Driving Competitive Advantage with Data-driven IT

ExtraHop

Contents

Introduction 2
I. Data Friction: the cause, the reality, and the costs 3
II. Survey Results: Network Monitoring Trends 4
III. The Road to Data-driven IT: rethink the network with ExtraHop 7
IV. Use Cases 8
V. Success Scenarios 9
VI. Conclusion: The ExtraHop Effect 10
Introduction

The role of network operations is evolving as teams are asked to do more to support strategic initiatives. This is the “digital transformation” that many people are talking about. But the reality is, many network teams spend most of their time triaging and troubleshooting.

Of course, troubleshooting is essential, but in order to meet the strategic demands of the business, network teams must think beyond break/fix. This means partnering more directly with lines of business to solve real problems and improve processes.

To start, many IT organizations are drowning in complexity. In fact, 71% of IT organizations aren’t proactive with innovation, efficiency, and security – simply because they’re too busy reacting! That impacts key business activities. Take project delivery: 70% of organizations report that they are delivering projects late.¹

This inability to keep up with the data flow will worsen as traffic volumes increase. The approaches that worked at 1 Gbps and that were severely stretched at 10 Gbps will be completely inadequate for 100 Gbps, and the speed of business is just going to keep accelerating. Data continues to grow, proliferating across on-premise, cloud, and remote sites. There are more users and more things, e.g., devices and apps communicating and interacting with each other.

Organizations overwhelmingly want to be data-driven, but the inability to access and parse high quality data at the speed of business is an increasingly significant barrier. Read on to learn how network operations teams can overcome these challenges, flip the status quo, and drive the business forward.

¹ 2016 State of the CIO survey: conducted by CIO.com
I. Data Friction: the cause, the reality, and the costs

At organizations around the world, there’s a troublemaker that no one is talking about: data friction. Data friction restricts IT from knowing quickly what’s going on across the enterprise, responding immediately, and maintaining a secure experience for employees and customers.

The Cause
Digital transformation efforts are creating all kinds of new business initiatives, resulting in constant churn and IT sprawl for IT. This churn combined with the increase in data volumes creates data friction, which limits visibility, adds complexity, and introduces security threats.

The Reality
Here are some startling statistics:

8 Out of 10 IT Teams Rely on users to notify them of problems
IT Teams Spend Up to 50 days each year troubleshooting
It Takes an average of 229 days to identify a data breach

The Cost
The Ponemon Institute reports data friction costs include direct, indirect, and opportunity costs from data center outages, including damage to mission-critical data, impact of downtime on organizational productivity, damage to equipment, legal and regulatory repercussions, and lost confidence and trust among key stakeholders. Findings suggest $7,900/min or $474,000 per hour. Thirty-seven percent of this cost is due to reputation damages and customer churn.

According to survey data from Information Technology Intelligence Consulting (ITIC), 98% of organizations say a single hour of downtime costs more than $100,000; 81% of those respondents indicate that 60 minutes of downtime costs their business more than $300,000; and for a third (33%) of them, that one hour of downtime costs their firms $1 million to more than $5 million.

Furthermore, feedback states that anytime a customer cuts ties, companies experience the negative impact of customer churn. While some churn is a normal part of any business, a high churn rate can cripple the growth of any organization. It’s important for businesses to understand what contributes to churn in order to address those issues—and ultimately drive customer retention. Unfortunately, when customers have bad experiences, 95% share them publicly.

Data friction, the precursor to downtime, costs the enterprise real money and is the primary barrier to IT teams as they strive to become more data-driven.
II. Survey Results: network monitoring trends

ExtraHop sponsored a Gatepoint Research survey with a focus on network monitoring trends. More than 100 system application and infrastructure executives representing senior IT decision-makers from a wide variety of industries participated and shared what they’re monitoring, how they’re monitoring it, some of their challenges, and what they wished they could improve.

The respondents reported that the IT environments they monitored included multiple data centers (83% of respondents), remote sites (69%), cloud computing (66%), and SaaS applications (59%).

Almost three out of four (72%) respondents use network data for monitoring, two-thirds (66%) use machine/log data, and more than half (56%) use agent-based data sources.

In the past three months, more than half (54%) of respondents reported an outage of a critical system. The majority (88%) have experienced outages during the past year.
II. Survey Results: network monitoring trends

When was the last time you had an unplanned outage of a critical system?

- 2% Currently
- 13% Within the Last Week
- 24% Within 30 Days
- 15% Within 90 Days
- 34% During the Past Year
- 13% Never

When respondents were asked to list their top challenges, problems with IT sprawl came to the forefront: too many tools in place (45%), lack of expertise (44%), managing the infrastructure (43%), gaps in visibility (42%), as well as costs and complexity.

What are some of your biggest monitoring challenges?

- 45% Too Many Tools
- 44% Lack of Expertise
- 43% Managing Infrastructure
- 42% Gaps in Visibility
- 38% Prohibitive Costs
- 28% Complexity
- 21% Doesn’t Map to Work Flows
- 19% Outgrown Tools - Failure to Scale
- 15% Lack Timely Data

Trying to monitor IT sprawl leads to frustrations with data friction. When asked what they wished their network monitoring solution could deliver, well over half of the respondents wanted an integrated real-time view (59%) and proactive warnings about problems (57%).

Nearly half wanted to be able to identify underlying causes of poor performance (49%) and spot and counteract security threats (48%).
II. Survey Results: network monitoring trends

Continued

What do you wish your network monitoring was better at?

- Delivering an Integrated Real-time View Across All Tiers: 59%
- Proactive Warning of Potential Problems: 57%
- Identifying Definitively the Underlying Cause of Poor Application Performance: 49%
- The Ability to Spot and Categorize Security Threats Quickly: 48%
- Integrating with My Existing Management Systems: 43%
- Offering Detailed Information on the Activities of Affiliate Networks and Partner Transactions: 26%
III. The Road to Data-Driven IT: rethink the network with ExtraHop

In order to be data-driven, organizations need to harness the abundance of data that proliferates across their business. To avoid data friction, they need real-time intelligence built into every digital interaction that informs IT when and where help is needed. ExtraHop provides the means to do this at the pace of business. The ExtraHop platform provides true insight from a definitive data source: the network.

As businesses continue to undergo digital transformation, the network has become the common denominator tying everything together, since every user, device, app, and exploit transacts on the wire.

In the past, enterprises have treated the network simply as a delivery mechanism for digital experiences. Today, ExtraHop makes it possible to mine the communications between devices for real-time insights.

The company offers a patented stream processor to discover and observe behavior on the network, combined with powerful machine learning so IT organizations can unlock the hidden value in their networks and solve the challenge of data friction by discovering, observing, and analyzing every digital interaction as it occurs.

This rich source of insights is referred to as "wire data," and it is the most critical source of data for decision-making. ExtraHop tears down barriers, and delivers real-time, objective insight that makes data-driven operations a reality.
IV. Use Cases:
how network operations teams thrive with ExtraHop

Business initiatives succeed or fail based on the ability to understand what's happening in the network. ExtraHop enables the visibility to analyze all application communication in real-time. Here are just a few use cases where ExtraHop makes an impact.

▶ Triage and Troubleshooting
ExtraHop transforms in-flight data into structured wire data to deliver cross-tier, real-time visibility across the organization. This means network operations teams can see problems as they occur, isolate them, and get the entire team aligned to solve the problem.

Users can:
- Stay on top of performance, with real-time monitoring
- Surface empirical metrics around availability, performance, and security
- Trace issues across all dependent systems

▶ Security and Compliance
To maintain a consistently strong security posture in the face of advanced threats on the network, network operations teams need full visibility into network behavior in real time.

ExtraHop enables users to see into every transaction that passes across the network in real time. Machine learning-driven analysis of structured L2 to L7 wire data is the key to real-time threat detection at any stage of the attack lifecycle. The solution delivers deep analytics to help users understand the source of threats, the scope of an incident, and how to keep attackers out.

▶ Datacenter Migration
Datacenter migration can be daunting with so many dependencies and complications in the environment. It might seem impossible to guarantee a seamless end user experience during the move — and customer churn due to poor performance is only one fraction of potential migration costs.

Real-time IT analytics from ExtraHop allows users to map the entire IT infrastructure across on-premises, hybrid, and cloud environments for a comprehensive, up-to-the-minute understanding of the complete environment for a stress-free, low-cost migration.

▶ Cloud Migration and Monitoring
Cloud migration of applications and infrastructure is a complex process that requires careful planning and deliberation. Once apps are in the cloud, IT teams need a way to benchmark performance, manage virtual machines to control costs, and ensure the performance, availability, and security of the critical systems on which the business relies.

ExtraHop delivers real-time visibility into assets and their dependencies, offering a complete and accurate understanding of the infrastructure. With this awareness, critical systems and applications can be migrated to the cloud with minimal risk and service disruption. ExtraHop then automatically and continuously monitors performance.

There are more examples that show how ExtraHop helps organizations succeed with IT and IT-driven business initiatives here.
v. Success Scenarios

Following are some examples of how ExtraHop has helped organizations succeed with data-driven business initiatives.

- **Multi-billion Dollar Financial Services Company Improves Time to Incident Response by More Than 60%**
  A multi-billion dollar financial services company needed to retain certain records to satisfy standards and regulations. It wanted to cut down on the computation and labor costs associated with packet capture and manual post-hoc analysis. It also wanted to perform real-time analysis of specified data sets, set alerts, and pick out anomalies and trends, all while maintaining the security of the data.

  The company uses an ExtraHop solution to conduct real-time analysis on performance metrics across its network, cutting provisioning costs and sharing analytics with the team without compromising data security. Not only did the time to incident response improve by more than 60 percent but also the Network Manager discovered 43 DNS servers that they thought had been decommissioned but were still active, which was costing the company money and leaving gaping security holes in their system.

- **Online Retailer Consolidates Datacenters 2 Months Ahead of Schedule, Saves $100,000**
  An online retailer needed to consolidate datacenters, but was wary of potentially causing outages in the process. The goal was to identify and decommission unused servers without affecting customer access.

  Using the ExtraHop platform’s automatic application discovery capability, the retailer was able to quickly and easily create an inventory of all of its servers. Overall, the consolidation saved the company $100,000 and was completed two months ahead of schedule.

- **Large Enterprise Gains Real-time Visibility, Moves from a Reactive to Proactive Mode of Operations**
  A large enterprise with both incoming and outgoing SSL traffic found that it was becoming increasingly difficult to manage the infrastructure. It wanted to understand how certificates are used, plan SSL hardware purchases, and remove unused certificates.

  The team used ExtraHop to view the entire set of SSL behaviors on their network and the company determined that its SSL hardware was sufficient to carry their SSL needs for several more quarters at the present rate of growth.

  Additionally, there are many more real-world examples of ExtraHop in action [here](#).
VI. Conclusion: the ExtraHop effect

Keep your team out of the war room.

All organizations want to be data driven, but data friction up to this point has been an insurmountable problem. Traditional IT management suites have not kept pace with the exponential increases in data, complexity and dynamism in IT operations. Lacking in insight, these solutions are also costly to maintain and unwieldy to manage.

ExtraHop delivers a fundamentally different wire data-centric approach that is simpler, more scalable, and more effective at delivering the type of insights that make a difference for your business.

Drive competitive advantage with data-driven IT.

ExtraHop makes real-time data-driven IT operations possible. By harnessing the power of wire data in real time, network, application, security, and business teams make faster, more accurate decisions that optimize performance and minimize risk. Hundreds of organizations, including Fortune 500 companies such as Sony, Lockheed Martin, Microsoft, Adobe, and Google, start with ExtraHop to discover, observe, analyze, and intelligently act on all data in flight, on-premises and in the cloud.

Click here to learn how ExtraHop can help you analyze every single digital interaction occurring in your IT environment and turn that data into the most accurate and timely source of intelligence.

Source: Network Monitoring Trends Pulse Report, December 2016 (except where otherwise noted).

Sponsored by:

ExtraHop Networks, Inc.
520 Pike Street, Suite 1700
Seattle, WA 98101 USA
www.extrahop.com
info@extrahop.com