The Business Value of Qualys

Megan Szurley
Senior Research Analyst,
Business Value Strategy Practice, IDC

Philip D. Harris, CISSP, CCSK
Research Director,
Risk, Advisory, Management, and Privacy, IDC

Table of Contents

CLICK ANY HEADING TO NAVIGATE DIRECTLY TO THAT PAGE.

Executive Summary

The cybersecurity risk management solutions and services markets are accelerating in growth, and much of it is due to organizations realizing a greater need to understand their overall risk posture and elevate awareness to executive management. Executives and board members are now having to place more emphasis and focus on cybersecurity risks than ever before. Service providers like Qualys are stepping up to the plate with greater capabilities that enable cybersecurity teams to raise the bar on overall risk management across the breadth of the IT estate.

IDC conducted interview-based research that explored the value and benefits for organizations utilizing Qualys Platform for IT, Security and Compliance to achieve a consolidated view for IT and security concerns that enables them to identify, analyze, and respond to threats in real time.

Based on the data attained from the interviewed organizations, IDC calculates that interviewed Qualys customers will achieve business value benefits worth an annual average of $5.1 million ($102,000 per 1,000 internal users) by:

- Boosting the overall efficiency of security teams by enabling them to detect and respond to threats before they become impactful.
- Enabling greater productivity for IT infrastructure, development, and compliance teams.
- Significantly lowering the occurrence of security breaches, application downtime, and compliance-related fines.

Business Value Highlights

Click highlights below to navigate to content within this document.

403%
3-year ROI

$5.1 million
in average annual benefits

$102,000
average annual benefits per 1,000 internal users

5 month
payback period

24%
more efficient security teams

65%
less unplanned application downtime

66%
quicker to resolve events

24%
reduction in the risk of compliance-related fines

Situation Overview

Cybersecurity teams continuously struggle to make certain they are identifying all risks and prioritizing mitigation based upon the most critical risks. Various solutions in the marketplace have their version of prioritization; however, many of these prioritizations do not consider risk in the business context and prioritize remediation based upon the most critical risks to the business.

What's needed is a method by which prioritization considers the information about an asset within a configuration management database (CMDB), how it is categorized or classified, combined with other factors such as misconfiguration, threat landscape, the overall attack surface of the organization, various threat indicators, and whether there's active malware associated with the vulnerabilities. By considering these factors plus more, cybersecurity teams can now be surgical in their efforts to remediate how risks are prioritized in a manner that reduces considerably more risk than by just remediating a bunch of vulnerabilities that may or may not contribute to overall risk reduction.

Qualys Overview

Qualys IT Security and Compliance Cloud Platform

With the current threat landscape cyber risk has become business risk — with risks growing faster than what traditional security tools can manage. Security and IT teams need both a new and complete approach to tackle cyber threats that derive a clear understanding of cybersecurity risks and automate workflows for rapid response.

The Qualys Platform provides a continuous, always-on assessment of an organization's global IT, security, and compliance posture, with two-second visibility across all IT assets in the estate. This platform brings a level of automation, built-in threat prioritization, patching, and other response capabilities, creating a comprehensive end-to-end security solution. QTP is comprised of several integrated modules that by themselves concentrate on specific security functions and when combined provide complete visibility into the risks that enable cybersecurity teams to surgically focus efforts to mitigate as soon as possible. These modules include Asset Management, Vulnerability and Configuration Management, Risk Remediation, Threat Detection and Response, Continuous Compliance, and Cloud Security.

Each of these modules perform specific functionality:

Asset Management.
A risk-based approach to cybersecurity built on a foundation of attack surface management where Security and IT gain both an attackers and defenders view of their environment for complete, 360-degree visibility of assets, asset groups, domains, and subdomains, including end-of-life tracking.

Vulnerability and Configuration Management.
Cyber risk is business risk — with risks growing faster than what traditional VM and SIEM tools can manage. Security and IT teams need a new approach to tackle cyber threats with a clear understanding of cybersecurity risk and automate workflows for rapid response.

Risk Remediation.
Streamline and accelerate vulnerability remediation for all your IT assets.

Threat Detection and Response.
Pinpoint your most critical IT security threats and prioritize patching by prioritizing vulnerability remediation with automated and streamlined analysis.

Compliance.
Simplifies, automates, and improves compliance to reduce audit failures, security breaches, and lawsuits through policy compliance and file integrity monitoring.

Cloud Security.
Discover, Assess, Prioritize, Defend, and Remediate vulnerabilities, threats, and misconfigurations across a multicloud environment.

The Business Value of Qualys

Study Firmographics

IDC conducted primary research that explored the cost, value, and benefits for organizations using Qualys to protect their applications and assets at scale. In total, eight organizations were interviewed that had robust experience and knowledge about the costs and benefits attained in their deployment and usage of Qualys. During the interviews, study participants were asked a wide variety of quantitative and qualitative questions about the impact of Qualys on their security operations, overall business, and costs.

Table 1 (next page) presents study firmographics. Companies ranging from 750 to 400,000 employees were included in the research initiative (average 63,319 in total). Those interviewed had a total of 1,230 business applications that were supported by 1,047 IT staff and 144 security staff. An array of countries were represented in the study, including the United States (5), Australia (2), and the United Kingdom. There was also a variety of vertical markets which were represented including the healthcare (4), education (2), insurance, and financial services sectors.

TABLE 1

Firmographics of Interviewed Organizations

Firmographics	Average	Median	Range
Number of employees	63,319	3,550	750–400,000
Number of IT staff	1,047	550	38–4,000
Number of security staff	144	50	2–500
Number of total employees using information systems for job	50,481	3,050	750–300,000
Number of customers/ external users	3.2M	17,500	25M–34M
Number of business applications	1,230	213	15–5,000
Annual revenue	$31.1B	$4.6B	$136.0M–$156.0B
Countries	United States (5), Australia (2), United Kingdom		
Industries	Healthcare (4), education (2), insurance, financial services		

n = 8, Source: IDC Business Value In-Depth Interviews, August 2023

Choice and Use of Qualys

The organizations interviewed by IDC discussed in detail their rationale for selecting Qualys. Overall, the organizations looked to Qualys to provide better support when discovering assets and accessing their vulnerability than their previous solution. Qualys also met their selection criteria because the platform proved to be both highly reliable and scalable. Importantly, Qualys also provided participants with high-quality, very functional modules, which would increase their security capabilities through greater automation. Participants also felt that this highly functional platform provided the needed features and functions at a reasonable price point.

Study participants elaborated on these benefits below:

Increased reliability for vulnerability assessment:

"We deployed Qualys as a replacement for a vulnerability assessment solution that we had already been using for some period of time. We were already doing vulnerability assessments, and that tool got acquired and became less reliable and useful, and so we did a new solution. Qualys was acquired as a replacement for that existing solution."

Better technology stack vulnerability discovery support:

"When my organization first selected Qualys, the first requirement of the solution was that we needed support to discover vulnerability across the stack of technology. We also wanted to do that discovery continuously. At the time that we were looking for solutions, Qualys had this unique ability."

To support cyber essentials accreditation:

"In the UK, we have something which is called "cyber essentials", this is a standard from the government. In order to get government funding, we need to be 'cyber essentials' accredited. We have been working for the last two years on cyber essentials and Qualys has been part of making sure that all of our assets have a supportive operating system."

Ability to scale effectively:

"Qualys got selected because it could scale. Scaling is a problem for everything we deploy. We tested a competitor, and it failed, it actually brought down our network during the pilot."

Price-sensitive platform with modules:

"The price of Qualys was one of the biggest attractions. My organization also liked the abilities of the various modules which Qualys has. My organization wanted to extend our information security practice, and our use of Qualys modules gives us a very good opportunity to do this with fewer investment dollars. It was easier to expand. That was the biggest factor against other strong competitors — at that time, they didn't have modules."

Table 2 (next page) describes the organizational usage of Qualys for study participants at the time of interviews. As shown, Qualys supported 58 branches, 50,400 internal users, and 1,213 business applications. On average, interviewed organizations stated that Qualys was tied to 76% or their total revenue and 3 million external users. Additional metrics are presented in the table.

TABLE 2

Organizational Usage of Qualys

	Average	Median
Branches	58	9
Campuses	8	6
Internal users	50,400	3,050
External users	3M	513
Business applications	1,213	113
Percentage of total revenue	76%	88%

n = 8, Source: IDC Business Value In-Depth Interviews, August 2023

Business Value and Quantified Benefits

Interviewed organizations confirmed that Qualys had a positive impact on their security and business operations. After adoption, these organizations found that the Qualys platform had exceedingly functional modules and automated once highly manual tasks. This created efficiencies for several functional areas like security, infrastructure management, development, and compliance teams. Importantly, these organizations also benefited from a consolidated approach to managing and accessing the risk of applications and other assets. They gained greater visibility of their assets, better control when remediating risk, and were able to maintain their reputation through better compliance.

When asked, interviewed organizations found that Qualys had the most significant impact on visibility, discoverability, and prioritization.

Study participants offered these comments about Qualys' most significant benefits:

Better asset visibility:

"Qualys has been very instrumental in having visibility of the assets, which are supported, and which are not supported. For those which are not supported, Qualys helps make sure

that we have controls to remediate those legacy assets by upgrading, disconnecting those from the network. We have increased our use of Qualys by deepening the Qualys agent into an asset, giving us that visibility to be able to improve our work-security posture."

Asset discovery and threat response:
"The two biggest benefits of Qualys are that it increased our ability to perform asset discovery and improves threat response."

Increased visibility and compliance:
"The largest benefits of Qualys are the increased visibility of our vulnerabilities and compliance to security requirements."

Better information prioritization:
"Qualys has impacted our response to information. It categorizes things in a way that's solution oriented. It helps us prioritize."

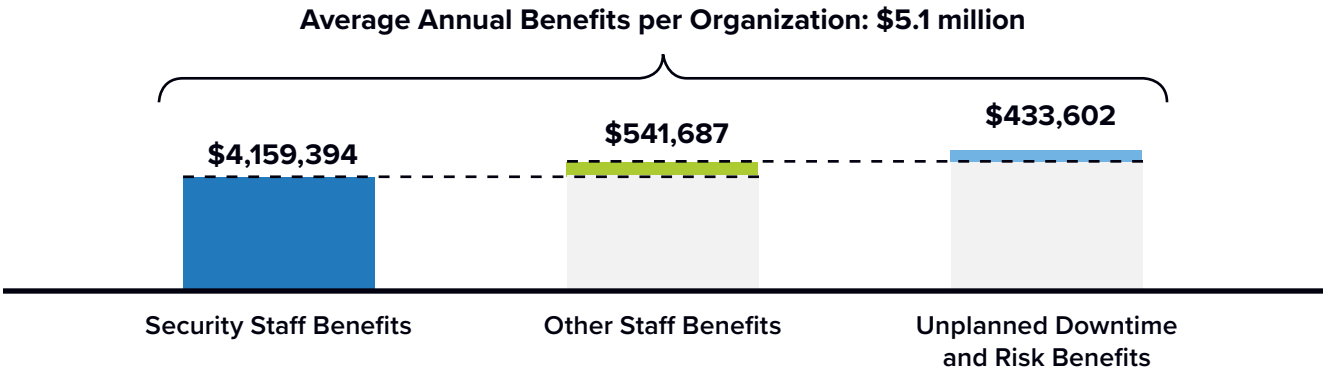
Ability to maintain information security reputation:
"The most significant benefit of Qualys is that it gives us the ability to maintain our information security reputation, internally and externally."

Figure 1 showcases IDC's calculations of benefits achieved by interviewed organizations after the adoption of Qualys, factoring in deployment time. Average annual benefits were quantified at $5.1 million per organization, or $102,000 per 1,000 internal users. As shown, Qualys had a tremendous impact on the security operations of interviewed organizations, but also impacted line-of-business users and risk management. The figure breaks out the three areas of benefits attained from deployment of Qualys in greater detail.

FIGURE 1

Average Annual Benefits per Organization

($ per organization)



n = 8, Source: IDC Business Value In-Depth Interviews, August 2023

For an accessible version of the data in this figure, see Figure 1 Supplemental Data in Appendix 2.

Risk Reduction Impact of Qualys

Enterprises today face an ever-changing and challenging ecosystem of risk and threats. Organizations must do everything in their power to minimize unplanned downtime, stay compliant within industry regulations, and be resilient. More importantly, interviewed organizations reported that Qualys aided in overall risk reduction. The platform helped not only decrease the amount of unplanned application downtime occurrence at interviewed organizations, but also decreased the impact on application end users. Qualys also greatly reduced their risk of compliance-related fines and helped maintain their overall outward-facing reputation.

Study participants explained in greater detail about how Qualys helped their organization manage risk:

Reduced risk of cyber incidents:

"Qualys has reduced the risk and impact of a cyber incident. It has improved our security posture, given better confidence to our board, and protected the university brand."

Increased breach prevention:

"A big benefit of Qualys is that it is contributing to breach prevention and the protection of patient health information."

Better prepared for cyberattacks

"The change of the threat landscape and increased number of attacks, has raised awareness about Qualys to our board. Qualys has given us visibility of vulnerabilities and the assets we have. We've been able to put plans in place to better respond to risks and to improve our security posture. This has reduced the level of risk to the university, and we hope that, should we have a cyberattack, the impact is going to be less."

Ability to assess risk tolerance:

"Qualys hasn't impacted our exposure, but it's impacted our understanding and quantification of risk. Vulnerabilities were present before, now we know what they are and can quantify them better. Qualys gives an "at-risk" score for assets, so I can show exactly how many assets we have at each risk score. We have a tolerance level that the board is willing to accept around asset scores, and anything above that tolerance level we must go and fix. So, we have increased transparency to risk, guidance on how to address the risk. Those two factors are allowing us to have better communication with management informed by how much risk the company is under and what the tolerance is."

Identification of unknown assets and risks:

"Qualys helps us identify our unknown risks and assets. It has allowed us to identify and focus on vulnerabilities in our environment that need to be corrected to reduce risk."

Less susceptible to vulnerabilities:

"Qualys keeps our systems more up to date and less susceptible to vulnerabilities."

IDC noted that Qualys drastically reduced the frequency of unplanned application downtime /outages/breaches from occurring, while also improving the time it takes to resolve a breach. This enabled greater end-user productivity levels and better business-critical application availability. **Table 3** quantifies the reduction in unplanned downtime. The annual frequency of unplanned downtime was reduced by 65%. In addition, when an event did occur, they were remediated 66% faster. These two areas combined for a reduction in staff productivity loss per year of 88% and amounted to an average annual value of $228,173 per organization. This potentially offers organizations the ability to redeploy critical staff to focus on other priorities requiring attention.

TABLE 3

Unplanned Application Downtime/Security Breach Impact

	Before Qualys	With Qualys	Benefit	Benefit
Number of outages per year	60.0	21.0	39.0	65%
MTTR, hours	6.7	2.3	4.5	66%
Users impacted by downtime	28.8	28.8	–	–
Percentage of productivity loss	60%	60%	–	–
Total FTE loss in productivity per year	3.7	0.4	3.3	88%
Value of lost productive time per year	$258,521	$30,348	$228,173	88%

n = 8, Source: IDC Business Value In-Depth Interviews, August 2023

Security Staff Benefits from Qualys

There is ever-increasing pressure on security teams to work effectively at managing organizational risk. They are responsible for many functions, including but not limited to preventing discovering, prioritizing, and mitigating threats. The Qualys Platform was designed in a manner to help security teams achieve a singular look at risk, scale with need, automate once manual tasks, and maintain their trustworthy reputation.

Study participants discussed the various operational benefits of their security staff achieved from their Qualys usage. They greatly appreciated that Qualys helped increase the bandwidth of their security team through the use of modules, like automated patch management. Qualys was also successful at scanning, and did so with greater frequency than previous solutions, enabling interviewed organizations to respond to threats before they became impactful. The platform also provided greater visibility into vulnerabilities because it became their singular risk management platform.

Study participants elaborated on these security staff benefits below:

Use of patch management module to increase bandwidth:

"By using the Qualys patch management module, we have been able to increase the bandwidth of our security operations team. Previously they were maxed out with other things, because during the global pandemic we have increased the number of devices while the number of staff has remained the same. We have been able to scale and maintain a good security posture by using the Qualys platform. We always have real-time visibility of assets; this is a huge impact."

Automated patch management:

"Qualys is monitoring existing and new assets and automatically applying patches to those assets where the patches are missing. That's a big relief on the operations team. Qualys also applies patches to applications that we don't necessarily support, but applications that we tolerate."

Ability to act and respond with speed:

"Qualys gives us the ability to scan more frequently, which ultimately gives helps us act and respond to issues quicker."

Enhanced vulnerability scanning:

"We use Qualys to enhance our breadth of scanning. We scan more assets, but have also increased the depth of scanning, so we're discovering more stuff. Over the past few years, there's been a constant growth in the vulnerabilities my team is discovering because we have better tools. The team is accountable and has a KPI to discover more."

Singular view of vulnerabilities:

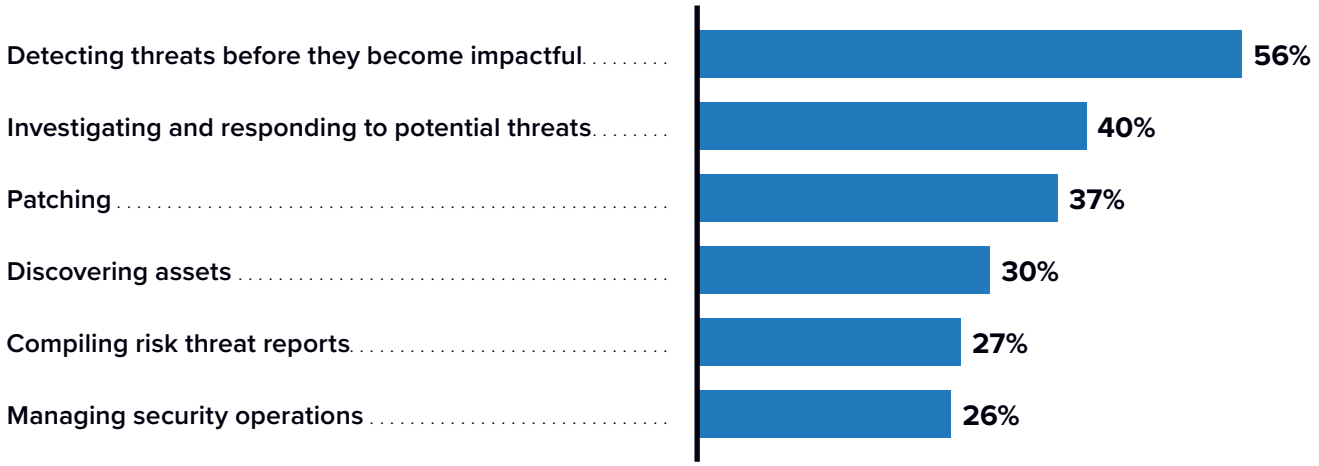
"We can see all our shortcomings through one dashboard. Instead of using two or three different dashboards which we must compare to each other, now we get the majority through one."

Figure 2 (next page) illustrates the key performance indicators (KPIs) that security teams achieved in using Qualys. Interviewed organizations made it abundantly clear that Qualys increased the effectiveness of the team in a significant manner, especially regarding threat detection, investigation, and patching.

FIGURE 2

Security Team KPIs

(% more effective)



n = 9, Source: IDC Business Value In-Depth Interviews, August 2023

Keeping in mind the discussion and KPIs above, **Table 4** further quantifies these benefits in terms of the efficiency gains achieved by the security team of interviewed organizations. As shown, interviewed companies avoided hiring 11.1 FTEs because of the simplification and automation provided by Qualys. This is incredibly impactful given talent shortages. Factoring in this hiring avoidance and their overall ability to work with greater speed, the IT security team saw an overall 24% efficiency gain. This resulted in an average value of staff time per year of $4.6 million for each organization.

TABLE 4

Security Team Efficiency Gain

	Before Qualys	With Qualys	Benefit	Benefit
Total FTE count	178.9	143.6	35.3	20%
Hiring avoidance	11.1	–	–	–
Adjusted FTE	190.0	143.6	46.4	24%
Value of staff time per year	**$19.0M**	**$14.4M**	**$4.6M**	**24%**

n = 8, Source: IDC Business Value In-Depth Interviews, August 2023

Line-of-Business Impact of Qualys

IDC then evaluated the impact of Qualys on the key operational areas of infrastructure management, development, and compliance. Qualys broke down organizational silos and became a singular repository tool for security and operations teams to review and look at data. There was no longer debate surrounding risk management in the various groups, as information and modules were consolidated into one platform. This created greater consistency in their approach to risk management.

Study participants discussed these benefits and more below:

Decreased organizational silos:

"Qualys has reduced overhead for security and operations teams. The benefit is, we all look at the same data and use the same tool. That reduces the amount of debate we have. There are efficiencies in access and maintenance, we can grant access to individuals to various modules. It makes it easier to maintain."

Consistent organizational view of assets:

"We have that many assets covered. Qualys gives every facility a consistent view in to where they're vulnerable. In a big organization, that's a big deal. It keeps people from having to have 16 different ways of doing it."

Easier data access:

"Qualys has helped in that there were multiple, disparate systems before. While those systems are not gone, it is now easier to access data."

Saves employee time without sacrificing security:

"Qualys helps us secure our environment, know our assets, and resolve issues quickly. It ultimately saved our employees' time and helped us be more secure at the same time."

First, IDC evaluated the impact of Qualys on IT infrastructure teams within the interviewed organizations. This team gained efficiency from the singular, consolidated view of assets and data provided by Qualys. In using the same tool as the security team, the silo between the two teams evaporated. They benefited from having access to the same data regarding their IT assets. Interviewed companies saw a 4% efficiency gain in the work performed by their IT infrastructure teams. This resulted in an average annual value of staff time of $295,313 for each organization.

IDC then looked at the impact of Qualys on developers within interviewed organizations. As with the IT infrastructure team, developers benefited from having a consolidated applications control center within the Qualys platform. Qualys also provided tighter applications integrations, which ultimately increased the effectiveness of the team. As a direct result of using Qualys, developers were able to work with the productivity of two additional FTEs, a 3% productivity gain. IDC valued this benefit at $200,893 per year.

Compliance teams also derived benefits from the deployment of Qualys within their organization. Study participants reported that this team was more efficient at demonstrating compliance and meeting regulatory demands (HIPPA, GDPR, PCI, etc.) as a result of the vulnerability management provided by Qualys. This team saw a 7% productivity improvement that resulted in an average annual business value of $47,578 for each organization.

IDC also noted that interviewed organizations were able to reduce their risk of compliance-related fines on an annual basis (see **Table 6**, page 18). As a result of being more compliant with industry regulations, interviewed organizations were able to reduce their risk of fines by a significant 24%. This amounted to an annual compliance fine cost avoidance of $255,313.

ROI Summary

Table 5 presents IDC's return on investment and analysis for study participants' use of Qualys. IDC calculated that these companies achieved three-year discounted benefits worth an average of $12,169,200 per organization through more efficient staff performance and the reduction of risk. These benefits compare with total three-year discounted costs of $2,419,500 per organization. These levels of benefits and investment costs resulted in an average three-year ROI of 403% and a payback of five months.

TABLE 5

3-Year ROI Analysis

	Per Organization	Per 1,000 Internal Users
Discounted Benefits	$12.2M	$241,452
Discounted Investment	$2.4M	$48,006
Net present value (NPV)	$9.7M	$193,446
ROI	403%	403%
Payback	5 months	5 months
Discount Factor	12%	12%

n = 8, Source: IDC Business Value In-Depth Interviews, August 2023

Challenges/Opportunities

This study represents an opportunity for Qualys to demonstrate the depth and breadth of their offerings, especially the capabilities beyond their vulnerability management solution. Qualys has been steadily creating new offerings, like asset management, cloud security, patch management, and compliance that enable customers to expand their vulnerability management programs to include overall cyber risk management. Qualys has a series of modules that capitalize upon each other, creating a continuous integrated risk management offering that exposes risks across the enterprise IT estate and empowers cybersecurity and IT teams to mitigate and reduce these risks.

The current challenge is for Qualys to expose the market to their complete offerings in the risk management space that enables organizations to have a complete risk management platform and the ability to report to executive management the current risk posture at any requested point in time.

Conclusion

Executives and board members must place emphasis and focus on cybersecurity risks more now than ever before. Compounding the current frustrations, cybersecurity teams still struggle to make certain they identify, prioritize, and mitigate these risks based upon criticality. While there are various solutions in the marketplace, many have their own version of prioritization, and many of these prioritizations do not consider the business context of these risks and prioritize based upon the most critical risks to the business. Service providers like Qualys are stepping up to the plate with greater capabilities that enable cybersecurity teams to raise the bar on overall risk management across the breadth of the IT estate.

Appendix 1: Methodology

IDC's standard ROI methodology was utilized for this project. This methodology is based on gathering data from current users of Qualys as the foundation for the model.

Based on interviews with organizations using Qualys, IDC performed a three-step process to calculate the ROI and payback period:

1. **Gathered quantitative benefit information during the interviews using a before-and-after assessment of the impact of Qualys.** In this study, the benefits included IT cost reductions and avoidances, staff time savings and productivity benefits, and revenue gains.
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 Qualys 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 Qualys 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 productivity savings. For the purposes of this analysis, IDC has used assumptions of an average fully loaded $100,000 per year salary 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 Qualys requires 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.

Appendix 2: Additional ROI Metrics Calculated

TABLE 6

Annual Compliance Fine Avoidance

	Qualys Impact	Per 1,000 Internal Users
Annual cost of compliance-related fines	$1.0M	$21,329
Reduction in risk of compliance-related fines with Qualys	24%	24%
Total compliance-related fine cost avoidance	**$255,313**	**$5,066**

n = 8, Source: IDC Business Value In-Depth Interviews, August 2023

TABLE 7

IT Infrastructure Team Efficiency Gain

	Before Qualys	With Qualys	Benefit	Benefit
Total FTE count	78.8	75.8	3.0	4%
Value of staff time per year	$7.9M	$7.9M	$295,313	4%

n = 8, Source: IDC Business Value In-Depth Interviews, August 2023

TABLE 8

Development Team Productivity Gain

	Before Qualys	With Qualys	Benefit	Benefit
Equivalent productivity level, FTEs	64.3	66.3	2.0	3%
Value of staff time per year	$6.4M	$6.6M	$200,893	3%

n = 8, Source: IDC Business Value In-Depth Interviews, August 2023

TABLE 9

Compliance Team Productivity Gain

	Before Qualys	With Qualys	Benefit	Benefit
Equivalent productivity level, FTEs	21.0	22.5	1.5	7%
Value of staff time per year	$1.5M	$1.6M	$107,800	7%

n = 8, Source: IDC Business Value In-Depth Interviews, August 2023

Appendix 3: Supplemental Data

This appendix provides an accessible version of the data for the complex figure in this document. Click "Return to original figure" below the table to get back to the original data figure.

FIGURE 1 SUPPLEMENTAL DATA

Compliance Team Productivity Gain

	Security Staff Benefit	Other Staff Benefits	Unplanned Downtime and Risk Benefits
Per Organization	$4.2 million	$541,687	$433,602
Average Annual Benefits per Organization		**$5.1M**	

n = 8, Source: IDC Business Value In-Depth Interviews, August 2023

Return to original figure

About the IDC Analysts

Philip D. Harris, CISSP, CCSK

Research Director, Risk, Advisory, Management, and Privacy, IDC

Phil Harris is the Research Director for Risk, Advisory, Management, and Privacy (RAMP). He is responsible for developing and socializing IDC's point of view on risk, advisory, and privacy services, including surrounding as governance and compliance with enterprises, IT suppliers, and service providers. Phil develops research on business strategies, and the impact of relevant service offerings on enterprises. Phil also works with other worldwide and regional analysts to develop a holistic set of thought leadership and actionable research for IT buyers and suppliers. Phil's primary focus is advising technology-based clients on business strategies related to their investment in risk, privacy, governance, and compliance advisory and management services.

More about Philip D. Harris

Megan Szurley

Senior Research Analyst, Business Value Strategy Practice, IDC

Megan Szurley is a senior research analyst for the Business Value Strategy Practice, responsible for creating custom business value research that determines return on investment (ROI) and cost savings for enterprise technology products. Megan's research focuses on the financial and operational impact of these products for organizations once deployed and in production. Prior to joining the Business Value Strategy Practice, Megan was a consulting manager within IDC's Custom Solutions division, delivering consultative support across every stage of the business life cycle: business planning and budgeting, sales and marketing, and performance measurement. In her position, Megan partners with IDC analyst teams to support deliverables that focus on thought leadership, business value, custom analytics, buyer behavior, and content marketing. These customized deliverables are often derived from primary research and yield content marketing, market models, and customer insights.

More about Megan Szurley

IDC Custom Solutions

IDC Research, Inc.
140 Kendrick Street, Building B, Needham, MA 02494, USA
T +1 508 872 8200

@idc @idc idc.com

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. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.