FORRESTER®

The Total Economic Impact™ Of Cisco Umbrella Secure Internet Gateway (SIG) And Security Service Edge (SSE)

Cost Savings, Business Benefits, And Risk Reduction Enabled By Umbrella SIG/SSE

JANUARY 2023

A FORRESTER TOTAL ECONOMIC IMPACT™ STUDY COMMISSIONED BY CISCO

Table Of Contents

Consulting Team: Henry Huang
Kara Luk

ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key transformation outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute on their priorities using a unique engagement model that tailors to diverse needs and ensures lasting impact. For more information, visit forrester.com/consulting.

Executive Summary

> The shift toward hybrid environments with greater cloud and internet usage is transforming how organizations think about securing their workers and environments. Securing internet and network access at the edge is what's important today with distributed workforces. Cisco Umbrella SIG/SSE provides such a capability, securing internet access and controlling application usage across networks, branch offices, and roaming users. As workers become increasingly mobile, SASE capabilities need be the next point of emphasis for security.

Cisco Umbrella SIG/SSE is a cloud-delivered security service that secures user access to the internet and usage of applications with a simplified experience. It helps protect people and data everywhere, enforce granular access and activity controls, and streamline the user experience and administrative duties.

KEY STATISTICS

Return on investment (ROI)
231%

Net present value (NPV)
$1.96M

Organizational users move between locations — whether it's through internal networks, hotel in Europe, a SD-WAN site in Australia, or at home through public internet. With users located anywhere accessing data and applications services, securing access at the service edge (SASE) and applying a Zero Trust Edge (ZTE) approach become more important than ever. With the divided work environments, organizations need to address security for users connected to the corporate network as well roaming users who are now freely moving and commonly falling under a different security shelter. Senior Analyst David Holmes of Forrester said, "In the future, as technologies like secure web gateway (SWG), cloud access security broker (CASB), and data loss prevention (DLP) are integrated into the [security] stack, organizations will look to put all their network traffic through these ZTE networks."[1]

Efficacy of DNS and SWG beyond legacy tools

30%

Cisco commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Umbrella SIG/SSE.[2] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Umbrella on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed representatives from seven different organizations with experience using Cisco Umbrella SIG/SSE. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization as a holistic representation. The composite organization is global enterprise that has embraced hybrid work and cloud usage. Detailed information on the composite is available via the link above.

Prior to using Umbrella, many of the interviewees noted how their organizations were in a phase of adjustment as workloads transitioned more towards cloud- and internet-based applications and services. Having visibility into and being able to secure this frontier was a newfound challenge where remote and hybrid work became the norm virtually overnight, driven by the pandemic. New and more exposed attack surfaces were now made available to threat actors, especially when users were off the corporate network. Utilizing legacy proxies to block certain ports was simply insufficient and inefficient. Organizations required an efficient, consolidated, yet comprehensive set of security services delivered from the cloud to secure the new work landscape.

After the investment in Umbrella, the interviewees gained features such as DNS security, secure web gateway, and cloud access security broker (CASB), among other capabilities — all delivering security to users wherever and whenever.

Key results from the investment included improved security efficacy, enhanced security posture through quicker policy establishment and enforcement, reduced chance of data breaches, and lower operational effort.

KEY FINDINGS

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

- **Security efficacy improvement of 30% reduces security incidents and associated remediation work.** Protecting users at the top layers of DNS and SWG with greater defense efficacy reduces the number of incidents, investigations, and remediation efforts at the composite organization. Information security (infosec) investigations tasks go down by as much as 80% in some organizations. Over three years, this new level of protection is worth more than $526,200 to the composite organization, particularly the information security (infosec) team.

> **“The end-user is on the edge now and Umbrella is the product that allows our users to be secure wherever they are. Users can no longer hide behind [corporate] firewalls. You can no longer think you’re safe behind a proxy. Umbrella allows us to secure all that web traffic.”**
>
> *IT security specialist, utilities*

- **Policy establishment and enforcement time savings.** Establishing and maintaining policies on Umbrella was much more straightforward as opposed to establishing policies on multiple appliances or individual services— such as firewalls and proxies — across multiple devices, especially with Active Directory integrations. The time it takes the composite organization to provision, establish, and enforce rules is reduced by 65% with Umbrella from its prior environment.

  “We set it and forget it with the ease to adjust. Without Umbrella, it’d be a huge exercise,” stated the Head of global network and technologies at a pharmaceutical organization.

- **Reduction of breach-related costs.** Blocking threats reduces data breaches to the tune of 21%, a figure that represents Umbrella SIG’s capabilities, efficacy, and its role in the security stack. Adjustments to the impact on breach reduction based upon these factors as well as

Decrease in the effort to deploy and enforce web and cloud policies

65%

risks were factored into the analysis.[3] The reduction of breach likelihood translates into lower compensatory, remedial, regulatory, reputational costs, among others, for the composite organization. The solution also minimizes internal user downtime, which also plays a factor. The present value of the total three-year loss reduction is just north of $1 million.

- **Decreased operational costs.** Policy operations across the network become simpler and more consistent with the cloud managed Umbrella solution. As a result, the composite organization reallocates up to 50% of its people's effort to other centers within the infosec group. This drastically reduces management of the services and physical appliances running security by 67%. The present value of this benefit over three-years amounts to $354,300.

- **Avoided costs of legacy services.** Utilizing Cisco Umbrella can often replace the need for legacy disparate solutions like CASB, web gateway licenses, and separate firewalls for cloud security. The Umbrella SIG/SSE licenses combine these functions in a single solution along with DNS-layer security. The deprecation of existing solutions amounts to $231,300 in a three-year period.

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

- **Data loss prevention adds intellectual property (IP) protection, but it is too early to be quantified.** Several interviewees indicated that DLP was being implemented, but the value of it is yet to be measured. The composite organization similarly has IP to be protected but, as every organization assigns a different value to their trade secrets and IP, the value of this protection varies greatly between organizations and is not represented in this study's calculations.

> **"We wanted a solution that would protect us both on and off the network. No matter where people go in the world, our policies became easily manageable from a central point on Umbrella. That was key to us being able to keep security [posture] consistent across the globe."**
>
> *Senior network engineer, manufacturing org*

- **Faster integration with existing environments.** Many of the interviewees' organizations had Cisco components in their existing network and security stacks, and the use of Umbrella led to a much faster integration. For instance, policies were migratable across environments, which allowed for quicker changes as needed. Contextual data flow between devices also allowed for better visibility across the board.

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

- **Licensing and implementation costs.** The Umbrella SIG Essentials licensing package with enhanced support has a three-year PV cost of approximately $673,100. Implementation efforts are also incorporated, which are minimal for this cloud-centric solution.
- **Training and administration costs.** The internal costs of adjustment, training, and administration are assumed when moving to the Umbrella cloud-delivered service. The new assessments of policies along with realignment and testing require approximately 112 hours for infosec personnel at the composite organization. Training provided to business users on average amounts to 15 minutes per user. Total costs over three years are $175,600, PV.

The representative interviews and financial analysis found that a composite organization experiences benefits of $2.81M over three years versus costs of $849K, adding up to a net present value (NPV) of $1.96M and an ROI of 231%.

EXECUTIVE SUMMARY

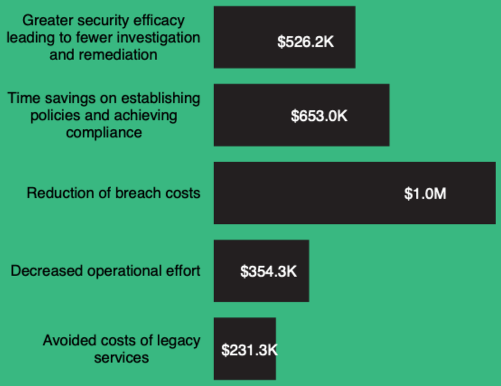
ROI
231%

BENEFITS PV
$2.81M

NPV
$1.96M

PAYBACK
<12 months

Benefits (Three-Year)



3.5 hours of investigation effort saved per true incident that Umbrella repels.

65% decrease in the effort to deploy and enforce web and cloud policies.

30% improvement in detection over legacy solutions.

> **“The network is tremendously more secured now, and the fact that we're protecting machines off network with the same rule sets that we have on network eliminated a ton of threats for our hybrid workforce.”**
>
> — Senior network engineer, manufacturing org

TEI FRAMEWORK AND METHODOLOGY

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

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 Umbrella can have on an organization.

The seven in-depth customer interviews, conducted in Q4 2022, were the primary source of data for this TEI analysis. Supplemental data came from an online survey that Forrester Consulting conducted in November 2020 of 351 cybersecurity leaders at global enterprises in the US, the UK, Canada, Germany, and Australia. Survey participants included managers, directors, VPs, and C-level executives who are responsible for cybersecurity decision-making, operations, and reporting. Questions provided to the participants sought to evaluate leaders' cybersecurity strategies and any breaches that have occurred within their organizations.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by Cisco and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the study to determine the appropriateness of an investment in Umbrella.

Cisco reviewed and provided feedback to Forrester, but Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study.

Cisco provided the customer names for the interviews but did not participate in the interviews.

DUE DILIGENCE
Interviewed Cisco stakeholders and Forrester analysts to gather data relative to Umbrella.

INTERVIEWS
Interviewed representatives at seven organizations using Umbrella SIG/SSE to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION
Designed a composite organization based on characteristics of the interviewees' organizations.

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.

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 Cisco Umbrella Customer Journey

🟩 Drivers leading to the Umbrella investment

Interviews

Role	Industry	Region	Total Employees
Systems programmer	Utilities	North America	10,000+
Senior network engineer Cybersecurity engineer	Manufacturing	Global, 200+ countries	50,000+
Cybersecurity engineer	Healthcare	North America	3,000+
IT security specialist	Utilities	Asia Pacific	500+
Head of global networking	Pharmaceuticals	Global, 50+ countries [Europe based]	10,000+
Senior cybersecurity analyst	Government	North America	3,500+
Executive director of enterprise architecture and cybersecurity	Utilities and energy	North America	1,000+

KEY CHALLENGES

The fast-paced transition to the new hybrid work environment challenged interviewees' organizations. Users are no longer beholden to the office, which is behind the traditional protection of corporate network defenses. As users moved off the network and onto the internet and more cloud-oriented applications, exposure to new attack surfaces and lateral movement became top of mind for organizations. With the new changes in how work was being done and the need to sharply improve overall security posture, the organizations set out to flesh out their security stack.

The interviewees noted how their organizations struggled with common challenges, including:

- **The changing work environment required new forms of cyber protection.** The COVID-19 pandemic forced most employees to work from home. While some have come back to the office, many of these organizations were facing the truth that remote work and hybrid work was here to stay — meaning that workers who now roamed off the corporate network were no longer protected with the same measures as provided by the corporate security stack, necessitating new protection mechanisms. Endpoint detection systems too, were no longer adequate. As a senior cybersecurity engineer from a government entity put it, "We need to protect devices and roaming clients regardless of where they work, in a manageable way."

> **"Our existing solution ground to a screeching halt because there was so much traffic to get decrypted, inspected, re-encrypted and sent up, which was a recipe for disaster because we just didn't have the manpower."**
>
> *Systems programmer, utilities*

> **"During the times of COVID-19 and on, many malware and hacking attempts were put on to our SOC system. We needed to protect our clients when they're not present and when they're not connected to the company resources."**
>
> *Network security manager, pharmaceuticals*

- **A continued shift to cloud services changed the security equation.** Interviewees commented on too many policies spread across a plethora of on-premises appliances, generating extensive maintenance and inconsistent policy enforcement. With the move to the cloud, organizations needed streamlined, easily manageable policies and rules with granular controls such as tenant controls or what actions are/are not allowed within a cloud app.
- **Congestion at legacy proxies and data centers.** Protecting remote users and those that traveled off of the network was important to the organizations. However, using VPN and hauling data back and forth to company data centers was simply inefficient. The general performance of workloads was subpar, but connectivity and being able to conduct any business with reasonable efficiency was also questionable at times.

  The network security department manager at a pharmaceuticals company stated: "Before Umbrella, we used a proxy that was on VPN, tunneling all traffic back to HQ and then back to the user. We realized eventually that it wasn't providing an optimal user experience and there was no purpose to move that back traffic back and forth from HQ when there was a cloud solution in Umbrella."

  Another interviewee identified similar inefficiencies in data transport prior to Umbrella and stated that the choke points where data moved through was strangling user performance.

INVESTMENT OBJECTIVES

The interviewees' organizations searched for a solution that could:

- Secure workers while off the corporate network.
- Offload traffic from their data center security stack where possible.
- Leverage security at the DNS layer to stop threats early in the chain.
- Simplify integration with the existing security stack.
- Streamline and simplify management of security rules and policies.
- Add visibility into user activity to simplify remediation.

> **"We needed protection for our web traffic and DNS queries to outside in the world to be able to secure our environment there. Cisco, with how their products play well together, was our choice."**
>
> *Cybersecurity engineer, healthcare*

After a request for proposal (RFP) and business case process evaluating multiple vendors, the interviewees' organizations chose Umbrella and began deployment.

COMPOSITE ORGANIZATION

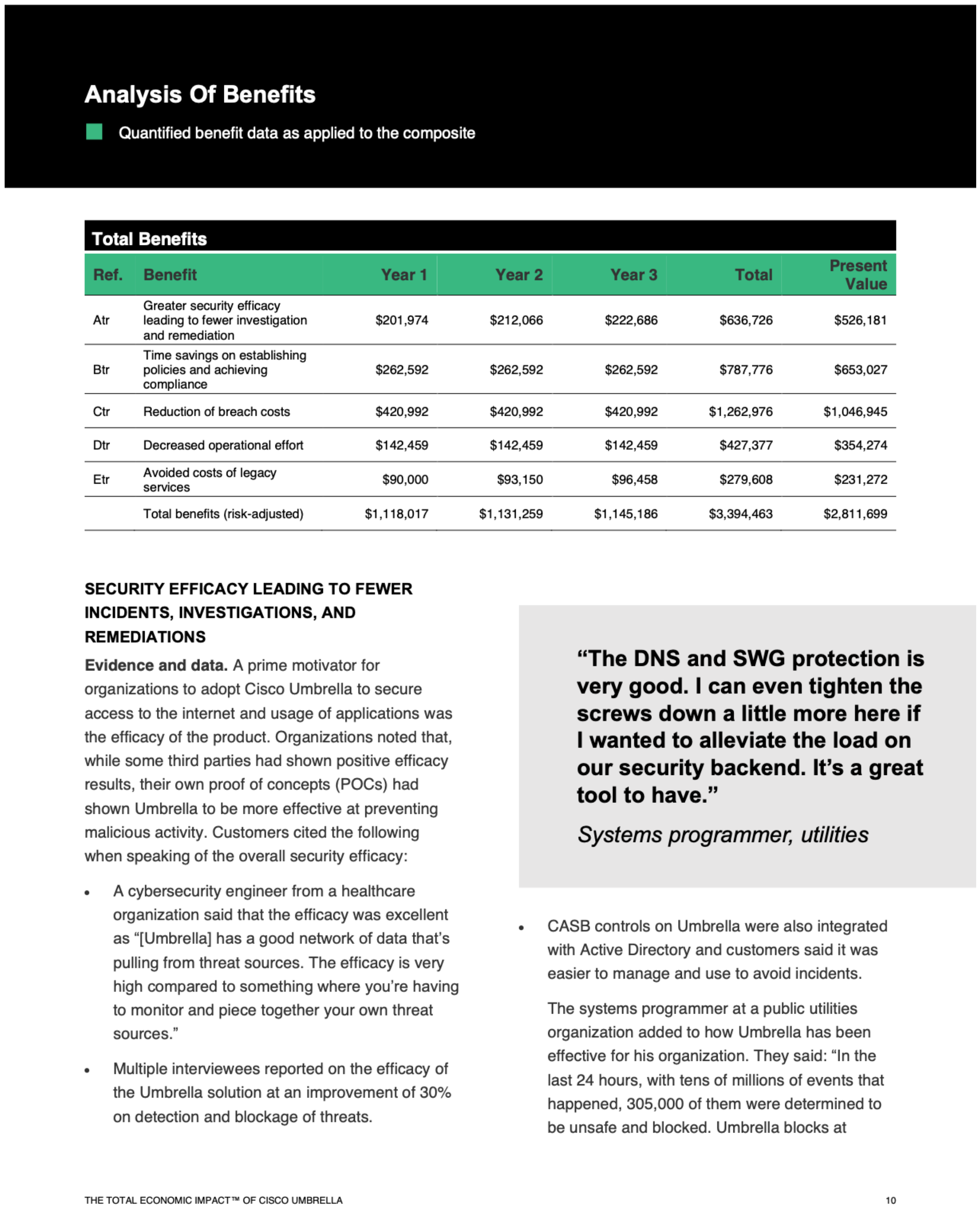
Based on the interviews, Forrester constructed a TEI framework, a composite company, and an ROI analysis that illustrates the areas financially affected. The composite organization is representative of the seven interviewees, and it is used to present the aggregate financial analysis in the next section.

The composite organization is necessary for the comprehensive financial analysis, yet it is instructive to note that Umbrella SIG/SSE is being used in organizations ranging from very small to very large, across all industries, in all geographies.

Description of composite. The composite is a global organization with over 10,000 employees operating in a hybrid work environment with some workers in office and some off the corporate network. It has been on a digital transformation journey with many of its applications services now in the cloud. With the shift towards more cloud-delivered applications, it seeks to focus on security at the edge with a cloud-brokered solution. The composite understands that work may never return to a fully back-to-office approach, especially with workers becoming more globally distributed. Finally, the composite had a significant security stack and global data centers. There is a heavy desire to keep things tightly knit in the Cisco family with the optionality to integrate with other security providers.

Key Assumptions

- **Global organization**
- **10,000+ employees**
- **40% of workloads in the cloud**
- **Priority — Protect hybrid work environment**
- **Umbrella SIG/SSE usage — DNS, SWG, CASB policies**



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	Greater security efficacy leading to fewer investigation and remediation	$201,974	$212,066	$222,686	$636,726	$526,181
Btr	Time savings on establishing policies and achieving compliance	$262,592	$262,592	$262,592	$787,776	$653,027
Ctr	Reduction of breach costs	$420,992	$420,992	$420,992	$1,262,976	$1,046,945
Dtr	Decreased operational effort	$142,459	$142,459	$142,459	$427,377	$354,274
Etr	Avoided costs of legacy services	$90,000	$93,150	$96,458	$279,608	$231,272
	Total benefits (risk-adjusted)	$1,118,017	$1,131,259	$1,145,186	$3,394,463	$2,811,699

SECURITY EFFICACY LEADING TO FEWER INCIDENTS, INVESTIGATIONS, AND REMEDIATIONS

Evidence and data. A prime motivator for organizations to adopt Cisco Umbrella to secure access to the internet and usage of applications was the efficacy of the product. Organizations noted that, while some third parties had shown positive efficacy results, their own proof of concepts (POCs) had shown Umbrella to be more effective at preventing malicious activity. Customers cited the following when speaking of the overall security efficacy:

- A cybersecurity engineer from a healthcare organization said that the efficacy was excellent as "[Umbrella] has a good network of data that's pulling from threat sources. The efficacy is very high compared to something where you're having to monitor and piece together your own threat sources."
- Multiple interviewees reported on the efficacy of the Umbrella solution at an improvement of 30% on detection and blockage of threats.
- CASB controls on Umbrella were also integrated with Active Directory and customers said it was easier to manage and use to avoid incidents.

  The systems programmer at a public utilities organization added to how Umbrella has been effective for his organization. They said: "In the last 24 hours, with tens of millions of events that happened, 305,000 of them were determined to be unsafe and blocked. Umbrella blocks at

> **"The DNS and SWG protection is very good. I can even tighten the screws down a little more here if I wanted to alleviate the load on our security backend. It's a great tool to have."**
>
> *Systems programmer, utilities*

multiple levels but blocking more at the DNS level in particular helps us save money. It helps prevent work from trickling down further into the security stack where more work would come up."

He went on to say, "The SWG helped filter and stop the bad stuff ahead of time in the cloud before it made it to our environment while also reducing noise. DLP is a piece that we expect to provide another layer of protection over time."

Security Efficacy Leading To Fewer Incidents, Investigations, And Remediations

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Efficacy/detection improvement of Umbrella from legacy solutions, inclusive of DNS and web gateway	Interviews	30%	30%	30%
A2	Total number of alerts through DNS and web gateway, per year, prior to Umbrella	Interviews	2,555	2,683	2,817
A3	Decreased true positive alerts, per year	Interviews	766.5	804.8	845.1
A4	Time required per alert for investigation (hours)	Forrester internal metrics	3.5	3.5	3.5
A5	Time required per alert for remediation (hours)	Forrester internal metrics	3.8	3.8	3.8
A6	Percent of investigations needing remediation	Forrester internal metrics	15%	15%	15%
A7	Cost of security analyst per hour	TEI standard	$68.15	$68.15	$68.15
At	Security efficacy leading to fewer incidents, investigations, and remediations	A1*A2*A3*A4	$212,604	$223,228	$234,406
	Risk adjustment	↓5%			
Atr	Security efficacy leading to fewer investigations, and remediations (risk-adjusted)		$201,974	$212,066	$222,686
	Three-year total: $636,726		Three-year present value: $526,181		

Modeling and assumptions. Forrester modeled the output based upon on the following in conjunction with what is presented in Table A:

- Alerts and threats in general are expected to rise over time. As such, Forrester modeled this into its analysis.
- The rise in efficacy from the introduction of Umbrella is 30% for the composite organization, resulting in a deflection of threats that would potentially penetrate its defenses.
- The DNS, CASB, and SWG defense layers are all accounted for in the 30% estimation of deflection improvement.
- The time required for investigations, triage, and remediation are based upon Forrester's internal Cost of a Security Breach done in Q4 2020, with a sample of 351 respondents.[4]

Risks. Forrester has incorporated two risks into this model category:

- Variability in existing in-house capabilities with previous technologies.
- Augmented security staff using managed service providers (MSPs) change the benefit to the organization.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $526,200.

TIME SAVINGS ON ESTABLISHING POLICIES AND ACHIEVING COMPLIANCE

Evidence and data. The interviewees noted saving time and costs on not only establishing policies but also maintaining the established policies. The number of prior disparate solutions and numerous policies spread across these solutions led to duplicative efforts to set and then maintain these policies. Gaining compliance was achieved more quickly because of the faster policy deployment and easier enforcement. Primary drivers of the efficiency gain and faster achievement of compliance are rooted in the following:

- Switching from a varied number of disparate solutions to a centralized solution reduced the number of policies for interviewees' organizations by as much as 90%, with one going from more than 400 rules to 15 by centralizing on Umbrella.
- Organizational representatives saw that provisioning policies for instances with Umbrella were much faster than their traditional on-premises exercises, even if they were provisioning virtually.
- Achieving compliance and maintaining it became easier as visibility on a single pane of glass simplified monitoring of errant user activity.

  One interviewee stated that the task of updating and maintaining policies reduced manual effort by two-thirds, especially as policies in Umbrella were linked to Active Directory.
- For example, the utilities organization needed to allow the term "firearms" for certain groups for investigative work. The systems programmer at the organization said, "Normally the term is blocked across a myriad of devices, but we could change it very quickly in a few minutes on Umbrella."

> **"Cisco SIG integrates with Active Directory so we're able to clearly delineate who should have access to what easily. We have a set of polices in one place and don't have to do duplicative work to get it done. It's efficient to manage all of that and it's instantaneous."**
>
> *Cybersecurity engineer, healthcare*

Modeling and assumptions. Forrester has modeled the output based upon on the following in conjunction with what is presented on Table B.

- The organization — which again is in a hybrid work setup — uses 200 web and cloud access policies as a whole.
- Coming from a solution based on disparate proxies, firewalls, and CASB solutions, the organization greatly reduces the quantity of policies with Umbrella SIG/SSE with simplified and centralized policy management leading to consistent policy enforcement. This leads to a 65% improvement in enforcement efficiency.
- Changes to policies are also quicker and are included in the 65% decrease in effort stated above.

Risks. Forrester has identified some risks that can impact the benefit depicted in this section:

Time Savings On Establishing Policies And Achieving Compliance

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Web and cloud policies across existing legacy environment	Interviews	200	200	200
B2	Decrease in effort to deploy and enforce web and cloud policies	Interviews	65%	65%	65%
B3	Security analyst FTE required for policy deployment and enforcement	Assumption	3	3	3
B4	Security analyst FTE annual compensation	TEI standard	$141,750	$141,750	$141,750
Bt	Time savings on establishing policies and achieving compliance	B1*B2*B3*B4	$276,413	$276,413	$276,413
	Risk adjustment	↓5%			
Btr	Time savings on establishing policies and achieving compliance (risk-adjusted)		$262,592	$262,592	$262,592
Three-year total: $787,776		Three-year present value: $653,027			

- The number of cloud policies is hinged on the degree of shift to the cloud apps.

Results. To account for this risk, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $653,000.

REDUCTION OF BREACH COSTS

Evidence and data. The interviewees of this study cited benefits of reduced breaches. Forrester internal research indicates that organizations are breached on average 2.5 times per year, with costs amounting to over $600,000 per breach and further cost impacts on internal users[5].

Security efficacy on the front line with DNS-layer security and deeper, more granular security from SWG and CASB capabilities were key to many of the customers. The ability to properly posture their security policies — and adjust as necessary to activities and threats — was important.

The interviewee from a healthcare organization stated, "With [Umbrella] SWG, we were able to manage the policies on a granular level and filter what really stops the bad stuff ahead of time so that it doesn't even get into our environment."

> **"We're securing our web traffic and DNS traffic on every single endpoint, no matter where they are in the world. That's the number one thing about Umbrella."**
>
> *IT security specialist, utilities*

Automated blocking helped another customer prevent breaches by stopping it at the top layers. The senior cyber security analyst from a government entity said: "It comes down to the availability of it being able to travel with our devices anywhere they go. The automation of just being able to check at the DNS and web filter level is important as those are the busiest traffic pieces — and it's far too much for anyone to attempt to sort and deal with on a case-by-case basis. The tool automation is absolutely necessary and the way that Umbrella gives us the tools to manage those policies and apply those protections are absolutely critical."

Most importantly, interviewees cite that as their traffic has migrated off-network, Umbrella has become a critical part of cyber defense. In conjunction with other tools like Cisco SecureX, threats were stopped before any lateral movement could transpire.

Modeling and assumptions. Forrester models the composite organization as follows:

- Forrester internal research suggests an average of 2.5 severe breaches per year for an enterprise of the composite organization's size.
- The average cost of a breach for an organization of this size is $605,274 exclusive of lost worker productivity.
- Internal worker productivity loss is estimated to be $150,000 per year based on 15% of 10,000 workers that are affected per incident. A productivity recapture rate on the costs is applied and reflected in the $150,000 cost.
- The percentage of attacks that can be reduced by Umbrella, with the understanding that technology, people, and process all play a role, is 21%.

Risks. The risk of a material breach may vary with the following:

- The number of actual breaches experienced.
- The vertical of the organization.
- The regulatory/geographical footprint of the organization.

Reduction Of Breach Costs

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Likely number of breaches annually	Forrester internal metrics	2.5	2.5	2.5
C2	Cost of a material breach	Forrester internal metrics	$605,274	$605,274	$605,274
C3	Attribution of breach reduction to coverage by Umbrella	Interviews and Forrester metrics	21%	21%	21%
C4	Subtotal: risk reduction cost due to Umbrella	C1*C2*C3	$317,769	$317,769	$317,769
C5	Percentage of internal users impacted by each breach (of 10,000 FTE)	Interviews and Forrester metrics	15%	15%	15%
C6	Average fully burdened hourly rate of general employee	TEI standard	$40	$40	$40
C7	Subtotal: cost to internal users on downtime and lost productivity	C1*C5*C6*10,000	$150,000	$150,000	$150,000
Ct	Reduction of breach costs	C4+C6	$467,769	$467,769	$467,769
	Risk adjustment	↓10%			
Ctr	Reduction of breach costs (risk-adjusted)		$420,992	$420,992	$420,992
	Three-year total: $1,262,976		Three-year present value: $1,046,945		

> **“We have sandboxing tools built into our environment that are fed by Umbrella SIG, so when people are downloading files, it’s automatically sandboxing those, making sure they’re safe before they’re executed. That puts us in a much better position.”**
>
> *Senior cybersecurity analyst, government*

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $1 million.

DECREASED OPERATIONAL EFFORT

Evidence and data. Operational effort prior to Cisco Umbrella at the interviewees’ organizations was concentrated on on-premises appliances and a number of proxy servers. With the shift to Umbrella, these organizations diverted operational effort to Cisco’s cloud services.

.

- Interviewed Cisco customers spoke of operational efficiency from using a single cloud-based pane of glass to manage policies and control measures.
- Without multiple proxy servers to manage, interviewees cited those operational efforts decreased by as much as 75%, with many stating a decrease of two-thirds of their work effort.

Modeling and assumptions. Forrester assumes for the composite the following in the calculations:

- The composite organization shifts from an on-premises heavy model to a cloud-centric model and thus reduces operational requirements and costs.

Decreased Operational Effort

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Operational management effort for disparate legacy solutions, in FTE	Interviews	3	3	3
D2	Percentage of effort dedicated to web / DNS/CASB security	Interviews	50%	50%	50%
D3	Reduction in management and operational effort	Interviews	67%	67%	67%
D4	Security analyst FTE annual compensation	TEI standard	$141,750	$141,750	$141,750
Dt	Decreased operational effort	D1*D2*D3*D4	$142,459	$142,459	$142,459
	Risk adjustment	0%			
Dtr	Decreased operational effort (risk-adjusted)		$142,459	$142,459	$142,459
	Three-year total: $427,377		Three-year present value: $354,274		

- The centralization of cloud controls reduces the effort necessary to manage policies by 67% percent.

Results. With all factors accounted for, Forrester projects a three-year, total PV of $354,300 attributable to a decrease in operational effort.

> **“We went from three people managing a weekly task to one person that now does Umbrella. It’s just that much of a simpler tool.”**
>
> *Executive director, cybersecurity, APAC energy*

AVOIDED COSTS OF LEGACY SERVICES

Evidence and data. Many interviewees mentioned that their enterprises were fairly mature with their security programs and moved to Cisco Umbrella SIG/SSE from existing security appliances and separate cloud services to leverage new capabilities and efficiency benefits. Being able to move away from legacy services provided avoided license and service costs.

- Organizations recognized the shift to remote and hybrid work and consequently moved to secure those users, which equated to the implementation of CASB, DNS, and SWG level protections.
- Interviewees generally spoke of being able to sunset existing solutions by migrating to Cisco Umbrella.
- Costs of preexisting CASB and SWG products varied but fell between $1 to $10 per user for the products.

Modeling and assumptions. For the composite, Forrester models the following:

- Legacy CASB and SWG licenses are now replaced by Umbrella (with new costs represented in the cost sections).
- DNS costs are not accounted for as the variance in using proxies, true DNS protection, and band-aid solutions was inconclusive between organizations. Readers should consider the cost of sunsetting DNS protection as an added benefit if it applies.

> **“Our entire CASB project was able to be replaced with this. It saved time and it saved me money while giving me something that I was sure was going to work.”**
>
> *Systems programmer, utilities*

Risks. The benefit from sunsetting prior solutions will vary depending on:

- The types and extensiveness of CASB within the prior state.
- Existing SWG licensing terms, should it be for user-based, bandwidth-based, or another metric.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $231,300.

Avoided Costs Of Legacy Services

Ref.	Metric	Source	Year 1	Year 2	Year 3
E1	Legacy CASB and web gateway security licenses	Composite	10,000	10,500	11,025
E2	Cost per CASB license	Composite	$6	$6	$6
E3	Cost of additive CASB options	Composite	$1	$1	$1
E4	Cost of web gateway license	Composite	$30,000	$30,000	$30,000
Et	Avoided costs of legacy services	E1*(E2*E3)+E4	$100,000	$103,500	$107,175
	Risk adjustment	↓10%			
Etr	Avoided costs of legacy services (risk-adjusted)		$90,000	$93,150	$96,458
	Three-year total: $279,608		Three-year present value: $231,272		

UNQUANTIFIED BENEFITS

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

- **Data loss prevention is a top-of-mind line item.** Company IP is the crux of how organizations succeed. Even with external attacks extinguished, internally leaked (intentionally or inadvertent) material can lead to high costs. Interviewees' organizations, especially those in the critical infrastructure verticals, cited that any loss of IP would result in a dramatic loss in organizational value and crippling effects at worst.

  Many of the interviewees were incorporating DLP as a part of Umbrella but the value was yet unclear as the implementation and plans to implement were only recent. Depending on the type of business vertical, this value can vary significantly.

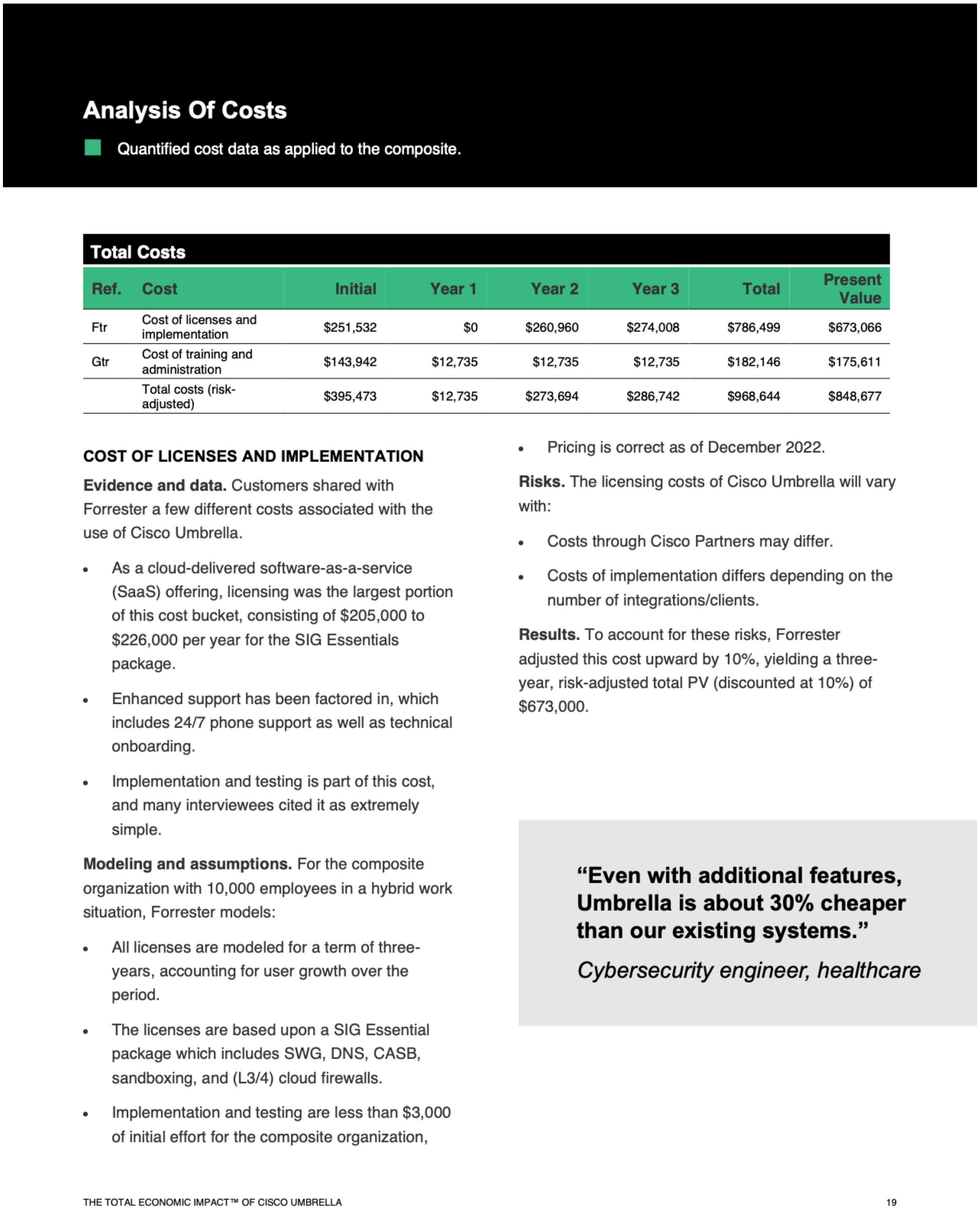
- **Quicker and tighter knit integration with Cisco security products.**
  - **Make changes faster and do things quicker with integrations.** Cisco network infrastructure is prevalent, from switches to firewalls and beyond. Interviewees reported quick integrations and the ability to observe on a consolidated pane of glass for activities. While this effect hasn't been quantified, Forrester believes the time to value and greater context shared between solutions benefits both the infosec and operational side and provides business level benefits of decreased downtime.

FLEXIBILITY

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

- **The use of Umbrella in conjunction with other Cisco products, such as firewalls, endpoint detection, and SecureX amplify protection.** Built-in, native connectivity between the products inherently provides a deeper level of information flow between systems, leading to better and faster contextualized information. Control is also smoother in such situations, which makes for improved protection and faster response times.

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
Ftr	Cost of licenses and implementation	$251,532	$0	$260,960	$274,008	$786,499	$673,066
Gtr	Cost of training and administration	$143,942	$12,735	$12,735	$12,735	$182,146	$175,611
	Total costs (risk-adjusted)	$395,473	$12,735	$273,694	$286,742	$968,644	$848,677

COST OF LICENSES AND IMPLEMENTATION

Evidence and data. Customers shared with Forrester a few different costs associated with the use of Cisco Umbrella.

- As a cloud-delivered software-as-a-service (SaaS) offering, licensing was the largest portion of this cost bucket, consisting of $205,000 to $226,000 per year for the SIG Essentials package.
- Enhanced support has been factored in, which includes 24/7 phone support as well as technical onboarding.
- Implementation and testing is part of this cost, and many interviewees cited it as extremely simple.

Modeling and assumptions. For the composite organization with 10,000 employees in a hybrid work situation, Forrester models:

- All licenses are modeled for a term of three-years, accounting for user growth over the period.
- The licenses are based upon a SIG Essential package which includes SWG, DNS, CASB, sandboxing, and (L3/4) cloud firewalls.
- Implementation and testing are less than $3,000 of initial effort for the composite organization,
- Pricing is correct as of December 2022.

Risks. The licensing costs of Cisco Umbrella will vary with:

- Costs through Cisco Partners may differ.
- Costs of implementation differs depending on the number of integrations/clients.

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 $673,000.

> **"Even with additional features, Umbrella is about 30% cheaper than our existing systems."**
>
> *Cybersecurity engineer, healthcare*

Cost Of Licenses And Implementation

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	Umbrella SIG Essentials licensing	Vendor provided	$205,400		$215,670	$226,454
F2	Umbrella enhanced support	Vendor provided	$20,539		$21,566	$22,644
F3	Implementation effort	40 hours at $68.15/hour	$2,726			
Ft	Cost of licenses and implementation	F1+F2+F3	$228,665	$0	$237,236	$249,098
	Risk adjustment	↑10%				
Ftr	Cost of licenses and implementation (risk-adjusted)		$251,532	$0	$260,960	$274,008
	Three-year total: $786,499		Three-year present value: $673,066			

COST OF TRAINING AND ADMINISTRATION

Evidence and data. Interviewees shared their experiences of training and administration of the Umbrella product with Forrester, which was spread between the following:

- A large part of this cost bucket belonged to a period of assessment, adjustment, and realignment of policies — a reset, as some interviewees put it.

> **"Policies took about a couple of weeks and then the overall deployment was about two to three months, taking about an hour a week for the infosec team."**
>
> *Senior cybersecurity analyst, government*

- Integration with other parts of the security stack was necessary for many of the organizations, but it was minimal and only in the initial deployment phase.
- Training material for end users was negligible but training for the end users amounted to 15 minutes per employee.

Modeling and assumptions. For the composite organization, Forrester models:

- The assumption of 15 minutes of training applies to the composite organization of 10,000 employees, with ongoing costs reflective of employee turnover at 10%.
- Policy enforcement and adjustment is an ongoing task and is assumed to be minimal at a rate of $3,544 per year.
- Administrative costs on this cloud platform beyond policy adjustments is negligible and hence left out of calculations.

Risks. The cost of training and administration can vary with the following:

- Vertical related deltas and distribution of workforce.

- The footprint of the organization and variance in footprints along with the associated requirements.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $175,600.

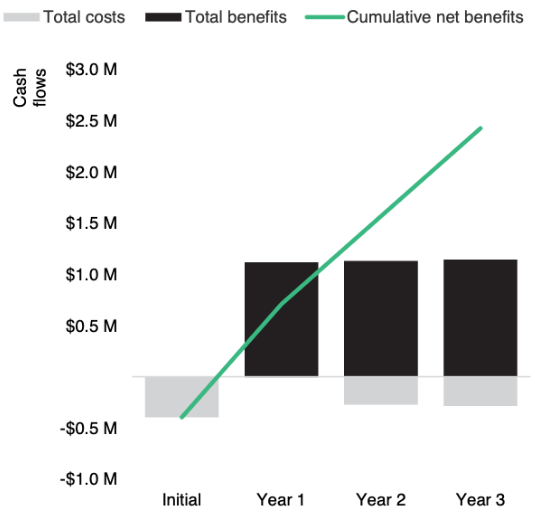
Cost Of Training And Administration

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
G1	Policy realignment and deployment (hours)	Composite	112			
G2	Average fully burdened hourly rate	TEI standard	$68.15			
G3	Time and cost of policy realignment and deployment	G1*G2	$30,531			
G4	Policy enforcement and adjustments	Composite		$3,544	$3,544	$3,544
G5	Integration effort to security stack	Composite	$20,000			
G6	Training time (hours)	Composite	.25			
G7	Average fully burdened hourly rate	TEI standard	$35.70			
G8	Number of employees trained	Composite	9,000			
G9	Employee training	G6*G7*G8	$80,325	$8,033	$8,033	$8,033
Gt	Cost of training and administration	G3+G4+G5+G9	$130,856	$11,577	$11,577	$11,577
	Risk adjustment	↑10%				
Gtr	Cost of training and administration (risk-adjusted)		$143,942	$12,735	$12,735	$12,735
	Three-year total: $182,146			**Three-year present value: $175,611**		

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 Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($395,473)	($12,735)	($273,694)	($286,742)	($968,644)	($848,677)
Total benefits	$0	$1,118,017	$1,131,259	$1,145,186	$3,394,463	$2,811,699
Net benefits	($395,473)	$1,105,283	$857,565	$858,444	$2,425,818	$1,963,022
ROI						231%
Payback period (months)						<12

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."

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.

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.

Appendix B: Endnotes

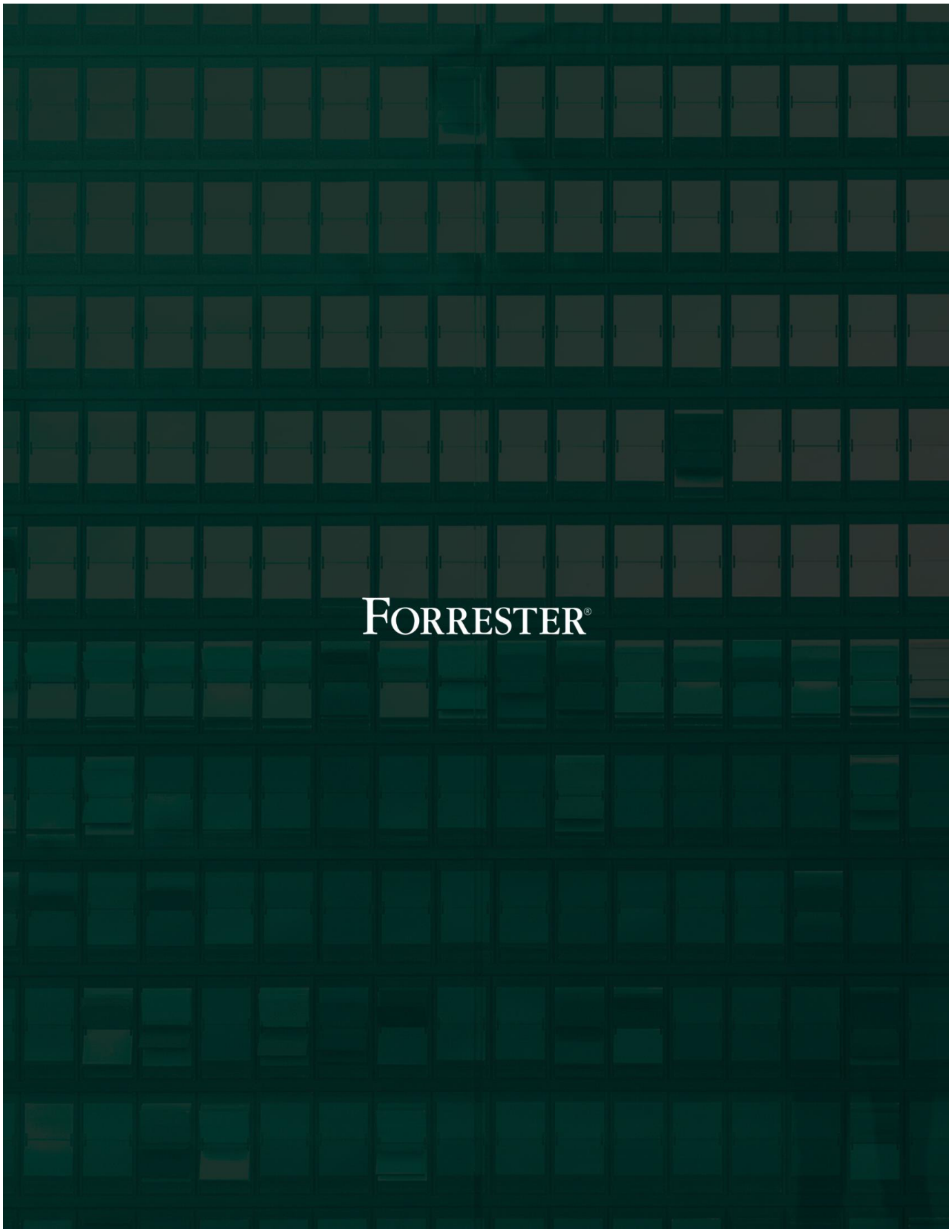
[1] Source: “Take Security To The Zero Trust Edge,” Forrester Research, Inc., February 16, 2021.

[2] 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.

[3] Source: Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q1 2021.

[4] Source: Ibid.

[5] Source: Ibid.


FORRESTER®