FORRESTER®

The Total Economic Impact™ Of Zscaler Internet Access

Cost Savings And Business Benefits Enabled By Zscaler Internet Access

A FORRESTER TOTAL ECONOMIC IMPACT STUDY
COMMISSIONED BY ZSCALER, APRIL 2025

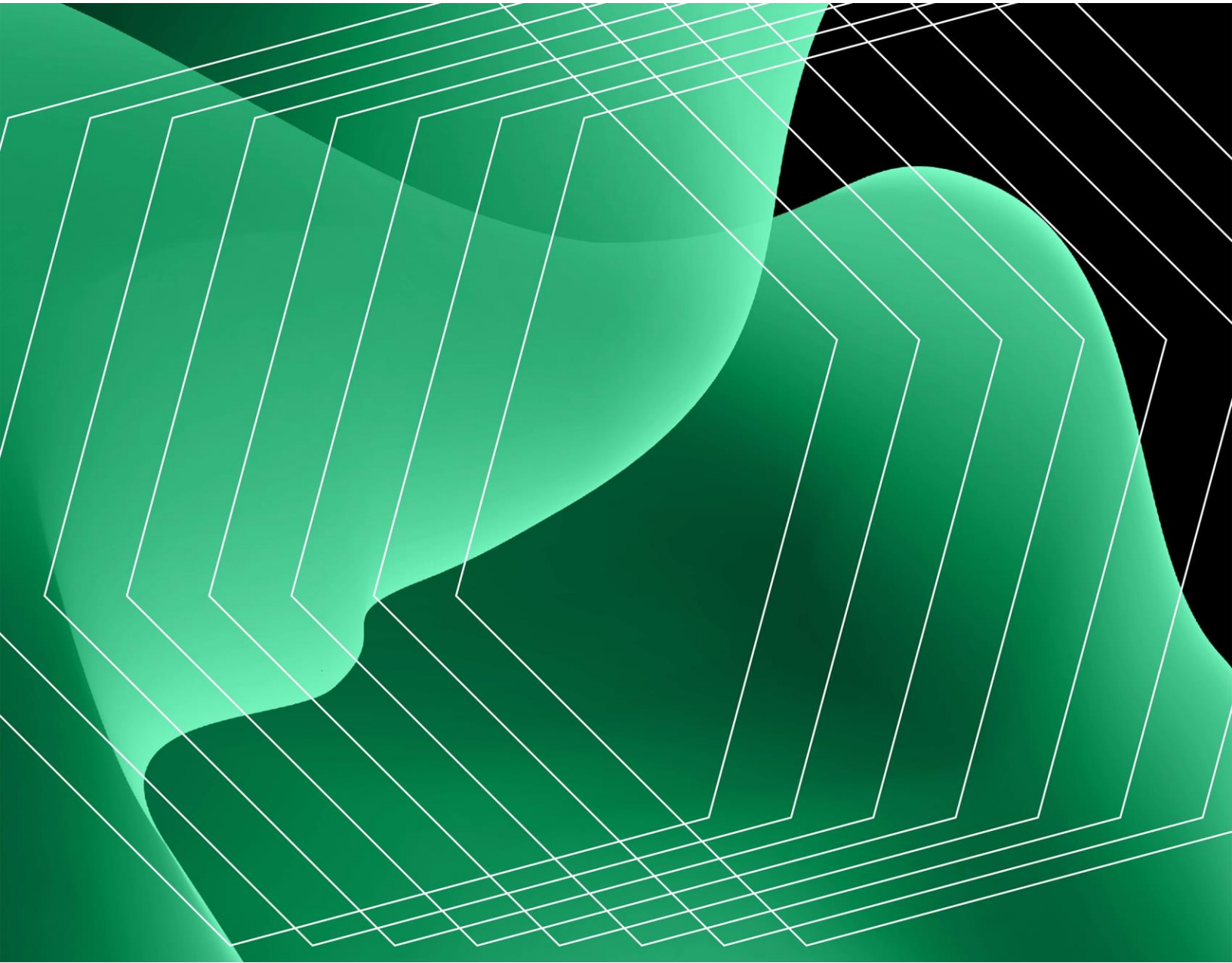


Table Of Contents

Consulting Team:

Luca Son

Executive Summary

In today's rapidly evolving digital landscape, organizations face challenges in ensuring secure, efficient, and reliable internet access for their workforce. Advanced cloud-native security solutions offer transformative benefits that address these critical needs. By leveraging these technologies, organizations can enhance operational efficiency, strengthen security, and improve user experience. Decision-makers will discover how adopting cloud-native security solutions can drive productivity, agility, and resilience, ultimately positioning their organizations for success in an increasingly interconnected world.

Zscaler Internet Access (ZIA) is a cloud-native security solution designed to provide secure, fast, and reliable internet access for organizations. It addresses key problems like protecting against sophisticated cyberthreats, including encrypted attacks, ensuring compliance with regulatory requirements, and improving user experience by inspecting and filtering internet traffic in real time without adversely impacting performance. ZIA enables organizations to enhance their security posture while maintaining high performance and scalability.

Zscaler commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Zscaler Internet Access.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Zscaler Internet Access on their organizations.

Return on investment (ROI)
267%

Net present value
$3.2M

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed five decision-makers with experience using Zscaler Internet Access. For the purposes of this study, Forrester aggregated the experiences of the interviewees and combined the results into a single composite organization, which is a global organization with 15,000 employees and revenue of $10 billion per year.

Interviewees said that prior to using Zscaler Internet Access, their organizations relied on complex, legacy point solutions for security web gateways (SWG), proxies, firewalls, data loss

prevention (DLP), sandboxing, secure sockets layer (SSL)/transport layer security (TLS) inspection, URL filtering, and multiprotocol label switching (MPLS) routing with on-premises or virtualized deployments. However, these prior legacy security solutions and deployment models were not effective, leaving them with high operational costs, scalability issues, and fragmented security policies. These limitations led to inefficiencies, poor user experiences, and increased the risk of security breaches.

After the investment in ZIA, the interviewees' organizations experienced a streamlined, scalable, and cloud-native approach to secure internet access with inline inspection of encrypted traffic. Key results from the investment include increased technology cost savings, improved operational efficiency, strengthened security posture, and enhanced user experience and productivity.

KEY FINDINGS

Quantified benefits. Three-year, risk-adjusted present value (PV) quantified benefits for the composite organization include:

- **Reduced legacy technology licensing, hardware, and management costs.** Implementing ZIA results in significant technology cost savings for the composite organization. By transitioning to Zscaler's cloud-native architecture, the composite organization eliminates or reduces legacy licensing, networking, and hardware and software costs associated with disparate and sprawling legacy point solutions for SWG, proxies, firewalls, DLP, sandboxing, SSL/TLS inspection, URL filtering, and MPLS routing. Additionally, the composite organization reduces operational expenses associated with maintenance and upgrades of its legacy environment. This shift provides a more scalable and cost-effective solution, contributing to substantial savings in maintenance and support costs. This is worth $1.5 million over three years for the composite organization.
- **Increased security and IT operational efficiency for managing security policies by 75%.** Zscaler Internet Access improves IT, network, and security operational efficiency for the composite organization. By transitioning to Zscaler, IT, network, and security professionals save substantial hours previously spent on configuring and managing security policies, SSL/TLS inspection, and troubleshooting issues. With Zscaler, policies are enforced consistently across all users and devices, whether they are on-premises or remote. This ensures uniform security standards and reduces the complexity of managing policies and performing SSL/TLS inspection in disparate systems. This shift

not only reduces the operational burden but also allows these professionals to focus on more strategic tasks, enhancing overall productivity. This is worth $427,000 PV over three years for the composite organization.

- **Reduced the risk of exposure to breach costs by 65%.** Implementing Zscaler Internet Access strengthens security and improves overall security architecture for the composite organization. By transitioning to Zscaler's Zero Trust architecture, the composite organization enhances its security posture, improves threat detection and response capabilities, and reduces the likelihood of cybersecurity breaches. This shift provides better visibility and control over network traffic and ensures compliance with regulatory requirements, thereby reducing overall risk. This is worth $1.0 million PV over three years for the composite organization.
- **Saved 6.5 hours per year for Zscaler users from improved internet access.** Implementing ZIA improves user experience and productivity for the composite organization. By transitioning to Zscaler, employees experience faster, more reliable access to applications and websites, reduced latency, and seamless connectivity. This shift enhances user satisfaction and boosts overall productivity by minimizing disruptions and improving task completion times. This is worth $1.5 million PV over three years for the composite organization.

Unquantified benefits. Benefits that provide value for the composite organization but are not quantified for this study include:

- **Agility and scalability.** Zscaler's cloud-native architecture enhances the composite organization's agility and scalability, allowing the organization to support growing traffic and distributed user bases efficiently. This capability enables quick setup of new offices and efficient handling of high-bandwidth applications.
- **Global coverage.** Zscaler's global coverage with local internet breakouts ensures fast and reliable access to applications and data from anywhere in the world for the composite organization.
- **Compliance and reporting.** Zscaler provides better compliance and reporting capabilities to the composite organization with customizable policies and detailed insights into user activity and security incidents.
- **Employee satisfaction.** The composite organization improves user experience by providing seamless access to the internet and applications.

Costs. Three-year, risk-adjusted PV costs for the composite organization include:

- **Zscaler fees of $783,000 over three years.** Zscaler fees are typically structured on a per-user basis, reflecting the composite organization's specific needs and the range of services included. The fees can vary based on the number of users, the specific features required, and any additional professional services or support packages opted for. This flexible pricing approach allows the composite organization to scale its security solutions according to its growth and evolving needs, ensuring cost-effectiveness and robust security coverage.
- **Implementation, training, and ongoing costs of $427,000 over three years.** Indirect costs for implementing Zscaler primarily involve internal labor. The composite organization dedicates a team to set up infrastructure, configure policies, integrate systems, and manage change activities. Professional services from Zscaler may be used to ensure efficient implementation. Training for security, network, and IT roles is essential to proficiently manage the platform. Ongoing management requires IT operations professionals to monitor, update, and adjust the system for optimal performance and security.

The financial analysis that is based on the interviews found that a composite organization experiences benefits of $4.4 million over three years versus costs of $1.2 million, adding up to a net present value (NPV) of $3.2 million and an ROI of 267%.

> "ZIA has improved network performance and made application access faster and more reliable. Its cloud-based approach reduces delays and ensures secure, seamless connectivity. Users benefit from better speed, scalability, and security without the need for complex setups."
>
> NETWORK SECURITY LEAD, TECHNOLOGY

ROI	BENEFITS PV	NPV	PAYBACK
267%	**$4.4M**	**$3.2M**	**<6 months**

Benefits (Three-Year)

TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment Zscaler Internet Access.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that Zscaler Internet Access can have on an organization.

1. **Due Dilligence**
   Interviewed Zscaler stakeholders and Forrester analysts to gather data relative to Zscaler Internet Access.
2. **Interviews**
   Interviewed four representatives at organizations using Zscaler Internet Access to obtain data about costs, benefits, and risks.
3. **Composite Organization**
   Designed a composite organization based on characteristics of the interviewees' organizations.
4. **Financial Model Framework**
   Constructed a financial model representative of the interviews using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewees.
5. **Case Study**
   Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

The Zscaler Internet Access Customer Journey

Drivers leading to the Zscaler Internet Access investment

Interviews				
Role	**Industry**	**Region**	**Annual Revenue**	**Number Of Zscaler Users**
SVP of infrastructure	Financial services	APAC HQ, global operations	$20B+	230,000
Network security lead	Technology	APAC HQ, global operations	$20B+	40,000
Director of cybersecurity	Insurance	US HQ, global operations	$15B+	6,000
VP of enterprise security Security architecture manager	Telecommunications	EMEA HQ, global operations	$3B+	8,000

KEY CHALLENGES

Prior to adopting Zscaler Internet Access, the interviewees' organizations relied on a complex array of legacy solutions and infrastructure to secure their internet access. These solutions typically included on-premises or virtualized secure web gateways, web filtering, intrusion prevention system (IPS), sandboxing, and firewalls, which required significant resources for maintenance and management. The legacy environment was characterized by multiple tools that all addressed specific security needs, leading to a fragmented and inefficient security posture. The on-premises nature of these solutions often resulted in scalability issues, high operational costs, and limited flexibility, especially in the face of evolving security threats and the need for remote work capabilities. Interviewees noted how their organizations struggled with common challenges, including:

- **High operational costs.** For the interviewees' organizations, maintaining and managing the legacy infrastructure was costly, both in terms of financial resources and human effort. These organizations incurred significant expenses for licensing, hardware maintenance, and operational support. The SVP of infrastructure at a financial services

organization said, “We used to pay somewhere around 60 million INR, [or about $700,000] for the proxies, including the filtering licenses and all.”

- **Operational inefficiencies.** Managing and maintaining legacy solutions required extensive manual intervention, leading to high operational costs and inefficiencies for the interviewees’ organizations. This often involved time and effort from IT staff to keep systems updated and secure, especially for on-premises environments. The VP of enterprise security at a telecommunications organization said, “We had around 100 on-prem gateways, which was becoming very difficult to manage from a patching point of view.” The director of cybersecurity at an insurance organization said, “[Our legacy SWG appliances] were falling over, we had enough SSL traffic that they were struggling, and it was really difficult to maintain operation of those boxes.”
- **Scalability issues.** Interviewees noted their organizations’ legacy infrastructures struggled to handle increasing traffic and user demands, particularly during the shift to remote work or expansion to new offices. The SVP of infrastructure at a financial services organization said: “Before [Zscaler], we had a closed environment. Zscaler has allowed us to break out internet between branches, avoiding MPLS backhauling through data centers.”
- **User experience problems.** Legacy solutions often resulted in poor user experience at the interviewees’ organizations due to latency and connectivity issues. Users faced challenges when connecting to public Wi-Fi or company portals, leading to frequent disruptions and support tickets. The network security lead at a technology organization said: “Before Zscaler, our biggest challenge was ensuring secure connections for remote users, especially when they accessed the internet through captive portals or public Wi-Fi. Zscaler has transformed this experience, providing seamless and secure internet access regardless of the connection type.”
- **Security gaps.** The fragmented nature of legacy solutions at the interviewees’ organizations led to gaps in security coverage, increasing the risk of breaches. This lack of comprehensive visibility and control over internet-bound transactions left these organizations vulnerable to threats. The network security lead at a technology organization said, “After Zscaler, we have effective security posture in place but prior to Zscaler, we didn’t have sufficient information on internet transactions traffic.”
- **Complex security policy management and integration.** Integrating multiple legacy tools and solutions was complex and often resulted in inconsistent security policies and management. Interviewees noted this disjointed experience made it difficult to ensure seamless integration and consistent security across hybrid environments. The security

architecture manager at a telecommunications organization said: “It was a disjointed experience. … We had allow-listed a website and it hadn’t quite yet applied on-prem or in the cloud.”

WHY ZSCALER

Interviewees noted their organizations chose Zscaler for its unique value proposition that addressed their specific needs and challenges. These features and benefits made Zscaler the preferred choice for the interviewees’ organizations, which were looking to enhance their security posture, improve user experience, and streamline policy management.

- **Cloud-native solution.** Interviewees noted that Zscaler’s cloud-native approach provided the scalability and flexibility needed to handle increasing traffic and user demands. The security architecture manager in a telecommunications organization said, “A cloud-first solution was probably one of the main drivers to go towards Zscaler because we tried the hybrid approach and there were clearly some complexities.”
- **Comprehensive security features.** According to the interviewees, Zscaler offered a range of security features, including SSL inspection, DLP, sandboxing, and DNS security, which helped their organizations optimize their security posture. The SVP of infrastructure at a financial services organization said, “Zscaler is helping us in terms of the one-time decrypt and pass to all the other technology like a sandbox or DLP as a single-pass architecture.”
- **Ease of policy configuration and management.** Zscaler’s centralized policy management eliminated the need for the interviewees’ organizations to set the same policies multiple times across different environments, simplifying the process and ensuring consistency. The network security lead at a technology organization said, “When users are connected from office, we were able to bypass the call out of firewalls to ensure that all the traffic goes through Zscaler in that way we have uniformity and centralized logging and policy setup.”
- **Improved user experience and global coverage.** Interviewees noted that Zscaler’s ability to provide local egress points and reduce latency improved user experience significantly, particularly for the needs of enterprises operating in multiple geographies.
- **Platform extensibility.** The interviewees noted their organizations invested in Zscaler due to its platform extensibility, which allowed for a more seamless integration and easy activation of additional solutions like Zscaler Private Access (ZPA), Zscaler Digital

Experience (ZDX), and other Zscaler offerings. This cloud-native architecture enabled the interviewees' organizations to consolidate their security tools, reducing complexity.

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an ROI analysis that illustrates the areas financially affected. The composite organization is representative of the interviewees' organizations, and it is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. The global, multibillion-dollar organization generates $10 billion in annual revenue. It is headquartered in the US and has a globally distributed workforce with multiple hubs and satellite offices that require fast, secure, and reliable internet access. The organization employs 15,000 individuals, of which 10,000 use Zscaler Internet Access to ensure secure and reliable connectivity for remote work, high-bandwidth applications, and compliance with security policies.

Deployment characteristics. The composite organization begins using ZIA in Year 1 after a four-month implementation period. The implementation includes all geographies and channels, ensuring comprehensive coverage and support for the organization's diverse and widespread operations.

KEY ASSUMPTIONS

$10 billion in annual revenue
10,000 Zscaler users
Global distributed workforce

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits						
Ref.	**Benefit**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Atr	Technology cost savings	$587,988	$587,988	$587,988	$1,763,963	$1,462,238
Btr	Operational efficiency	$171,850	$171,850	$171,850	$515,549	$427,365
Ctr	Strengthened security	$419,523	$419,523	$419,523	$1,258,570	$1,043,292
Dtr	Improved user experience and productivity	$607,750	$607,750	$607,750	$1,823,250	$1,511,384
	Total benefits (risk-adjusted)	$1,787,110	$1,787,110	$1,787,110	$5,361,331	$4,444,279

TECHNOLOGY COST SAVINGS

Evidence and data. Implementing Zscaler Internet Access resulted in technology cost savings for interviewees' organizations. By transitioning to Zscaler's cloud-native architecture, interviewees noted their organizations eliminated or reduced legacy licensing, networking, hardware, and software costs associated with disparate and sprawling legacy point solutions for SWG, proxies, firewalls, DLP, sandboxing, SSL/TLS inspection, and MPLS routing. Additionally, interviewees' organizations reduced operational expenses associated with the maintenance and upgrades of their legacy environments. This shift not only provided a more scalable and cost-effective solution but also contributed to substantial savings in maintenance and support costs.

- A director of cybersecurity said their insurance organization retired a substantial amount of legacy hardware, including appliances that were financially untenable. The estimated cost of deploying these appliances at every remote office would have been around $5 million, whereas Zscaler's licensing costs were lower, providing a more cost-effective solution. On the management front, the interviewee's insurance organization went from spending 80 hours a week managing its legacy web security solution to 8 hours a week with Zscaler.

- Similarly, the security architecture manager at a telecommunications organization reported that their organization experienced considerable savings by migrating from a hybrid solution to Zscaler. The previous setup was a hybrid model that combined both on-premises servers and cloud-managed web gateways. This setup required around 100 on-premises servers, which were resource-intensive and costly to maintain. By switching to Zscaler's cloud-native architecture, this interviewee's organization was able to eliminate these servers, saving on infrastructure costs and reducing its carbon footprint. Although the licensing cost for Zscaler was higher than the previous solution, the overall savings from reduced server maintenance and improved operational efficiency made the investment worthwhile. Additionally, the interviewee said their organization saved "hundreds to thousands of total IT infrastructure hours" supporting patching activities.
- An SVP of infrastructure at a financial services organization said their organization also benefited from technology cost savings by implementing Zscaler. This interviewee's organization decommissioned various legacy solutions, including legacy SWGs, proxies, DLP, and sandboxing, which collectively amounted to significant annual expenses. Additionally, the interviewee's organization avoided the upgrade costs for MPLS WAN routers and third-party DNS security solutions, further contributing to its savings. The transition to Zscaler not only optimized its security infrastructure but also provided a more scalable and cost-effective solution for its growing network demands. The senior VP of infrastructure said, "We avoided buying any third-party DNS security solution, which could be some around 8 million INR." Finally, the SVP of infrastructure noted their financial services organization saved three FTEs worth of IT labor from deploying and managing legacy solutions.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- With Zscaler, the composite organization avoids a total of $220,000 in annual legacy web security solution licensing costs, which includes web gateway appliances, DLP, SSL/TLS inspection, and web filtering capabilities.
- The composite organization also avoids a total of $168,000 in legacy networking, MPLS, and hardware costs.
- Prior to Zscaler, the composite organization employed three IT operations FTEs to maintain legacy solutions. With Zscaler, the IT operations FTEs fully reallocate 75% of their time to other strategic tasks, as they eliminate all tasks related to maintaining point, legacy security solutions.

- The average fully burdened annual salary for an IT operation FTE is $135,000, which includes a 1.35x fully burdened multiplier.

Risks. Forrester recognizes that these results may not be representative of all experiences. The impact of this benefit will vary depending on:

- Size, complexity, and maturity of legacy infrastructure.
- Technical support skill set, availability, and effectiveness.
- Ongoing management complexity

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.5 million.

Time savings for IT operations managing legacy infrastructure
75%

"If I tried to deploy [our legacy on-premises web security solution] at every remote office that I have, it would have been financially untenable. It would have been around $50K a box. When you start multiplying that by hundreds of sites, it is just untenable."

DIRECTOR OF CYBERSECURITY, INSURANCE

Technology Cost Savings					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Legacy solutions licensing costs	Composite	$220,000	$220,000	$220,000
A2	Legacy networking, MPLS, and hardware costs	Composite	$168,000	$168,000	$168,000
A3	**Subtotal: Avoided legacy technology costs**	**A1+A2**	**$388,000**	**$388,000**	**$388,000**
A4	IT operations FTEs required to support and maintain legacy solutions	Composite	3	3	3
A5	IT operation time savings with Zscaler	Interviews	75%	75%	75%
A6	Fully burdened annual salary for an IT operation FTE	Composite	$135,000	$135,000	$135,000
A7	**Subtotal: Reallocated maintenance labor**	**A4*A5*A6**	**$303,750**	**$303,750**	**$303,750**
At	Technology cost savings	A3+A7	$691,750	$691,750	$691,750
	Risk adjustment	↓ 15%			
Atr	Technology cost savings (risk-adjusted)		$587,988	$587,988	$587,988
	Three-year total: $1,763,963		**Three-year present value: $1,462,238**		

OPERATIONAL EFFICIENCY

Evidence and data. Zscaler Internet Access improved IT, network, and security operational efficiency for several of the interviewees' organizations. By transitioning to Zscaler, interviewees noted their IT, network, and security professionals were able to save substantial hours previously spent on configuring and managing security policies, SSL/TLS inspection, and troubleshooting issues. With Zscaler, policies could be enforced consistently across all users and devices, whether they were on-premises or remote. This ensured uniform security standards and reduced the complexity of managing policies and performing SSL/TLS inspection in disparate systems. This shift not only reduced the operational burden but also allowed these professionals to focus on more strategic tasks, enhancing overall productivity.

- A director of cybersecurity at an insurance organization said, "[Using Zscaler resulted in a] 10x time savings for administrative SSL inspection." Prior to Zscaler, managing SSL connectivity required two full-time employees; with Zscaler, this task was reduced to a fraction of one employee's time. This reduction in labor allowed the interviewee's organization to reallocate resources to other critical areas. Additionally, the streamlined

process of configuring and managing security policies through Zscaler's centralized platform further decreased the time and effort required from IT and security teams.

- A security architecture manager at a telecommunications organization reported considerable improvements in operational efficiency, noting, "The centralized management of security policies and the improved user experience also contributed to a more efficient and productive IT environment."
- An SVP of infrastructure at a financial services organization reported enhancing operational efficiency by implementing Zscaler. The interviewee's organization reduced the number of tickets generated due to website issues and misconfigurations, which previously required time and effort from the service desk and IT support teams. The improved categorization and troubleshooting capabilities of Zscaler minimized the need for manual intervention, allowing IT professionals to focus on more strategic initiatives and reducing overall operational costs.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- Prior to adopting Zscaler, the composite organization dedicated 4,992 hours (2.4 FTEs) of IT operations, network engineer, and security analyst time on policy management for legacy solutions.
- With Zscaler, these roles improve their policy management efficiency by 75%.
- Forrester applies a 75% productivity recapture rate, which quantifies the amount of efficiency gained and applied to other strategic tasks.
- The blended average fully burdened hourly rate for IT operations, network engineers, and information security analysts is $68, which is $142,000 annually.

Risks. Forrester recognizes that these results may not be representative of all experiences. The impact of this benefit will vary depending on:

- Implementation challenges.
- Training effectiveness.
- Resistance to change.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $427,000.

Improvement in security policy efficiency management
75%

"Managing SSL connectivity required two full-time employees [in our legacy environment] but with Zscaler, this task was reduced to a fraction of one employee's time."

DIRECTOR OF CYBERSECURITY, INSURANCE

Operational Efficiency

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	IT operations, network engineer, and security analyst time required for security policy management of legacy on-premises solutions (hours)	Composite	4,992	4,992	4,992
B2	Security policy management efficiency improvement	Interviews	75%	75%	75%
B3	Productivity recapture	Composite	75%	75%	75%
B4	Blended average fully burdened hourly rate for IT operations, network engineers, and information security analysts	Composite	$68	$68	$68
Bt	Operational efficiency	B1*B2*B3*B4	$190,944	$190,944	$190,944
	Risk adjustment	↓10%			
Btr	Operational efficiency (risk-adjusted)		$171,850	$171,850	$171,850
	Three-year total: $515,549			**Three-year present value: $427,365**	

STRENGTHENED SECURITY

Evidence and data. Interviewees noted that implementing ZIA strengthened security and improved overall security architecture at their organizations. By transitioning to Zscaler's Zero Trust architecture, the interviewees' organizations enhanced their security posture, improved threat detection and response capabilities, and reduced the likelihood of cybersecurity breaches. This shift not only provided better visibility and control over network traffic but also ensured compliance with regulatory requirements, thereby reducing overall risk.

- A security architecture manager at a telecommunications organization estimated that Zscaler reduced the overall risk of incurring security breaches by at least 30%. The interviewee said, "Zscaler inspects internet traffic at scale, processing 6.7 billion transactions and blocking 476,000 security threats quarterly." Additionally, the interviewee cited Zscaler's categorization and threat detection capabilities as one reason their organization reduced the risk of breaches: "Zscaler has high quality categories. … They're not often wrong. We're no longer dealing with problems around categorization."
- A network security lead at a technology organization said Zscaler blocked around 5 million threats per quarter, leading to better protection while ensuring fast connectivity for users.
- An SVP of infrastructure said their financial services organization gained better visibility into network traffic and improved its threat detection capabilities with Zscaler Internet Access. The interviewee said: "There are a lot of shadow IT applications being used. For example, there are a lot of personal [cloud storage services] with various methods to sneak in. … Zscaler's reporting is a key feature that provides us visibility into what is happening." The SVP also noted that the improved visibility and threat detection capabilities reduced their organization's risk, stating: "Zscaler has significantly enhanced my security insights, elevating the threat index beyond previous levels. Unlike before, when we relied solely on SIEM [security information and event management] triggers, Zscaler provides a more comprehensive and proactive approach to threat detection."
- Additionally, the director of cybersecurity at an insurance organization confirmed that Zscaler reduced their organization's overall risk of breach as evidenced by industry awards they received for their Zero Trust project. This interviewee stated that they believed using Zscaler led to a reduction in cyber insurance premiums, signaling a more secure and robust Zero Trust architecture.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- Based on the size and defining characteristics of the composite organization, Forrester estimates the total annual cost of breaches to be $4,427,000. Forrester calculates breach cost by considering a range of factors, including labor for issue prevention, identification, and remediation from across the organization; the cost of fines, lawsuits, lost revenue, and more; and the negative impact on employee productivity, stock price, and investment capabilities.[2]
- The composite has a 68% likeliness of experiencing one or more breaches per year.[3]
- Sixty-seven percent of breaches originate from external attacks targeting remote environments, internal incidents, attacks or incidents involving the external ecosystem.[4] Zscaler addresses 40% of these attacks.
- Zscaler reduces the risk of breaches by 65%.

Risks. Forrester recognizes that these results may not be representative of all experiences. The impact of this benefit will vary depending on:

- Organization size, industry, and existing security posture.
- Evolving threat landscape.
- Integration with existing systems.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.0 million.

Reduced risk of exposure to breach costs from addressable attacks with Zscaler

65%

> “ZIA has improved SSL/TLS inspection by providing deep visibility into encrypted traffic without slowing down performance. It helps detect threats hidden in secure connections, ensuring better protection while maintaining fast and seamless access for users.”
>
> **NETWORK SECURITY LEAD, TECHNOLOGY**

> “I never worry about Zscaler. It’s not a technology that keeps me up at night.”
>
> **DIRECTOR OF CYBERSECURITY, INSURANCE**

Strengthened Security					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Cumulative cost of breaches	Forrester research	$4,427,000	$4,427,000	$4,427,000
C2	Likelihood of experiencing one or more breaches	Forrester research	68%	68%	68%
C3	Percentage of breaches originating from external attacks targeting remote environments, internal incidents, attacks, or incidents involving the external ecosystem	Forrester research	67%	67%	67%
C4	Percentage of those attacks addressable with Zscaler Internet Access	Interviews	40%	40%	40%
C5	Annual risk exposure addressable with Zscaler Internet Access	C1*C2*C3*C4	$806,776	$806,776	$806,776
C6	Reduced risk of exposure to breach costs from addressable attacks with Zscaler Internet Access	Interviews	65%	65%	65%
Ct	Strengthened security	C5*C6	$524,404	$524,404	$524,404
		↓ 20%			
Ctr	Strengthened security (risk-adjusted)		$419,523	$419,523	$419,523
	Three-year total: $1,258,570		**Three-year present value: $1,043,292**		

IMPROVED USER EXPERIENCE AND PRODUCTIVITY

Evidence and data. Implementing ZIA improved user experience and productivity for the interviewees' organizations. By transitioning to Zscaler, interviewees noted their organizations' employees experienced faster, more reliable access to applications and websites, reduced latency, and seamless connectivity. This shift not only enhanced user satisfaction but also boosted overall productivity by minimizing disruptions and improving task completion times.

- A director of cybersecurity at an insurance organization estimated remote workers saved 3 to 5 minutes per day logging on with Zscaler. Prior to Zscaler, remote workers faced delays and disruptions due to the need to connect to a VPN for secure internet access. The interviewee stated: "If you're searching for a page load and you got to go halfway around the world, four times per packet, using rough math from a network perspective, you're talking 40 milliseconds. If you do that by 500 calls or 1,000 calls for a web page, now you're talking about noticeable delays that are occurring for these page loads." With Zscaler, remote workers could access the internet directly, significantly reducing page

load times and improving overall user experience. Additionally, the simplified process of connecting to the internet without the need for complex VPN setups allowed employees to work more efficiently from anywhere. The director of cybersecurity said, "From their perspective, they just boot up their laptop, and it works."

- Similarly, the security architecture manager at a telecommunications organization reported considerable improvements in user experience and productivity. The interviewee's organization's previous hybrid solution caused issues with localized websites and would often direct users to the wrong local websites. By switching to Zscaler's cloud-native architecture, the interviewee's organization eliminated these issues and provided users with faster, more reliable access to websites and applications. The security architecture manager noted: "We went with Zscaler because it was always cloud-hosted and you were always getting the local version of the website you needed. Zscaler has coverage in pretty much every European country." This improvement in user experience also contributed to better productivity, as employees faced fewer disruptions and could complete tasks more efficiently.
- The SVP of infrastructure noted their financial services organization also benefited from enhanced user experience and productivity because of Zscaler. Their organization reduced latency and improved application access for remote workers, leading to better performance and user satisfaction. The interviewee said: "For a work from home employee, it is direct internet connectivity. Earlier, we used to backhaul all the traffic onto the on-prem and then take it out. We saw a major benefit for the people who were using MPLS as a network."
- The network security lead at a technology organization said, "ZIA has made critical business applications run faster and more reliably by reducing delays and improving access, leading to a smoother user experience."

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- With Zscaler, users avoid 1.5 minutes of wait time due to performance issues they experienced in legacy environments. This amounts to 6.5 hours saved per user per year.
- The composite organization has a total of 10,000 annual ZIA users. Forrester does not scale users year over year for simplicity in modeling; however, it is reasonable to assume numbers of users can change year over year due to increased technology adoption and variance in the workforce size.
- Forrester recaptures 25% of user time savings from improved internet access.

- The fully burdened hourly rate for a user is $44, or $92,000 per year.

Risks. Forrester recognizes that these results may not be representative of all experiences. The impact of this benefit will vary depending on:

- Network performance variability.
- Initial implementation issues.
- Ongoing support needs.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.5 million.

Avoided wait time due to better internet connectivity with Zscaler

1.5 minutes

"ZIA has boosted user productivity and efficiency by providing fast, secure, and seamless access to applications. With reduced latency and direct-to-cloud connectivity, users experience fewer disruptions and faster load times. The simplified security model also eliminates the need for complex VPNs, allowing employees to work more efficiently from anywhere."

NETWORK SECURITY LEAD, TECHNOLOGY

Improved User Experience And Productivity					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
D1	Avoided wait time per day due to performance issues (minutes)	Interviews	1.5	1.5	1.5
D2	Hours saved per user per year	D1/60 minutes*260 days	6.5	6.5	6.5
D3	Number of ZIA users	Composite	10,000	10,000	10,000
D4	Productivity recapture	Composite	25%	25%	25%
D5	Fully burdened hourly rate for a ZIA user	Composite	$44	$44	$44
Dt	Improved user experience and productivity	D2*D3*D4*D5	$715,000	$715,000	$715,000
	Risk adjustment	↓ 15%			
Dtr	Improved user experience and productivity (risk-adjusted)		$607,750	$607,750	$607,750
	Three-year total: $1,823,250		**Three-year present value: $1,511,384**		

UNQUANTIFIED BENEFITS

Interviewees mentioned the following additional benefits that their organizations experienced but were not able to quantify:

- **Agility and scalability.** Interviewees noted Zscaler's cloud-native architecture enhanced agility and scalability, allowing their organizations to support growing traffic and distributed user bases efficiently. This capability enabled the quick setup of new offices, high responsiveness to hybrid-working demands, and efficient handling of high-bandwidth applications. The director of cybersecurity at an insurance organization said: "Instead of trying to provision dedicated circuits from a [telecommunications company], we're now installing internet circuits where the lead time is about a week. When you think about time to production for these offices, they move in and are up and running. They are not having to wait six months for the dedicated circuits to be provisioned and installed."
- **Global coverage.** According to interviewees, Zscaler's global coverage with local internet breakouts ensured fast and reliable access to applications and data from anywhere in the world. The security architecture manager at a telecommunications organization said: "Zscaler has coverage in pretty much every European country, and

then a lot more besides that as well. The main improvement was that we were able to further take traffic off the VPN and send more direct out to the cloud."

- **Compliance and reporting.** Zscaler provided interviewees' organizations with better compliance and reporting capabilities with customizable policies and detailed insights into user activity and security incidents. The VP of enterprise security at a telecommunications organization said: "The reporting features that we can utilize for us to review what is happening in the environment were easily available and easy to use. It helps us to see where the users are spending time, the productivity of the users and know the user patterns and then helps us fine-tune the policies."
- **Employee satisfaction.** Several interviewees noted that improved user experience and seamless access to applications led to higher employee satisfaction and productivity. The director of cybersecurity at an insurance organization said: "Zscaler's ability to provide local egress points and reduce latency significantly improved the user experience. Imagine having to VPN from a remote site in Hawaii to the corporate headquarters on the East Coast and then having to wait on the search to go back to Hawaii for the information on a local restaurant. Compare that to being at a [coffee shop] in Hawaii with Zscaler on, it hits the internet locally, so the search is done in Hawaii and returned to your laptop. The second option is obviously a lot faster."

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement Zscaler Internet Access and later realize additional uses and business opportunities, including:

- **Extensibility.** Interviewees noted that Zscaler provided their organizations with extensibility, as its cloud-native architecture allowed for the integration and activation of additional features like Zscaler Private Access (ZPA), further enhancing security, enabling technology consolidation, and improving operational efficiency. For example, while this study focuses on the benefits of Zscaler Internet Access, an interviewee said their insurance organization experienced notable incremental value enhancing their Zero Trust security architecture with ZPA. The director of cybersecurity said: "From a network perspective, we increased our security posture by about 95%. We base that number on what the bad actor would have access to after compromising an employee's credentials. Through a combination of using ZPA as well as requiring MFA to gain elevated or

administrator privileges, the bad actor is very limited in the systems they can access. Users no longer have elevated rights on their account, nor do they have network access to every system, they are limited to the systems that align to their job function."

- **Future-proofing.** Interviewees reported that investing in a cloud-native, Zero Trust solution like ZIA could future-proof their organizations' security infrastructure, making it more adaptable to emerging threats and technological advancements.
- **Enhanced reputation and trust.** Strengthened security posture and compliance enhanced the interviewees' organizations' reputations and built trust with their customers, partners, and stakeholders.

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix A).

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Etr	Zscaler fees	$0	$315,000	$315,000	$315,000	$945,000	$783,358
Ftr	Implementation, training, and ongoing costs	$241,754	$74,360	$74,360	$74,360	$464,834	$426,676
	Total costs (risk-adjusted)	$241,754	$389,360	$389,360	$389,360	$1,409,834	$1,210,034

ZSCALER FEES

Evidence and data. Interviewees noted Zscaler fees were typically structured on a per-user basis, reflecting the interviewees' organizations' specific needs and the range of services included. The fees could vary based on the number of users, the specific features required, and any additional professional services or support packages opted for. This flexible pricing approach allowed the interviewees' organizations to scale their security solutions according to their growth and evolving needs, ensuring cost-effectiveness and robust security coverage.

- While several interviewees were using Zscaler Private Access (ZPA), Zscaler Digital Experience (ZDX), and other solutions, this cost component solely encompasses ZIA.
- Pricing may vary. Contact Zscaler for additional details.

Modeling and assumptions. Based on the interviews, Forrester assumes the composite organization pays Zscaler a fee of $30 per user per year for ZIA.

Risks. Forrester recognizes that these results may not be representative of all experiences. The impact of this cost will vary depending on:

- Pricing changes.
- Usage fluctuations.
- Contract terms.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $783,000.

Zscaler Fees						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	Zscaler fees	Composite		$300,000	$300,000	$300,000
Et	Zscaler fees	E1		$300,000	$300,000	$300,000
	Risk adjustment	↑ 5%				
Etr	Zscaler fees (risk-adjusted)		$0	$315,000	$315,000	$315,000
	Three-year total: $945,000			**Three-year present value: $783,358**		

IMPLEMENTATION, TRAINING, AND ONGOING COSTS

Evidence and data. Indirect costs incurred during the implementation of Zscaler at the interviewees' organizations primarily stemmed from internal labor. Interviewees typically dedicated an internal implementation team to set up the necessary infrastructure, configure policies, integrate with existing systems, and handle change management activities for proper training and adoption. Some interviewees opted to include professional services and support from Zscaler to aid in the implementation process to ensure that the system was set up correctly and efficiently. The interviewees noted their organizations allocated resources for training security, network, and IT roles on the new platform to ensure that these professionals were proficient in using Zscaler's features and could effectively manage the solution.

Additionally, interviewees dedicated IT operations or platform professionals' time to ongoing management of the Zscaler platform. These professionals were responsible for fine-tuning the system, managing policies, and addressing any issues that arise. This ongoing commitment could involve regular monitoring, updates, and adjustments to ensure optimal performance and security.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite organization employs five FTEs over four months for all change management, implementation, and rollout of ZIA in the initial period.

- The average fully burdened hourly rate for IT operations, network engineers, and information security analysts is $68, or $142,000 annually.
- There are two equivalent FTEs in IT operations, network engineering, and security analyst roles that dedicate 16 hours to learning and training with Zscaler.
- The composite organization employes half an IT operations FTE, or 1,040 hours, to ongoing management and ZIA.

Risks. Forrester recognizes that these results may not be representative of all experiences. The impact of this cost will vary depending on:

- Implementation delays.
- Training costs.
- Ongoing management complexity.
- Employee turnover.

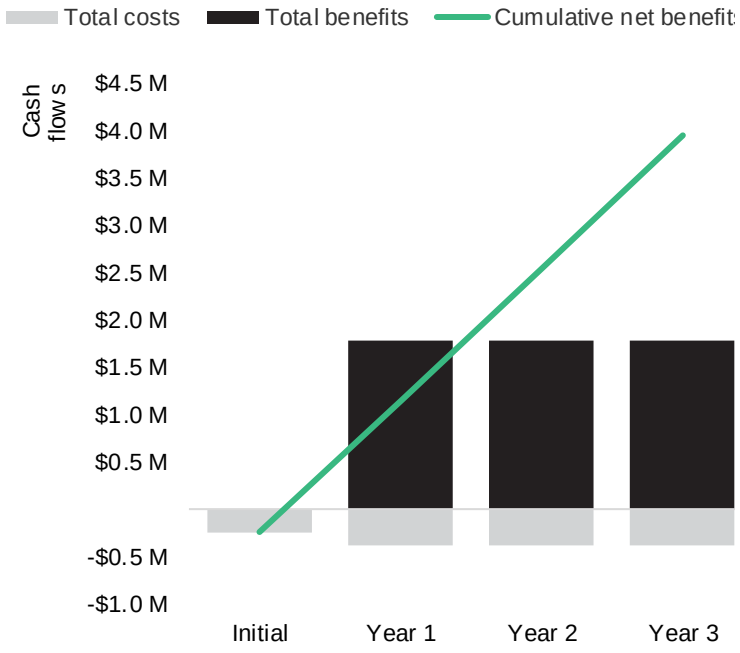
Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $427,000.

Implementation, Training, And Ongoing Costs						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
F1	Total implementation FTEs	Composite	5			
F2	Total implementation months	Composite	4			
F3	Total implementation hours	F1*F2*160 hours	3,200			
F4	Blended fully burdened hourly rate for IT operations, network engineers, and information security analysts	B4	$68			
F5	**Subtotal: Total internal implementation labor costs**	**F3*F4**	**$217,600**			
F6	Resources trained on ZIA	Composite	2			
F7	Hours of training required per IT operation and information security analyst	Interviews	16			
F8	Blended fully burdened hourly rate for IT operations, network engineers, and information security analysts	F4	$68			
F9	**Subtotal: Total training costs**	**F6*F7*F8**	**$2,176**			
F10	IT operations FTEs dedicated to ongoing management of Zscaler	Interviews		0.5	0.5	0.5
F11	Total hours dedicated to ongoing management	F10*2,080 hours		1,040	1,040	1,040
F12	Fully burdened hourly rate for IT operations	A6/2,080 hours		$65	$65	$65
F13	**Subtotal: Total ongoing costs**	**F11*F12**		**$67,600**	**$67,600**	**$67,600**
Ft	Implementation, training, and ongoing costs	F5+F9+F13	$219,776	$67,600	$67,600	$67,600
	Risk adjustment	↑10%				
Ftr	Implementation, training, and ongoing costs (risk-adjusted)		$241,754	$74,360	$74,360	$74,360
	Three-year total: $464,834			**Three-year present value: $426,676**		

Financial Summary

Consolidated Three-Year, Risk-Adjusted Metrics

Cash Flow Chart (Risk-Adjusted)



The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI, NPV, and payback period values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

Cash Flow Analysis (Risk-Adjusted)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($241,754)	($389,360)	($389,360)	($389,360)	($1,409,834)	($1,210,034)
Total benefits	$0	$1,787,110	$1,787,110	$1,787,110	$5,361,331	$4,444,279
Net benefits	($241,754)	$1,397,750	$1,397,750	$1,397,750	$3,951,497	$3,234,245
ROI						267%
Payback						<6 months

APPENDIX A: TOTAL ECONOMIC IMPACT

Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

Total Economic Impact Approach

Benefits represent the value delivered to the business by the product. The TEI methodology places equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization.

Costs consider all expenses necessary to deliver the proposed value, or benefits, of the product. The cost category within TEI captures incremental costs over the existing environment for ongoing costs associated with the solution.

Flexibility represents the strategic value that can be obtained for some future additional investment building on top of the initial investment already made. Having the ability to capture that benefit has a PV that can be estimated.

Risks measure the uncertainty of benefit and cost estimates given: 1) the likelihood that estimates will meet original projections and 2) the likelihood that estimates will be tracked over time. TEI risk factors are based on "triangular distribution."

Present Value (PV)

The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total NPV of cash flows.

Net Present Value (NPV)

The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made unless other projects have higher NPVs.

Return on investment (ROI)

A project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits less costs) by costs.

Discount rate

The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

Payback period

The breakeven point for an investment. This is the point in time at which net benefits (benefits minus costs) equal initial investment or cost.

The initial investment column contains costs incurred at “time 0” or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations in the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value calculations of the Total Benefits, Total Costs, and Cash Flow tables may not exactly add up, as some rounding may occur.

APPENDIX B: ENDNOTES

[1] Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists solution providers in communicating their value proposition to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of business and technology initiatives to both senior management and other key stakeholders.

[2] Regression analysis of the reported total cumulative costs of all breaches experienced by security decision-makers' organizations in the past 12 months. The composite organization's revenue is used as the input to the regression formula. Source: Forrester's Security Survey, 2024, "Using your best estimate, what was the total cumulative cost of all breaches experienced by your organization in the past 12 months?" Base: 1,660 global security decision-makers whose organization has experienced a breach in the past 12 months.

[3] Regression analysis of the likelihood of experiencing one or more breaches using the frequency that organizations experienced breaches in the past 12 months as reported by security decision-makers. The composite organization's revenue is used as the input to the regression formula. Source: Forrester's Security Survey, 2024, "How many times do you estimate that your organization's sensitive data was potentially compromised or breached in the past 12 months?" Base: 2,769 global security decision-makers

[4] Percentage of breaches by primary attack vector for breaches, as reported by security decision-makers whose organizations experienced at least one breach in the last 12 months. Source: Forrester's Security Survey, 2024, "Of the times that your organization's sensitive data was potentially compromised or breached in the past 12 months, please indicate how many of each fall into the categories below." Base: 1,542 global security decision-makers whose organization has experienced a breach in the past 12 months.

FORRESTER®