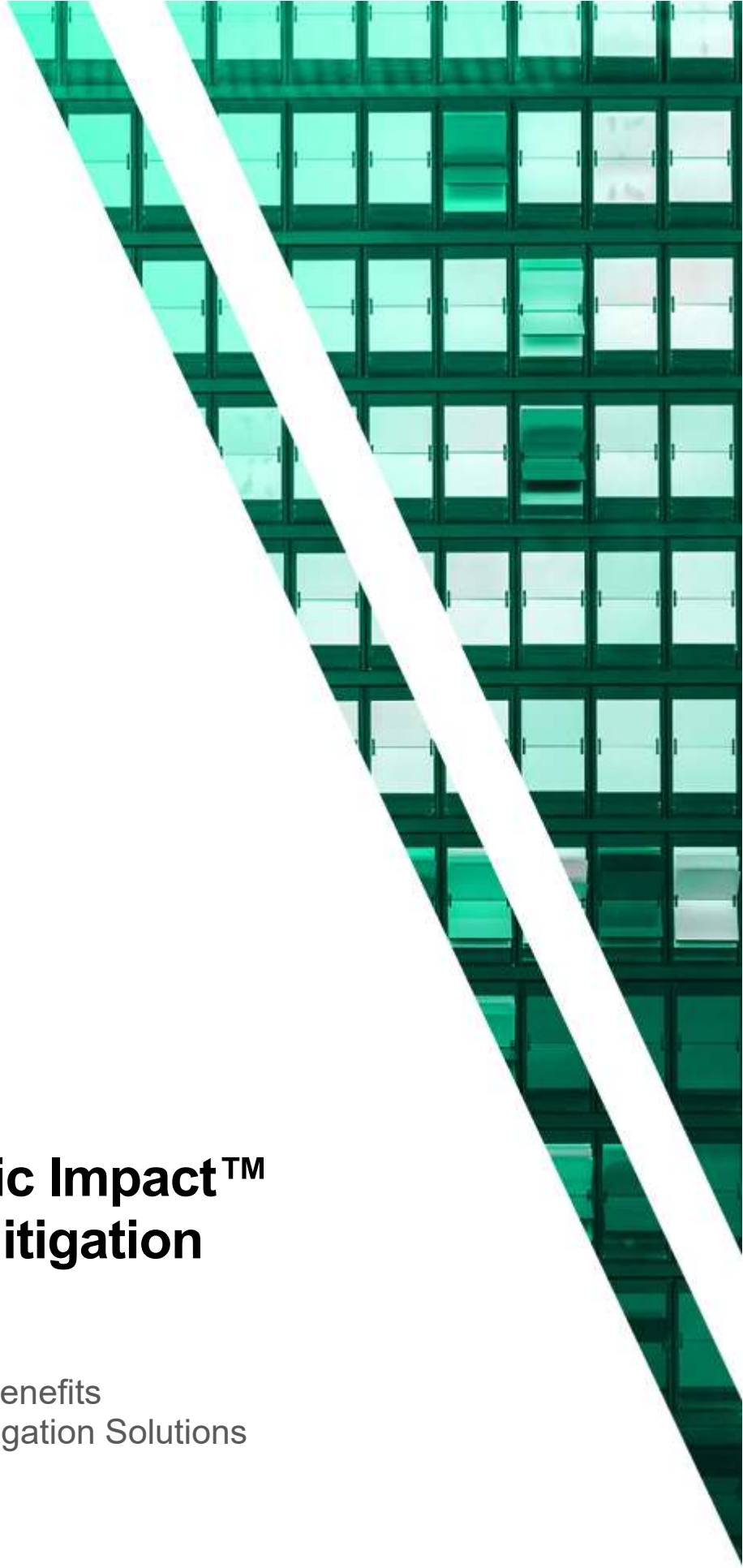
FORRESTER®



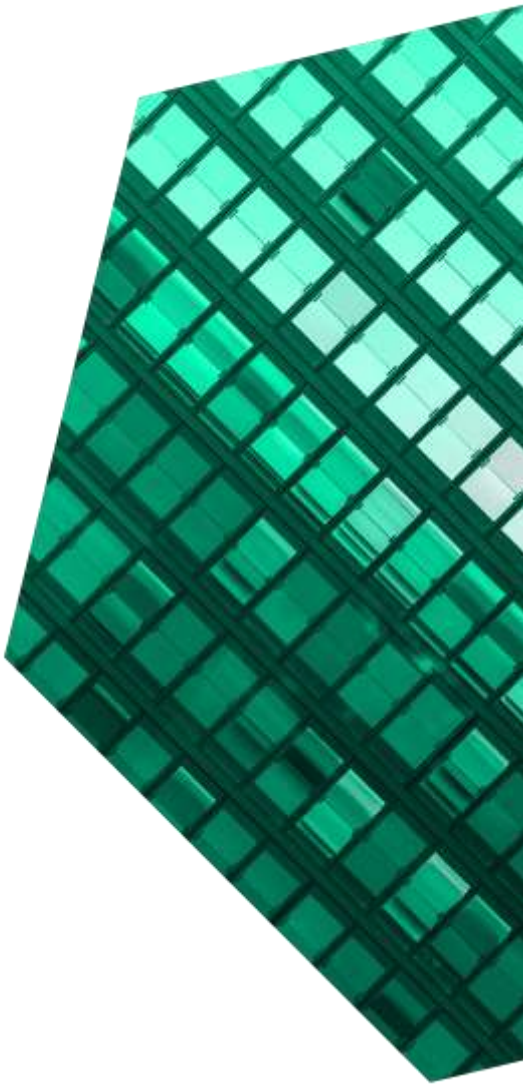
The Total Economic Impact™ Of Lumen DDoS Mitigation Solutions

Cost Savings And Business Benefits
Enabled By Lumen DDoS Mitigation Solutions

APRIL 2023

Table Of Contents

Consulting Team: Rachna Agarwalla
Rachel Ballard



ABOUT FORRESTER CONSULTING

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

Executive Summary

The threats of distributed denial of service (DDoS) attacks and other cyberattacks across the agile digital environment are growing and becoming more sophisticated as more businesses go online. Simultaneously, rising customer and employee expectations around site performance mean that frequent downtime can have a negative impact on brand reputation and the bottom line. Lumen DDoS Mitigation Solutions provide network and application layer protection, automate threat detection and blocking, and neutralize threats. That minimizes downtime and reduces costs.

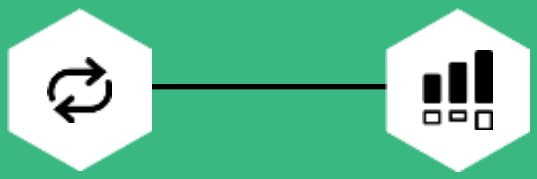
Lumen DDoS Mitigation Solutions® mitigate widespread security threats and consequences from cyberattacks on websites, applications, and internal systems. DDoS attacks can bring down business-critical digital assets, leading to profit and brand reputation losses. Lumen DDoS Mitigation Solutions help reduce the number of attacks through automatic threat blocking that involves scrubbing malicious traffic before it hits the victim. The solutions mitigate many attacks within seconds, provide robust analytics, and stay one step ahead of attackers.

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

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four representatives with experience using Lumen DDoS Mitigation Solutions. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization that is a digital commerce organization doing business in North America with 4,000 employees, an annual revenue of $2 billion, and a 10% operating profit margin. For the purposes of this study, digital commerce is defined as any business conducted online, including retail, fintech, gaming, healthcare, and others.

Prior to engaging Lumen for DDoS Mitigation Solutions, these interviewees noted that their organizations had been targeted and affected by DDoS attacks and had incurred expenses to get operations back on track. Their legacy solutions were limited and resolving these attacks was time-consuming for their IT teams. This resulted in significant network downtime, reduced productivity, and negative customer/employee experiences. In addition, prior DDoS solutions lacked scalability and the necessary features to adequately protect the interviewees' organizations as they grew, and they

KEY STATISTICS



Return on investment (ROI)
297%

Net present value (NPV)
$5.44M

31%

Fewer attacks seen by composite after investing in Lumen DDoS Mitigation Solutions

often required platform-specific, in-house expertise to appropriately manage.

After the investment in Lumen DDoS Mitigation Solutions, the interviewees reported a reduction in the number of attacks, a decrease in time spent addressing and resolving attacks, and an increase in peace of mind. Key results from the investment included increased operating profit, improved productivity, reduced costs associated with prior DDoS solutions, and decreased penalties related to security breaches.

KEY FINDINGS

Quantified benefits. Three-year, risk-adjusted present value (PV) quantified benefits for the composite organization include:[2]

- **Increase in net operating profit due to incremental revenue totals $3.4 million.** Lumen DDoS Mitigation Solutions enable the composite organization to increase its net operating profit due to an increase in gross sales revenue. The composite sees revenue grow in two ways because of the investment in Lumen DDoS Mitigation Solutions. First, the composite is able to retain its existing customers with its improved website uptime, which reduces churn and increases sales. Before the investment, the composite organization lost numerous dissatisfied customers as a result of network and site downtime. Second, the improvement in website uptime leads to a better customer experience. This leads to positive word of mouth that drives an increase in net new customers, further enhancing the revenue stream.
- **Improvement in productivity of IT, communications, and customer service teams with a value of $1.6 million.** Through its automated attack blocking features, Lumen DDoS Mitigation Solutions reduce successful attacks and limit the impact of the attacks that target the composite organization's infrastructure. This allows the composite organization to be proactive and spend more time on other business-critical issues instead of monitoring, analyzing, and mitigating DDoS attacks. Fewer attacks also result in fewer calls to customer service, as agents no longer retrieve calls concerning customers' inability to access the website. Finally, from a public relations perspective, the communications team spends less time addressing DDoS attacks and website downtime.
- **Sunsetting of legacy tools offers cost savings of $1.4 million.** Lumen DDoS Mitigation Solutions allow the composite organization to decommission less sophisticated DDoS mitigation technology, which lives in a manual, outdated environment and is limited in the prevention of DDoS attacks. Lacking interoperability and the ability to scale, legacy solutions often require in-house IT expertise and excessive hours to manage and use effectively. The sunsetting of these tools also allows the composite organization to realize savings on Amazon Elastic Compute Cloud (EC2) surges and calls to content delivery networks (CDNs).
- **Reduction in penalties and fines yield cost savings of $481,500.** Lumen DDoS Mitigation Solutions allow the composite to reduce the total number of DDoS attacks and thereby reduces the penalties and fines formerly paid to regulatory bodies in the event of a security breach or an audit failure.
- **Increase in productivity of compliance team due to fewer DDoS attacks totals $376,000.** The compliance team within the composite organization also experiences efficiencies with Lumen DDoS Mitigation Solutions. Fewer cyberattacks means the team needs less preparation time for internal, external, or regulatory audits.

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

- **Reliability and peace of mind.** Lumen DDoS Mitigation Solutions' modern technological capabilities result in more uptime for the composite's sites, networks, and systems. This reliability gives the composite organization a competitive advantage and provides peace of mind to many teams across the organization, especially the IT and cybersecurity teams that have the job of ensuring the site is up and reliable at all times.
- **Centralized governance and reporting.** Lumen DDoS Mitigation Solutions give the composite organization the ability to centralize security controls implemented across the different infrastructures into a single location. This allows the composite to transition from a siloed environment to one where IT teams can centrally troubleshoot and mitigate attacks. With a unified solution, the composite can take advantage of the Lumen DDoS Mitigation Solutions' advanced reporting capabilities that provide visibility into all cybersecurity vulnerabilities and events with ease.
- **Scalability.** Lumen DDoS Mitigation Solutions support multi-cloud architectures, which enables the composite to protect multiple layers of its technology infrastructure. Given that the solutions are software-as-a-service (SaaS) offerings, implementation at the composite organization can also occur on top of any environment across its locations. Implementing Lumen DDoS Mitigation Solutions across new projects, functions, and initiatives is a seamless experience.

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

- **Total license fees of $1.1 million.** Lumen charges a license fee for usage. While dependent on several factors, the total fee to Lumen amounts to 0.02% of the composite organization's total revenue.
- **Initial and ongoing costs of $734,000.** Upon purchase of Lumen DDoS Mitigation Solutions, the composite incurs some initial implementation costs. They include technical setup, integration with networks, setting governance policies, and training of intended users. Ongoing costs include managing the implemented solution, responding to incidents, analyzing successful attacks, and adding additional features.

The representative interviews and financial analysis found that a composite organization experiences benefits of $7.27 million over three years versus costs of $1.83 million, adding up to a net present value (NPV) of $5.44 million and an ROI of 297%.

"After our implementation of Lumen, we are still getting attacked, but the difference is that a lot of them are being prevented or blocked. As a result, we have not seen the site go down."

VP of IT, healthcare

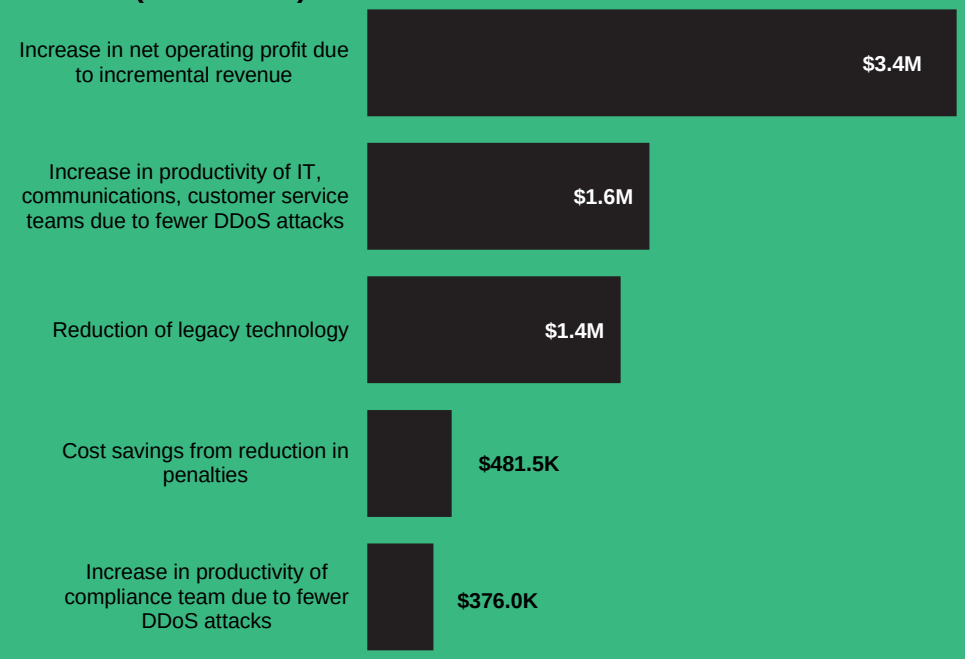
ROI
297%

BENEFITS PV
$7.27M

NPV
$5.44M

PAYBACK
<6 months

Benefits (Three-Year)



“Lumen has made things cheaper, better, and faster. We’ve been able to improve performance, reduce latency, and improve qualitative feedback from our customers, employees, contractors, and vendors who used to have a lot of trouble accessing our applications. All of this has definitely been very good.”

— Executive director, financial services

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 Lumen DDoS Mitigation Solutions.

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 Lumen DDoS Mitigation Solutions can have on an organization.

DUE DILIGENCE

Interviewed Lumen stakeholders and Forrester analysts to gather data relative to Lumen DDoS Mitigation Solutions.

INTERVIEWS

Interviewed four representatives at organizations using Lumen DDoS Mitigation Solutions to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

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

FINANCIAL MODEL FRAMEWORK

Constructed a financial model representative of the interviews using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewees.

CASE STUDY

Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

The Lumen DDoS Mitigation Solutions Customer Journey

Drivers leading to the Lumen DDoS Mitigation Solutions investment

Interviews

Role	Industry	Region	Investment Objectives
Director of IT	Healthcare	HQ US	Favorable pricing, easy integration, scalability, hardware protection
VP of IT	Healthcare	HQ US	Favorable pricing, easy implementation, easy to learn and use, SaaS, focus on innovation
Executive director, IT	Financial services	HQ US, global footprint	Centralization, incognito solution, DDoS mitigation at the borders, reduction in cyberbreaches
Director of IT/cybersecurity	Technology	HQ US, global footprint	Favorable pricing, easy to implement, platform agnostic

KEY CHALLENGES

Before investing in Lumen DDoS Mitigation Solutions, interviewees used a variety of different products for DDoS mitigation, ranging from competitor products to those bundled with cloud services. These options proved inadequate to prevent, stop, and reduce the number of attacks on their organizations. In addition, interviewees looked for more sophisticated solutions with advanced features, especially automation. A director of IT at a healthcare company noted: "Another reason we looked at Lumen was because its DDoS solutions offer automation. Also, Lumen scrubs traffic to our site and helps to mitigate some problems that one might experience."

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

- **Excessive DDoS attacks.** The biggest challenge most organizations faced was the costly downtime caused by an unacceptable number of DDoS attacks. An executive director of IT at a financial services firm said, "We were being attacked literally every hour, so it was extremely essential for us to invest in a central tooling that allowed us to proactively go out and mitigate."
- **Lack of scalability.** Many interviewees lacked solutions that allowed them to scale across cloud providers and varying locations. A director of IT at a healthcare organization commented: "We were looking for scalability because our organization is spread across different sites and in different locations. We really wanted to have some degree of scalability and be able to protect everything with a pretty broad approach."

"The DDoS offering from our cloud provider was basic and didn't grow with us. We needed a specialized tool that focused on DDoS, as attacks went up in the last two years because of the growth we had at our company. We became popular, so more hackers try to try to penetrate our systems."

Director of IT/cybersecurity, technology

In addition, interviewees needed a hyperscaler-agnostic DDoS solution that would serve across their organizations and allow for a uniform security policy. An executive director of IT at a financial services organization said: "Governance was a huge challenge for us — [we needed] management of security controls in a central location, policy creations, and a rollout. We wanted all our security policies to be sitting in one tool versus multiple, disparate tools, so we could optimize our resources. If you have one tool, you have a single set of resources managing the [solutions] versus different teams managing different lines of businesses with power of attorney over security tooling."

- **Need for automation, advanced features, and reporting.** Organizations also noted the need for solutions that could proactively and automatically prevent, detect, and mitigate attacks. A director of IT in the healthcare industry noted: "We wanted to understand what sort of events are tolerable and acceptable versus what is appropriate. We also needed help scrubbing the traffic to our website."

  Interviewees also required professional services to supplement their in-house DDoS expertise. A VP of IT at a healthcare company commented, "Our previous DDoS provider didn't maintain [its] platform and did not provide any in-house expertise or any professional services."

  Finally, organizations needed centralized reporting with data that is easy to access, easy to understand, and easy to use to help make business decisions as well as for compliance-related audits.

SOLUTION REQUIREMENTS/INVESTMENT OBJECTIVES

The interviewees' organizations searched for a solution that was:

- Effective in reducing number of attacks/cyberbreaches.
- Scalable across platforms and locations.
- Favorable with respect to pricing.
- Easy to implement, learn, and use.
- A SaaS offering.
- Able to provide reliable and meaningful data, analytics, and reporting.
- Focused on innovation.

"Our list of key evaluation criteria included the following: 1) easy to use, implement, and maintain; 2) good pricing; 3) shorter licensing periods, that is, two- or three-year agreements."

VP of IT, healthcare

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, 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 digital commerce organization has $2 billion in revenue generates sales online exclusively as well as in partnership with other sales channels. Since digital commerce is not limited to the retail sector, the composite organization could be a healthcare, financial services, technology, or other type of company as long as a portion of its sales are digital. The composite organization has strong brand recognition and has operations across North America. It has 4,000 employees and a 10% operating profit margin.

Key Assumptions

- **Digital commerce**
- **$2 billion in revenue**
- **4,000 employees**
- **10% operating margin**
- **Focused in North America**

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	Increase in net operating profit due to incremental revenue	$1,350,000	$1,350,000	$1,350,000	$4,050,000	$3,357,250
Btr	Increase in productivity of IT, communications, customer service teams due to fewer DDoS attacks	$646,380	$646,380	$646,380	$1,939,140	$1,607,451
Ctr	Reduction of legacy technology	$479,250	$639,000	$639,000	$1,757,250	$1,443,871
Dtr	Cost savings from reduction in penalties	$193,600	$193,600	$193,600	$580,800	$481,455
Etr	Increase in productivity of compliance team due to fewer DDoS attacks	$151,200	$151,200	$151,200	$453,600	$376,012
	Total benefits (risk-adjusted)	$2,820,430	$2,980,180	$2,980,180	$8,780,790	$7,266,039

INCREASE IN NET OPERATING PROFIT DUE TO INCREMENTAL REVENUE

Evidence and data. Interviewees reported the following:

- Lumen DDoS Mitigation Solutions allowed the interviewees' organizations to increase revenue in two ways. First, they retained customers who might have previously churned away due to dissatisfaction with the excessive downtime they experienced. A director of IT/cybersecurity of a technology company commented: "We are a SaaS company, and people need to be able to connect to our websites for them to be productive. With Lumen DDoS protection, we've been able to reduce our downtime due to DDoS attacks. This has sent a good message to our customers now that our uptime is 99% and above. As a result, people trust us more, are renewing their annual contracts with us, and are willing to sign two- or three-year deals."
- Second, the interviewees' organizations grew their customer bases due to a positive brand reputation around site uptime. The same director of IT/cybersecurity at the technology company noted: "We rely on word of mouth for new customers. If one IT or security professional is positive about our product, they talk about this with other leaders and peers in their community.

"The number one metric where we have improved is customer satisfaction. If customers can access applications quickly, they're using our applications a lot more. Business lines see direct growth in revenue."

Executive director, IT, financial services

So, a meaningful fraction of our sales may be attributed to this positivity and good feedback from our existing customers and partners."

Modeling and assumptions. For the composite organization, Forrester makes the following assumptions:

- The composite organization has annual revenue of $2 billion per year.
- The composite organization retains 0.3% of its total revenue as customer abandonment is no longer an issue.
- The composite organization gains 0.6% of its total revenue from positive word of mouth surrounding website uptime.
- The composite has a 10% operating profit margin.

Risks. Increases in net operating profit due to incremental revenue will vary depending on:

- Annual revenue of the organization.
- Total decrease in downtime.
- Operating profit margin according to industry.
- Percentage of improvement attributed to Lumen.

Results. To account for these risks, Forrester adjusted this benefit downward by 25%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $ $3.4 million.

Increase In Net Operating Profit Due To Incremental Revenue

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Sales Revenue	Composite	$2,000,000,000	$2,000,000,000	$2,000,000,000
A2	Percent of revenue no longer lost due to website being down	Interviews	0.3%	0.3%	0.3%
A3	Revenue no longer lost due to website being down	A1*A2	$6,000,000	$6,000,000	$6,000,000
A4	Percent of revenue gained from positive reputation re: website uptime	Interviews	0.6%	0.6%	0.6%
A5	Revenue gained from positive reputation re: website uptime	A1*A4	$12,000,000	$12,000,000	$12,000,000
A6	Operating profit margin	Composite	10%	10%	10%
At	Increase in net operating profit due to incremental revenue	(A3+A5)*A6	$1,800,000	$1,800,000	$1,800,000
	Risk adjustment	↓25%			
Atr	Increase in net operating profit due to incremental revenue (risk-adjusted)		$1,350,000	$1,350,000	$1,350,000
	Three-year total: $4,050,000			**Three-year present value: $3,357,250**	

INCREASE IN PRODUCTIVITY OF IT, COMMUNICATIONS, CUSTOMER SERVICE TEAMS DUE TO FEWER DDOS ATTACKS

Evidence and data. Interviewees reported the following:

- The implementation of Lumen DDoS Mitigation Solutions allowed the organizations to improve the productivity of the IT/cybersecurity, communications, and customer service teams. Due to automation and fewer attacks, these teams spent less time on issues related to DDoS mitigation. As a result, they focused on other more business-critical issues, resulting in an increase in productivity and innovation.
- A VP of IT at a healthcare organization commented: “Due to our investment in Lumen, we can complete assessments much quicker. We can also identify where the attack is, so it doesn’t potentially move on and impact other parts of the organization. Our ability to mitigate much faster is the value Lumen provides. Also, my team doesn’t spend that much time having to dig in and figure out what the issues are or where they might be coming from.”
- A director of IT/cybersecurity at a technology firm noted: “When things go down and the service is down for more than three or four hours, we get a lot of follow-up calls. With Lumen, we’ve been able to cut down the time spent on those calls by half.”

Modeling and assumptions. For the composite organization, Forrester makes the following assumptions:

- The composite organization saves the equivalent of three IT/cybersecurity FTEs who are each earning a fully loaded annual salary of $141,750.
- The composite saves the equivalent of seven customer service and communications team members who are each earning a fully loaded annual salary of $67,500.
- The composite organization is able to capture 80% of the time saved from an increase in productivity.

Risks. An increase in productivity of IT, communications and customer service teams will vary with:

- The size and experience of the IT/cybersecurity, communications, and customer service teams.
- The salary of each team member, which is based on location and skill level.
- Percent of productivity captured.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $ $1.6 million.

Increase In Productivity Of IT, Communications, Customer Service Teams Due To Fewer DDoS Attacks					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	Increase in productivity of IT and cybersecurity team members (FTEs)	Interviews	3	3	3
B2	Salary per IT and cybersecurity team member (fully burdened)	TEI standard	$141,750	$141,750	$141,750
B3	Increase in productivity of customer service and communications team members (FTEs)	Interviews	7	7	7
B4	Salary of customer service and marketing team member (fully burdened)	TEI standard	$67,500	$67,500	$67,500
B5	Percent captured	TEI standard	80%	80%	80%
Bt	Increase in productivity of IT, communications, customer service teams due to fewer DDoS attacks	((B1*B2)+ (B3*B4))*B5	$718,200	$718,200	$718,200
	Risk adjustment	↓10%			
Btr	Increase in productivity of IT, communications, customer service teams due to fewer DDoS attacks (risk-adjusted)		$646,380	$646,380	$646,380
	Three-year total: $1,939,140			**Three-year present value: $1,607,451**	

REDUCTION OF LEGACY TECHNOLOGY

Evidence and data. Interviewees reported the following:

- The interviewees' organizations reduced costs associated with legacy solutions. This includes previous DDoS mitigation solutions as well as EC2 and CDN spikes from traffic surges during attacks.
- A director of IT/cybersecurity at a technology organization noted: "With Lumen, we have seen a reduction in the number of back-and-forth calls from our CDN to our cloud provider. Our infrastructure auto scales. If our DDoS solution is not able to catch excessive malicious requests, we automatically have to scale up our EC2 instances and infrastructure to deal with this demand. These spikes and spinning up on infrastructure would happen a few times a month, but with Lumen that has now come down significantly since [its services are] filtering the traffic. It is stopping those botnet attacks from happening."

> **"There is less traffic going to the hyperscalers, so there is a reduction in cost."**
>
> *Executive director, IT, financial services*

Modeling and assumptions. For the composite organization, Forrester makes the following assumptions:

- The composite organization saves $710,000 annually on DDoS mitigation solutions, cloud providers, and CDN-related fees with Lumen DDoS Mitigation Solutions.
- Due to the required implementation and transition time of three months, the composite only recognizes 75% of that annual cost reduction in Year 1 for a savings of $532,500.

Risks. Reduction in legacy technology will vary depending on the following:

- The capabilities and functionalities of an organization's legacy technology.
- The level of reduction in the number of DDoS attacks.
- Level of adoption.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $ $1.4 million.

Reduction Of Legacy Technology

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Consolidation of legacy DDoS solution costs	Interviews	$532,500	$710,000	$710,000
Ct	Reduction of legacy technology	C1	$532,500	$710,000	$710,000
	Risk adjustment	↓10%			
Ctr	Reduction of legacy technology (risk-adjusted)		$479,250	$639,000	$639,000
	Three-year total: $1,757,250			**Three-year present value: $1,443,871**	

COST SAVINGS FROM REDUCTION IN PENALTIES

Evidence and data. Interviews reported the following:

- The interviewees' organizations faced penalties from audit and regulatory bodies due to their cybersecurity breaches. In addition, interviewees were constantly concerned about failing an audit and consequently having to pay a penalty.
- By decreasing the security risk and reducing the number of attacks, the interviewees reported that they saw a drop in penalties due to failed audits.

Modeling and assumptions. For the composite organization, Forrester makes the following assumptions:

- The composite organization has 4,000 employees.
- The estimated cost of breach per employee is $60.53 annually according to a survey done by Forrester.[3]

Risks. Cost savings from a reduction in penalties will vary with:

- Total number of employees.
- Level of reduction in number of DDoS attacks.
- The cost per breach, depending on industry and regulatory and compliance requirements.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of almost $481,500.

> **"Since we have the Lumen DDoS, it's preventing a lot of cybersecurity breaches for which we previously used to pay millions and millions of dollars in fines."**
>
> *Executive director, IT, financial services*

Cost Savings From Reduction In Penalties

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Reduced penalties due to breaches	TEI standard	$242,000	$242,000	$242,000
Dt	Cost savings from a reduction in penalties due to breaches	D1	$242,000	$242,000	$242,000
	Risk adjustment	↓20%			
Dtr	Cost savings from a reduction in penalties due to breaches (risk-adjusted)		$193,600	$193,600	$193,600
	Three-year total: $580,800		**Three-year present value: $481,455**		

INCREASE IN PRODUCTIVITY OF COMPLIANCE TEAM DUE TO FEWER DDOS ATTACKS

Evidence and data. Interviewees reported the following:

- Due to a decrease in the number of DDoS attacks thanks to Lumen DDoS Mitigation Solutions, compliance teams at the interviewees' organizations spent less time meeting about and preparing for audits. As their compliance results

improved and they met audit requirements more frequently, teams also spent less time reporting on attacks.

- An executive director of IT at a financial services firm noted: “We were spending a considerable amount of time addressing compliance issues or writing about them. Now we are not spending that much time because we are compliant.”

Modeling and assumptions. For the composite organization Forrester makes the following assumptions:

- The composite organization saves the equivalent of two compliance FTEs in productivity gains.
- The FTEs each earn a fully loaded annual salary of $94,500.

Risks. An increase in productivity of the compliance team will vary with:

- The size and experience of the compliance team.
- The salary of each team member, which is based on location and skill level.
- Previous audit and compliance records.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of over $376,000.

> **“We had two main objectives when investing in Lumen and one was the compliance. Our chief compliance officer was adamant about ensuring that our site was protected so we don’t lose out on any future business opportunities.”**
>
> *VP of IT, healthcare*

Increase In Productivity Of Compliance Team Due To Fewer DDoS Attacks

Ref.	Metric	Source	Year 1	Year 2	Year 3
E1	Increase in productivity of compliance team members (FTE's)	Interviews	2	2	2
E2	Salary per compliance team member (fully burdened)	TEI Standard	$94,500	$94,500	$94,500
Et	Increase in productivity of compliance team due to fewer DDoS attacks	E1*E2	$189,000	$189,000	$189,000
	Risk adjustment	↓20%			
Etr	Increase in productivity of compliance team due to fewer DDoS attacks (risk-adjusted)		$151,200	$151,200	$151,200
	Three-year total: $453,600			**Three-year present value: $376,012**	

UNQUANTIFIED BENEFITS

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

- **Reliability and peace of mind.** Lumen DDoS Mitigation Solutions allow companies to protect their external and internal websites, networks, and data centers from downtime due to DDoS attacks. This results in a more reliable experience

for their customers and employees, leading to a greater experience and level of satisfaction. This directly contributed to an improvement in peace of mind for the interviewees' organizations' IT and cybersecurity professionals. A VP of IT at a healthcare organization commented, "Lumen DDoS has made our life easy, one less thing to worry about by implementing their solution."

- **Centralized governance and reporting.** Lumen DDoS Mitigation Solutions centralized security event data and allowed the interviewees' organizations to see, manage, troubleshoot, and mitigate DDoS attacks from a single location. In addition, the organizations had the ability to generate data and reports across all instances. This made it easier for the interviewees' teams to assess their security posture at any given time. An executive director of IT at a financial services firm relayed, "Now that governance is central with security policies sitting in Lumen, it's easy for us to pull a report versus earlier when we would have to go to multiple different places and consolidate the reports into a single one."
- **Scalability.** Lumen DDoS Mitigation Solutions are scalable solutions that work across multiple locations, platforms, and cloud providers. This allowed the interviewees' organizations to have a single provider across a diverse infrastructure. A director of IT in healthcare said: "Our long-term strategy is to implement Lumen across the entire organization. I think that's very important and critical for us to do."

FLEXIBILITY

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

- **Innovation partner.** According to the interviewees, Lumen is one step ahead of hackers, monitoring traffic across its extensive global network to anticipate and mitigate new types of DDoS attacks. This proactively protects customers in the future and keeps their mind at ease as it relates to site security.
- **Enhanced collaboration.** With a consolidated dashboard and improved visibility of security event data, teams across an organization no longer need to rely on data from siloed business units, which often results in long turnaround times. Teams now interact on one platform, allowing for enhanced communication and collaboration, and they continuously improve their security postures and protecting their organizations from increasingly sophisticated future attacks.

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

> **"Our strategy is to migrate 100% of our front end onto Lumen. As we start migrating more and more assets into the cloud, we want every application to basically have traffic coming in through Lumen."**
>
> *Executive director, IT, financial services*

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Ftr	Total license fees	$0	$440,000	$440,000	$440,000	$1,320,000	$1,094,215
Gtr	Initial and ongoing costs	$600,000	$54,000	$54,000	$54,000	$762,000	$734,290
	Total costs (risk-adjusted)	$600,000	$494,000	$494,000	$494,000	$2,082,000	$1,828,505

TOTAL LICENSE FEES

Evidence and data. Pricing for Lumen DDOS Mitigation Solutions is flexible based on a variety of factors, such as instances.

Modeling and assumptions. For the composite organization, Forrester makes the following assumptions:

- The composite organization spends 0.02% of its revenue to license Lumen DDoS Mitigation Solutions.
- Pricing isn't necessarily linear and may depend on actual number of instances, organizational needs, and other variables. Contact Lumen for additional details.

Risks. Total license fees will vary with:

- Number of security events or instances.
- Annual revenue of the organization.
- Level of professional services needed.

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 $1.1 million.

Total License Fees						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
F1	Sales revenue	Composite		$2,000,000,000	$2,000,000,000	$2,000,000,000
F2	License fees as a percent of revenue	Interviews		0.02%	0.02%	0.02%
Ft	Total license fees	F1*F2	$0	$400,000	$400,000	$400,000
	Risk adjustment	↑10%				
Ftr	Total license fees (risk-adjusted)		$0	$440,000	$440,000	$440,000
	Three-year total: $1,320,000			**Three-year present value: $1,094,215**		

INITIAL AND ONGOING COSTS

Evidence and data. Initial and ongoing costs for Lumen DDOS Mitigation Solutions are flexible based on a variety of factors, such as instances, size of organization and number of attacks.

Modeling and assumptions. For the composite organization, Forrester makes the following assumptions:

- The composite organization incurs $500,000 initially to implement Lumen DDoS Mitigation Solutions across the organization.
- On an ongoing basis, various teams spend time doing due diligence, analyzing, and reporting. This includes the required time of project managers, IT leaders, security and network engineers, and communication team members. This amounts to an annual cost of $45,000.

Risks. Initial and ongoing costs will vary with:

- The size of the organization and the complexity of its security posture.
- The number of attacks the organization experiences.
- The organization's legacy DDoS solutions and its level of sophistication.

Results. To account for these risks, Forrester adjusted this cost upward by 20%, yielding a three-year, risk-adjusted total PV of $734,000.

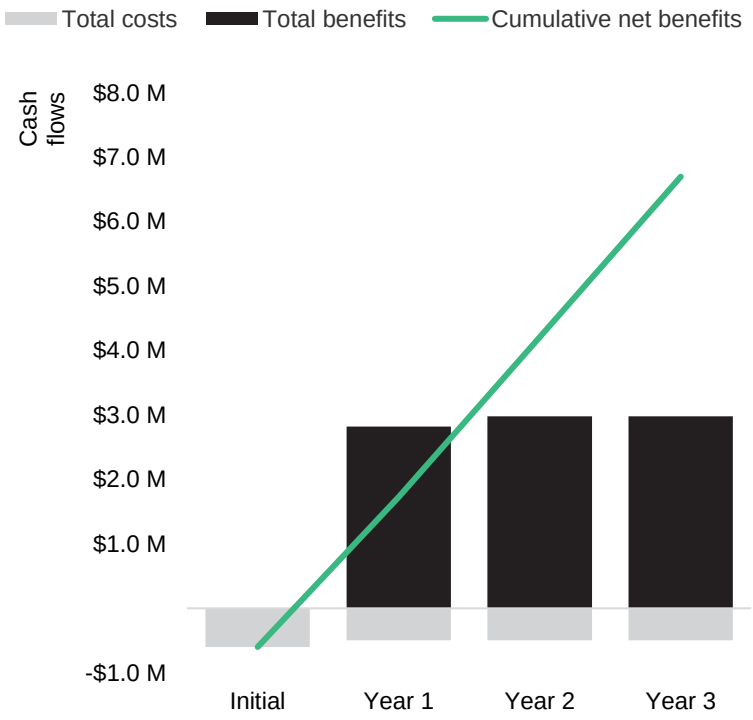
Initial And Ongoing Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
G1	Initial implementation costs	Interviews	$500,000			
G2	Ongoing costs	Interviews		$45,000	$45,000	$45,000
Gt	Initial and ongoing costs	G1+G2	$500,000	$45,000	$45,000	$45,000
	Risk adjustment	↑20%				
Gtr	Initial and ongoing costs (risk-adjusted)		$600,000	$54,000	$54,000	$54,000
	Three-year total: $762,000			**Three-year present value: $734,290**		

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



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

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

Cash Flow Analysis (Risk-Adjusted Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($600,000)	($494,000)	($494,000)	($494,000)	($2,082,000)	($1,828,505)
Total benefits	$0	$2,820,430	$2,980,180	$2,980,180	$8,780,790	$7,266,039
Net benefits	($600,000)	$2,326,430	$2,486,180	$2,486,180	$6,698,790	$5,437,534
ROI						297%
Payback period (months)						<6

Appendix A: Total Economic Impact

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

TOTAL ECONOMIC IMPACT APPROACH

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

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

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

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

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

PRESENT VALUE (PV)

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

NET PRESENT VALUE (NPV)

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

RETURN ON INVESTMENT (ROI)

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

DISCOUNT RATE

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

PAYBACK PERIOD

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

Appendix B: Endnotes

[1] 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] Study conducted from August of 2022 to April of 2023, but certain study data is presented here over an extended time period and adjusted for applicable factors.

[3] Source: Forrester's Security Survey, 2022.


FORRESTER®