FORRESTER®

The Total Economic Impact™ Of Cloudflare's Connectivity Cloud

Cost Savings And Business Benefits Enabled By Cloudflare

A FORRESTER TOTAL ECONOMIC IMPACT STUDY
COMMISSIONED BY CLOUDFLARE, SEPTEMBER 2024

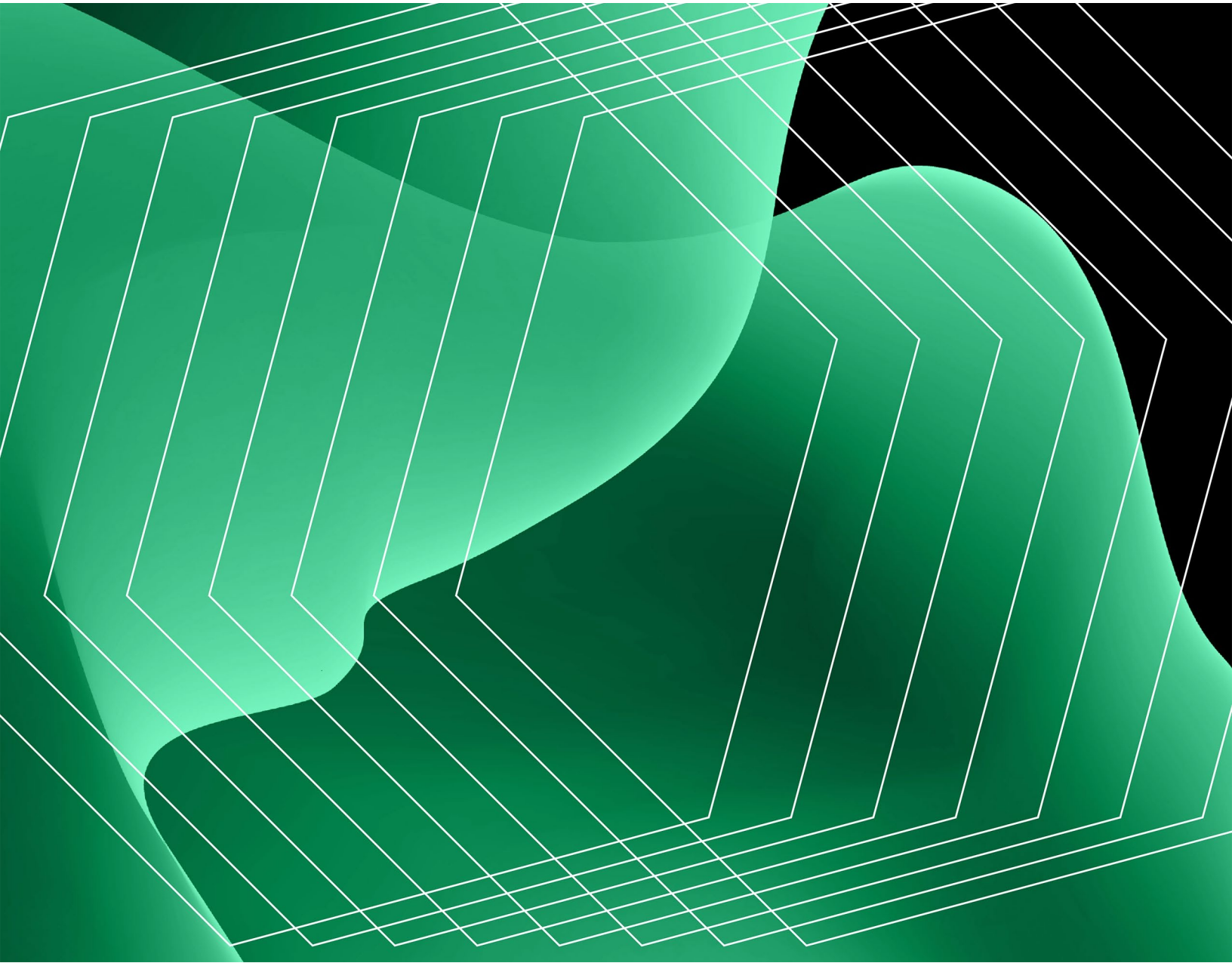


Table Of Contents

Consulting Team:

Sam Conway

ABOUT FORRESTER CONSULTING

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

Executive Summary

Enterprises are seeing increased complexity with distributed employees, distributed applications, and myriad siloed networks and vendors. With this growing complexity comes a more dangerous threat landscape — highlighting the importance of investing in a purpose-built platform to reduce attack surfaces and improve performance across a wide array of enterprise assets.

Cloudflare is a connectivity cloud, a unified platform of cloud-native services designed to help enterprises regain control over complex IT environments. Powered by an intelligent, programmable global cloud network, Cloudflare offers improved security, performance, visibility, and reliability across customer-facing applications, corporate networks, software-as-a-service (SaaS) apps, clouds, and more.

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

Return on investment (ROI)
238%

Net present value (NPV)
$6.0M

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four representatives with experience using an array of Cloudflare services. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization.

Interviewees said that prior to using Cloudflare, their organizations tried multiple legacy and point solutions to protect against cyberattacks and ensure high availability and performance of their applications and networks. However, myriad point solutions led to unnecessary complexity and failed to properly mitigate against downtime and performance issues.

After the investment in Cloudflare, the interviewees reduced complexity, improved internal operations, strengthened security, and reduced costs.

KEY FINDINGS

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

- **Improved security efficiency by up to 29%.** Cloudflare reduces the amount of time spent responding to bot attacks and investigating DDoS attacks for security analysts within the composite organization. Additionally, analysts benefit from working in a single toolset with centralized visibility and better correlation. For the composite organization, improved security efficiency is worth $998,000 in saved team time.
- **Improved IT operational efficiency by up to 13%.** By replacing legacy point solutions and deploying Cloudflare, the composite organization simplifies, automates, and eliminates a number of tasks formerly performed manually by its IT professionals. The composite organization realizes $984,000 of value in saved team time.
- **Strengthened security and reduction in the risk of web application breach by up to 25%.** Cloudflare helps the composite organization adopt a comprehensive security approach, securing its customer-facing web applications and thereby reducing risk and the likelihood of a costly external breach. Over a three-year period, the reduction of breach risk is worth $620,000.
- **Increased employee productivity by up to 2.5%.** Power users are more productive with faster and safer access to applications using Cloudflare Zero Trust Network Access. Additionally, better availability and performance of critical applications ensure users can spend more time on important tasks and less time waiting. For the composite organization, the three-year productivity benefit is worth $3.5 million.
- **Consolidated point solutions and eliminated legacy spend.** The composite organization is able to retire numerous point solutions as its usage of Cloudflare expands. Over a three-year period, the organization realizes $1.1 million in savings on hardware, maintenance, and licensing fees.

- **Reduced downtime and increased availability of critical apps.** Cloudflare's connectivity cloud provides the composite with improved network performance and reduces downtime due to bot or DDoS attacks. Additional hours of uptime for revenue-generating web applications are worth $957,000 over three years for the composite.
- **Reduced bandwidth costs by offloading data to Cloudflare.** In addition to improved performance, Cloudflare's content delivery network (Cloudflare CDN) allows the composite organization to reduce bandwidth costs with locally cached content. Cloudflare's Bandwidth Alliance offers additional savings for the composite organization by reducing transfer fees with key vendors. Reduced bandwidth costs are valued at $238,000 for the composite over three years.

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

- **Improved customer experience.** Improved reliability, availability, and performance for external applications lead to an overall better customer experience.
- **Improved employee experience.** Employees have faster access to better-performing applications. Additionally, IT and security professionals no longer have to perform manual processes with legacy tools.
- **Improved competitiveness.** Better performance of web applications improves overall competitiveness in highly contested markets. Furthermore, Cloudflare helps prevent anticompetitive actions like web scraping.
- **Satisfied compliance requirements.** Cloudflare helps streamline data compliance, eliminating risk associated with using multiple point solutions and manual processes.
- **Enabled potential additional consolidation.** Cloudflare's continually evolving platform offers additional opportunities to replace point solutions and recognize cost savings.

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

- **Licensing costs of $1.6 million over three years.** These costs include licensing and consumption fees for the Cloudflare platform.

- **Implementation costs of $260,000 over three years.** The composite organization incurs internal labor costs during its initial six-month deployment.
- **Ongoing management costs of $594,000 over three years.** The composite organization incurs labor costs related to the ongoing usage of Cloudflare.

The representative interviews and financial analysis found that a composite organization experiences benefits of $8.5 million over three years versus costs of $2.5 million, adding up to a net present value (NPV) of $6.0 million and an ROI of 238%.

Improved security efficiency by up to

29%

"[Cloudflare] is our front door. It is what customers see and experience when they interact with us. It powers almost everything we do — providing all the security services that we depend on and a whole bunch of infrastructure services."

SENIOR PRINCIPAL SECURITY ENGINEER, E-COMMERCE

Return on investment (ROI)

238%

Benefits PV

$8.5 million

Net present value (NPV)

$6.0 million

Payback

<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 in Cloudflare.

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 Cloudflare can have on an organization.

DISCLOSURES
Readers should be aware of the following:

This study is commissioned by Cloudflare 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 Cloudflare.

Cloudflare 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.

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

Due Diligence
Interviewed Cloudflare stakeholders and Forrester analysts to gather data relative to Cloudflare.

Interviews
Interviewed four representatives at organizations using Cloudflare to obtain data about 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 Cloudflare Customer Journey

Drivers leading to the Cloudflare investment

Interviews			
Role	**Industry**	**Region**	**Revenue**
Head of cloud and virtualization services	IT	EMEA	N/A
Director of global governance, risk, and compliance	Manufacturing	US	$25 billion
Senior principal security engineer	E-commerce	APAC	$200 million
CISO	Airline	US	$2.5 billion

KEY CHALLENGES

Prior to investing in Cloudflare, the interviewees' organizations relied on legacy CDNs, VPNs, and security point solutions. The interviewees' organizations struggled with complexity, costly manual effort, and poor security results.

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

- **Too many point solutions.** Interviewees highlighted that their organizations had pieced together a large number of point solutions to fill their security and connectivity needs. While each solution provided a specific needed capability, this ecosystem became unmanageable at scale. Furthermore, many of the older solutions lacked automation or were poorly integrated with each other, resulting in unnecessary manual management effort. The CISO of an airline explained: "Part of the business objective for me was to reduce our tooling. We had a security team with 40 to 50 tools — how do you maintain a high level of expertise to effectively utilize those tools? I would much rather have less tools with a higher utilization and higher level of expertise so that we are getting all the functionality out of those tools instead of having a bunch of one-trick ponies."

- **Downtime from attacks.** Interviewees highlighted that their previous solutions had insufficiently protected them from DDoS attacks, resulting in downtime or degraded performance. The senior principal security engineer at an e-commerce firm stated, “We were previously on another platform and had a pretty serious incident that they couldn’t solve, and so we migrated.”
- **Poor bot management.** Similarly, prior solutions did a poor job protecting web applications from sophisticated bot schemes. Interviewees’ organizations struggled with slow performance and were vulnerable to schemes like bots scraping their pricing information. The director of global governance, risk, and compliance for a manufacturing firm explained: “We discovered we were getting scraped heavily by competitors. They were going out to our catalog sites and scraping our catalog. So, we had a lot of bot traffic.”
- **Security and compliance scrutiny within their industry or region.** Interviewees detailed that their firms were in regions or industries that had experienced notable breaches and attacks, leading to scrutiny and an organizational mandate to invest in more-hardened security. The head of cloud and virtualization services at the IT firm in EMEA stated: “The cybersecurity aspect here grew in importances. We had a couple of cyber incidents here locally, where locally known companies went offline due to ransomware attacks. They were not able to sell or distribute goods for a few weeks, which was disastrous. So, at the same time this happened we started investing in a dedicated cybersecurity department. It was only natural that after ransomware we started looking into other threats like DDoS and how to prevent them.”
- **Legacy solutions lacking automation.** Interviewees noted that incumbent solutions lacked the automation or ease-of-use features they desired to cut down on manual work. The senior principal security engineer for the e-commerce firm explained: “There were some organizational pain points, in that we didn’t like dealing with [our old vendor] and their product. There was no automation, so it was all manual working in a web console … click, click, click. You know, no infrastructure as code.”

SOLUTION REQUIREMENTS

The interviewees' organizations searched for a solution that could:

- Protect on-premises and cloud workloads.
- Quickly meet compliance needs.
- Provide a wide breadth of features, functionality, and service.
- Utilize infrastructure as code.
- Offer competitive pricing.

> "[Cloudflare is] a valuable partner, and delivering value to our customers would be significantly harder without them."
>
> SENIOR PRINCIPAL SECURITY ENGINEER, E-COMMERCE

> "We originally started with Cloudflare for WAF [web application firewall] protection, but as we got more visibility, we realized we had more issues that Cloudflare could help us with. We have been able to see more and put protections in place because of Cloudflare and the services we have running around it."
>
> DIRECTOR OF GLOBAL GOVERNANCE, RISK, AND COMPLIANCE, MANUFACTURING

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 four 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 composite organization has worldwide operations and revenue in the $1 billion to $2 billion range. A portion of the organization's revenue is through direct e-commerce sales.

Deployment characteristics. The composite organization utilizes a variety of Cloudflare solutions with usage growing over time. It uses Cloudflare Bot Management, WAF, CDN, R2 caching, Load Balancing, Argo Smart Routing, Zero Trust Network Access, DDoS mitigation, and Cloud Email Security.

Key Assumptions

$1 billion to $2 billion revenue

2,000 employees

500 developers

30 IT operations team members

10 security team members

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	Security efficiencies	$362,250	$393,750	$456,750	$1,212,750	$997,894
Btr	IT operations efficiencies	$308,610	$445,770	$445,770	$1,200,150	$983,873
Ctr	Reduced web application breach risk	$190,052	$253,402	$316,753	$760,206	$620,178
Dtr	Employee productivity	$999,000	$1,665,000	$1,665,000	$4,329,000	$3,535,154
Etr	Consolidation and eliminated legacy spend	$315,000	$472,500	$607,500	$1,395,000	$1,133,283
Ftr	Reduced downtime	$344,219	$408,260	$408,260	$1,160,740	$957,064
Gtr	Reduced bandwidth costs	$72,960	$91,200	$127,680	$291,840	$237,627
	Total benefits (risk-adjusted)	$2,592,091	$3,729,882	$4,027,712	$10,349,685	$8,465,073

SECURITY EFFICIENCIES

Evidence and data. Interviewees highlighted that Cloudflare was significantly easier for their security teams to use compared to a mixture of point solutions. Additionally, Cloudflare provided better visibility into, and protection from, bot and DDoS attacks. Interviewees highlighted that their teams spent less time each week responding to these attacks and benefited greatly from working in a single toolset with centralized visibility and better correlation.

- The CISO for the airline stated: “Cloudflare has most definitely saved us time on bot attacks. A few hours per week.”
- With regard to bot investigation and response, the director of global governance, risk, and compliance for the manufacturing firm stated: “We have a lot of bandwidth that goes against our sites. Without the visibility that Cloudflare

provides, we would know this stuff is happening generally, but we wouldn't know necessarily what was happening on the sites."

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

- The composite organization has 10 security analysts.
- Productivity improvements increase over time with maturity of use and deployment of additional Cloudflare services.
- The average fully burdened annual salary for a security analyst is $175,000.

Risks. Organizations may experience results that differ from those presented in the financial model due to:

- The size of the security team.
- Legacy solutions.
- Prevailing labor rates.

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 $998,000.

> "The analysts can go to the dash and they can see email, they can see web, they can see Zero Trust, all through one unified UI and just jump back and forth between them. That not only improves their productivity, but gives them better visibility because it's easier to get to as well as correlation between the tools."
>
> CISO, AIRLINE

29%

Improvement in security analyst productivity

Security Efficiencies					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Number of security analysts	Composite	10	10	10
A2	Improvement in productivity	Interviews	23%	25%	29%
A3	Fully burdened annual salary for a security analyst	Composite	$175,000	$175,000	$175,000
At	Security efficiencies	A1*A2*A3	$402,500	$437,500	$507,500
	Risk adjustment	↓10%			
Atr	Security efficiencies (risk-adjusted)		$362,250	$393,750	$456,750
	Three-year total: $1,212,750			**Three-year present value: $997,894**	

IT OPERATIONS EFFICIENCIES

Evidence and data. Interviewees stated that the ease of using automations and the infrastructure-as-code provided by Cloudflare were a key criteria in vendor selection. Organizations were able to automate or outright eliminate previously manual efforts performed monthly, such as managing secure sockets layer/transport layer security (SSL/TLS) certificates, load balancing and caching, managing infrastructure for legacy solutions, onboarding and offboarding users, and dealing with access requests and VPN issues.

- On managing SSL/TLS certificates, the senior principal security engineer for the e-commerce firm stated: “It was actually quite a significant headache. None of the providers have really good management tools that let you know when things are expiring. There would be something off in the corner that expired, and it would be a

key system, and everything goes down. That's just gone away as a problem because Cloudflare manages all that for us."

- On load balancing and caching, the head of cloud and virtualization services for the IT firm explained: "We had an on-prem load balancer team that was the first point of contact if something went wrong. If crash control needed to be done, if capacity needs to be managed. This has all gone away." The interviewee added: "Cloudflare relieves pressure from my team, saves them from working on weekends. If there was something suspicious that would require us to patch our load balancer locally, we no longer have to do that because Cloudflare handles the threat."
- On onboarding and offboarding users, the senior principal security engineer for the e-commerce firm detailed: "If you have 100 legacy systems, when someone leaves you have to offboard them from 100 systems manually and things get missed because they're not linked to a central directory. With a single directory linked to Cloudflare Access, everybody spends less time in onboarding and offboarding users."

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

- The composite organization has 30 IT professionals impacted by Cloudflare.
- Each member of the team previously spent, on average:
  - One hour per month managing SSL/TLS certificates.
  - Eight hours per month on load balancing and caching.
  - Up to 4 hours per month managing legacy solution infrastructure.
  - Four hours per month onboarding and offboarding users.
  - Up to 4 hours per month dealing with access requests or VPN issues.
- Productivity improvements increase over time as Cloudflare usage expands and more tasks are automated or deprecated.
- The average fully burdened annual salary for a team member is $127,000.

Risks. Organizations may experience results that differ from those presented in the financial model due to:

- The size of IT team.
- Legacy processes and tools.
- Prevailing labor rates.

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 $984,000.

13%

Improvement in IT operations productivity

IT Operations Efficiencies					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	Number of IT operations professionals	Composite	30	30	30
B2	Improvement in productivity	Interviews	9%	13%	13%
B3	Fully burdened annual salary for a team member	Composite	$127,000	$127,000	$127,000
Bt	IT operations efficiencies	B1*B2*B3	$342,900	$495,300	$495,300
	Risk adjustment	↓10%			
Btr	IT operations efficiencies (risk-adjusted)		$308,610	$445,770	$445,770
	Three-year total: $1,200,150			**Three-year present value: $983,873**	

REDUCED WEB APPLICATION BREACH RISK

Evidence and data. Interviewees reported that Cloudflare had opened their eyes to myriad threats, allowing their organizations to secure, protect, and reduce their overall threat surface. Cloudflare was an integral part of reducing organizational risk by securing previously exposed applications and domains.

- Interviewees noted that prior to deploying Cloudflare, their firms had exposed applications and domains that exposed them to external risk. Quickly discovering and moving these behind Cloudflare shielded their organizations from malicious activity. The senior principal security engineer for the e-commerce firm explained: "Now nearly everything across the board is behind Cloudflare Access. It's a reduction in our attack surface area and protects all our homegrown, handwritten tools in a standardized way."
- The CISO of the airline stated that their organization had experienced a 15% improvement in security posture score since implementing Cloudflare.
- The director of global governance, risk, and compliance for the manufacturing firm explained, "Because of Cloudflare we have reduced the risk exposure of our business, and to me that is the greatest security return on investment."

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

- Without Cloudflare, the composite organization had an 84% chance of experiencing one or more breaches in a year.[2]
- The mean cumulative cost of total breaches per year totals $3.1 million for the composite organization.[3]
- The percentage of breaches coming from external attacks targeting the organization or attacks on third parties, which the Cloudflare deployment protects against, is 67.6%.[4] The Cloudflare solutions adopted by the composite address 80% of threat types in this category of risk.
- The composite organization reduces its risk of breach by 15% to 25% with Cloudflare. Risk reduction improves over time as the organization adopts additional Cloudflare products.

Risks. Organizations may experience results that differ from those presented in the financial model due to:

- Threat detection and remediation capabilities in legacy environments.
- The size and industry of the organization.

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 $620,000.

Up to 25%

Reduction in risk of breaches

"You sleep much better at night knowing that if someone does attempt a DDoS that Cloudflare will handle it. You have peace of mind; how do you even judge that in terms of money?"

HEAD OF CLOUD AND VIRTUALIZATION SERVICES, IT

Reduced Web Application Breach Risk					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Likelihood of experiencing one or more breaches per year	Forrester research	84%	84%	84%
C2	Mean cumulative cost of breaches	Forrester research	$3,099,000	$3,099,000	$3,099,000
C3	Percentage of breaches originating from external attacks and attacks on third parties	Forrester research	67.6%	67.6%	67.6%
C4	Percentage of external attacks addressable with Cloudflare	Composite	80%	80%	80%
C5	Annual risk exposure addressable with Cloudflare	C1*C2*C3*C4	$1,407,789	$1,407,789	$1,407,789
C6	Reduced risk of breaches with Cloudflare	Interviews	15%	20%	25%
Ct	Reduced web application breach risk	C5*C6	$211,168	$281,558	$351,947
	Risk adjustment	↓10%			
Ctr	Reduced web application breach risk (risk-adjusted)		$190,052	$253,402	$316,753
	Three-year total: $760,206			**Three-year present value: $620,178**	

EMPLOYEE PRODUCTIVITY

Evidence and data. Interviewees noted that using Access (Cloudflare's Zero Trust Network Access service) allowed their firms to secure previously exposed SaaS applications used by internal users and improve the access to applications that had required a VPN. Interviewees' organizations were able to pair Cloudflare Access with their identity provider (IDP), ensuring that employees had fast and secure access through a single corporate login.

- The senior principal security engineer for the e-commerce firm explained: "A huge benefit [of Cloudflare Access] is that it is linked with our IDP. All the Cloudflare Access applications are linked up to that. One corporate login means you can access all your SaaS applications and email and all that. That makes things simple for developers, and it means all those staff applications are effectively protected behind a single identity." The interviewee added: "We've greatly improved on people not losing access when they shouldn't and losing access when they should by having this link between our corporate directory and our applications in Zero Trust … it's essentially all automatic."

- The CISO of the airline added: “Replacing the VPN and going to an always-on Zero Trust security model has improved our security posture and also created a better experience for our employees. It makes it easier for them to do the secure thing and also save time by not having to deal with login information.”

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

- Within the composite organization, 500 employees are impacted by replacing the VPN with Cloudflare Access. These are power users using critical protected applications.
- The improvement in productivity increases over time with the growing maturity of the composite organization’s Cloudflare deployment.
- The average fully burdened annual salary for an impacted employee is $148,000.

Risks. Organizations may experience results that differ from those presented in the financial model due to:

- The size of organization, employee base, and breadth of VPN use.
- Prevailing labor rates.

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 $3.5 million.

Up to 2.5%

Improvement in employee productivity

> "I turn on my laptop and I'm on the network and in the security stack. This makes employees more productive and gives them an easier and better experience with security."
>
> CISO, AIRLINE

Employee Productivity					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
D1	Number of users	Composite	500	500	500
D2	Improvement in productivity with Cloudflare	Interviews	1.5%	2.5%	2.5%
D3	Fully burdened annual salary for an impacted employee	Composite	$148,000	$148,000	$148,000
Dt	Employee productivity	D1*D2*D3	$1,110,000	$1,850,000	$1,850,000
	Risk adjustment	↓10%			
Dtr	Employee productivity (risk-adjusted)		$999,000	$1,665,000	$1,665,000
	Three-year total: $4,329,000			**Three-year present value: $3,535,154**	

CONSOLIDATION AND ELIMINATED LEGACY SPEND

Evidence and data. Interviewees noted that with Cloudflare their organizations were able to retire multiple legacy solutions, which saved money on licensing, hardware, and maintenance. Typically, interviewees' organizations started with Cloudflare's CDN, web application firewall (WAF), and/or DDoS protection services and expanded use over time as they identified new redundancies covered by Cloudflare's capabilities. Interviewees noted that their firms had replaced legacy CDNs, VPNs, HTTP accelerators, email security, bot management, and Zero Trust solutions.

- The CISO for the airline explained: “We had [multiple major security vendors] and we have consolidated down to one. We are eliminating all of them and implementing Cloudflare as our unified security edge.”
- Interviewees highlighted that they were constantly looking for new ways to leverage additional Cloudflare capabilities to displace operational spend.

Modeling and assumptions. Based on the interviews, Forrester assumes the composite organization displaces its legacy CDN, VPN, email security, and bot management solutions. This is done on an iterative basis as the organization identifies and executes on consolidation opportunities.

Risks. Organizations may experience results that differ from those presented in the financial model due to:

- The legacy tech stack.
- Required capabilities.
- Existing contractual terms.

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 $1.1 million.

> “The trigger for the [switch to Cloudflare] at the time — something that is probably still true today — is that our leadership was very sensitive to downtime of the customer-facing applications.”
>
> SENIOR PRINCIPAL SECURITY ENGINEER, E-COMMERCE

Consolidation And Eliminated Legacy Spend					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
E1	Legacy spend	Interviews	$350,000	$525,000	$675,000
Et	Consolidation and eliminated legacy spend	E1	$350,000	$525,000	$675,000
	Risk adjustment	↓10%			
Etr	Consolidation and eliminated legacy spend (risk-adjusted)		$315,000	$472,500	$607,500
	Three-year total: $1,395,000			**Three-year present value: $1,133,283**	

REDUCED DOWNTIME

Evidence and data. A critical outcome of Cloudflare improving the interviewees' organizations' security posture was a reduced likelihood in websites and critical applications being taken offline. Prior to investment in Cloudflare, the interviewees' organizations had exposed vulnerabilities, insufficient DDoS mitigation, and poor bot management that resulted in unexpected outage or downtime. For interviewees' organizations with revenue-generating public web applications, every hour of downtime or reduced performance meant lost sales, upset customers, or violated SLAs.

- The senior principal security engineer for the e-commerce firm explained: "At one point, we were using a ridiculous number of SaaS products. And their model was that it's available over the public internet. For whatever cultural reason, that was just how we kind of did things and our staff's tools were exposed to the public internet. It's not like everyone in the world could access them, but it was all code our developers wrote, and people found bugs that could crash an app or make it misbehave."
- The head of virtualization and cloud services for the IT firm stated: "With Cloudflare, we can control the DDoS protection better than what our ISP does. Our ISP knows layer 2 and maybe layer 3. When we terminate traffic at Cloudflare, we can inspect requests a lot better, like repeated hits on a URL instead of just an IP address. The way that Cloudflare processes requests and ties it into further steps, like going through the WAF or bot detection, is just much better."

- The director of global governance, risk, and compliance for the IT firm explained, “If an event does occur, [Cloudflare] reduces any of the impacts because we’re able to adjust to the bot traffic.”

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

- With Cloudflare, the composite organization is able to improve from globally average availability to 99.9%.
- $750 million of revenue is derived from applications protected by Cloudflare, and the composite organization has average margins of 11%.

Risks. Organizations may experience results that differ from those presented in the financial model due to:

- Organizational size, geography, industry, and revenue mix.
- Average availability in legacy environments.

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 $957,000.

> “Cloudflare is our insurance that we are protected from any malicious attacks, specifically DDoS.”
>
> HEAD OF CLOUD AND VIRTUALIZATION SERVICES, IT

Reduced Downtime					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
F1	Additional availability with Cloudflare (hours)	Interviews	43	51	51
F2	Annual revenue impacted by outages	Composite	$750,000,000	$750,000,000	$750,000,000
F3	Average hourly cost of downtime	F2/8,760	$85,616	$85,616	$85,616
F4	Margin	Composite	11%	11%	11%
Ft	Reduced downtime	F1*F3*F4	$404,964	$480,306	$480,306
	Risk adjustment	↓15%			
Ftr	Reduced downtime (risk-adjusted)		$344,219	$408,260	$408,260
	Three-year total: $1,160,740		**Three-year present value: $957,064**		

REDUCED BANDWIDTH COSTS

Evidence and data. Interviewees noted that Cloudflare enabled their organizations to save on bandwidth fees by caching content closer to users and reducing origin-server requests. Additionally, they reported that Cloudflare's Bandwidth Alliance offered discount and zero-rated egress fees from a roster of major cloud service providers. Interviewees noted that these elements of the Cloudflare solution resulted in savings on consumption costs and helped their organizations avoid increasing commitment levels on fixed-bandwidth contracts.

- The head of virtualization and cloud services for the IT firm explained: "The bandwidth that we no longer have to funnel through our pipes is helping us to avoid a bandwidth increase on our connectivity. Cloudflare has helped us avoid the tipping point where we need to order more."
- The senior principal security engineer for the e-commerce firm detailed: "It depends on an application-by-application basis but if we can offload, we do 100%. Some applications have a ridiculously high hit ratio because they are all static content. We offload a lot of bandwidth volume through Cloudflare, and a significant fraction of that is cached content that we're therefore not paying [our CSP] to either cache or to serve up dynamically."

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

- The composite organization offloads between 80 and 140 TB per month to Cloudflare.
- Egress savings per TB with Cloudflare are $80.

Risks. Organizations may experience results that differ from those presented in the financial model due to:

- The makeup of applications, type of content, and ability to cache.
- The participation of vendors in Bandwidth Alliance.

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 $238,000.

> "It's a significant amount of dollars we are saving by offloading some content to be served out of Cloudflare's network."
>
> SENIOR PRINCIPAL SECURITY ENGINEER, E-COMMERCE

Reduced Bandwidth Costs					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
G1	TB per month offloaded to Cloudflare	Composite	80	100	140
G2	Egress savings per TB with Cloudflare	Composite	$80	$80	$80
Gt	Reduced bandwidth costs	G1*G2*12	$76,800	$96,000	$134,400
	Risk adjustment	↓5%			
Gtr	Reduced bandwidth costs (risk-adjusted)		$72,960	$91,200	$127,680
	Three-year total: $291,840			**Three-year present value: $237,627**	

UNQUANTIFIED BENEFITS

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

- **Improved customer experience.** Making applications and site performance better leads to an overall better customer experience. Interviewees highlighted that their firms implemented numerous traffic management policies that ensured that customers had better access to their services. The CISO of the airline explained: “Some of the stuff we’re able to easily do with Cloudflare, like the customer waiting rooms, is a nice touch for high traffic periods. Obviously being able to push more content to the edge and closer to customers has definitely been a performance and customer experience improvement.”
- **Improved employee experience.** Interviewees also highlighted that removing friction between security and internal users had led to a better employee experience. The CISO of the airline detailed, “If we make security easier and a more pleasant experience for our employees, it just makes it easier for them to do their jobs and makes them more effective.”
- **Improved competitiveness.** The director of global governance, risk, and compliance for the manufacturing firm highlighted that major competitors had been using bots to scrape information off publicly exposed catalog sites. With Cloudflare, exposed sites could be moved behind Cloudflare, and Cloudflare’s bot management tools could be used to thwart malicious actions.

- **Satisfied compliance requirements.** Interviewees noted a number of regulations that Cloudflare helped them meet. The head of cloud and virtualization services for the IT organization cited Cloudflare as a key part of meeting EU banking regulations. The interviewee noted, “Working with Cloudflare is just easier because they are more professional than our small service provider.” The senior principal security engineer for the e-commerce firm noted that Cloudflare had helped them build compliance into their applications — their organization had multiple global entities with different regulatory rules, and Cloudflare helped them standardize in order to meet the regulations of the most onerous regions across all other entities.
- **Enabled potential for additional consolidation.** Interviewees expressed interest in continuing to expand their Cloudflare deployments and explore new ways to consolidate costs. The CISO of the airline detailed that their organization was exploring replacing their on-premises firewalls in airports with Cloudflare.

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**
Htr	Licensing	$0	$350,000	$700,000	$1,000,000	$2,050,000	$1,648,009
Itr	Implementation	$259,875	$0	$0	$0	$259,875	$259,875
Jtr	Ongoing management	$0	$238,875	$238,875	$238,875	$716,625	$594,047
	Total costs (risk-adjusted)	$259,875	$588,875	$938,875	$1,238,875	$3,026,500	$2,501,931

LICENSING

Evidence and data. Interviewees shared that Cloudflare charged them licensing and usage fees dependent on services and bandwidth. Contact Cloudflare for additional details.

Modeling and assumptions. Based on the interviews, Forrester assumes the composite organization deploys a wide range of Cloudflare solutions with its deployment growing each year. Products deployed over a three-year period include Bot Management, WAF, CDN, R2 Caching, Load Balancing, Argo Smart Routing, Zero Trust Access, DDoS Mitigation, and Cloud Email Security.

Risks. Cloudflare fees vary depending on:

- The number of Cloudflare features deployed.
- The size, scale, and usage of Cloudflare deployment.

Results. Forrester did not adjust this cost for risk, yielding a three-year total PV (discounted at 10%) of $1.6 million.

Licensing						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
H1	Licensing fees	Composite	$0	$350,000	$700,000	$1,000,000
Ht	Licensing	H1	$0	$350,000	$700,000	$1,000,000
	Risk adjustment	0%				
Htr	Licensing (risk-adjusted)		$0	$350,000	$700,000	$1,000,000
	Three-year total: $2,050,000			**Three-year present value: $1,648,009**		

IMPLEMENTATION

Evidence and data. Interviewees noted that their organizations dedicated some internal resources to the initial Cloudflare implementation when changing over from legacy solutions and, in some cases, engaged professional services. Implementation times took anywhere from three to 12 months and were dependent on the complexity of their organizations' legacy environments, makeup, and familiarity with mapping rules.

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

- The composite organization spends six months on its initial implementation.
- Ten FTEs are involved in the implementation period, spending one-third of their time on this effort.
- The average fully burdened annual salary for an FTE involved in implementation is $150,000.

Risks. Implementation costs will vary depending on:

- The size, scope, and complexity of deployment and legacy environment.
- Internal skill sets.
- Organizational agility.
- Prevailing wages.

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 $260,000.

Implementation						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
I1	Months of implementation	Composite	6			
I2	FTEs involved	Composite	10			
I3	Percentage of time spent on project	Composite	33%			
I4	Fully burdened annual salary for an FTE involved in implementation	Composite	$150,000			
It	Implementation	I1*I2*I3*(I4/12)	$247,500	$0	$0	$0
	Risk adjustment	↑5%				
Itr	Implementation (risk-adjusted)		$259,875	$0	$0	$0
	Three-year total: $259,875			**Three-year present value: $259,875**		

ONGOING MANAGEMENT

Evidence and data. Interviewees stated that their organizations had dedicated limited internal resources to the ongoing usage and management of Cloudflare. Management resources were concerned with managing the Cloudflare relationship as well as strategic planning for the evolving use of Cloudflare within their organizations. Operations teams were tasked with monitoring Cloudflare and responding to issues.

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

- The composite organization dedicates a single management resource to Cloudflare; this resource spends 20% of their time on overseeing the use and strategic expansion of Cloudflare. The average fully burdened annual salary for a management resource is $200,000.
- The composite organization has three operations team members spending half their time managing and monitoring Cloudflare. The average fully burdened annual salary for an operations team member is $125,000.

Risks. Ongoing management costs will vary based on:

- Organizational makeup.
- Prevailing wages.

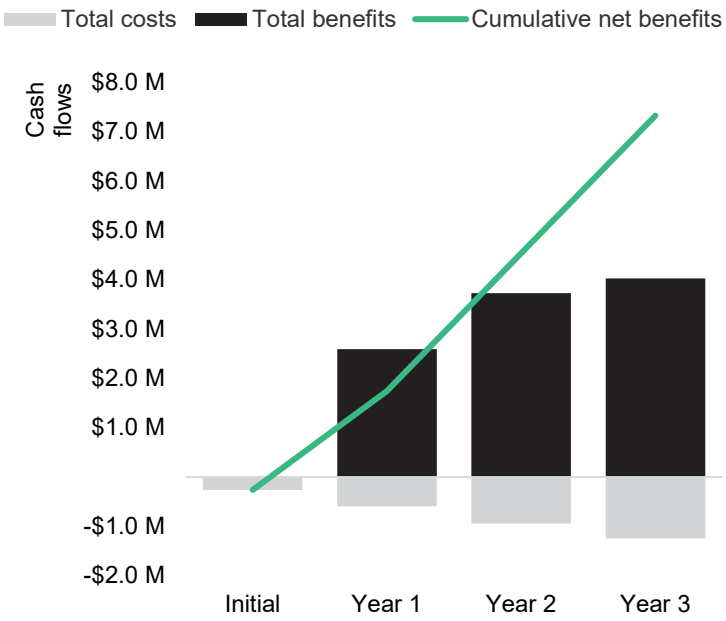
Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $594,000.

Ongoing Management						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
J1	Number of management resources used for ongoing management	Composite		1	1	1
J2	Percentage of time dedicated to Cloudflare	Composite		20%	20%	20%
J3	Fully burdened annual salary for a management resource	Composite		$200,000	$200,000	$200,000
J4	Number of operations team members used for ongoing management	Composite		3	3	3
J5	Percentage of time dedicated to Cloudflare	Composite		50%	50%	50%
J6	Fully burdened annual salary for an operations team member	Composite		$125,000	$125,000	$125,000
Jt	Ongoing management	(J1*J2*J3)+ (J4*J5*J6)	$0	$227,500	$227,500	$227,500
	Risk adjustment	↑5%				
Jtr	Ongoing management (risk-adjusted)		$0	$238,875	$238,875	$238,875
	Three-year total: $716,625			**Three-year present value: $594,047**		

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	($259,875)	($588,875)	($938,875)	($1,238,875)	($3,026,500)	($2,501,931)
Total benefits	$0	$2,592,091	$3,729,882	$4,027,712	$10,349,685	$8,465,073
Net benefits	($259,875)	$2,003,216	$2,791,007	$2,788,837	$7,323,185	$5,963,142
ROI						238%
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 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.

[2] Source: Forrester's Security Survey, 2023; Base: 79 security decision-makers from organizations with a revenue of $1 billion to $2 billion with network, data center, app security, or security ops responsibilities and that have experienced a breach in the past 12 months.

[3] Source: Forrester's Security Survey, 2023; Base: 65 security decision-makers from organizations with a revenue of $1 billion to $2 billion with network, data center, app security, or security ops responsibilities and that have experienced a breach in the past 12 months.

[4] Source: Forrester's Security Survey, 2023; Base: 830 security decision-makers with network, data center, app security, or security ops responsibilities who have experienced a breach in the past 12 months at companies with $10 million or more in annual revenue.

FORRESTER®