A Forrester Total Economic Impact™
Study Commissioned By CenturyLink
May 2020

# The Total Economic Impact™ Of CenturyLink DDoS Mitigation Service

## Cost Savings And Business Benefits Enabled By CenturyLink DDoS Mitigation Service

FORRESTER®

# Table Of Contents




**Project Director:**
Jennifer Adams

**Associate Consultant:**
Connor Maguire


ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.



FORRESTER®

## Benefits And Costs

Total benefits:
**$1.6 million**

Reduce MTTD and MTTR DDoS attacks by:
**75%**

CenturyLink's network-based DDoS Mitigation Service cost:
**$0.3 million**

# Executive Summary

CenturyLink provides a network-based Distributed Denial of Service (DDoS) Mitigation Service that helps protect its customers against DDoS attacks. This type of attack accounted for 24% of all external security attacks in 2019, according to a recent Forrester survey.[1] CenturyLink's network-based DDoS Mitigation Service helps ensure the availability of mission-critical applications, preserves brand reputation, and enhances end customer digital experience.

CenturyLink commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying CenturyLink's network-based DDoS Mitigation Service. The purpose of this study is to provide readers with a framework to evaluate the potential financial benefit of the DDoS Mitigation Service to their organizations.

To better understand the benefits and costs associated with this investment, Forrester interviewed several current CenturyLink DDoS customers with years of experience using a DDoS mitigation solution. The network-based CenturyLink DDoS Mitigation Service routes network traffic through a global network of 15 scrubbers, and it utilizes 85 terabits per second of FlowSpec capacity on the backbone as a first line of defense.

Prior to using CenturyLink's network-based DDoS Mitigation Service, customers experienced mission-critical application downtime due to DDoS attacks that resulted in lost revenue, costs to remediate and mitigate attacks, damage to brand reputation, and negative impact on customer experience.

## Key Findings

**Quantified benefits.** The following risk-adjusted present value (PV) quantified benefits are representative of those experienced by the companies interviewed. Total benefits were $1.6 million present value (PV) over a three-year period:

- **Minimized loss of revenue due to DDoS attacks: $0.3 million benefit.** With CenturyLink's network-based DDoS Mitigation Service, the organizations virtually eliminated outages due to DDoS attacks. Annual downtime for key applications dropped from 2 hours to 5 minutes. Digital assets including eCommerce and online banking were up and running and generating revenue.
- **Streamlined network security team: $1.2 million benefit.** The network security teams now spend less time identifying, understanding, and mitigating DDoS attacks.
- **Reduced the mean time to detect and resolve DDoS attacks by more than 75%.** Mean time to detect (MTTD) a DDoS attack dropped from 2 hours to 5 minutes, and CenturyLink sends an alert within 1 minute of a DDoS attack. Mean time to resolve (MTTR) a DDoS attack also dropped from 20 minutes to 5 minutes. CenturyLink automated and managed much of the DDoS mitigation, freeing network security teams to work on other activities.
- **Decommissioned legacy DDoS protection product: $0.1 million benefit.** The companies decommissioned their legacy DDoS protection products after installing CenturyLink's network-based DDoS Mitigation Service.



FORRESTER®

**ROI**
**222%**

**Benefits PV**
**$1.6 million**

**NPV**
**$1.1 million**

**Payback**
**<6 months**

**Unquantified benefits.** The interviewed organizations experienced the following benefits, which are not quantified for this study:

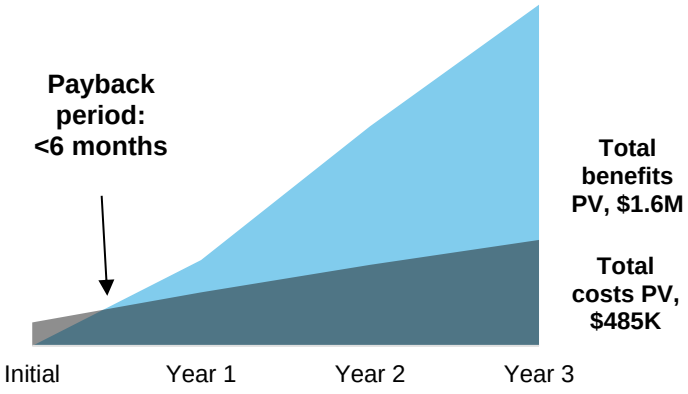
- **Reduced DDoS threat potential.** In addition to reducing application downtime due to DDoS attacks, CenturyLink's network-based DDoS Mitigation Service stopped threats before they reached the customer by routing traffic through the CenturyLink scrubbing centers and removing malicious traffic. After implementing CenturyLink's network-based DDoS Mitigation Service, suspicious activity decreased 20%, and attempted intrusions decreased by 25% on average.
- **Avoided additional costs associated with DDoS attacks.** In addition to losing revenue and time to resolve a DDoS attack prior to using CenturyLink, the organizations also paid additional costs for legal fees, public relations, end customer support services, end customer credits, and regulatory compliance. These costs were often many multiples of the actual lost revenue.
- **Protected brand reputation and enhance digital customer experience (CX).** The companies safeguarded their brands and reputations with better protection against DDoS attacks. Their digital customers had better experiences with reduced digital asset outages and downtime.

**Costs.** The interviewed organizations experienced the following risk-adjusted PV costs over three-years:

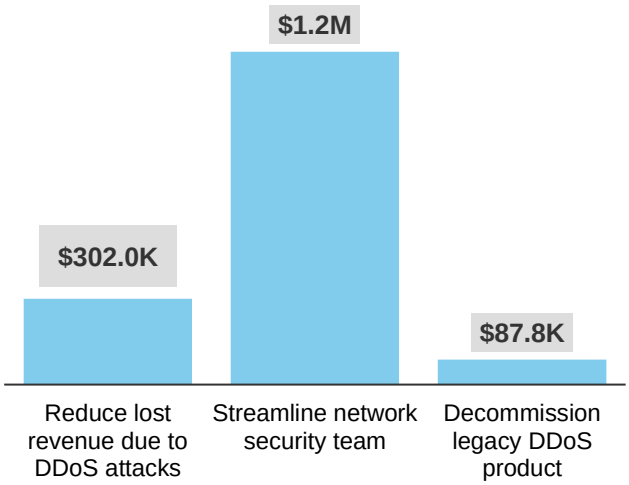
- **CenturyLink's network-based DDoS Mitigation Service: $0.2 million cost.** The CenturyLink network-based DDoS Mitigation Service cost is $8,000 per month for one gigabyte per second of traffic ingestion capacity.
- **Internal network security team to research and install DDoS mitigation: $0.1 million cost.** Internal network security teams spent six weeks to research and select CenturyLink's network-based DDoS Mitigation Service. Network security teams spent three weeks working with CenturyLink to install the service.
- **Internal network security team dedicated to DDoS mitigation: $0.1 million cost.** Network security teams logged into the CenturyLink portal each shift to check on suspicious activity and monitor any network vulnerabilities.

Forrester's interviews with five existing customers and subsequent financial analysis found that a representative organization would experience benefits of $1,560,408 over three years versus costs of $484,550, adding up to a net present value (NPV) of $1,075,858 and an ROI of 222%.

**Financial Summary**




**Benefits (Three-Year)**






FORRESTER®

## TEI Framework And Methodology

From the information provided in the interviews, Forrester has constructed a Total Economic Impact™ (TEI) framework for those organizations considering implementing CenturyLink's network-based DDoS Mitigation Service.

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 CenturyLink's network-based DDoS Mitigation Service can have on an organization:

The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

**DUE DILIGENCE**
Interviewed CenturyLink stakeholders and Forrester analysts to gather data relative to DDoS Mitigation Service.

**CUSTOMER INTERVIEWS**
Interviewed five organizations using network-based DDoS Mitigation Service to obtain data with respect to costs, benefits, and risks.

**COMPOSITE ORGANIZATION**
Designed a composite organization based on characteristics of the interviewed 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 interviewed organizations.

**CASE STUDY**
Employed four fundamental elements of TEI in modeling CenturyLink network-based DDoS Mitigation Service's impact: benefits, costs, flexibility, and risks. Given the increasing sophistication that enterprises have regarding ROI analyses related to IT investments, Forrester's TEI methodology serves to provide a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by CenturyLink 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 report to determine the appropriateness of an investment in CenturyLink network-based DDoS Mitigation Service.

CenturyLink 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.

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

# The DDoS Mitigation Service Customer Journey

**BEFORE AND AFTER THE DDOS MITIGATION SERVICE INVESTMENT**

## Interviewed Organizations

For this study, Forrester conducted five interviews with CenturyLink DDoS Mitigation Service customers. Interviewed customers include the following:

- A US retailer with $17 billion in annual revenue, 130,000 employees, and more than 20 eCommerce websites. CenturyLink's Always-On DDoS Mitigation Service protects five to 10 gigabytes of daily traffic.
- A US software-as-a-service (SaaS) company with $4 billion in annual revenue and 17,000 employees. CenturyLink's On-Demand DDoS Mitigation Service protects 10 gigabytes of daily traffic, as necessary.
- A US software company with $11 billion in annual revenue, 23,000 employees, and a B2C eCommerce website. CenturyLink's Always-On DDoS Mitigation Service protects one gigabyte of daily traffic.
- A US financial services company with $18 billion in annual revenue and 50,000 employees offering online banking and investing services. CenturyLink's Always-On DDoS Mitigation Service protects one gigabyte of daily traffic.
- A US-headquartered multinational technology company with $52 billion in annual revenue and 75,000 employees. CenturyLink's Always-On DDoS Mitigation Service protects one gigabyte of daily traffic.

## Key Challenges

Prior to their investments in the CenturyLink network-based DDoS Mitigation Service, the interviewed companies faced the following challenges:

- **DDoS attacks brought down mission-critical applications.** The prior legacy DDoS mitigation product did not provide adequate support against DDoS attacks. These attacks brought down mission-critical applications including eCommerce, online banking, and SaaS product offerings. Severe DDoS attacks could bring down websites, commerce platforms, and other digital assets for several hours, which resulted in significant revenue loss. The DDoS attacks also impacted internal applications such as corporate intranets.
- **The network security teams had limited visibility into DDoS attacks** It was challenging for network security teams to identify and understand when a DDoS attack was happening. Although teams were usually able to identify most kinds of attacks quickly, it could take up to several hours to identify a DDoS attack. It was time-consuming for network security teams to resolve a DDoS attack. While legacy DDoS mitigation vendors provided some support, there was a lot of back and forth.

> "I had to make the switch because our prior DDoS protection solution failed us. CenturyLink DDoS Mitigation is better because of its scrubbing centers. [CenturyLink] has different regional scrubbing centers with significant attack congestion capacity, and they also have application layer attack mitigation capabilities."
>
> *Director of network security, software*



FORRESTER®

- **Company brand reputation could be compromised.** DDoS attacks could potentially expose the companies to extortion requests and breaches of sensitive customer data. Even if a DDoS attack did not breach customer data, it could generate bad publicity and imply weak overall security controls.

## Key Results

The interviews revealed that key results from CenturyLink's network-based DDoS Mitigation Service investment included:

- **CenturyLink reduced successful DDoS attacks.** With CenturyLink's Always-On, network-based DDoS Mitigation Service, the interviewed companies experienced virtually no downtime or outages due to DDoS attacks. CenturyLink's network-based DDoS Service reduced website and application downtime and minimized lost revenue and costs associated with DDoS attacks.
- **CenturyLink identified and remediated DDoS attacks more quickly**. With CenturyLink, the interviewed companies automated much of their DDoS mitigation processes. They chose how to set up alerts from CenturyLink about potential security issues and reduced alert time to 1 minute or less on average.
- **The organizations streamlined network security teams.** The interviewed organizations required fewer internal resources for DDoS attack identification and remediation after deploying the CenturyLink DDoS Mitigation Service. They streamlined their network security teams' DDoS mitigation activities and freed up time for other activities.
- **CenturyLink's DDoS portal provided real-time metrics**. Network security teams had easy access to the CenturyLink DDoS portal, which provided metrics on network security.
- **The companies protected their brand reputations and sensitive customer data.** The impact of a DDoS attack can go beyond just lost revenue and remediation costs. It can also impact market and customer perceptions of a company's overall security and strength. By mitigating DDoS attacks, the organizations reduced their exposure to negative press and sentiment.

> "CenturyLink has helped us mitigate risk in terms of attacks. We caught attacks that would have cost us in the past. It helps us mitigate financial, legal, and reputational risks. It helped us streamline how we mitigate these attacks and reduce some of our internal labor cost."
>
> *Director of network security, retail*

## Composite Organization

Based on the interviews, Forrester constructed a TEI framework, a composite organization, and an associated ROI analysis that illustrates the areas financially affected. The composite organization is representative of the five companies that Forrester interviewed, and is used to present the aggregate financial analysis in the next section. The composite organization that Forrester synthesized from the customer interviews has the following characteristics:

**Description of composite.** The organization is a global $10 billion enterprise with 35,000 employees. It generates 30% of its revenue from online digital assets.

**Deployment characteristics.** The organization operates a global network with five gigabytes of daily traffic and it has a network security team of 250 security professionals. The organization uses CenturyLink's network-based DDoS Mitigation Service to protect mission-critical assets including customer-facing websites, corporate intranet, and internal applications. It uses the Always-On CenturyLink DDoS Mitigation Service, so its network traffic is continually routed through CenturyLink's global scrubbers. The CenturyLink DDoS Mitigation Service replaced a competing DDoS protection product.

**Key assumptions**

$10 billion enterprise

Digital assets account for 30% of revenue

Uses the Always-On DDoS Mitigation Service

# 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 | Minimize lost revenue due to DDoS attacks | $121,440 | $121,440 | $121,440 | $364,320 | $302,003 |
| Btr | Streamline network security team | $288,000 | $576,000 | $576,000 | $1,440,000 | $1,170,609 |
| Ctr | Decommission legacy DDoS product | $21,600 | $43,200 | $43,200 | $108,000 | $87,796 |
| | Total benefits (risk-adjusted) | $431,040 | $740,640 | $740,640 | $1,912,320 | $1,560,408 |

The table above shows the total of all benefits across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total benefits to be a PV of more than $1.6 million.

### Minimize Lost Revenue Due To DDoS Attacks

CenturyLink's Always-On, network-based DDoS Mitigation Service helps the composite organization avoid downtime due to DDoS attacks. With CenturyLink, the company keep its customer-facing applications such as eCommerce, online banking, and SaaS offerings up and running, generating revenue, and enhancing customer experience.

- Before using CenturyLink's network-based DDoS Mitigation Service, DDoS attacks brought down key revenue-generating and customer-facing applications. The average downtime was 2 hours per year, but CenturyLink's network-based DDoS Mitigation Service reduced downtime to 5 minutes per year or less.
- The company generates $12,000 of revenue per minute from its customer-facing websites.
- Forrester assumes an 11% operating margin, the historic corporate average.

The reduced lost revenue benefits will vary with:

- Frequency and severity of DDoS attacks.
- Organization size and industry, including percentage of revenue generated online or via other channels vulnerable to DDoS attacks.
- Operating margin.

To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year risk-adjusted total PV of $302,003.

Impact risk is the risk that the business or technology needs of the organization may not be met by the investment, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for benefit estimates.

| Minimize Lost Revenue Due To DDoS Attacks: Calculation Table | | | | | |
|---|---|---|---|---|---|
| **Ref.** | **Metric** | **Calculation** | **Year 1** | **Year 2** | **Year 3** |
| A1 | Website and application downtime before CenturyLink DDoS (minutes per year) | | 120 | 120 | 120 |
| A2 | Website and application downtime with CenturyLink DDoS (minutes per year) | | 5 | 5 | 5 |
| A3 | Lost revenue per minute of downtime | | $12,000 | $12,000 | $12,000 |
| A4 | Operating margin (%) | | 11% | 11% | 11% |
| At | Minimize lost revenue due to DDoS attacks | (A1-A2)*A3*A4 | $151,800 | $151,800 | $151,800 |
| | Risk adjustment | ↓20% | | | |
| Atr | Reduce lost revenue due to DDoS attacks (risk-adjusted) | | $121,440 | $121,440 | $121,440 |

## Streamline Network Security Team

With CenturyLink's always-on, network-based DDOS Mitigation Service, all network traffic is routed through CenturyLink scrubbers around the globe. CenturyLink takes responsibility for identifying and mitigating DDoS attacks, and it alerts the composite organization's internal network security team to DDoS attacks. The internal team now spends less time monitoring potential DDoS attacks and analyzing whether or not network issues are due to a DDoS attack. In the case of a DDoS attack, CenturyLink quickly takes responsibility for attack mitigation.

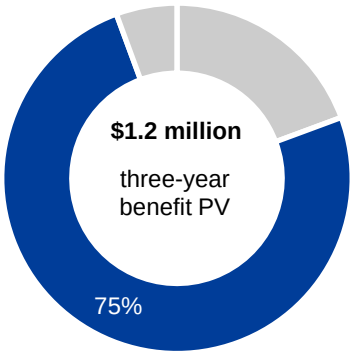
For the composite organization, Forrester assumes that CenturyLink's network-based DDoS Mitigation Service:

- Reduces the MTTD a DDoS attack from 2 hours to 5 minutes.
- Alerts to DDoS attacks within 1 minute.
- Reduces the MTTR a DDoS attack from 20 minutes to 5 minutes.
- Network security team time is freed up for other value-added tasks. The time savings ramp as the legacy DDoS product is decommissioned in Year 1.
- The average fully loaded network security employee salary is $160,000.

The streamline network security team benefit will vary with:

- The complexity of the network.
- Likelihood of DDoS attacks. DDoS attacks may target high-profile companies more often.[2]
- The network security team size, roles, and average fully loaded compensation.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $1,170,609.




Streamline network security team: 75% of total benefits



FORRESTER®

| Streamline Network Security Team: Calculation Table | | | | | |
|---|---|---|---|---|---|
| **Ref.** | **Metric** | **Calculation** | **Year 1** | **Year 2** | **Year 3** |
| B1 | Reduction in network security team (FTEs) | | 2 | 4 | 4 |
| B2 | Network security team average annual salary, fully loaded | | $160,000 | $160,000 | $160,000 |
| Bt | Streamline network security team | B1*B2 | $320,000 | $640,000 | $640,000 |
| | Risk adjustment | ↓10% | | | |
| Btr | Streamline network security team (risk-adjusted) | | $288,000 | $576,000 | $576,000 |

## Decommission Legacy DDoS Product

After installing CenturyLink's Always-On, network-based DDoS Mitigation Service, the composite organization decommissions its legacy DDoS protection product.

- The company runs both DDoS mitigation systems for six months and then decommissions the prior legacy DDoS mitigation product.
- The organization saves $4,000 per month by decommissioning the legacy product.

The benefit from decommissioning the legacy DDoS product will vary based on:

- Type and cost of the legacy DDoS protection product.
- Speed of legacy product decommissioning.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $87,796.

| Decommission Legacy DDoS Product: Calculation Table | | | | | |
|---|---|---|---|---|---|
| **Ref.** | **Metric** | **Calculation** | **Year 1** | **Year 2** | **Year 3** |
| C1 | Legacy DDoS product cost (per month) | | $4,000 | $4,000 | $4,000 |
| C2 | Phased decommissioning (%) | | 50% | 100% | 100% |
| Ct | Decommission legacy DDoS product | C1*C2*12 months | $24,000 | $48,000 | $48,000 |
| | Risk adjustment | ↓10% | | | |
| Ctr | Decommission legacy DDoS product (risk-adjusted) | | $21,600 | $43,200 | $43,200 |

## Unquantified Benefits

The interviewed organizations experienced the following benefits, which are not quantified for this study:

- **Reduced DDoS threat potential.** In addition to reducing application downtime due to DDoS attacks, CenturyLink's network-based DDoS Mitigation Service stopped attacks before they reached the customer by routing traffic through CenturyLink scrubbing centers and removing malicious traffic. With CenturyLink, suspicious activity decreased 20% and attempted intrusions decreased by 25% on average.
- **Avoided additional costs associated with DDoS attacks.** In addition to losing revenue and time to resolve a DDoS attack prior to using CenturyLink, there were additional costs including legal fees and regulatory compliance costs. These costs were often many multiples of the actual lost revenue.
- **Protected brand reputation and enhanced digital CX.** The companies' brand and reputation were kept safe with better protection against DDoS attacks. Their digital customers had better experiences with reduced digital asset outages and downtime.

## Flexibility

The value of flexibility is clearly unique to each customer, and the measure of its value varies from organization to organization. There are multiple scenarios in which a customer might choose to implement CenturyLink's network-based DDoS Mitigation Service and later realize additional uses and business opportunities, including:

- **Support new initiatives and shift to digital.** Digital assets are increasingly important in the shift to digital transformation. CenturyLink's network-based DDoS Mitigation Service helps protect those assets and new digital product offerings that are under development for future deployment.

Flexibility would also be quantified when evaluated as part of a specific project.

Flexibility, as defined by TEI, represents an investment in additional capacity or capability that could be turned into business benefit for a future additional investment. This provides an organization with the "right" or the ability to engage in future initiatives but not the obligation to do so.

# 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 |
|---|---|---|---|---|---|---|---|
| Dtr | CenturyLink's Always-On, network-based DDoS Mitigation Service cost | $0 | $105,600 | $105,600 | $105,600 | $316,800 | $262,612 |
| Etr | Internal network security staff to research and implement the CenturyLink DDoS service | $106,615 | $0 | $0 | $0 | $106,615 | $106,615 |
| Ftr | Internal network security staff dedicated to DDoS mitigation | $0 | $46,373 | $46,373 | $46,373 | $139,120 | $115,323 |
| | Total costs (risk-adjusted) | $106,615 | $151,973 | $151,973 | $151,973 | $562,535 | $484,550 |

The table above shows the total of all costs across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total costs to be a PV of more than $0.48 million.

### CenturyLink's Always-On, Network-Based DDoS Mitigation Service Cost

The composite organization chooses CenturyLink's Always-On, network-based DDoS Mitigation Service. With this service, CenturyLink routes all of the organization's network traffic through CenturyLink scrubbers.

- The organization pays $8,000 per month for CenturyLink's Always-On, network-based DDoS Mitigation Service.
- Pricing is based on one gigabyte per second of clean traffic return capacity.

The cost will vary based on:

- Volume of clean traffic routed through the CenturyLink scrubbers.
- Choice of Always-On vs. On-Demand DDoS mitigation service.
- Organization specific pricing.

To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year risk-adjusted total PV of $262,612.

Implementation risk is the risk that a proposed investment may deviate from the original or expected requirements, resulting in higher costs than anticipated. The greater the uncertainty, the wider the potential range of outcomes for cost estimates.

| CenturyLink's Always-On, Network-Based DDoS Mitigation Service Cost: Calculation Table | | | | | | |
|---|---|---|---|---|---|---|
| **Ref.** | **Metric** | **Calculation** | **Initial** | **Year 1** | **Year 2** | **Year 3** |
| D1 | CenturyLink's Always-On, network-based DDoS Mitigation Service cost (per month) | | | $8,000 | $8,000 | $8,000 |
| D2 | Speed (gigabits per second) | | | 1 | 1 | 1 |
| Dt | CenturyLink's Always-On, network-based DDoS Mitigation Service cost | D1*12 months | $0 | $96,000 | $96,000 | $96,000 |
| | Risk adjustment | ↑10% | □ | | | |
| Dtr | CenturyLink's Always-On, network-based DDoS Mitigation Service cost (risk-adjusted) | | $0 | $105,600 | $105,600 | $105,600 |

## Internal Network Security Staff To Research And Implement The CenturyLink DDoS Service

The composite organization researched alternative DDoS solutions before choosing CenturyLink. Once it makes the decision, the organization assembles an internal team to work with CenturyLink to get the DDoS mitigation service up and running.

- The organization spends six weeks researching DDoS mitigation solutions, and two network security FTEs support the process.
- CenturyLink works with the organization to install the DDoS mitigation service. Installation takes three weeks, and an internal team of seven network security FTEs supports the installation.
- The average fully loaded network security employee salary is $160,000.

The cost will vary based on:

- DDoS attacks in process. If an organization is under attack, CenturyLink can work with the company to install the network-based DDoS Mitigation Service very quickly.
- The size and complexity of the organization's network.
- The skillset of the internal network security team.

To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year risk-adjusted total PV of $106,615.

**Nine weeks**
to research and install

| Internal Network Security Staff To Research And Implement The CenturyLink DDoS Service: Calculation Table | | | | | | |
|---|---|---|---|---|---|---|
| **Ref.** | **Metric** | **Calculation** | **Initial** | **Year 1** | **Year 2** | **Year 3** |
| E1 | Time to research the best DDoS solution (weeks) | | 6 | | | |
| E2 | Network security team dedicated to research (FTEs) | | 2 | | | |
| E3 | Time to install the CenturyLink DDoS service (weeks) | | 3 | | | |
| E4 | Network security team dedicated to installing the CenturyLink DDoS service (FTEs) | | 7 | | | |
| E5 | Network security team average annual salary fully loaded | | $160,000 | | | |
| Et | Internal network security staff to research and implement the CenturyLink DDoS service | (E1*E2+E3*E4)*E5/52 weeks | $101,538 | $0 | $0 | $0 |
| | Risk adjustment | ↑5% | □ | | | |
| Etr | Internal network security staff to research and implement the CenturyLink DDoS service (risk-adjusted) | | $106,615 | $0 | $0 | $0 |

## Internal Network Security Staff Dedicated To DDoS Mitigation

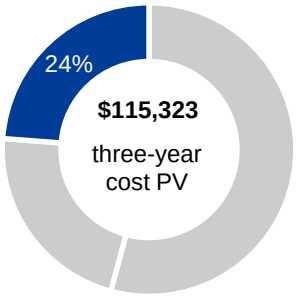
The composite organization's network security team uses CenturyLink's cloud-based DDoS portal and data to view attack activity and mitigations. CenturyLink takes responsibility to identify threats, send alerts, and mitigate DDoS attacks. The internal network security team now spends a relatively small amount of time monitoring DDoS activity.

- One network security team member logs into the CenturyLink DDoS portal each shift to check on activity. The network security team member spends 30 minutes reviewing the data via the CenturyLink DDoS portal. Each shift is 8 hours, and there are three shifts per day.
- The average fully loaded network security employee salary is $160,000.

The cost will vary based on:

- Severity of DDoS attacks. A severe DDoS attack may require the internal team to spend more time in coordination with CenturyLink on attack mitigation and resolution.

To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year risk-adjusted total PV of $115,323.




Internal network security staff dedicated to DDoS mitigation: 24% of total costs



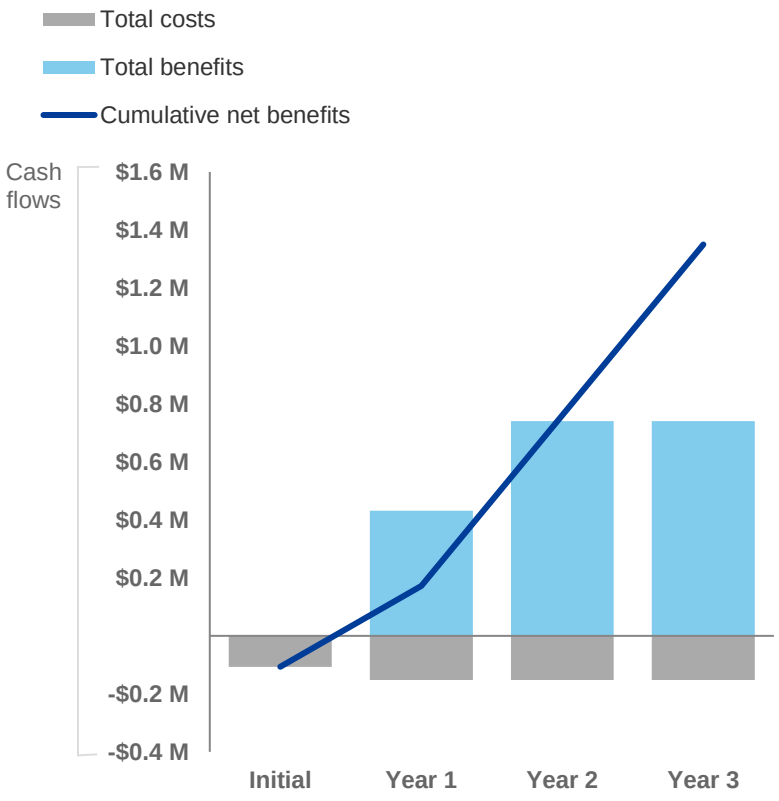
FORRESTER®

| Internal Network Security Staff Dedicated To DDoS Mitigation: Calculation Table | | | | | | |
|---|---|---|---|---|---|---|
| **Ref.** | **Metric** | **Calculation** | **Initial** | **Year 1** | **Year 2** | **Year 3** |
| F1 | Hours per day to support DDoS mitigation | | | 1.5 | 1.5 | 1.5 |
| F2 | Network security team average annual salary, fully loaded | | | $160,000 | $160,000 | $160,000 |
| F3 | Network security team average salary, fully loaded (per hour) | F2/2,080 hours (rounded) | | $77 | $77 | $77 |
| Ft | Internal network security staff dedicated to DDoS mitigation | F1*F3*365 days | $0 | $42,158 | $42,158 | $42,158 |
| | Risk adjustment | ↑10% | | | | |
| Ftr | Internal network security staff dedicated to DDoS mitigation (risk-adjusted) | | $0 | $46,373 | $46,373 | $46,373 |

# 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 | ($106,615) | ($151,973) | ($151,973) | ($151,973) | ($562,535) | ($484,550) |
| Total benefits | $0 | $431,040 | $740,640 | $740,640 | $1,912,320 | $1,560,408 |
| Net benefits | ($106,615) | $279,067 | $588,667 | $588,667 | $1,349,785 | $1,075,858 |
| ROI | | | | | | 222% |
| Payback period (months) | | | | | | <6 |



FORRESTER®

# CenturyLink Network-Based DDoS Mitigation Service: Overview

The following information is provided by CenturyLink. Forrester has not validated any claims and does not endorse CenturyLink or its offerings.

## Defense In-Depth DDoS Mitigation

With years of experience and expertise mitigating volumetric and mixed-application layer attacks, CenturyLink owns DDoS mitigation. Did you know we have one of the largest global internet backbones and DDoS attack detection and mitigation deployments in the industry?

Because of CenturyLink's highly distributed network edge and deep peering, bandwidth-intensive volumetric DDoS traffic can be absorbed by CenturyLink's ~85+ Tbps of global backbone FlowSpec capacity and/or dropped at the network edge and directed to scrubbing centers only when needed, improving scale and performance. By shifting the attack detection and the first line of defense upstream, the CenturyLink network can block malicious activity before it impacts customer environments or consumes resources connecting to that environment.

As a second line of defense, CenturyLink has deployed a multi-tiered global-scrubbing infrastructure to support DDoS attack mitigation within the network. CenturyLink's three-tier scrubbing architecture is designed to minimize network latency and the impact of multiple large-scale attacks operating at the same time, whether directed at an organization's web-facing sites and applications or another CenturyLink customer being served within our local and regional centers. Very large attacks are automatically and intelligently routed to super scrubbing centers when thresholds are exceeded, thereby reducing the potential of collateral damage when other customers on the same mitigation platform experience significant volumetric attacks.

This architecture provides clear advantages for CenturyLink® DDoS customers including that any increase in latency, while under mitigation, is minimized.

**Why CenturyLink for DDoS mitigation?**

**Scalable attack mitigation capacity:** Fifteen global, intelligent scrubbing centers backed by 85 Tbps of FlowSpec mitigation capacity to detect and drop malicious traffic at our network edge.

**Carrier-agnostic protection and detection:** CenturyLink can reroute and scrub all internet connections, not just CenturyLink internet.

**Enhanced performance and reduced latency:** More than 9,000 unique AS interconnects* and 120+ Tbps of network capacity help maximize performance.

**Multilayered attack protection:** Ability to control threats through network routing, filtering, and rate limiting, providing relief from layer 3, layer 4 volumetric to layer 7 application-based attacks.

**Proven attack traffic visibility:** CenturyLink's global IP, CDN, and DNS networks, combined with Black Lotus Labs threat intelligence provide CenturyLink with extensive visibility into attack traffic and advancing threats.

As a recognized leader in global networking and security services, CenturyLink is focused on simplifying the security experience to empower enterprise defenders. Let us help you maintain application availability and infrastructure accessibility through comprehensive, always-on and on-demand DDoS mitigation solutions.

*Telegeography, Global Internet Geography Executive Summary, 2018

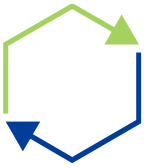
# Appendix A: Total Economic Impact

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

## Total Economic Impact Approach

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

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



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

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

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

**Present value (PV)**

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

**Net present value (NPV)**

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

**Return on investment (ROI)**

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

**Discount rate**

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

**Payback period**

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

# Appendix B: Endnotes

[1] Source: Forrester's Business Technographics Global Security Survey, 2019.
[2] For example, DDoS attacks have targeted retailers during the busiest shopping season of the year. Source: "Retailers, Prepare Wisely: DDoS Remains a Holiday Threat," Forrester Research, Inc., November 26, 2019.