

Total Economic Impact

The Total Economic Impact™ Of Cloudflare

Cost Savings And Business Benefits Enabled By Cloudflare

A FORRESTER TOTAL ECONOMIC IMPACT STUDY COMMISSIONED BY CLOUDFLARE, JANUARY 2026

The Forrester logo is displayed in white, serif, all-caps font within a black rectangular box. The box is positioned on the left side of a large, abstract graphic that features flowing, organic shapes in various shades of green and teal, set against a black background.

FORRESTER®

Executive Summary

Organizations across industries face escalating cybersecurity threats, increasing regulatory scrutiny, and growing complexity across multicloud environments and global operations. At the same time, they need to deliver fast, reliable digital experiences to customers and employees while reducing costs and operational overhead. Traditional on-premises security and IT solutions struggle to keep pace with these demands due to long deployment cycles, high maintenance requirements, and limited scalability. Businesses require a unified platform that can provide robust security against DDoS attacks, bots, and application-layer threats; ensure compliance and data protection; improve performance through global content delivery and caching; and enable Zero Trust access for a distributed workforce.¹

Cloudflare offers an integrated, cloud-native platform that combines security, performance, and agility of organizations to accelerate time to market, simplify operations, and support modern work models.

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.² The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Cloudflare on their organizations.

227%

Return on investment (ROI)

\$21.4M

Net present value (NPV)

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed five decision-makers with experience using Cloudflare. For the purposes of this study, Forrester aggregated the experiences of the interviewees and combined the results into a single composite organization.

Prior to implementing Cloudflare, interviewees across organizations faced frequent bot and DDoS attacks, inefficient access controls and phishing protection, poor network performance fragmented security tools, and manual VPN management that led to high support ticket volumes. These challenges created risk exposure, inefficiencies, and limited scalability, prompting the need for a centralized, cloud-based security and connectivity solution.

After the investment in Cloudflare, interviewees reported that their organizations reduced downtime, boosted bot mitigation, improved security posture through centralized controls, streamlined IT management, and achieved better web application performance. These outcomes contributed to measurable cost savings, enhanced operational efficiency, and increased confidence in regulatory compliance.

Key Findings

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

- **Strengthened security.** The composite organization benefits from unified protection, improving its overall security posture and saving the composite \$2.7 million.
- **Increased revenue from reduced downtime.** Cloudflare's reliability reduces outages, allowing the composite organization to maintain uptime and preserve revenue during high-traffic periods, saving the composite \$11.2 million.
- **Streamlined IT operations.** Cloudflare replaces fragmented legacy domain name system (DNS) and security tools with a centralized SaaS platform, simplifying management and reducing operational effort across infrastructure teams and saving the composite just under \$8.7 million.
- **Improved access performance.** Cloudflare's Zero Trust Network Access solution replaces traditional VPNs, offering faster, more secure access and reducing help desk tickets related to connectivity saving just under \$5.2 million.
- **Reduced bandwidth and cloud costs from caching efficiency.** Cloudflare's caching capabilities reduce bandwidth and cloud egress costs for the composite by serving more traffic closer to end users, improving performance while lowering spend by just

under \$430,000.

- **Reduced fees.** By combining multiple vendors into a single Cloudflare contract, the composite organization lowers licensing costs and eliminates redundant support expenses by 20%, saving just under \$1.8 million.

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

- **Improved customer trust and regulatory confidence.** Centralized reporting, consistent protection, and programmable global infrastructure helped the composite meet regulatory requirements and build trust with its users.
- **Improved IT experience from faster onboarding and reduced weekend work.** The composite's teams increased job satisfaction due to smoother onboarding processes, the elimination of weekend maintenance, and a reduction in firefighting.
- **Improved user experience and team satisfaction.** Faster access and more stable connections increased satisfaction across all departments at the composite.
- **Improved reliability and reputational protection.** Cloudflare helped the composite avoid downtime during critical periods and enabled secure growth and partnerships.
- **Increased peace of mind for developers and consistent secure sockets layer (SSL).** Consistent SSL management and reduced operational burden helped the composite's developers focus on innovation rather than maintenance.

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

- **Licensing and support fees.** The composite incurs Cloudflare fees of just over \$9.0 million.
- **Maintenance.** The composite dedicates 0.5 of an FTE to maintenance, incurring a cost of \$233,000.
- **Implementation and deployment.** The composite dedicates a team of four DevOps and IT engineers for configuration, rollout, and testing for two months. This incurs a cost of \$147,000.

The financial analysis that is based on the interviews found that a composite organization experiences benefits of \$29.9 million over three years versus costs of \$9.4 million, adding up to a net present value (NPV) of \$20.5 million and an ROI of 218%.

“Cloudflare gives us enterprise-grade security across thousands of applications. We can confidently tell regulators and customers that our platform is protected — and we’ve had zero downtime from attacks since implementation.”

Head of web platforms, pharmaceuticals/life sciences

Key Statistics

227%

Return on investment (ROI)

\$30.8M

Benefits PV

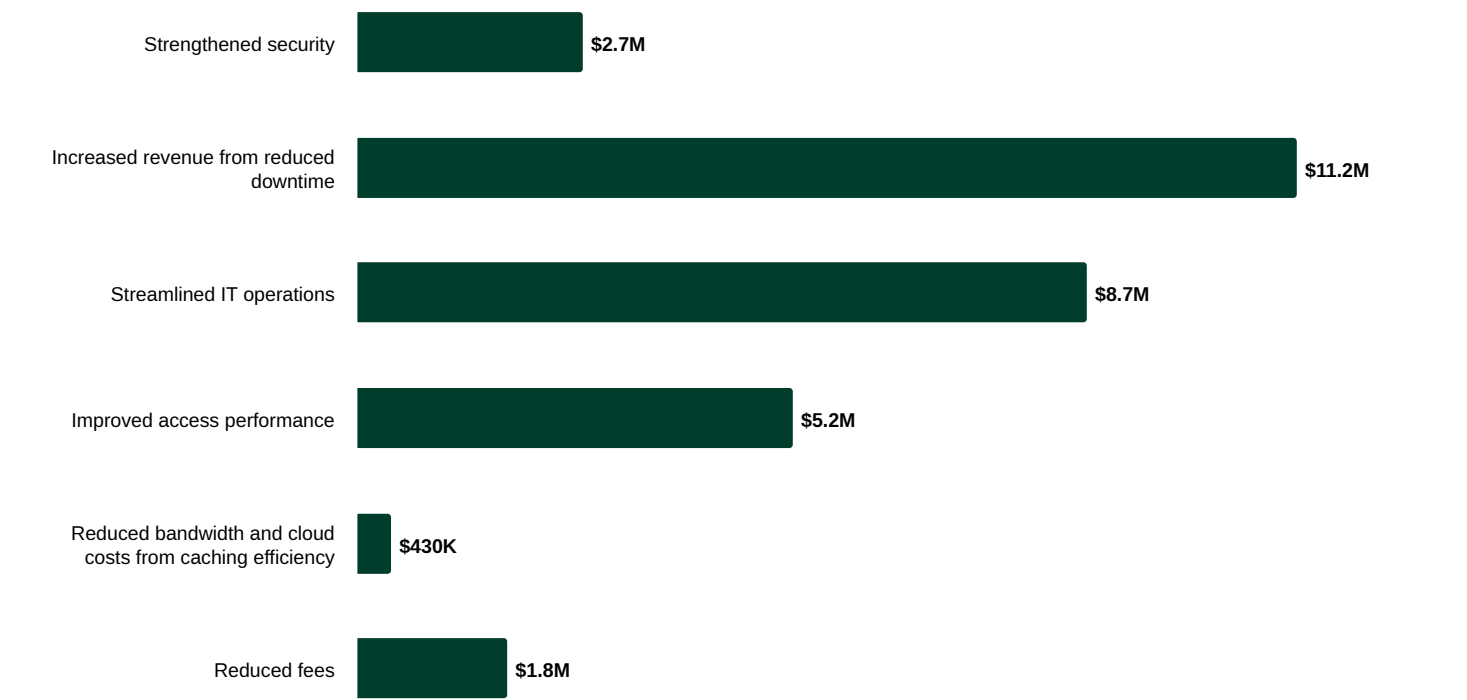
\$21.4M

Net present value (NPV)

<6 months

Payback

Benefits (Three-Year)



The Cloudflare Customer Journey

Drivers leading to the Cloudflare investment

Interviews			
Role	Industry	Region	Annual Revenue
Director of digital platforms	Healthcare medical devices	United States	\$8 billion
Global director of network services	Insurance/professional services	Global (headquartered in the UK)	\$16 billion
CTO	Online gaming/gambling	Mexico	\$438 million
Head of cybersecurity	Retail/consumer electronics	United Kingdom	\$11.5 billion
Head of web platforms	Pharmaceuticals/life sciences	Switzerland	\$70 billion

Key Challenges

Before adopting Cloudflare, interviewees’ organizations faced a range of operational and security challenges that hindered performance, increased risk, and created inefficiencies. Legacy environments relied on fragmented point solutions, on-premises hardware, and manual processes that were costly to maintain and slow to adapt. These limitations resulted in frequent downtime, inconsistent security coverage, complex vendor management, and poor user experiences — particularly for remote access and global application delivery. Interviewees noted how their organizations struggled with common challenges, including:

- **Security gaps and inconsistent protection.** Many interviewees said their organizations lacked a unified web application firewall (WAF) or DDoS solution. Some external-facing applications had no protection at all, leaving them vulnerable to attacks and compliance risks.
- **Frequent downtime and attack disruptions.** Interviewees’ organizations experienced outages from DDoS attacks, bot abuse, and credential-stuffing attempts. Interviewees from retail and gaming firms said that downtime during peak events like Black Friday or major sports games caused lost revenue and customer churn.
- **Complex, fragmented vendor landscape.** Multiple point solutions (e.g., Akamai, F5, Infoblox) created operational complexity at the interviewees’ organizations. Their teams had to manage different consoles, policies, and hardware across regions, slowing response times and increasing costs.
- **On-prem hardware and maintenance burden.** Interviewees said DNS and security services often ran on physical appliances, requiring monthly maintenance windows and weekend work. Coordinating global downtime for upgrades was disruptive and unpopular with staff.
- **Slow time to market for new apps.** Before Cloudflare, launching new applications at the interviewees’ organizations required provisioning hardware, securing licenses, and scheduling maintenance windows, which often took weeks or months.
- **VPN performance and user frustration.** Legacy VPN solutions were slow, unreliable, and difficult to scale for remote work. Interviewees said their employees faced latency and frequent disconnections, especially during global events like the COVID-19 pandemic.
- **Limited visibility and reporting.** Security teams at the interviewees’ organizations struggled to provide consistent compliance evidence and incident response across multiple tools, increasing audit complexity and risk.

“We had successful DDoS attacks on our previous platforms. We had considerable downtime. We had bots that would often try and mine or buy a large number of products and then resell them. We had 10s of hours of serious disruption. That has gone to nothing.”

Head of cybersecurity, retail/consumer electronics

Composite Organization

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

- **Description of composite.** The composite organization has worldwide operations and annual revenue of \$10 billion. A portion of the organization's revenue is through direct e-commerce sales.
- **Deployment characteristics.** The composite organization utilizes a variety of Cloudflare solutions for security and performance, including DDoS mitigation, bot management, WAF, content delivery network (CDN), load balancing, and Argo smart routing, as well as secure access service edge (SASE), including Zero Trust network access and cloud email security.

KEY ASSUMPTIONS

- \$10 billion in annual revenue
- 10,000 employees
- Global

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	Strengthened security	\$1,067,792	\$1,067,792	\$1,067,792	\$3,203,377	\$2,655,442
Btr	Increased revenue from reduced downtime	\$4,500,000	\$4,500,000	\$4,500,000	\$13,500,000	\$11,190,834
Ctr	Streamlined IT operations	\$3,480,750	\$3,480,750	\$3,480,750	\$10,442,250	\$8,656,110
Dtr	Improved access performance	\$2,436,480	\$2,436,480	\$2,436,480	\$7,309,440	\$6,059,165
Etr	Reduced bandwidth and cloud costs from caching efficiency	\$172,800	\$172,800	\$172,800	\$518,400	\$429,728
Ftr	Reduced fees	\$712,800	\$712,800	\$712,800	\$2,138,400	\$1,772,628
	Total benefits (risk-adjusted)	\$12,370,622	\$12,370,622	\$12,370,622	\$37,111,867	\$30,763,907

Strengthened Security

Evidence and data. Interviewees consistently emphasized that Cloudflare significantly improved their organizations' ability to protect critical applications and data across multiple cloud providers. By consolidating WAF, DDoS mitigation, bot management, Zero Trust access, and email security into a single globally distributed platform, the interviewees' organizations reduced exposure to attacks and simplified enforcement of security policies.

- The CTO at an online gaming/gambling firm said: "We were getting hammered with credential stuffing attacks. Cloudflare's bot management and WAF stopped them cold. It was night and day."
- The director of digital platforms at a healthcare/medical devices organization said: "We needed cloud-agnostic security. Cloudflare was the only vendor that could do it without locking us in."
- The global director of network services at an insurance/professional services company said: "We consolidated multiple fragmented WAFs into one global solution. That alone strengthened our security posture significantly."

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

- The composite's total risk exposure to security breaches is \$4,427,000 per year.³
- For the composite organization, 67% of breaches originate from external attacks targeting organizations, external attacks targeting remote environments, internal incidents, or attacks or incidents involving the external ecosystem.⁴
- The value of this benefit incorporates the full cost of a breach, including labor, direct expenses, and lost revenue, while also accounting for savings from breach remediation and improvements to mean time to identify (MTTI) and mean time to resolve (MTTR).

Risks. Results may not be representative of all experiences, and the benefit will vary based on the extent to which the organization experiences malicious attacks.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of \$2.7 million.

\$2.7M

Savings from strengthened security

“The user experience improved dramatically. Faster access, fewer complaints, and a smoother login process across the board.”

CTO, online gaming/gambling

Strengthened Security					
Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Total annual risk exposure to security breaches	Forrester research	\$4,427,000	\$4,427,000	\$4,427,000
A2	Percentage of breaches originating from external attacks targeting organizations, external attacks targeting remote environments, and internal incidents	Forrester research	67%	67%	67%
A3	Percentage of attacks addressable with Cloudflare	Interviews	60%	60%	60%
A4	Annual risk exposure addressable with Cloudflare	A1*A2*A3	\$1,779,654	\$1,779,654	\$1,779,654
A5	Reduced risk of exposure to breach costs from addressable attacks with Cloudflare	Interviews	75%	75%	75%
At	Strengthened security	A4*A5	\$1,334,741	\$1,334,741	\$1,334,741
	Risk adjustment	↓20%			
Atr	Strengthened security (risk-adjusted)		\$1,067,792	\$1,067,792	\$1,067,792
Three-year total: \$3,203,377			Three-year present value: \$2,655,442		

Increased Revenue From Reduced Downtime

Evidence and data. Interviewees reported that moving to Cloudflare significantly reduced or eliminated the need for planned downtime during maintenance windows. With Cloudflare’s globally resilient cloud architecture, these maintenance windows were no longer necessary, resulting in near-zero planned outages and improved business continuity. The global director of network services at an insurance/professional services organizations said, “Before Cloudflare, we were spending 48 hours a month dealing with DNS-related outages and maintenance windows.”

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

- The composite earns an average retail revenue of \$200,000 per hour.
- It saves 250 hours of downtime each year.
- The composite has a margin of 10% on online retail sales.

Risks. Results may not be representative of all experiences, and the benefit will vary based on the following variables:

- The maturity of the previous solution.
- The amount of revenue the organization earns online.
- Other costs of downtime.

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 \$11.2 million.

250

Annual hours of avoided downtime

“Because Cloudflare does all its magic caching, even though the origin server was down, 98% of the website still functioned perfectly fine. That was amazing. We didn’t even notice until we checked the logs.”

CTO, online gaming/gambling

Increased Revenue From Reduced Downtime					
Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Average revenue per hour of weekend downtime	Composite	\$200,000	\$200,000	\$200,000
B2	Reduced downtime (hours)	Interviews	250	250	250
B3	Operating margin	Composite	10%	10%	10%
Bt	Increased revenue from reduced downtime	B1*B2*B3	\$5,000,000	\$5,000,000	\$5,000,000
	Risk adjustment	↓10%			
Btr	Increased revenue from reduced downtime (risk-adjusted)		\$4,500,000	\$4,500,000	\$4,500,000
Three-year total: \$13,500,000			Three-year present value: \$11,190,834		

Streamlined IT Operations

Evidence and data. Migrating DNS and security services to Cloudflare reduced manual maintenance tasks for the interviewees’ organizations, freeing up IT resources to focus on strategic initiatives and innovation. The global director of network services at an insurance/professional services organization said: “With Cloudflare’s SaaS-based model and global resiliency, we don’t have to take systems offline. Our engineers really appreciate getting their weekends back and our team can focus on strategic work instead of firefighting.”

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

- The composite employs 65 IT engineers.
- The IT engineers save 35% of their time over previous DNS and security solutions.
- The average fully burdened annual salary for an IT engineer is \$170,000.

Risks. Results may not be representative of all experiences, and the benefit will vary based on the following variables:

- The average annual salary for an IT engineer.
- The amount of down time the organization experiences.

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 \$8.7 million.

35%

Time saved on DNS and security maintenance

“My entire DNS team is no longer doing any maintenance work on DNS infrastructure. ... We freed up probably 30% to 40% of that time.”

Global director of network services, insurance/professional services

Streamlined IT Operations					
Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	DevOps engineers	Composite	65	65	65
C2	Percentage reduction in DNS maintenance effort	Interviews	35%	35%	35%
C3	Fully burdened annual salary for an IT engineer	Composite	\$170,000	\$170,000	\$170,000
Ct	Streamlined IT operations	C1*C2*C3	\$3,867,500	\$3,867,500	\$3,867,500
	Risk adjustment	↓10%			
Ctr	Streamlined IT operations (risk-adjusted)		\$3,480,750	\$3,480,750	\$3,480,750
Three-year total: \$10,442,250			Three-year present value: \$8,656,110		

Improved Access Performance

Evidence and data. Interviewees who said their organizations replaced their previous VPN solution with Cloudflare’s Zero Trust Network Access and device client (WARP) reported significant improvements in connection speed, reliability, and user satisfaction. By leveraging Cloudflare’s global network, their remote employees experienced faster access to critical applications without the latency and instability common with legacy VPN architectures. This improvement reduced help desk tickets and enhanced productivity for distributed teams.

- The CTO at an online gaming/gambling organization said: “Before Cloudflare Zero Trust, our support team was overwhelmed with VPN-related tickets — access issues, configuration problems, and user confusion. Since rolling out Zero Trust, those tickets have dropped by 85% to 90%.”
- The CTO at an online gaming/gambling organization noted: “Switching from our previous solution to Cloudflare’s Zero Trust platform was a game changer for both our users and our IT team. Even from the office, connections through the WARP client were 2.5x faster than direct access. Our remote teams saw fewer disconnections and reported a much better experience overall.”

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

- With Cloudflare, the composite avoids VPN license fees of \$400,000.
- It sees a 90% reduction in tickets per year related to VPN.
- It saves 45 minutes per incident, both for the response team and the employee who created the ticket and is waiting for resolution.
- The average fully burdened annual salary for an IT engineer is \$170,000.
- The average fully burdened annual salary for all employees across the organization is \$148,000.

Risks. Results may not be representative of all experiences, and the benefit will vary based on the following variables:

- The maturity of the previous solution.
- The number of remote access users.

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 \$5.2 million.

90%

Reduction in VPN-related tickets

“Cloudflare’s unified platform means we don’t have to stitch together multiple tools. It’s cleaner, faster, and easier to manage.”

Global director of network services, insurance/professional services

Improved Access Performance					
Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Avoided VPN license fees	Interviews	\$400,000	\$400,000	\$400,000
D2	Annual VPN tickets seen under previous solution	Interviews	25,000	25,000	25,000
D3	Percentage reduction in VPN tickets	Interviews	90%	90%	90%
D4	Annual eliminated tickets with Cloudflare	D2*D3	22,500	22,500	22,500
D5	Lost productivity per incident (hours)	Interviews	0.75	0.75	0.75
D6	Equivalent FTE	(D4*D5)/2,080	8.0	8.0	8.0
D7	Fully burdened annual salary for a DevOps engineer	Composite	\$170,000	\$170,000	\$170,000
D8	Fully burdened annual salary for an employee	Composite	\$148,000	\$148,000	\$148,000
D9	Recapture rate	TEI methodology	80%	80%	80%
D10	Productivity recapture	D6*(D7+(D8*D9))	\$2,307,200	\$2,307,200	\$2,307,200
Dt	Improved access performance	D1+D10	\$2,707,200	\$2,707,200	\$2,707,200
	Risk adjustment	↓10%			
Dtr	Improved access performance (risk-adjusted)		\$2,436,480	\$2,436,480	\$2,436,480
Three-year total: \$6,229,440			Three-year present value: \$5,163,898		

Reduced Bandwidth And Cloud Costs From Caching Efficiency

Evidence and data. Interviewees said their organizations achieved significant reductions in cloud infrastructure and bandwidth costs by leveraging Cloudflare’s global caching capabilities. By serving a large percentage of traffic from Cloudflare’s edge network, the interviewees’ organizations minimized origin server load and reduced egress charges from cloud providers. This efficiency not only lowered operational expenses but also improved application performance for end users. The head of web platforms for a pharmaceuticals/life sciences organization said: “With Cloudflare caching more than half of our traffic, we’ve dramatically reduced the load on our origin servers and cut cloud egress costs. It’s a clear financial and performance win.”

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

- The composite has an annual data volume of 400 TB.
- It offloads 50% of that volume to Cloudflare.
- With Cloudflare, the composite saves \$80 per TB.

Risks. Results may not be representative of all experiences, and the benefit will vary based on the following variables:

- The cost per TB the organization incurs.
- The makeup of applications, type of content, and ability to cache.

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 \$430,000.

50%

Data volume off-loaded to Cloudflare

“Cloudflare’s caching lets us serve more traffic locally, which not only improves performance but also cuts down on cloud costs.”

Head of web platforms, pharmaceuticals/life sciences

Reduced Bandwidth And Cloud Costs From Caching Efficiency					
Ref.	Metric	Source	Year 1	Year 2	Year 3
E1	Annual data volume (TB)	Composite	400	400	400
E2	Volume off-loaded to Cloudflare	Interviews	50%	50%	50%
E3	Cost per TB saved per month	Composite	\$80	\$80	\$80
Et	Reduced bandwidth and cloud costs from caching efficiency	E1*E2*E3*12	\$192,000	\$192,000	\$192,000
	Risk adjustment	↓10%			
Etr	Reduced bandwidth and cloud costs from caching efficiency (risk-adjusted)		\$172,800	\$172,800	\$172,800
Three-year total: \$518,400			Three-year present value: \$429,728		

Reduced Fees

Evidence and data. Interviewees reported measurable cost savings for their organizations due to consolidating multiple security and performance services under Cloudflare. By replacing legacy solutions with a single integrated platform, the interviewees’ organizations avoided overlapping licensing costs and reduced overall spend. In some cases, Cloudflare’s bundled pricing model and unmetered DDoS mitigation delivered double-digit percentage reductions compared to maintaining separate vendor contracts.

- The head of cybersecurity at a retail/consumer electronics organization said: “Cloudflare offered a more cost-effective solution than our previous solution. We estimate about a 20% reduction in fees plus the added benefit of simplified management.”
- The global director of network services at an insurance/professional services firm said: “We consolidated multiple vendors into one Cloudflare contract. That alone saved us a ton in licensing and support fees.”
- The head of web platforms at a pharmaceuticals/life sciences company said: “Cloudflare’s pricing is more transparent and predictable than our previous hardware-based DDoS tools. We no longer worry about surprise fees.”

Modeling and assumptions. Based on the interviews, Forrester assumes the composite saves 20% on license fees using Cloudflare.

Risks. Results may not be representative of all experiences, and the benefit will vary based on the following variables:

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

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 \$1.8 million.

20%

Cost savings due to consolidation of fees

“Cloudflare made Black Friday a nonevent. We used to brace for impact — now we trust the system to hold.”

Head of cybersecurity, retail/consumer electronics

Reduced Fees					
Ref.	Metric	Source	Year 1	Year 2	Year 3
F1	Previous fees	Interviews	\$3,960,000	\$3,960,000	\$3,960,000
F2	Percentage reduction in annual fees	Interviews	20%	20%	20%
Ft	Reduced fees	F1*F2	\$792,000	\$792,000	\$792,000
	Risk adjustment	↓10%			
Ftr	Reduced fees (risk-adjusted)		\$712,800	\$712,800	\$712,800
Three-year total: \$2,138,400			Three-year present value: \$1,772,628		

Unquantified Benefits

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

- **Improved customer trust and regulatory confidence.** Cloudflare’s programmable global infrastructure and compliance capabilities helped the interviewees’ organizations meet regulatory requirements and build trust with their users.
- **Improved IT experience from faster onboarding and reduced weekend work.** Interviewees said their teams experienced higher job satisfaction from smoother onboarding processes and fewer off-hours interventions due to Cloudflare’s unified platform and reliable performance.
- **Improved user experience and team satisfaction.** Employees and customers at the interviewees’ organizations benefited from faster access and more stable connections, leading to improved satisfaction across departments.
- **Improved reliability and reputational protection.** Cloudflare’s protection against DDoS and bot attacks ensured uptime during critical periods, helping safeguard the interviewees’ organizations’ brand reputation.
- **Increased peace of mind for developers and consistent SSL.** Interviewees said developers appreciated the consistent SSL management and reduction in operational burden, which allowed them to focus on innovation rather than maintenance.

“Cloudflare gave us peace of mind. We no longer worry about SSL expiring or inconsistent configurations across thousands of sites — it just works.”

Head of web platforms, pharmaceuticals/life sciences

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
Gtr	Licensing and support fees	\$0	\$3,630,000	\$3,630,000	\$3,630,000	\$10,890,000	\$9,027,273
Htr	Maintenance	\$0	\$93,500	\$93,500	\$93,500	\$280,500	\$232,521
ltr	Implementation and deployment	\$146,666	\$0	\$0	\$0	\$146,666	\$146,666
	Total costs (risk-adjusted)	\$146,666	\$3,723,500	\$3,723,500	\$3,723,500	\$11,317,166	\$9,406,460

Licensing And Support Fees

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

Modeling and assumptions. Based on the interviews, Forrester assumes the composite organization deploys a wide range of Cloudflare solutions. Products deployed over a three-year period include DDoS mitigation, bot management, WAF, CDN, load balancing, Argo smart routing, Zero Trust network access, and cloud email security. The composite also maintains a support contract with Cloudflare.

Risks. Results may not be representative of all experiences, and the cost will vary based on the following variables:

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

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 \$9.0 million.

“With Cloudflare technical support, we get to talk to real engineers, not just frontline support. That makes a huge difference when we’re troubleshooting complex issues.”

Head of web platforms, pharmaceuticals/life sciences

Licensing And Support Fees						
Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
G1	Cloudflare fees	Cloudflare		\$3,300,000	\$3,300,000	\$3,300,000
Gt	Licensing and support fees			\$3,300,000	\$3,300,000	\$3,300,000
		†10%				
Gtr	Licensing and support fees (risk-adjusted)		\$0	\$3,630,000	\$3,630,000	\$3,630,000
Three-year total: \$10,890,000				Three-year present value: \$9,027,273		

Maintenance

Evidence and data. Interviewees noted costs for ongoing maintenance. The head of cybersecurity at a retail/consumer electronics organization said, “We only need about a quarter of a full-time employee to manage the entire Cloudflare estate — it’s practically hands-off compared to our previous setup.”

Modeling and assumptions. Based on the interviews, Forrester assumes that the composite organization commits 0.5 FTE to maintenance.

Risks. Results may not be representative of all experiences, and the cost will vary based on the following variables:

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

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 \$233,000.

“Cloudflare’s support team helped us troubleshoot complex issues during implementation. They were fast, clear, and knew our environment well.”

Head of cybersecurity, retail/consumer electronics

Maintenance						
Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
H1	FTEs dedicated to Cloudflare maintenance	Interviews		0.5	0.5	0.5
H2	Fully burdened annual salary for a DevOps engineer	Composite		\$170,000	\$170,000	\$170,000
Ht	Maintenance	H1*H2	\$0	\$85,000	\$85,000	\$85,000
	Risk adjustment	±10%				
Htr	Maintenance (risk-adjusted)		\$0	\$93,500	\$93,500	\$93,500
Three-year total: \$280,500			Three-year present value: \$232,521			

Implementation And Deployment

Evidence and data. Interviewees described Cloudflare’s implementation process as generally smooth with several noting rapid deployment and minimal disruption.

- The director of digital platforms at a healthcare/medical devices organization said: “We ran a proof of concept and then rolled out quickly. Our internal security team led the charge.”
- The global director of network services at an insurance/professional services said: “We started with DNS then added CDN and WAF. It’s now our standard stack.”
- The CTO at an online gaming/gambling company said, “We started with WAF and expanded to the full stack over time.”
- The head of cybersecurity at a retail/consumer electronics firm said: “We migrated from our prior solution, which was complex. Cloudflare made it easier than expected.”

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

- The composite commits a team of four IT and DevOps engineers to implementation, deployment, and testing.
- Implementation and deployment take a period of two months.

Risks. Results may not be representative of all experiences, and the cost will vary based on the following variables:

- The number of Cloudflare features deployed.
- The size, scale, and usage of Cloudflare deployment.
- The deployment schedule as the organization determines.

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 \$147,000.

“Cloudflare is reliable, cost-effective, and better than [our previous solution]. It’s become a core part of our security stack.”

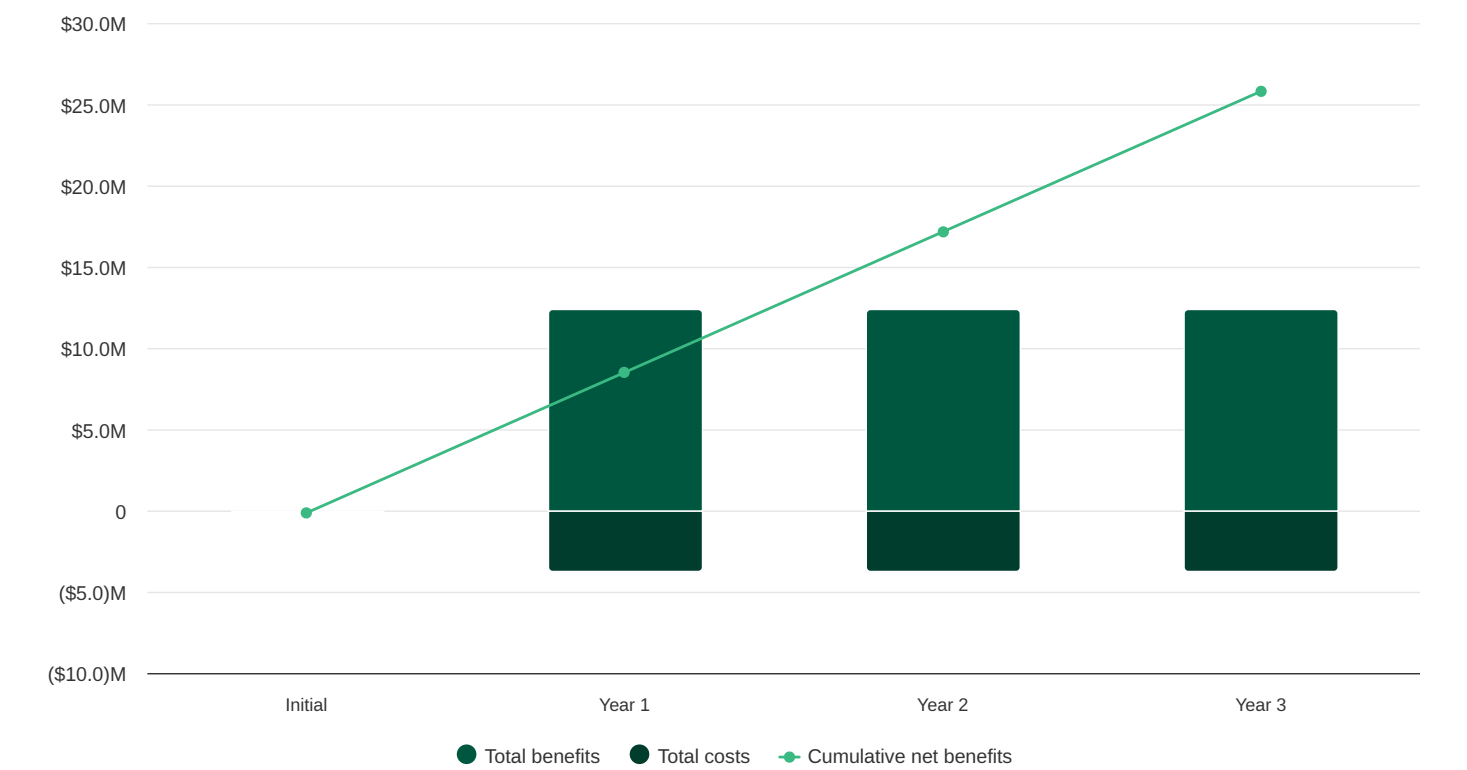
Head of cybersecurity, retail/consumer electronics

Implementation And Deployment						
Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
I1	IT engineers and DevOps engineers involved in implementation	Composite	4			
I2	Time spent on configuration, rollout, and testing (months)	Composite	2			
I3	Fully burdened annual salary for a DevOps engineer	Composite	\$200,000			
It	Implementation and deployment	(I1*I2*I3)/12	\$133,333	\$0	\$0	\$0
	Risk adjustment	↑10%				
Itr	Implementation and deployment (risk-adjusted)	20	\$146,666	\$0	\$0	\$0
Three-year total: \$146,666			Three-year present value: \$146,666			

Financial Summary

Consolidated Three-Year, Risk-Adjusted Metrics

Cash Flow Chart (Risk-Adjusted)



Cash Flow Analysis (Risk-Adjusted)						
	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	(\$146,666)	(\$3,723,500)	(\$3,723,500)	(\$3,723,500)	(\$11,317,166)	(\$9,406,460)
Total benefits	\$0	\$12,370,622	\$12,370,622	\$12,370,622	\$37,111,867	\$30,763,907
Net benefits	(\$146,666)	\$8,647,122	\$8,647,122	\$8,647,122	\$25,794,701	\$21,357,447
ROI						227%
Payback						<6 months

Please Note

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.

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.

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.

Due Diligence

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

Interviews

Interviewed five decision-makers 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.

Glossary

Total Economic Impact Approach

Benefits

Benefits represent the value the solution delivers to the business. The TEI methodology places equal weight on the measure of benefits and costs, allowing for a full examination of the solution's effect on the entire organization.

Costs

Costs comprise all expenses necessary to deliver the proposed value, or benefits, of the solution. The methodology captures implementation and ongoing costs associated with the solution.

Flexibility

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

Risks

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."

Financial Terminology

Present value (PV)

The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PVs 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

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

Appendixes

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 solution providers in communicating their value proposition to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of business and technology initiatives to both senior management and other key stakeholders.

APPENDIX B

Endnotes

¹ Source: Devin Dickerson, James Plouffe, and Joseph Blankenship, [Developer-Led Growth Meets Enterprise-Grade Security And Distributed Infrastructure At Cloudflare Connect 2025](#), Forrester Blogs.

² Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists solution providers in communicating their value proposition to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of business and technology initiatives to both senior management and other key stakeholders.

³ Cumulative breach costs are computed using the composite organization's size (revenue or number of employees) as an input to a regression analysis of reported total cumulative costs for all breaches for organizations that experienced at least one breach in the past 12 months. Source: Forrester's Security Survey, 2025, "Using your best estimate, what was the total cumulative cost of all breaches experienced by your organization in the past 12 months?" Base: 1,740 global security decision-makers who have experienced a breach in the past 12 months. The cumulative breach cost is then multiplied by a 67% likelihood for organizations to experience one or more breaches in a given year. Source: Forrester's Security Survey, 2025, "How many times do you estimate that your organization's sensitive data was potentially compromised or breached in the past 12 months?" Base: 2,643 global security decision-makers

⁴ Percentage of breaches by primary attack vector, as reported by security decision-makers whose organizations experienced at least one breach in the last 12 months. Source: Forrester's Security Survey, 2025, "Of the times that your organization's sensitive data was potentially compromised or breached in the past 12 months, please indicate how many of each fall into the categories below." Base: 1,766 global security decision-makers who have experienced a breach in the past 12 months

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.

Consulting Team:

Mary Barton

PUBLISHED

January 2026