Business Value White Paper, sponsored by Zscaler
APRIL 2023

REGION FOCUS: WORLDWIDE

The Business Value of Zscaler Data Protection

Christopher Rodriguez
Research Director,
Security & Trust, IDC

Matthew Marden
Research Vice President,
Business Value Strategy Practice, IDC

Table of Contents

CLICK BELOW TO NAVIGATE TO EACH SECTION IN THIS DOCUMENT.

Executive Summary

Businesses are embracing digital transformation to navigate the challenges of economic uncertainty, leveraging new technologies to improve productivity and speed to market. While these new technologies offer efficiencies over legacy systems, they may also introduce new attack vectors and vulnerabilities that increase business risk. Meanwhile, cybercriminals remain persistent in their efforts to compromise defenses, wreak havoc, and steal valuable data.

As a result, security requirements continue to expand each year, straining budgets and overtaxing IT organizations. Yet the importance of a strong cybersecurity practice is widely underestimated. Numerous high-profile data breaches and ransomware attacks have driven a propensity to view the topic through a narrow lens, including a hyperfixation on the avoidance a few specific negative outcomes. Unfortunately, this approach provides an incomplete picture of the value of cybersecurity in the modern era of digital business.

IDC interviewed organizations using Zscaler Data Protection to understand its impact on their efforts to minimize risk related to data loss and other security events across their hybrid IT environments. Study participants linked their use of Zscaler Data Protection to an improved ability to proactively identify and resolve security-related risks in terms of both business outcomes and operational efficiencies.

Overall, IDC calculates that interviewed Zscaler customers will achieve benefits worth an annual average of $2.19 million per organization ($86,100 per 1,000 users) by:

- **Reducing the direct costs of security breaches and other data-related incidents** through much-improved identification and resolution
- **Ensuring robust access to applications and services with fewer interruptions,** thereby increasing employee productivity levels and ensuring high-quality customer digital experiences
- **Supporting development activities** by ensuring uncompromised security as IT extends to match business needs
- **Generating operational efficiencies** in terms of the staff time required to secure and support hybrid IT environments and direct costs related to security and data loss prevention solutions

Business Value Highlights

Click each highlight below to navigate to related content within this document.

385%
three-year ROI

8 months
to payback

173%
more data-related security incidents proactively identified

27%
faster to resolve data loss

14%
reduced risk of major data-related security incidents

37%
faster to scale to new environments

22%
more efficient IT infrastructure teams

Situation Overview

The cyberthreat landscape continues to escalate with each passing year. Ransomware is a top-of-mind concern, as IDC research shows that businesses paid substantially steeper ransom payments in 2022, increasing 144% on average in North America, from $145,000 in December 2021 to $354,000 in August 2022 (source: IDC's *Future Enterprise Resiliency and Spending Survey, Wave 7,* August 2022, n = 260). Threat actors also employ more stealthy tactics to quietly steal valuable customer data, irreplaceable intellectual property, and the most sensitive proprietary data they can find.

The cybersecurity challenge is further hampered by evolving IT environments. Business leaders are eagerly embracing technological advancements and flexible business practices such as cloud services and hybrid work. These initiatives ultimately deliver improved customer experiences, worker productivity, cost efficiencies, and business agility. Unfortunately, emerging technologies and related business practices also introduce unexpected vulnerabilities and new threat vectors.

The increasing prevalence of data breaches has driven a steady expansion of cybersecurity regulatory requirements meant to protect consumer data, critical infrastructure, and state secrets. Regulations such as GDPR, HIPAA, and PCI require businesses to implement specific data protection practices to protect customer data and include auditing and penalties for noncompliance. Furthermore, several state and federal laws in the United States have been enacted that require public reporting of data breaches affecting consumers or critical infrastructure.

Given the growing attack surface, a harrowing threat landscape, and tightening compliance requirements, cybersecurity has proven to be an arduous process fraught with complexity and technical challenges. While these concerns are all understandable and worthy of top prioritization, the value of a strong security posture must be viewed through a holistic lens. For example, when organizations were asked to identify the top barriers to participation in industry ecosystems, IP protection and cybersecurity concerns (11.3%) and regulatory compliance concerns (10.8%) were the second and third leading answers (source: IDC's *Future Enterprise Resiliency and Spending Survey, Wave 9,* October 2021, n = 800). Ultimately, cybersecurity weakness must be understood as a business hindrance, and a strong security posture is gaining recognition as a business enabler.

Zscaler Data Protection

Zscaler Data Protection (DP) is a cloud-delivered security service that implements access controls, threat detection engines, and policy enforcement to protect sensitive data from theft, destruction, or other compromise. Combined with an endpoint client and endpoint DP, Zscaler Data Protection leverages an advanced security analytics engine for data classification and discovery, dynamically and without static rules. The approach offers security visibility about data usage, enforces policies to protect data from unapproved access, prevents risky or suspicious user behavior, and blocks sophisticated attempts at data theft.

Zscaler Data Protection includes advanced features such as exact data match and indexed data match to identify specific data sets or sensitive forms, and optical character recognition to recognize data in images. Depending on the deployment type, Zscaler Data Protection can also detect historical policy violations and enforce retroactive remediations when necessary. Importantly, the solution is designed to simplify the compliance process, with streamlined reporting options.

Zscaler Data Protection is offered as a subscription service and can be added on to Zscaler enterprise security offerings, including Zscaler Private Access (ZPA) and Zscaler Internet Access (ZIA). As such, the Zscaler Data Protection solution can leverage existing architectural components including endpoints agents, points of presence, and APIs to monitor data access and usage. This approach also offers a consistent protection experience across on-premises, remote access, and cloud infrastructure-as-a-service environments. In 2022, Zscaler extended cloud DP protections for data on endpoints as well as data shared via email, resulting in a unified DP security posture across software as a service (SaaS), email, private applications, web and SaaS applications, and endpoint.

The Business Value of Zscaler Data Protection

Study Demographics

IDC conducted in-depth interviews with IT managers and decision makers to assess the impact of using Zscaler Data Protection. The interviews sought to understand both the quantitative and qualitative impact of using Zscaler Data Protection in areas such as data-related risk, data and application availability, IT staff activities, and security-related costs.

Table 1 presents the averages and medians for interviewed Zscaler customers in terms of organizational attributes. As shown, they operate at an enterprise level, with 33,257 employees and annual revenue of $7.79 billion on average (medians of 12,000 employees and $5.89 billion in revenue). These organizations were based in North America and Asia/Pacific and offered the experiences of various industry verticals, including the financial services, consumer, healthcare, IT infrastructure provider, software-as-a-service, and travel and leisure sectors.

TABLE 1

Demographics of Interviewed Organizations

	Average	Median
Number of employees	33,257	12,000
Number of IT staff	3,751	300
Number of business applications	1,019	350
Revenue per year	$7.79B	$5.89B
Countries	United States (5), Australia, Hong Kong	
Industries	Financial services (2), consumer, healthcare, IT infrastructure provider, SaaS, travel and leisure	

n = 7; Source: IDC Business Value in-depth interviews, March 2023

Choice and Use of Zscaler Data Protection

Study participants described choosing to use Zscaler Data Protection after concluding that they faced specific challenges related to securing data flowing across their organizations that they could not fully address with existing security infrastructures. In particular, changing patterns of access to and use of data in terms of user location and means of access created new risk related to data loss or breaches. They realized that they needed a solution that ensured robust protection regardless of how and when their employees accessed data and their IT systems.

Interviewed Zscaler customers detailed their considerations and the capabilities of Zscaler Data Protection that drove their purchase decisions:

Providing security for all types of employees and ensuring robust regulatory compliance:

"We were looking for a solution to help protect our employees not just when they are in the office but when they are outside the office. We looked at Zscaler Data Protection to be able to protect both in the office and outside the office. Another key piece is that Zscaler Data Protection catches any credit card information or PII (personally identifiable information) *information being sent out."*

Selection based on features and capabilities:

"When we chose Zscaler Data Protection, it was based on the features and capabilities of the tool, for example, the SSL inspection — not just blocking the site but also basically inspects the traffic and offers geography blocking."

Enhanced capabilities that reduce risk exposure:

"Zscaler Data Protection brings capabilities that [our previous solution] didn't have. Our off-network policy set can be the same as on-network with Zscaler and we couldn't do that with [our previous solution]. If we had stayed with our [previous solution], we would have had greater risk exposure."

Cloud-based solution meeting the needs of a growing and distributed business:

"We have a very distributed workforce, and having a cloud-based solution with Zscaler Data Protection allows us to ensure we're protecting employees regardless of where they are in the world. … Our big driver with Zscaler Data Protection is consolidation of data assets."

Study participants reported that they are using Zscaler Data Protection to protect most of their business activities, as shown in **Table 2** (next page). In addition to using it for most business applications (806 on average) accessed by an average of 25,400 employees, they rely on Zscaler Data Protection for its functionality across their distributed business operations that include an average of 75 sites/branches and four cloud availability zones.

TABLE 2

Use of Zscaler Data Protection by Study Participants

	Average	Median
Number of business applications supported	806	100
Number of cloud availability zones	4	4
Number of sites/branches supported	75	6
Number of cloud-based VMs/VIs	292	50
Number of users of applications	25,400	12,000

n = 7; Source: IDC Business Value in-depth interviews, March 2023

Business Value Results

Study participants reported that Zscaler Data Protection allows them to more efficiently and robustly secure their hybrid IT environments. With Zscaler Data Protection, they can ensure robust inspection of traffic regardless of location or time and have minimized risk related to security breaches and data loss. As a result, interviewed Zscaler customers have improved employee productivity levels and business results while optimizing staff time requirements and tool costs.

They spoke about how they have benefited from using Zscaler Data Protection:

Ability to minimize data loss and block the use of unsanctioned applications:

"There's a huge risk with data loss through use of unsanctioned applications, and Zscaler Data Protection has given us the ability to block applications and repositories to which people submit data. .... In terms of unsanctioned apps, we are currently blocking about 25 unsanctioned apps with Zscaler Data Protection."

Strong inspection capabilities regardless of access location:

"Zscaler Data Protection allows us to inspect any traffic regardless of location because all the traffic goes through Zscaler, and it's very seamless in terms of the rules that we apply and if anyone is violating it, we get the same kind of message, whether they are at home or they are using one of the computers onsite."

Ensuring security for hybrid environment:

"We have adopted a more hybrid approach with Zscaler Data Protection, which has helped significantly in terms of risk because we were previously challenged by not having a clear understanding of our traditional datacenter infrastructure."

IDC's analysis shows that study participants are realizing benefits with Zscaler Data Protection in terms of business results and risk minimization, as well as IT staff and cost efficiencies.

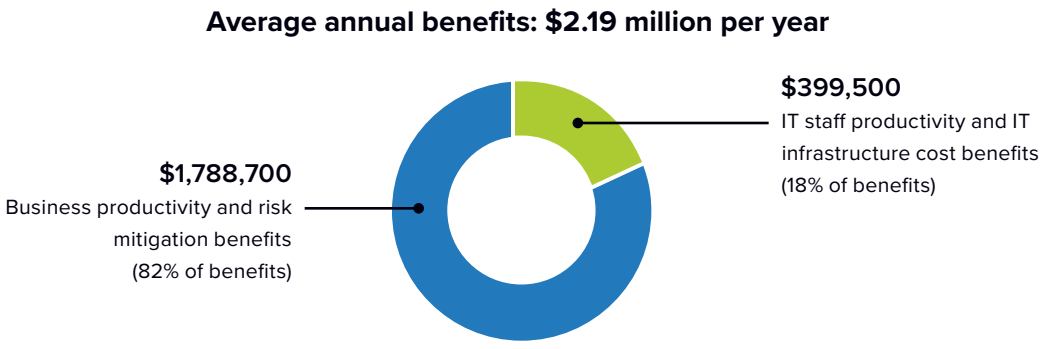
In total, IDC calculates that they will see benefits worth an annual average of $2.19 million per organization ($86,100 per 1,000 users) in the following areas (see Figure 1):

- **Business productivity and risk mitigation benefits:** By ensuring robust and secure access to business applications and reducing the impact of data-related loss and problems, study participants reduce losses associated with data-related business interruptions. IDC projects that these benefits in higher user productivity, increased revenue, and lower direct costs of security issues constitute around four fifths of the total benefits and will be worth an annual average of $1.79 million per organization ($70,400 per 1,000 users).
- **IT staff productivity and IT infrastructure cost reduction benefits:** By reducing the amount of manual inspection required, minimizing problems to be addressed, and providing enhanced data loss and security functionality with a cloud-based solution, study participants free up staff time and optimize tool- and solution-related costs. IDC projects that they will realize IT staff efficiencies and cost savings worth an annual average $399,500 per organization ($15,700 per 1,000 users).

FIGURE 1

Average Annual Benefits per Organization

($ per organization)



n = 7; Source: IDC Business Value in-depth interviews, March 2023

Improved Traffic Inspection and Threat Detection Capabilities to Minimize Risk

Study participants chose to implement Zscaler Data Protection in large part because they realized they needed to better inspect traffic and prevent data-related security issues from occurring across their operations. They acknowledged that they struggled to keep up with growing data and network traffic volumes and changing user access patterns. As a result, they found it challenging to minimize risk associated with data-related loss or breaches.

Interviewed Zscaler customers reported using the solution for significant volumes of data crossing their networks on a daily basis:

- **Daily transaction volumes** of 10.62 million on average (5.0 million median), with average growth to volumes with Zscaler of more than three times (220%)
- **Amount of data scanned** of an average of 12,505PB (median of 10.2PB), with Zscaler scanning an average of 367% more volume than interviewed organizations could previously scan (200% more by median)

Interviewed Zscaler customers linked use to improvements in their capabilities around monitoring and inspecting traffic and proactive identification of data-related anomalies or threats. With Zscaler Data Protection, they know that security policies will be applied consistently regardless of how data is accessed (e.g., onsite or remote, online or offline, in flight or at rest). This reduces their security threat exposure, especially as their employees access important business applications and organizational networks from more locations and in more situations. Further, they connected their ability to inspect a higher percentage of traffic to their use of Zscaler Data Protection, even as their traffic continues to grow rapidly.

Interviewed Zscaler customers provided examples of improvements in these areas:

Visibility and understanding that allow for growth without user impact:

"We can monitor what paths and what data people are putting in those applications with Zscaler Data Protection, so we've been able to grow without worrying about more user impact."

Improved security posture through alerts and proactive blocking of actions:

"Zscaler Data Protection helps when any user with internet access tries to browse a third-party website with the ability to upload sensitive information or share documents. Zscaler Data Protection comes into play because it scans that content being uploaded and based on data loss prevention policies can trigger an alert and on certain occasions outright block the upload from happening."

Improved rate of traffic inspection and identification:

"Before Zscaler Data Protection, we were able to pre-identify 65% of traffic that was going through our cloud. With Zscaler Data Protection and its features, we're now closer to 85% in terms of identifying what bad actors are doing and what's being scanned through our cloud."

For study participants, enhanced data inspection and threat detection capabilities with Zscaler Data Protection allow them to make important gains in risk reduction related to data. They can more readily prevent users from getting themselves into potentially risky situations through the consistent application of policy and take quick action to prevent impactful problems as needed.

They provided specific examples of how Zscaler Data Protection has helped them achieve these gains:

Ability to prevent potential data loss:

"The biggest benefit for us of using Zscaler Data Protection is being able to ensure that data is not lost through public channels like file sharers, social media, webmail, those types of common attack vectors."

Much faster detection of issues; ability to proactively block risky actions:

"It's easier for us to meet SLAs (service-level agreements) *in terms of how quickly we can detect issues with Zscaler Data Protection. Especially for PII and GDPR, we now meet 100% of our requirements. … Also, from our perspective, there's less risk with Zscaler Data Protection. We can detect if something is being sent out that should not be and block it immediately."*

Ability to bring cost of data loss close to zero:

"We have two to three data loss incidents a month that are now no longer going to inappropriate locations because of Zscaler Data Protection, so our productivity loss due to data loss is basically zero. Before, if someone lost data, we'd have to figure out where it went and take steps to pull back the files."

Study participants linked their use of Zscaler Data Protection to tangible improvements in data loss and security-related outcomes, including:

- **Proactively identifying** an average of 173% more potential security incidents
- **Resolving actual data loss instances** an average of 27% faster

- **Reducing the risk of major data-related security incidents or loss** by an average of 14%

These improvements help interviewed Zscaler customers avoid impactful security events and reach resolution faster when they do occur. As a result, Zscaler customers expend fewer staff resources and incur lower third-party costs in handling such incidents and are less likely to experience business losses in the form of lost revenue or productivity. IDC puts the value of risk-related costs reduced with Zscaler Data Protection at an average of $434,800 per organization per year.

Delivering Better User and Customer Experience

Study participants also linked their use of Zscaler Data Protection to an improved ability to ensure a strong user experience for employees and customers in terms of accessibility and performance. Interviewed Zscaler customers understand that access challenges or poor performance can negatively affect business performance by holding down productivity levels or delivering a poor customer experience.

Interviewed organizations described how Zscaler Data Protection delivers improved performance by minimizing risk and helping optimize network and application performance:

Improved network performance enables users:

"Zscaler Data Protection saves time for our employees; really the entire employee population saves time because of optimized network performance. I would estimate around 10% efficiencies due to network performance."

Improved security posture enhances business confidence:

"Zscaler Data Protection probably protects revenue because we're able to now use the tool for data leakage, and then also for the ability to block unwanted traffic on the way out. For example, if a bulletin is released that a site is malicious, we're able to easily go into the console and block and make the necessary changes in the console and know that we're protected. Before, it was a 50/50 chance with the previous tool. Now, our confidence has grown to very close to 100% with Zscaler Data Protection."

As shown in **Table 3** (next page), study participants attributed important tangible gains in productivity levels for employees across their business operations to use of Zscaler Data Protection. In total, they cited productivity gains worth almost 87 full-time equivalents (FTEs) per organization per year, equating to more than six hours of additional time per user per year. With thousands of employees using applications and services supported by Zscaler Data Protection, these productivity gains add up quickly to deliver significant operational value for study participants.

TABLE 3

Impact on User Productivity

Business Enablement — Higher User Productivity	Per Organization	Per 1,000 Users
Higher gross productivity (FTEs)	86.9	3.4
Hours per year of additional productivity	163,300	6,400
Higher net productivity (FTEs)	13.0	0.5
Annual value of higher net productivity	$912,200	$35,900

n = 7; Source: IDC Business Value in-depth interviews, March 2023

As shown in **Table 4**, study participants also cited improved business results in the form of higher revenue from their use of Zscaler Data Protection. Specifically, they noted that their ability to move more quickly and with more confidence to address business opportunities helps them win more new business, while ensuring the quality and minimizing the risk of services and products lead to higher satisfaction for existing customers. On average, interviewed Zscaler customers reported revenue gains of almost $5 million per year, which IDC applies to its financial model as an average net revenue gain of $740,100 per organization per year after applying a 15% margin assumption (see **Appendix 1**: Methodology for additional details).

TABLE 4

Business Productivity Benefits — Higher Revenue

Revenue Impact	Per Organization	Per 1,000 Users
Total additional revenue per year	$4.93M	$194,300
Assumed operating margin	15%	15%
Total additional net revenue per year	$740,100	$29,100

n = 7; Source: IDC Business Value in-depth interviews, March 2023

Enhanced Business Ability

Interviewed customers also appreciated the much-enhanced scalability that Zscaler Data Protection provides as it helps them extend robust data inspection and security capabilities in far less time across their hybrid IT and work environments. Without this scalability, study participants were previously left with the less-than-ideal choice of either having to wait to extend capabilities to new environments or accepting potential operational risk.

Several interviewed Zscaler customers described the practical effect of having a scalable cloud-based platform:

Near real-time scalability to support expansion:

"Zscaler Data Protection is scalable because we don't have to create new capacity. It used to take longer to expand, whereas it's now instant, say five minutes with Zscaler Data Protection. .... It really wasn't even applicable before because we didn't try to expand because it was too much effort and would have taken too long. Practically, it would have taken more than six months."

Scalable and adaptable to the business environment:

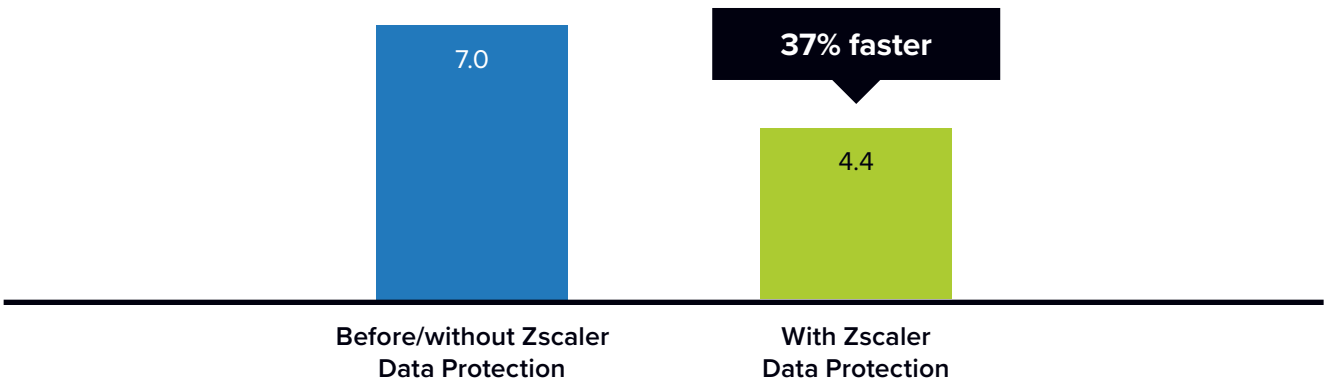
"It's been very easy for us to scale with Zscaler Data Protection simply because it's a cloud solution. ... When COVID-19 started, it was easy for us to send people home and protect them, and we hadn't thought about that before."

Figure 2 shows the extent to which Zscaler Data Protection has reduced the wait required to extend inspection and security capabilities to new environments. On average, IDC calculates that study participants have shaved more than 2.5 weeks off a typical extension, which is 37% faster with Zscaler.

FIGURE 2

Impact on Time to Scale

(Number of weeks)



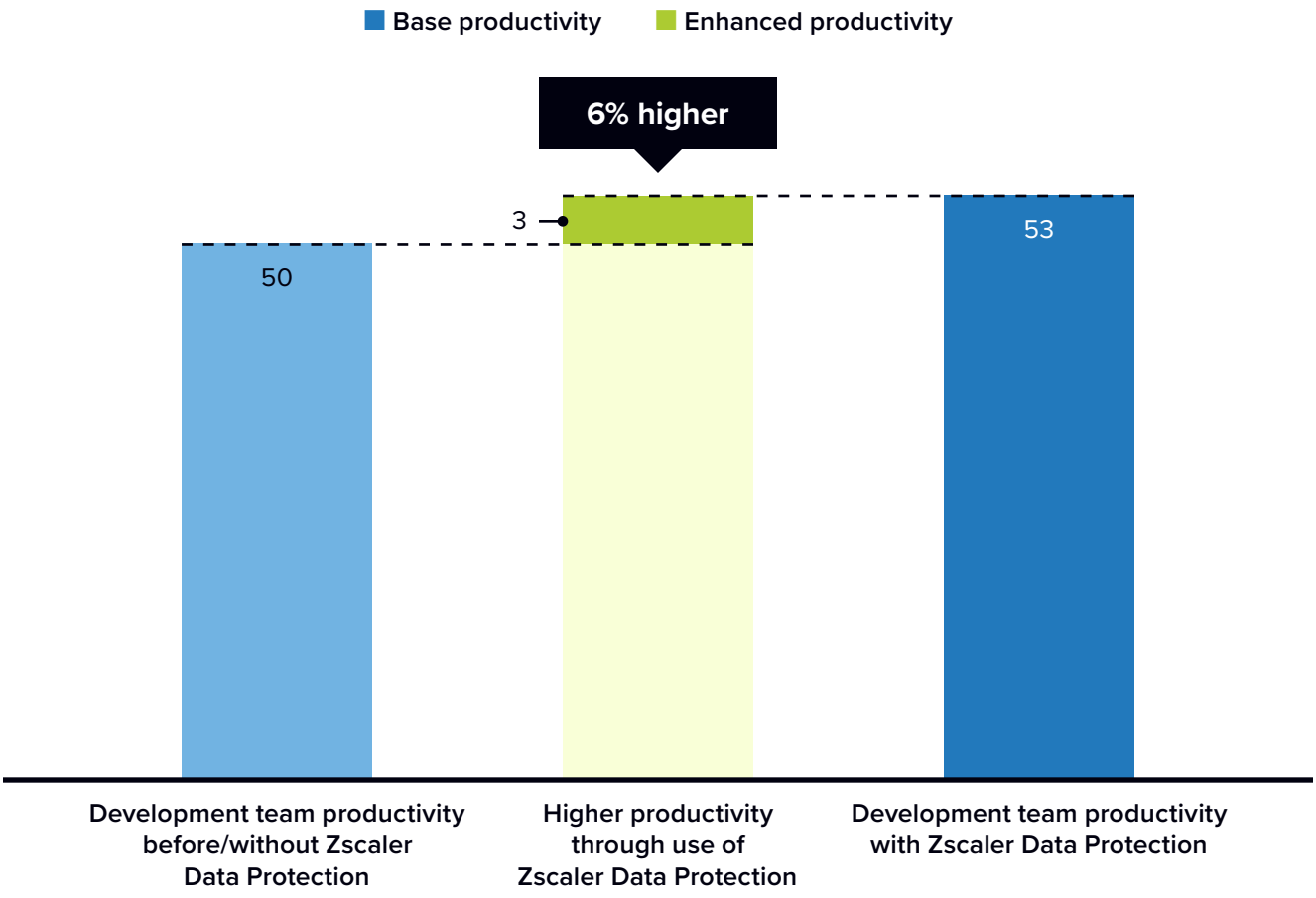
n = 7; Source: IDC Business Value in-depth interviews, March 2023

In addition to business gains from higher revenue, study participants connected enhanced scalability and performance with Zscaler Data Protection to more effective application development activities. They noted that better scalability and performance with Zscaler Data Protection reduce the need for repetitive testing efforts, thus allowing development teams to deliver new functionality in less time to the business. One study participant explained: *"Our developers are positively impacted with Zscaler Data Protection because it can inspect more traffic, so things that would have gone unnoticed previously are now being identified more often. Our team would need to do additional testing because their traffic was not being picked up earlier and they would know there were extra risks, which would create more work in additional test cases."* As shown in **Figure 3**, IDC quantifies the value for developers of using Zscaler Data Protection at a 6% average productivity gain, representing an important incremental improvement in development team throughput and capabilities.

FIGURE 3

Impact on Development Team Productivity

(Equivalent productivity, FTEs per organization)



n = 7; Source: IDC Business Value in-depth interviews, March 2023

For an accessible version of the data in this figure, see Figure 3 Supplemental Data in Appendix 3.

Staff Time and Cost Efficiencies

Interviewed organizations have also captured staff and cost efficiencies through their use of Zscaler Data Protection.

They cited time and cost savings from using a single, robust solution instead of multiple tools, as well as efficiencies from having a cloud-based solution that provides immediate access to reports and data:

Consolidated tool environment that results in cost and staff savings:

"Because we can use one tool with Zscaler Data Protection to handle our VPN access, data loss prevention, web proxying, and our threat detection blocking, we've saved money on tools. Also, I'm the one person who handles Zscaler Data Protection, but if we were to have multiple other tools, we might need up to four other individuals."

Time and cost efficiencies:

"Without Zscaler Data Protection, we would have had to get multiple tools and it would take more staff time to manage and support. We need 5–10 hours per month to maintain Zscaler Data Protection, and we would have to double that and pay about 10% more for other tools."

Staff time savings through cloud-based upgrades:

"The reporting capabilities of Zscaler Data Protection and the fact that it's a cloud-based application mean that when there are upgrades, we don't have to worry about change control and having the resources to do the changes. This generates another 10 hours per month of staff time savings."

Visibility driving compliance team time savings:

"If our compliance team had to gather data manually now, they would probably spend 4–5 hours per week to gather data to see what had moved and whether there were incidents. Now, with Zscaler Data Protection, they can just look at a graph and get these numbers."

Study participants linked their use of Zscaler Data Protection to staff and solution cost efficiencies, including:

- **IT infrastructure team efficiencies** of 22% on average, saving time worth 0.8 FTE per organization
- **Data protection team efficiencies** of an average of 0.5 FTE per organization
- **Security tool and solution cost reductions** of an average of 5%, saving an average of $22,300 per organization per year
- **Compliance team efficiencies** worth 0.3 FTE per organization, including 33% faster completion of compliance reports

ROI Analysis

Table 5 presents IDC's findings on the net benefits and costs related to study participants' use of Zscaler Data Protection. IDC's analysis shows that they will realize discounted benefits in reduced costs of risk, increased employee productivity levels and revenue, application development team productivity gains, and other staff and cost efficiencies worth an average of $5.15 million per organization ($202,700 per 1,000 users). These benefits from Zscaler Data Protection compare with total average discounted investment costs of $1.06 million per organization ($41,800 per 1,000 users). These benefits and investment costs would result in an average three-year ROI of 385%, with interviewed Zscaler customers breaking even on their investment in an average of eight months.

TABLE 5

Three-Year ROI Analysis

	Average per Organization	Average per 1,000 Users
Benefit (discounted)	$5.15M	$202,700
Investment (discounted)	$1.06M	$41,800
Net present value (NPV)	$4.09M	$160,900
Return on investment (ROI)	385%	385%
Payback period	8 months	8 months
Discount rate	12%	12%

n = 7; Source: IDC Business Value in-depth interviews, March 2023

Challenges/Opportunities

Generally, the topic of DP covers a wide breadth of potential capabilities, with some features in greater demand than others. For Zscaler, the challenge is to identify the licensing model that delivers the greatest value to customers while balancing the cost of goods sold and minimizing customer confusion.

Zscaler has increasingly standardized on a step-up pricing model, with the Zscaler for Users bundle offered in three tiers: Business, Transformation, and Unlimited. Each tier builds upon the previous, with added threat protection capabilities, support for new or advanced use cases, and increasingly powerful data protection capabilities. For IT buyers, the simplified model provides a streamlined buying process and less confusion overall. The approach is generally sound, as cloud security services such as ZPA and ZIA are natural integration points for DP.

However, one unintended consequence of the strategy is that Zscaler Data Protection capabilities are spread out across various Zscaler licensing bundles. A secondary impact of this bundling approach is the inhibition of IT buyers' understanding of the value of Zscaler Data Protection, specifically and separately from that of ZIA and/or ZPA. Zscaler Data Protection may also represent one-off costs, which may ultimately be unavoidable as advanced capabilities such as EDM inherently require more processing power and therefore more resources.

Conclusion

Digital transformation enables businesses to use new technologies to their competitive advantage by increasing productivity levels and moving faster to meet customer demand. However, while new technologies typically generate operational efficiencies and provide business advantages, they can increase business risk by increasing reliance on sensitive data and introducing new attack vectors and vulnerabilities. In turn, these factors can create business risk that can mitigate or even offset business gains. Thus organizations need to establish cybersecurity practices and use solutions that enable comprehensive control, threat detection, and policy enforcement wherever their data resides and business activities occur.

This IDC study demonstrates how Zscaler Data Protection solutions ensure more effective and efficient security practices in support of business activities. Importantly, study participants described improving data security regardless of user location or means of access, thus minimizing data-related risk across their hybrid IT and work environments. The ability to ensure robust inspection of traffic regardless of location or time reduces business risk from security breaches and data loss. For interviewed Zscaler customers, this results in higher employee productivity levels and better business results, even as they optimize staff time requirements and the cost of security- and monitoring-related tools. As a result, IDC finds that study participants will achieve strong value compared with investment in Zscaler Data Protection, with an average three-year ROI of 385% and breakeven occurring in an average of eight months.

Appendix 1: Methodology

IDC's standard Business Value and ROI methodology was utilized for this white paper. This methodology is based on gathering data from organizations currently using Zscaler Data Protection solutions as the foundation for the model. Based on interviews with these study participants, IDC has calculated the benefits and costs to these organizations related to their use of Zscaler Data Protection.

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 using Zscaler Data Protection.** In this study, the benefits included higher employee productivity, reduced risk costs, higher revenue, IT staff time savings and efficiencies, and security-related cost savings.
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 Zscaler Data Protection and 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 Zscaler Data Protection 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 $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).
- Downtime values are a product of the number of hours of downtime multiplied by the number of users affected.
- The impact of unplanned downtime is quantified in terms of impaired end-user productivity and lost revenue.

- Lost productivity is a product of downtime multiplied by burdened salary.
- 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.

Because every hour of downtime does not equate to a lost hour of productivity or revenue generation, IDC attributes only a fraction of the result to savings. As part of our assessment, we asked each interviewed organization what fraction of downtime hours to use in calculating productivity savings and the reduction in lost revenue. IDC then taxes the revenue at that rate.

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.

Appendix 2: Calculations

Average Annual Benefits per Organization

Table 6 shows the areas of value that study participants attributed to their use of Zscaler Data Protection. On average, IDC calculates that they will realize benefits worth an average of $2.19 million per year per organization over three years.

TABLE 6

Calculations: Annual Benefits from Use of Zscaler Data Protection

Category of Value	Average Quantitative Benefit	Calculated Average Annual Value*
Net user productivity gains	6.4 additional productive hours per user per year, 15% margin assumption, $70,000 salary, 13.0 FTE net gain	$774,400
Higher net revenue	$4.93M higher total revenue, 15% margin assumption	$628,300
Reduced cost of security breaches/data loss	$434,800 savings per year in direct and remediation costs	$369,100
Compliance team efficiencies	0.3 FTE efficiency, $70,000 salary assumption	$16,900
Data protection team efficiencies	0.5 FTE efficiency, $100,000 salary assumption	$40,000
IT infrastructure team efficiencies	0.8 FTE efficiency, $100,000 salary assumption	$67,800
Development team efficiencies	3.2 FTEs productivity gain, $100,000 salary assumption	$272,900
Security tool cost savings	5% cost savings, $22,300 savings per year	$18,900
Total annual benefits through use of Zscaler Data Protection	$2.19M	

n = 7; Calculated average annual value takes into account 5.4 months' deployment time in year 1

Source: IDC Business Value in-depth interviews, March 2023

Appendix 3: Supplemental Data

The table in 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 3 SUPPLEMENTAL DATA

Impact on Development Team Productivity

	Development Team Productivity Before/ Without Zscaler Data Protection	Higher Productivity Through Use of Zscaler Data Protection	Development Team Productivity with Zscaler Data Protection
Base productivity	50	50	53
Enhanced productivity		3	

n = 7; Source: IDC Business Value in-depth interviews, March 2023

Return to original figure

About the IDC Analysts

Christopher Rodriguez
Research Director, Security & Trust, IDC

Christopher Rodriguez is a research director in IDC's Security & Trust research practice, focused on the products designed to protect critical enterprise applications and network infrastructure. IDC's Security & Trust research services to which Chris contributes include Network Security Products and Strategies, and Active Application Security and Fraud.

More about Christopher Rodriguez

Matthew Marden
Research Vice President, Business Value Strategy Practice, IDC

Matthew Marden is responsible for carrying out custom business value research engagements and consulting projects for clients in a number of technology areas, with a focus on determining the return on investment (ROI) of their use of enterprise technologies. Matthew's research often analyzes how organizations are leveraging investment in digital technology solutions and initiatives to create value through efficiencies and business enablement.

More about Matthew Marden

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell, and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.

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