need to not only deliver application and service awareness, without requiring rigorous and inflexible modeling, but also provide operational insights in true real time.

Using Real-time Data to Inform Business Operations

Moving to a real-time view and operating model within IT requires the use of live, real-time sources of monitoring and management insight. There are many sources from which to choose when it comes to operational monitoring data; however, not all are equally fit for live operational intelligence. Device-based metrics and measurements, harvested from network or compute systems, are helpful but tend to be periodic in frequency and will normally represent the statistical sampling or summary of activity, not actual/detailed sessions or transactions. Session detail records, such as NetFlow, AppFlow, or IPFIX, provide a better view of individual application and user activity; however, as these records are not normally generated until the end of the session or at some periodic interval during the session, they can fall short when seeking to understand what is happening or who is active at any discrete moment in time.

An alternative that holds great promise as a core data set from which to draw live operational intelligence is the direct monitoring of packets as they cross the network – often referred to as "wire data." However, the volume of wire data can prevent any meaningful analysis unless it can be transformed into structured data for IT and business analytics. Structured data is created using real-time stream processors analyzing bi-directional transactions and their data payloads. As with any data source, there are limits to what structured wire data can show you, but it is deeper and richer and more complete than the vast majority of alternatives. Wire data reveals, in true sub-second real time, precisely which users are active, which applications and services they are using, what volume of activity they are driving, which specific actions are being taken, as well as the likely quality of their experience.

Further, wire data includes a tremendously rich set of details regarding which data and application functions are being executed and operated on. Specific commands and transaction types can be recognized in real time within each session, and can highlight specific business activity results. For instance, it's possible to view each step in a web transaction, from browsing to selection to adding options to checkout and finally to order confirmation. Wire data can also reveal specific machine-to-machine activities, such as electronic authorizations or settlement transactions, or database queries against individual files or data types. With such granular information, it becomes possible to go beyond simply recognizing business activity to establish a clear and discrete understanding of business results, including any behavioral or technical issues that stand in the way of success.

Wire data includes a tremendously rich set of details regarding which data and application functions are being executed and operated on.

While wire data may indeed be one of the best choices for an operational intelligence data source, it does bring with it a few significant challenges. First of all, wire data comes in very large volumes. Intelligence gathering typically requires only a small portion of the actual packets being transferred, but data rates are regularly measured in tens of gigabits per second. Consequently, instrumentation for collecting and analyzing wire data must be capable of consuming high rates and volumes without missing or dropping any details. When monitoring network links with exceptionally high and continuous loads, this can require purpose-built, optimized hardware appliances. In those settings where data volumes and rates are not as high, or where it is impossible to deploy a hardware appliance, soft or virtual appliances can be utilized, as long as load can be balanced and an adequate depth of granular detail can be provided.

Transforming Wire Data into Operational Intelligence

Metrics generated by collecting and studying wire data can deliver tremendous insights into business activity; however, they remain only part of the bigger story. The real payoff comes when wire data is combined with other sources of information available within the IT realm. Augmentation with complementary data sources enables wire data to be transformed into operational intelligence.

Augmentation with complementary data sources enables wire data to be transformed into operational intelligence.

For example, some of the data sets that are most helpful for supplementing wire data are those that relate names and places to numerical identifiers used within electronic business transactions and activity. Doing DNS or Active Directory lookups can translate IP addresses into human-readable names (a step that is absolutely essential for those organizations moving to IPv6). Adding geographic location via geocode lookups can also enhance IP addresses. CRM systems or other customer information databases can provide translations between transaction ID codes and actual customer/client names. Transaction type IDs can be translated

for easy recognition or grouping. And the list goes on – wire data often contains many of these fields and indicators that can be readily used for technical monitoring, but must be translated to make the analysis business-relevant. In many cases, this information may also be extracted via wire data analysis.

Beyond data augmentation lies another highly useful category of translation and analysis techniques known broadly as "analytics." This term is often used as a catchall to indicate any amount of advanced data modeling and processing. For the purposes of our discussion here, however, analytics refers to the automated data analysis techniques that can transform a stream of augmented wire data into the operational intelligence upon which observations and decisions regarding IT and business activities can be based. Examples include automated generation of derived metrics, statistical analysis of data streams, and behavioral models for recognizing normal versus abnormal variations. The importance of automation cannot be overstated here. Wire data comes in large volumes and at high rates – automated analytics is the only practical approach to making wire data useful for real-time, operational intelligence use cases.

Leveraging the Results

Once you have transformed your monitoring data into true operational intelligence, what can you do with it? The number of doors this opens is truly stunning. For example, transaction types can be organized by business priority, so that the most essential activities can receive the most attention. In another case, enabling services and applications, such as electronic records management, credit card authorization, and payment processing, can receive the special monitoring they need for prioritized response whenever something goes awry and proactive intervention whenever and wherever possible. Further, dashboards can include direct, live measurements of internal and external business activity as well as results, so everyone in the organization can be aware of business activity and success. In the end, this is immensely valuable and powerful information, and it can be the ticket for the IT operations team to transcend break-fix reactive firefighting to become empowering business partners.

This is immensely valuable and powerful information, and it can be the ticket for the IT operations team to transcend break-fix reactive firefighting to become empowering business partners.

Operational intelligence is most valuable when it is shared in a collaborative manner. This means building dashboards and reports that show live views of activity as well as trends over time, to better inform both real-time operations and business planning. Some of these capabilities can be provided directly by operational monitoring systems while others will come from combining real-time operational intelligence with other business data sets (often via a Big Data repository or initiative) for wide-ranging, multi-variant data analysis and mining.

The ExtraHop Solution: Operational Intelligence from Wire Data

While several providers of monitoring and management tools have built solutions that collect and process wire data, ExtraHop has focused on the real-time stream processing technique exclusively and as a result has advanced the state of the art as much or more than any other vendor. Founded in 2007, ExtraHop provides solutions that are now widely deployed by commercial and enterprise organizations large and small for real-time monitoring of application transaction and session performance leveraging wire data. To do this, the solution has been architected for scalability and extensibility, and has been steadily expanded to address applications and protocols ranging from http/web to detailed database queries, from file transfers to server-based computing such as Citrix ICA, and most everything in

between. The solution has been specifically optimized to see through the complexity of networking protocols to expose real-time insights and measures of application (and hence business) activity.

ExtraHop has evolved its solutions from network and application monitoring to business-facing operational intelligence via new features included in its fourth generation release in late 2014. In particular, this release included the following important new capabilities:

- **Universal Payload Analysis to isolate and augment business-relevant metrics from wire data from nearly any TCP or UDP-based application stream** – Though this capability has long been part of the underlying technology with the ExtraHop solution, it has been simplified and magnified, and elevated to a primary level of visibility and configurability within the system
- **Data Visualization via a new workflow-oriented, role-based user interface redesign** – Enhancements have been made to facilitate rapid discovery, exploration, configuration, and comparison of operational metrics of which any set can be overlaid on any other for effective real-time modeling. This capability fully supports any metrics collected via Universal Payload Analysis (see figure 2).
- **Data-agnostic approach to analysis and presentation, treating all metrics as of equal importance** – This is particularly important for equitable support of custom-defined metrics that are unique to an individual organization and managed/monitored environment. Such custom metrics inherit the same data visualization and modeling functions as the 2900+ native metrics already provided within the ExtraHop solution.
- **Time-based analytics** – Abilities have been added to facilitate comparison of metrics versus prior similar time periods, such as the same hour of the prior day or the same day of the prior week. This makes immediately obvious whether value variations, trends, and spikes are normal or abnormal.
- **Streaming data sharing** – The new Open Data Stream feature allows a continuous feed of operational intelligence metrics to be published to external data stores so that data can be combined with other data sets for more complex, multi-variant, post-hoc analysis.

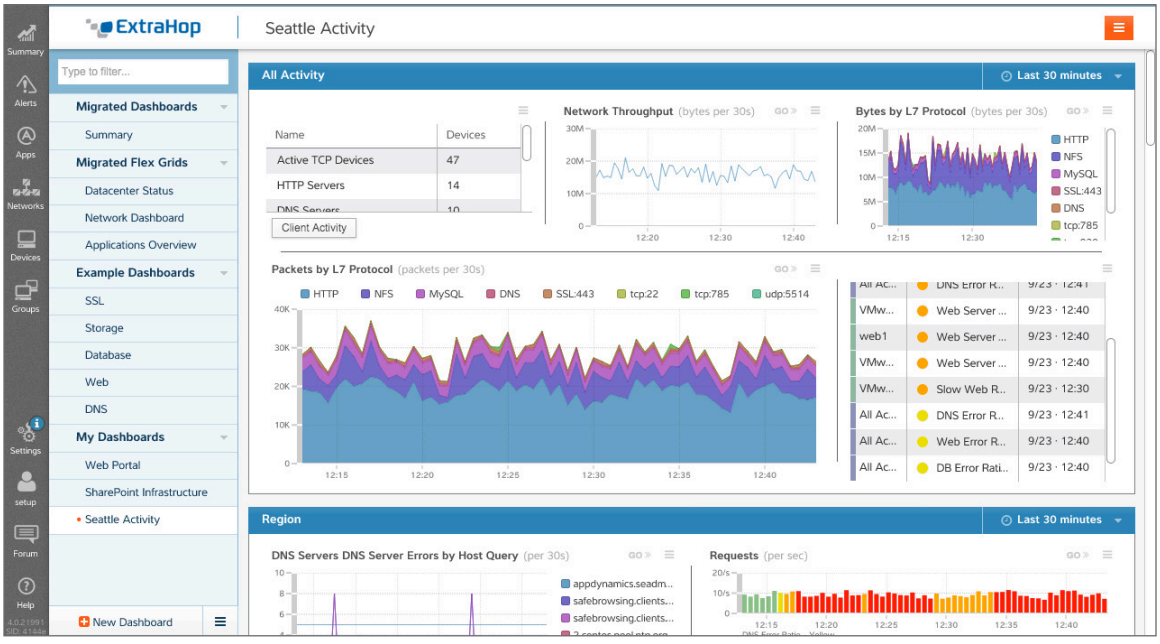

Figure 2. Fourth-generation ExtraHop console interface with time-based comparative analytics

These latest enhancements provide the means for transforming wire data into operational intelligence that can be tuned and optimized to the specific needs of any IT-enabled organization. In particular, the ExtraHop solution provides the architecture and features to:

1. Gather wire data effectively and reliably, as a core source of rich operational metrics.
2. Augment that data via external data sources that translate wire data values into business-relevant indicators, via the new Open Data Context API.
3. Apply automated analytics to identify important and action-worthy behavioral changes.
4. Rapidly analyze operational intelligence via intuitive, flexible operator consoles and dashboards.
5. Share operational intelligence across IT and non-IT constituents via customized views and reports as well as external analysis systems via the Open Data Stream feature.

Collectively, the ExtraHop solution represents a monitoring technology platform that allows IT operations to assemble and share operational intelligence based on wire data. And going beyond simply providing enabling technology, ExtraHop will use this platform to deliver pre-built operational intelligence solutions for specific industry verticals, such as healthcare, education, financial services, and others, as defined by common applications, protocols, and work tasks. Such solutions will be constructed based on the experiences that existing ExtraHop customers have had in deploying the system and tuning it to their own environments, allowing best practices to be baked in and shared by organizations with similar business objectives and work processes.

EMA Perspective

The time has come for IT to move out of the shadows and into the limelight. Businesses and organizations that depend on IT should expect more than just available and stable technology. When the business runs on IT, IT has the opportunity to measure and report on the pulse of the business. More than that, IT has the obligation to use its viewpoint to the best possible advantage of the organization it serves and supports. For years, monitoring and operations practices have been focused on simply keeping IT up and running. But now the data and means are there for IT operations to do far more than that. By leveraging the amazingly rich insights available via harvesting and analyzing wire data, IT operations can go beyond simple metrics, and instead generate continuous operational intelligence that can be used to assess, optimize and protect IT functions as well as business processes, activity, and even business success.

With the most recent release of its solution, ExtraHop has put in place the rest of the pieces required for turning structured wire data into continuous operational intelligence.

The key to successfully building a continuous operational intelligence apparatus is in finding solutions that can effectively harvest wire data, extract the relevant details in real time, augment that data with business-specific translations and mappings, and analyze the patterns and trends of activity to recognize and highlight actionable trends and anomalies. ExtraHop has always offered a highly capable solution for gathering and analyzing wire data. With the most recent release of its solution, ExtraHop has put in place the rest of the pieces required for turning structured wire data into continuous operational intelligence in a manner that keeps pace with the way applications are consumed and business activity occurs – in real time. And while such capabilities are impressive in and of themselves, even more inspiring is what lies ahead, as ExtraHop proceeds to pre-build overlays based on best practices to accelerate the time-to-value for organizations within specific vertical economic sectors.

About ExtraHop

ExtraHop is the global leader in real-time wire data analytics. The ExtraHop Operational Intelligence platform analyzes all L2–L7 communications, including full bidirectional transactional payloads. This innovative approach provides the correlated, cross-tier visibility essential for application performance, availability, and security in today's complex and dynamic IT environments. The winner of numerous awards from Interop, TechTarget, and others, the ExtraHop platform scales up to 20Gbps in a single appliance, deploys without agents, and delivers tangible value in less than 15 minutes. Learn what we mean at http://www.extrahop.com/ or follow us on Twitter @ExtraHop

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

2984.100914

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

2984.100914