ExtraHop Delivers Better User Experience and Security for Enterprises

Sponsored by: **ExtraHop**

Authors:
Tim Grieser
Harsh Singh

August 2018

Business Value Highlights

740%
three-year ROI

4 months
to break even

95%
reduction in time to detect threats

59%
less time to resolve security threats

85%
less time needed to repair application degradation

86%
reduction in unplanned downtime

EXECUTIVE SUMMARY

IT organizations are under enormous pressure to achieve performance and service quality objectives in the face of constant technological change and explosive growth. Rapidly increasing volumes of digital applications, huge data volumes, and ongoing cloud enablement are generating challenges for IT system and network management. At the same time, increasingly distributed environments, which include edge, datacenter, and cloud deployments, create a vast attack surface subject to ever more sophisticated threats. Business success in fast-paced and highly competitive digital business environments depends on fast, reliable, and secure applications delivering consumerlike experience to network-connected users. Solutions for managing, optimizing, and securing network infrastructure and operations, while supporting infrastructure modernization and controlling costs, are essential for achieving the critical performance and reliability standards needed for effective digital business applications. ExtraHop provides solutions for managing, optimizing, and securing network infrastructure and operations.

IDC interviewed 10 organizations that are utilizing ExtraHop to provide real-time analysis of their IT infrastructures and security operations. Study participants reported that ExtraHop helps them identify and proactively address issues in their networks, applications, and security infrastructure, which enables organizations to operate with increased confidence. These ExtraHop customers reported not only establishing more efficient IT operations but also providing better security, reliability, and performance for their end users. IDC quantified the value of the improvements these organizations are realizing at $2.04 million per organization per year ($13,417 per 100 internal users) by:

- **Allowing IT operations and security teams** to identify and resolve issues more quickly
- **Enabling end users to be more productive** by reducing application performance degradation and outages
- **Freeing up IT employees** to focus on more strategic and growth-oriented projects

Situation Overview

Digital business is driving rapid growth for a wide variety of services, applications, and content deployed in diverse settings including on-premises and private, public, and multicloud environments. These facilities are being accessed directly by end users using a variety of devices, both behind and outside edge firewalls. Providing competitive, consumerlike responsiveness for end users without slowdowns, interruptions, security events, or crashes is a critical success factor for IT organizations to meet their digital business imperatives.

IT organizations are faced with an abundance of operational challenges as they work to support digital business environments. IT needs to monitor, manage, and optimize systems, networks, applications, and end-user experience to ensure that performance, reliability, and security standards are being met. The ability to expeditiously detect and resolve anomalous conditions to prevent impacts on end users is essential. If slowdowns, outages, or breaches do occur, IT needs to have efficient processes and solutions for incident identification and remediation.

Achieving operational management in today's environments poses enormous challenges given the scale and complexity of modern IT infrastructures, unpredictable workloads, dynamic infrastructures, and high volumes of machine-generated and human-generated data. IT analytics and security solutions need to provide real-time views and analysis at scale. To achieve this, these solutions need to incorporate IT operational analytics capabilities with the ability to analyze and correlate network transaction data across the application payload to give end-to-end views. Advanced statistics and machine learning can establish normal baselines, detect anomalies, provide root cause analysis, and implement remediation. Security analytics can identify threats and initiate actions to resolve incidents.

ExtraHop

ExtraHop is a Seattle-based company, founded in 2007, that provides solutions for managing and optimizing network infrastructure, operations, and security based on real-time operational intelligence. The ExtraHop solution begins by consuming a copy of unstructured network traffic from a tap or port mirror. The ExtraHop stream processor then performs line-rate decryption on SSL/TLS, decoding for over 55 protocols, and full-stream reassembly for every network transaction. The result is structured wire data composed of over 5,000 metrics to which analytics and machine learning are then applied to instantly and accurately surface performance and security anomalies.

ExtraHop provides extensive visualization capabilities through dashboard-based graphics including live, interactive activity maps of real-time transactions. Standard, role-based, and customizable dashboards provide views for a wide variety of infrastructure and application metrics across edge, datacenter, and cloud infrastructure. ExtraHop visualization surfaces real-time

insights to help detect and resolve issues before users are impacted. This helps IT organizations deliver highly secure and responsive performance and reliability experiences for end users, without slowdowns or interruptions — important requirements for successful digital business applications.

ExtraHop uses stream-based analytics to deliver comprehensive management functions. These include performance monitoring, anomaly detection, troubleshooting, root cause analysis, and security analytics across the entire application payload for all network-connected infrastructure and applications. Comprehensive analytics and machine learning include autodiscovery, classification, and mapping of all devices and assets on the network; continuous baselining; and automated detection and investigation of performance anomalies. These capabilities are designed for use by IT, network, and security operations staff and do not require the knowledge or skills of a data scientist.

ExtraHop supports a variety of key business initiatives and use cases, including the following:

- **Improving application service delivery.** Support, identify, and resolve network and application performance issues; provide SaaS visibility; and monitor customer experience.
- **Enhancing network security.** Support threat detection and response; identify threats; enable faster investigation; and improve cloud security.
- **Accelerating IT modernization.** Support cloud migration and network connectivity and accelerate deployment of new applications.
- **Providing more efficient IT and network operations.** Improve triage and troubleshooting (less time to troubleshoot and faster time to repair).

With these capabilities, ExtraHop helps IT organizations achieve operational efficiencies, improve network and application performance, and monitor and understand the service experienced by customers and end users.

The Business Value of ExtraHop

Study Demographics

For this study, IDC interviewed 10 organizations about the IT, network operations, security, and business outcomes and results after deploying the ExtraHop solution. Table 1 characterizes the firmographics of these organizations. The size of the companies surveyed represented a diverse mix, ranging from very large enterprises to smaller and medium-sized organizations. This is reflected in the average employee base of 20,900 and the average customer base of 1.58 million users. The companies surveyed represent a broad mix of vertical industries including the healthcare, financial services, retail, government, media, and entertainment sectors.

TABLE 1

Demographics of Interviewed Organizations

	Average	Median
Number of employees	20,900	8,750
Number of IT staff	942	450
Number of internal IT users	18,465	7,125
Number of customers (external users)	1,582,696	575,000
Revenue per year	$6.2 billion	$1.9 billion
Industries	Financial services, retail, healthcare , media, government, and entertainment	

n = 10

Source: IDC, 2018

Interviewed Organizations' Usage of ExtraHop

The organizations that IDC interviewed stressed the need for having better visibility as they seek to improve network and application performance and minimize the friction that performance and security issues can exert on their businesses. Interviewed organizations said that ExtraHop has helped them monitor and address performance challenges by providing IT operations and security teams better real-time insights. This has helped them be more proactive in identifying and attacking problems as they arise.

Study participants provided a number of reasons for deploying ExtraHop, including:

- **Proactive identification of performance issues:** *"ExtraHop allows us to be proactive. We can look at every packet and the associated latency. We will know if a user is having a problem or will have a problem. We can proactively look at what the end user is doing. Using statistics, we create models of every person including trends and anomalies and where there might be a problem."*
- **Easier, proactive network management:** *"ExtraHop is helping us move from being reactive to being proactive. We're seeing problems ahead of time and are able to react to them before they become major."*
- **Real-time view of network impacts:** *"We sometimes will make a change to our network, and ExtraHop tells us if it will have a negative impact. We have actually backed out of planned changes after seeing that kind of proactive information."*
- **Actionable data and trend analysis:** *"With ExtraHop, we have real-time end-user monitoring of the data and can do trend analysis down to the user level. When there's a departure from the norm, there's an actionable alert."*

"ExtraHop is helping us move from being reactive to being proactive. We're seeing problems ahead of time and are able to react to them before they become major."

To develop a full picture of use patterns, IDC gathered data on how study participants have deployed the ExtraHop solution as well as detailed information. For example, the interviewed companies support an average of 354 business applications and 12,291 network devices, with ExtraHop being tied to 88% of total revenue (see Table 2). Table 2 also provides additional metrics on ExtraHop usage.

TABLE 2

Interviewed Organizations' Usage of ExtraHop

	Average	Median
Number of branches/sites	1,813	18
Number of ExtraHop-supported internal users	15,250	4,100
Number of business applications	354	200
Number of network devices	12,291	3,500
Total revenue supported (%)	88	100

n = 10

Source: IDC, 2018

ExtraHop has yielded significant financial benefits, which IDC quantified as having an average annual value of $2.04 million per organization per year over three years ($13,417 per 100 internal users).

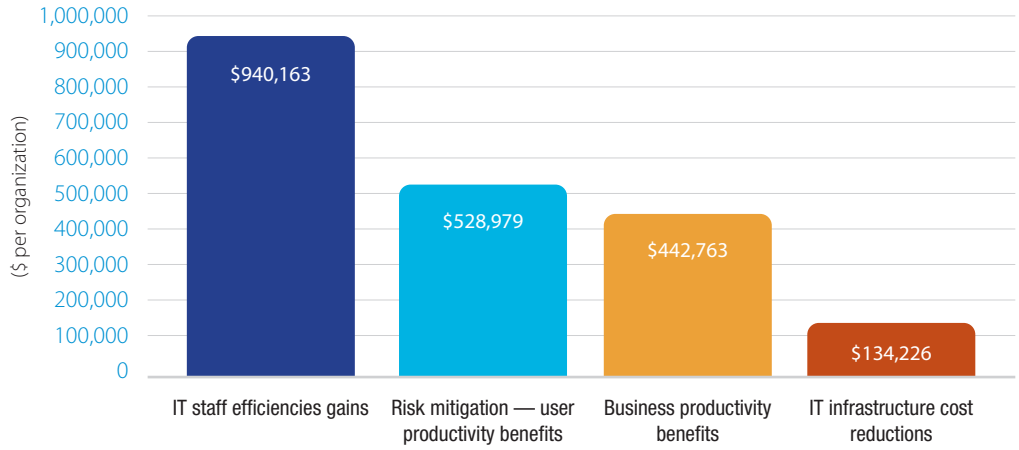
Business Value Analysis

Study participants reported employing ExtraHop to give their IT teams actionable insight that enables them to better address application service delivery problems and performance degradation. As a result, ExtraHop enables more productive IT operations with better reliability for its end users. For study participants, ExtraHop has yielded significant financial benefits, which IDC quantified as having an average annual value of $2.04 million per organization per year over three years ($13,417 per 100 internal users). As shown in Figure 1, these benefits are being realized in the following areas:

- **More efficient IT staff:** Instead of spending time reacting to network-related issues, various IT teams could find issues faster and resolve them in a timely manner. As a result, these teams had more time to work on more strategic business projects. IDC quantifies these time savings at $940,163 per organization ($6,165 per 100 internal users).
- **Better risk mitigation:** Since IT teams can proactively address issues, they can reduce the amount of unplanned downtime end users have to deal with and minimize operational risks associated with security breaches and other outages. IDC puts the value of this increase in end-user productivity at an average of $528,979 per organization ($3,469 per internal end user).
- **Improved business productivity:** Another benefit of better handling user experience issues is reducing the extent to which application performance degradation impacts end users. IDC assesses the value of increased user productivity at an average of $442,763 per organization ($2,903 per 100 internal users).
- **Reduced costs:** Some surveyed organizations reported reducing costs related to hardware, tools, and bandwidth use. IDC calculates this benefit as being worth $134,226 per organization per year ($880 per 100 internal users).

FIGURE 1

Average Annual Benefits per Organization



Source: IDC, 2018

IDC ANALYZE THE FUTURE

Improving Application Performance

Study participants spoke about how ExtraHop is enabling better application performance by decreasing incidents that involve degradation of service. ExtraHop customers reported being able to reduce the number of incidents because they could address major issues the first time around.

Commenting on the ability of ExtraHop to improve system reliability, one study participant said, "Using ExtraHop, we now know if a server is not acting correctly. Before we wouldn't know about a bad server until tickets started coming in. Now we get reports from the servers regularly. As a result, we can create tools that automatically take that server out if needed and send traffic to another one."

Table 3 provides metrics on the impact of the ExtraHop deployment on application degradation incidents. Especially noteworthy is the average time to repair per degradation (in hours), which showed a level of improvement of 85%. In addition, hours of productive time lost per user (annually) showed a level of improvement of 75%.

TABLE 3

Application Degradation Impact

	Before ExtraHop	With ExtraHop	Benefit (%)
Frequency of degradation per week	4	1.6	60
Average time to repair per degradation (hours)	7.9	1.2	85
Users impacted by degradation (%)	20	18	10
Hours of productive time lost per user per year	0.9	0.2	75
User impact — FTE equivalent per organization per year	7.6	1.9	75

n = 10

Source: IDC, 2018

Network security was cited by ExtraHop customers as a key area of post-deployment improvement. Security teams often use a combination of firewall logs and signature-driven alerts, which can result in false positives, whereas ExtraHop combines application analysis with behavioral analytics to create high-fidelity alerts. Study participants reported that this helps them identify more threats and automate data gathering. In addition, organizations said they were able to detect and resolve network security issues faster using the ExtraHop solution over alternative approaches.

Commenting on these network security benefits, one study participant said, *"Our network security team is able to look at packets and see errors. With ExtraHop, we're able to identify what those issues are. We haven't reduced our costs, but it increased our reliability score, which is very important to our business."*

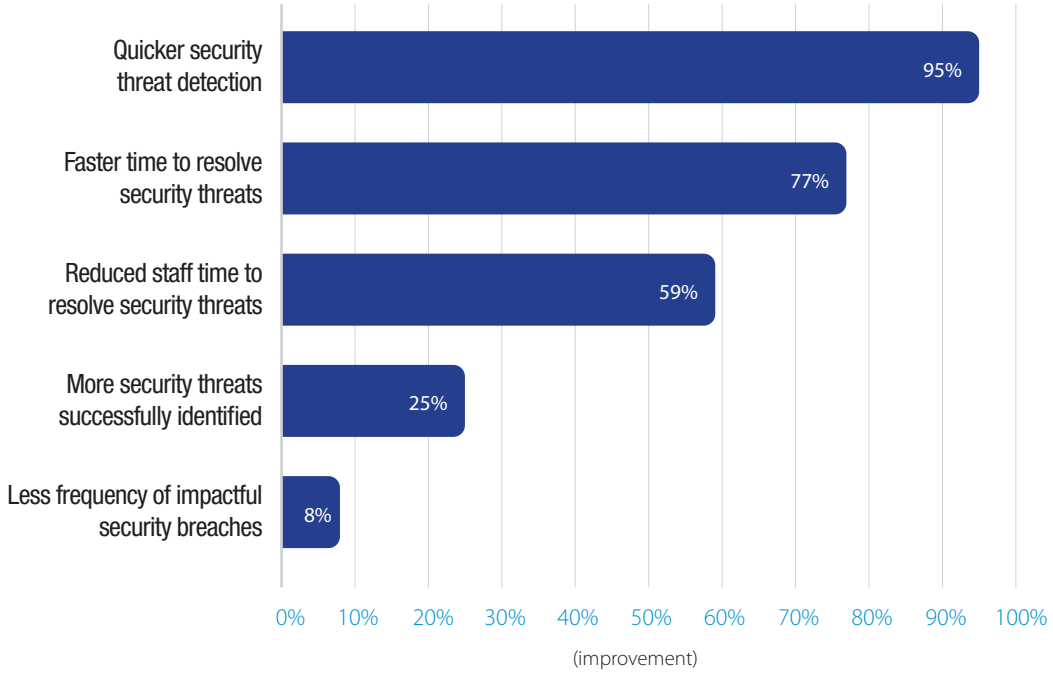
There was a significant level of improvement of 95% on the speed of security threat detection. Threats could also be resolved more quickly (77%), with another significant reduction in the staff time required to resolve them (59%).

Another study participant said, *"ExtraHop hasn't decreased the number of impactful security breaches, but it did help us identify 20% more threats. We use geolocation map functionality, and it identifies where all our traffic comes from so we can analyze it. This helped us be more aggressive in our external geosensing."*

Figure 2 provides a granular breakdown on the security benefits reported by ExtraHop customers. There was a significant level of improvement of 95% on the speed of security threat detection. Threats could also be resolved more quickly (77%), with another significant reduction in the staff time required to resolve them (59%).

FIGURE 2

ExtraHop Impact on Security



Source: IDC, 2018

IDC ANALYZE THE FUTURE

Reduction in Unplanned Downtime Leading to Significant Business Impact

In today's business environments, unplanned downtime is a productivity killer. Study participants spoke to IDC about how ExtraHop's capabilities such as the ability to monitor and address problems within their networks, applications, and security operations via real-time insights has led to the reduced incidence of unplanned downtime.

Table 4 shows the impact of the use of ExtraHop on the incidence of unplanned downtime in terms of restoration times and other key factors. Especially noteworthy is the "hours lost per user" category, which showed a level of improvement of 86%. In addition, IDC calculated that the time required to resolve downtime incidence showed a level of improvement of 73%.

TABLE 4

Unplanned Downtime

	Before ExtraHop	With ExtraHop	Change (%)
Frequency per year	15.4	6.7	56
Time to resolve (hours)	6.1	1.7	73
Hours lost per user	0.88	0.12	86
FTE impact — lost productivity due to unplanned outages	7.1	1	86

n = 10

Source: IDC, 2018

Better overall stability in network and IT operations is leading to two additional benefits for ExtraHop customers. Study participants talked about how their organizations are now able to meet more of their service-level agreement (SLA) requirements for specified LAN, WAN, internet, and enterprise network performance. Table 5 lays out specific levels of improvement in the ability to meet both internal and external requirements.

TABLE 5

SLA Impact (%)

	Before ExtraHop	With ExtraHop	Change (%)
Internal SLAs met	85	97	15
External SLAs met	96	99	3

n = 10

Source: IDC, 2018

"Because we are able to identify issues a lot faster, ExtraHop has elevated the role of the IT team from just purely troubleshooting and monitoring."

"ExtraHop allows us to complete revenue-generating business projects faster because we have more time dedicated to them."

Study participants in some organizations reported that the implementation of ExtraHop allowed them to elevate the role of IT to be more strategic. This can have attendant benefits in terms of revenue impact. Table 6 presents specific improvement metrics on revenue impact. For example, total additional revenue per year was $451,900 on a per-organization basis.

Regarding the ability to move IT operations to be more strategic, one study participant noted, *"Because we are able to identify issues a lot faster, ExtraHop has elevated the role of the IT team from just purely troubleshooting and monitoring."* With respect to working on more revenue-generating projects, another study participant said, *"ExtraHop allows us to complete revenue-generating business projects faster because we have more time dedicated to them."*

TABLE 6

Revenue Impact

	Per Organization	Per 100 Users
Total additional revenue per year	451,900	2,963
Assumed operating margin (%)	15	15
Total recognized revenue per year*	67,785	444

**The IDC model assumes a 15% operating margin for all additional revenue.*

Source: IDC, 2018

Increased IT and Network Team Efficiency

Study participants described how the ExtraHop deployment increased IT operations efficiency by providing a single view of the organization's network, application, and security data. As a result, teams such as cloud, network management, network security, and applications development can work more efficiently. This was enabled by the ability to identify and therefore address issues more proactively through autodiscovery and classification of every transaction, flow, session, device, and asset in the enterprise, from remote branch sites to datacenters to cloud-hosted applications and infrastructure to edge devices. A less tangible but important side benefit was that IT operations and security teams had more confidence in the day-to-day operation of the IT environment and their ability to detect threats within it.

Commenting on the increase in efficiency made possible by being able to resolve issues quickly and proactively through effective troubleshooting, one study participant said, *"We develop our own apps, and the developers have been getting a major error for about a year. We would get a delay or a failure to connect to a database, and no one could figure out why. However, within two hours of installing ExtraHop for a proof of concept, we had an answer and the problem was solved."*

Table 7 provides specific metrics for how ExtraHop has impacted troubleshooting-related tasks. It is noteworthy that with ExtraHop, study participants need an average of 90% less time to identify an issue and a total of 78% less time to troubleshoot an issue.

TABLE 7

Impact on Troubleshooting

	Before ExtraHop	With ExtraHop	Benefit (%)
Number of issues to troubleshoot per week	38	30.1	21
Time to identify issue (hours)	3.5	0.4	90
Total time to troubleshoot issue (hours)	4.9	1.1	78
Troubleshooting staff impact — FTE equivalent per organization per year	2.2	0.8	65

n = 10

Source: IDC, 2018

As shown in Table 8, these benefits also extended to both network management and network security teams. The productivity impacts for both teams in terms of equivalent FTEs were identified as increasing 11% and 9%, respectively. With respect to network teams being able to identify issues more effectively, one study participant said, *"Our network security team is able to look at packets and see errors. Previously, we used an external company to do the scans. They would look at our traffic and tell us we were not meeting certain categories. With ExtraHop, we're able to identify what those issues are. We haven't reduced our costs, but we have increased our reliability score, which is very important to the business."*

"We recently had a networkwide slowdown, and everyone was complaining about speed issues. We turned to ExtraHop and realized we had a DNS server that was having problems. It would have taken us days to find that issue previously, yet within a few minutes we fixed it."

Another study participant commented on the ability to resolve network issues faster, *"We recently had a networkwide slowdown, and everyone was complaining about speed issues. We turned to ExtraHop and realized we had a DNS server that was having problems. It would have taken us days to find that issue previously, yet within a few minutes we fixed it."*

TABLE 8

IT Network Staff Productivity Impact

	Before ExtraHop	With ExtraHop	Benefit(%)
IT network management teams — equivalent FTEs	9.9	8.8	11
IT network security teams — equivalent FTEs	9.7	9	7

n = 10

Source: IDC, 2018

Study participants reported that increased troubleshooting capability helps development teams deliver more value to their organizations, typically measured by the number of new features or releases rolled out along with improvements in development life-cycle times. The customers that IDC spoke with attributed improvements in application development to their deployment of ExtraHop, allowing users and customers to access the advantage of entirely new features and apps and more frequent and timely delivery of updates and enhancements. As shown in Table 9, IDC calculated the relative productivity gain for application development teams at an average level of improvement of 13%.

TABLE 9

IT Network Staff Productivity Impact ($M)

	Before ExtraHop	With ExtraHop	Benefit (%)
Net development teams' productivity impact — equivalent FTEs	16	13.9	13
Value of staff time cost per year per organization	1.6	1.4	13

n = 10

Source: IDC, 2018

ROI Analysis

IDC calculates that over three years, these ExtraHop customers will realize discounted benefits worth an average of $4.88 million per organization by investing an average total of $580,545 per organization. For study participants, this would result in a three-year return on investment (ROI) of 740%.

Table 10 presents IDC's analysis of the financial benefits and costs related to interviewed organizations' use of ExtraHop. IDC calculates that over three years, these ExtraHop customers will realize discounted benefits worth an average of $4.88 million per organization ($31,984 per 100 internal users) by investing an average total of $580,545 per organization ($3,807 per 100 internal users). For study participants, this would result in a three-year return on investment (ROI) of 740% and breakeven on their investment in four months.

TABLE 10

Three-Year ROI Analysis

	Per Organization	Per 100 Users
Benefit (discounted)	$4.9 million	$31,984
Investment (discounted)	$580,000	$3,807
Net present value (NPV)	$4.3 million	$28,177
Return on investment (ROI)	740%	740%
Payback period	Four months	Four months
Discount rate	12%	12%

Source: IDC, 2018

Challenges and Opportunities

ExtraHop operates in a crowded IT and network analytics marketplace. As competitive pressures increase, ExtraHop must continue to differentiate the scope and benefits of its solutions. Key differentiation for ExtraHop comes from its real-time analytics and machine learning, its ability to decrypt SSL/TLS at line rate, the visibility it provides across hybrid environments, and its ability to scale to datacenter speeds up to 100Gbps.

ExtraHop needs to position wire data–based capabilities in the context of other sources including APM metrics and log data, showing the specific benefits that wire data brings to the picture and how these multiple data sources can be used together. Specific partnerships and integrations should be highlighted.

Conclusion

Business success in fast-paced and highly competitive digital business environments depends on responsive, reliable, and secure applications. Solutions for managing, optimizing, and securing network infrastructure and operations, while supporting infrastructure modernization and controlling costs, are essential for meeting critical performance and reliability standards for digital business applications.

ExtraHop's solutions for managing, optimizing, and securing network infrastructure and operations address these requirements and provide measurable benefits, as quantified in this study. The key benefits experienced by ExtraHop customers include improved application and network performance, enhanced security and threat investigation, more proactive IT operations, and increased end-user productivity. The ExtraHop customers surveyed have realized an average return on investment of 740% over three years.

Appendix

IDC's standard ROI methodology was utilized for this study. This methodology is based on gathering data from organizations currently using ExtraHop solutions as the foundation for the model. Based on interviews with these study participants, IDC has calculated the benefits and costs to these organizations of using ExtraHop solutions. IDC used the following three-step method for conducting the ROI analysis:

1. **Gathered quantitative benefit information during the interviews using a before and after assessment of the impact of ExtraHop.** In this study, the benefits included staff time savings and productivity benefits, increased revenue, and operational cost reductions.
2. **Created a complete investment (three-year total cost analysis) profile based on the interviews.** Investments go beyond the initial and annual costs of using ExtraHop and can include additional costs related to migrations, planning, consulting, and staff or user training.
3. **Calculated the ROI and payback period.** IDC conducted a depreciated cash flow analysis of the benefits and investments for the organizations' use of ExtraHop solutions over a three-year period. ROI is the ratio of the net present value (NPV) and the discounted investment. The payback period is the point at which cumulative benefits equal the initial investment.

IDC bases the payback period and ROI calculations on a number of assumptions, which are summarized as follows:

- Time values are multiplied by burdened salary (salary + 28% for benefits and overhead) to quantify efficiency and manager productivity savings. For purposes of this analysis, based on the geographic locations of the interviewed organizations, IDC has used assumptions of an average fully loaded salary of $100,000 per year for IT staff members and an average fully loaded salary of $70,000 for non-IT staff members. IDC assumes that employees work 1,880 hours per year (47 weeks x 40 hours).
- The net present value of the three-year savings is calculated by subtracting the amount that would have been realized by investing the original sum in an instrument yielding a 12% return to allow for the missed opportunity cost. This accounts for both the assumed cost of money and the assumed rate of return.
- Further, because IT solutions require a deployment period, the full benefits of the solution are not available during deployment. To capture this reality, IDC prorates the benefits on a monthly basis and then subtracts the deployment time from the first-year savings.

Note: All numbers in this document may not be exact due to rounding.

IDC Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC
ANALYZE THE FUTURE