A Forrester Total Economic Impact™
Study Commissioned By Snyk
November 2019

The Total Economic Impact™ Of Snyk

Cost Savings And Business Benefits Enabled By Snyk

FORRESTER®

Table Of Contents

Project Director:
Corey McNair

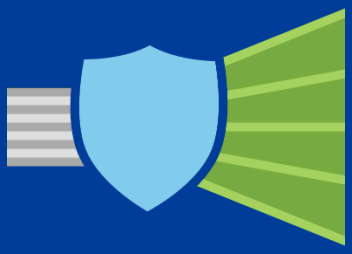
ABOUT FORRESTER CONSULTING

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®

Snyk's Benefits And Costs

Reduced risk of a cyberbreach:
$1,599,228



Savings from reduced time spent investigating and remediating vulnerabilities:
$350,784

Snyk licensing costs:
$179,053

Executive Summary

In a recent Forrester survey, 31% of global security decision makers identified the changing and evolving nature of security threats as one of their leading challenges.[1] To keep up with this challenge, businesses often seek solutions that are both agile and comprehensive for remediating security threats as they appear. Otherwise, businesses face the loss of sensitive information, damage to their brand reputation, and nearly $4 million in average total costs.[2]

Snyk, a developer-first security company, helps developers and security teams to automatically find and fix vulnerabilities in open source libraries and container images. The platform displays where third-party vulnerabilities exist and integrates with a variety of third-party developer tools to notify and remediate the risk. In addition, Snyk provides a proprietary database of vulnerabilities that is separate from those provided by the National Vulnerability Database (NVD).

Snyk commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Snyk. The purpose of this study is to provide readers with a framework to evaluate the potential positive financial impact of using Snyk across their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed a cloud security manager at one technology vendor with two years of experience using Snyk.

Prior to using Snyk, the customer did not have a security solution in place, and its security team conducted manual vulnerability reviews on its digital infrastructure. According to the cloud security manager, the Apache Struts bug that triggered the 2017 cyberbreach of Equifax, which exposed the personal information of 143 million US consumers, was a wakeup call for the organization.[3]

The interviewee explained: "That incident helped to give us the justification we needed to push forward internally to adopt a security intelligence solution. The Equifax breach was a remote code execution, and the bugs that can potentially attack us are remote code as well, which spurred urgency in finding a solution."

The tech vendor's primary criteria for selecting a security solution was to find one that would automate the delivery of intelligence on high security threats, to enable rapid remediation, and to easily integrate into existing developer tools and workflows. Snyk was a clear choice, especially since some developers were already using a freemium version of the solution.

Key Findings

Quantified benefits. The interviewed organization experiences the following risk-adjusted present value (PV) quantified benefits:

- **Automation of security analysis and thorough reporting on threats has cut the risk of a breach in half.** Previously, the organization's security team spent hours and sometimes days manually analyzing its infrastructure for vulnerabilities, which often resulted in failure to see issues or threat reports missing key details. Now, the Snyk solution is thorough in its ongoing monitoring of threats and comprehensive in its reporting, reducing the risk for a potential breach.

FORRESTER®

Snyk ROI
340%

Benefits PV
$1.98 million

NPV
$1.53 million

Snyk Payback
<3 months

› **Security researchers avoid spending on average 45 minutes every time they filed a ticket on a vulnerability.** Since adopting Snyk, security researchers no longer have to manually write out a ticket with details of a discovered security threat or spend time cross-comparing the ticket with other filed reports to validate the threat. The security intelligence solution automates the delivery into existing ticketing and reporting tools, removing hundreds of hours of tedious work.

› **Security engineers avoid on average 8 hours of labor when investigating and remediating a vulnerability.** Before Snyk, when security developers would receive a ticket for a vulnerability, they would often spend time manually digging up additional details to determine the best approach to remediate it. Today, Snyk provides an abundance of information including the recommended fix or patch for the identified vulnerability, which reduces the need for additional research and increases the velocity of remediation.

Unquantified benefits. The interviewed organization also experiences the following benefits, which are not quantified for this study:

› **Snyk's ability to integrate with a wide variety of developer tools and existing workflows.** A key reason the interviewed organization adopted Snyk is because the solution offers broader and easier flexibility for integration with relevant technologies than other evaluated solutions. Snyk's ability to integrate with other platforms made for seamless deployment, to the point where some engineers had no disruption at all to their day-to-day processes.

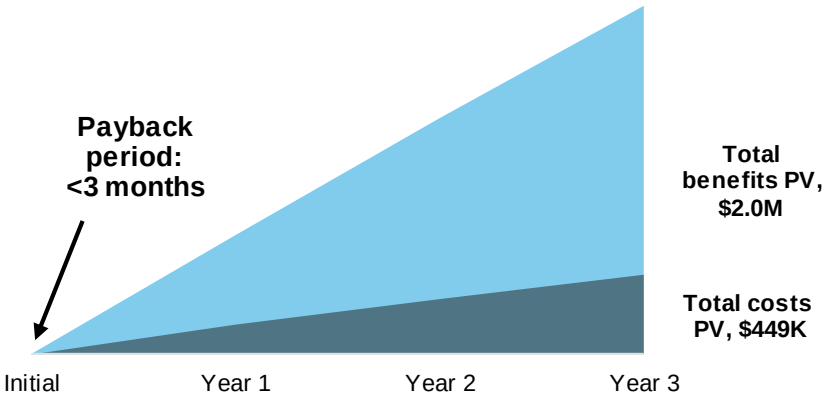
› **Improved confidence in security information.** The interviewed cloud security manager reported that Snyk's proprietary vulnerability database has reassured the team that more vulnerabilities are being caught, and much earlier, than those listed in the NVD, reducing the need to search for unidentified threats.

Costs. The interviewed organization has experienced the following risk-adjusted PV costs:

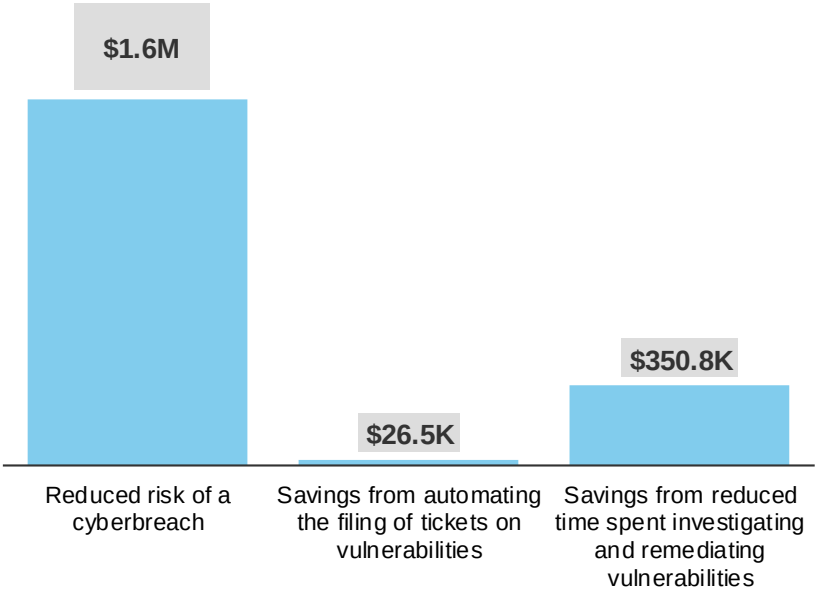
› **Implementation, licensing, and hardware costs.** The organization spent a short amount of time on deployment of Snyk and now pays for the Snyk license based on the number of developers using the solution. The company also invested in its own servers to have a proxy between Snyk and on-premises hosted repositories.

Forrester's interview with an existing customer and subsequent financial analysis found that the interviewed organization experiences benefits of $1,976,483 over three years versus costs of $449,448, adding up to a net present value (NPV) of $1,526,995 and an ROI of 340%.

Financial Summary



Benefits (Three-Year)



FORRESTER®

TEI Framework And Methodology

From the information provided in the interview, Forrester has constructed a Total Economic Impact™ (TEI) framework for those organizations considering implementing Snyk.

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 Snyk 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 Snyk stakeholders and Forrester analysts to gather data relative to Snyk.

CUSTOMER INTERVIEW
Interviewed one organization using Snyk to obtain data with respect to costs, benefits, and risks.

FINANCIAL MODEL FRAMEWORK
Constructed a financial model representative of the interview using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewed organization.

CASE STUDY
Employed four fundamental elements of TEI in modeling Snyk'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.

The Snyk Customer Journey

BEFORE AND AFTER THE SNYK INVESTMENT

Interviewed Organization

For this study, Forrester conducted an in-depth interview with a cloud security manager at a technology vendor that has used the Snyk solution for two years:

- The technology vendor is located in North America and handles millions of pieces of sensitive information from other organizations.
- Security has become a top priority for the company as the number of cyberattacks increased over its nearly decade-long existence, placing its sensitive information at risk. The tech vendor evaluated several competitors to Snyk; however, they did not provide the same level of ease of use, integration into developer tooling, automated remediation, or breadth of vulnerability database.
- There are roughly 250 security engineers that use intelligence from Snyk at the company, but only one security researcher helps to service tickets for these vulnerabilities to the engineers.
- The tech vendor has a server to host Snyk Broker, a proxy between Snyk and on-premises hosted repositories.

Key Challenges

The interviewee from the organization shared the following issues and challenges:

- **Manual analysis led to oversights in vulnerabilities and unpreparedness for threats.** Mitigating the potential for human error was a key factor for adopting Snyk. As thorough as security researchers were when reviewing their product's code for vulnerabilities or hunting for other threats, the team wasn't confident that all vulnerabilities or threats were being caught as researchers can only catch so much information. To completely avoid manual analysis, the organization needed a solution that could help find and fix open source vulnerabilities and easily integrate into its existing tech stack.
- **Lack of detailed threat reporting led to slow remediation.** Manual scanning and analysis of vulnerabilities often produced reports that did not fully equip security engineers with enough information to know how to easily remediate their vulnerable code. As a result, engineers would spend additional hours investigating threats and their solution to try to mitigate the issues. When evaluating security solutions for adoption, the interviewed cloud security manager found that vulnerability reporting was often targeted toward informing the security team and not toward reporting the right information to engineers who can help fix the problem faster.

> "We want a solution that isn't solely dedicated to our security team, since we do not fix the issues. Our engineers need something that is effective in communicating the threat and guiding them on steps for remediation."
>
> *Cloud security manager, Snyk customer*

Solution Requirements

The interviewed organization searched for a solution that could:

- Provide automated intelligence for high-level security threats to the organization.

- Work well with existing development tooling and workflows by providing integrated intelligence about transitive vulnerabilities and not solely reporting on top-level, visible issues.
- Provide dashboards and seamless notifications to project owners, reducing the number of emails and communication discussing threats.

Key Results

The interview revealed several key results from the Snyk investment:

- **The interviewed organization integrated Snyk with several internal platforms, automating open source vulnerability scanning across its systems.** The cloud security manager reported that Snyk has a clean user interface (UI) that made it easy for developers to integrate the solution with other internal applications for continuous monitoring. In addition, the interviewee reported that Snyk's support team was helpful in onboarding the solution and responsive in answering any questions.
- **The security team became more confident in the consistency of vulnerability reporting.** By creating scripts for Snyk to follow and automate the notification of vulnerabilities, the team felt they were no longer lacking the visibility that could pose a challenge to them. Whereas the team could catch major security threats when they were reported in the news, Snyk helps in identifying vulnerabilities from third-party dependencies that can be as significant as threats widely reported on, greatly helping to reduce risk for the organization.
- **Developers reduced mean time to fix vulnerabilities as a result of higher-quality reporting.** Snyk provides granularity to the development team to identify where upgrades or patching is needed down to the version level. Snyk has especially been critical for providing context and information on dependency issues that would not have been possible with manual analysis.

> "Unlike other vendors, Snyk seamlessly fits in with our network. We rarely have to interact with the platform, and it independently takes care of recognizing threats for us."
>
> *Cloud security manager, Snyk customer*

> "When engineers receive tickets now, every piece of information they need is now within the ticket, and they can go straight to remediation. Next to no time is spent on additional research."
>
> *Cloud security manager, Snyk customer*

Analysis Of Benefits

QUANTIFIED BENEFIT DATA

Total Benefits

Ref.	Benefit	Year 1	Year 2	Year 3	Total	Present Value
Atr	Reduced risk of a cyberbreach	$606,000	$644,784	$686,050	$1,936,834	$1,599,228
Btr	Savings from automating the filing of tickets on vulnerabilities	$9,706	$10,677	$11,745	$32,128	$26,471
Ctr	Savings from reduced time spent investigating and remediating vulnerabilities	$128,621	$141,483	$155,631	$425,735	$350,784
	Total benefits (risk-adjusted)	$744,327	$796,944	$853,426	$2,394,697	$1,976,483

Reduced Risk Of A Cyberbreach

Before adopting Snyk, the interviewee was confident that the security team was keeping track of major security threats through news sources reporting on the latest bugs impacting businesses. Meanwhile, the team caught any other vulnerabilities during manual reviews of the infrastructure. According to the interviewee: "We all read 'Hacker News,' and we have distribution channels on that information. If there's a Metasploit exploit for a major bug, we're going to hear about it."

However, when the 2017 breach of Equifax occurred and impacted 143 million consumers, the team realized that they needed to be more agile to avoid a similar scenario, considering how much they used open source libraries in their software development process. The security team made the case internally that a single vulnerability could have significant impact on the business, including loss of customer information and negative impact to brand reputation. Since adopting Snyk, the team's concern over a cyberbreach has decreased. The cloud security manager said: "We just sleep a little bit better at night now that we have all of this information to know about open source vulnerabilities and fix issues as soon as they come up. In the past, it could have been very possible that we would miss a critical issue."

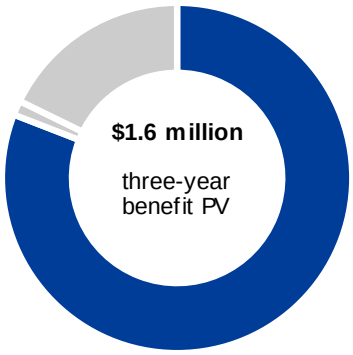
A major threat that Snyk has been helpful in addressing for the company has been those including external entity (XXE) injections and cross-site scripting. In one case, a PDF viewer on the company's site could have enabled remote code execution resulting in a significant breach. With the help of Snyk, the team was able to catch the vulnerability before it was exploited and use its intelligence to navigate patching the vulnerability.

The interviewee said the team still does some manual reviews for pieces of infrastructure that use C or C++ coding because of firmly established processes in place for analysis. However, the team plans to investigate utilizing Snyk for those products.

Modeling and assumptions:

› The average cost of a security breach for a technology company is $5,050,000 per the Ponemon Institute survey.[4]

The table above shows the total of all benefits across the areas listed below, as well as present values (PVs) discounted at 20%. Over three years, the interviewed organization expects risk-adjusted total benefits to be a PV of nearly $1.98 million.



Reduced risk of a cyberbreach: 81% of total benefits

FORRESTER®

- The cost of a data breach increases 6.4% per year, reflecting the reported 2018 average increase in data breach costs.
- Since adopting Snyk, the risk of a breach for the tech vendor's product has fallen from 30% to 15%. Snyk has helped the organization to resolve at least twice as many vulnerabilities than before in a similar one-year timeframe, driven by improved threat monitoring across key product lines. In addition, there's less lag time from when the team discovers a threat to when the developers fix it.
- This reduction factors in Forrester's Business Technographics® survey, where 51% of surveyed respondents indicated that their businesses experienced at least one breach in the past year.[5] This is weighed against the organization's prior efforts to manually search for threats, alongside various indicators from third-party research.

Variations to benefit result:

- The demographics of the organization will alter the value and likelihood of a cyberbreach, specifically company size, industry, and access to customer personal data.
- If an organization is already using a security intelligence solution, it may not be able to attribute all threats captured directly to Snyk alone as the threat notifications may come through alternative solutions.
- While Snyk provides security teams with the information necessary to find and fix vulnerabilities in open source libraries, organizations must ensure these processes are completed to fully reduce risk.

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.

To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year risk-adjusted total PV of $1,599,228.

Reduced Risk Of A Cyberbreach: Calculation Table

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
A1	Average cost of a data breach	Increasing at 6.4% per year	$5,050,000	$5,373,200	$5,717,085
A2	Risk of a data breach before Snyk	Interview	30%	30%	30%
A3	Risk of a data breach after Snyk	Interview	15%	15%	15%
At	Reduced risk of a cyberbreach	A1*(A2-A3)	$757,500	$805,980	$857,563
	Risk adjustment	↓20%			
Atr	Reduced risk of a cyberbreach (risk-adjusted)		$606,000	$644,784	$686,050

Savings From Automating The Filing Of Tickets On Vulnerabilities

Given that Snyk automates finding, fixing, and continuous monitoring of vulnerabilities, security researchers at the technology vendor no longer have to spend time on filing tickets for threats.

According to the interviewee, writing a file ticket on a discovered vulnerability took a security researcher at least 15 minutes to copy all of the necessary details. A researcher would take an additional half hour to crosscheck the vulnerability with other similar or related threats to collect

all relevant details and validate the vulnerability as a true positive threat before sending the ticket to their development team.

In some cases, when validating a threat, a security researcher would find that a ticket was already filed on the same threat. With Snyk deployed, the team no longer has to worry about collecting all of the information and cross-comparison, resulting in less wasted time and frustration for the team. The cloud security manager said, "Forty-five minutes may sound like a relatively small savings, but when you have to do this dozens of times per month, with much of the time spent on copying and pasting information, it's time-consuming and mentally taxing — especially when you run into dead ends."

Snyk's filing also helped to achieve another goal for the security team in that it reduced the number of emails being sent back and forth for additional details on a vulnerability. The solution works with internal chat systems to deliver notifications directly to engineers.

Modeling and assumptions:

- The interviewed organization created defined criteria for Snyk to exclusively report on critical vulnerabilities. As a result, Snyk reports on 500 critical vulnerabilities in Year 1 and increases to 605 by Year 3 at a rate of 10% annually, based on new products generating more potential vulnerabilities and an increasing number of cyberthreats.
- A security researcher avoids spending 45 minutes per vulnerability filing a ticket.
- The average hourly rate for a security researcher is $46.22, with the annual salary totaling $96,132.
- The security researcher reallocates 70% of their time saved to additional high-priority, security-related activities.

Variations to benefit result:

- Snyk may identify a varying number of reported vulnerabilities depending on the criteria defined to discover the most important threats for each customer. For the interviewed technology vendor, the number of reported threats skews on the smaller side because it primarily uses Snyk to identify medium- or high-level security threats.
- Time spent on ticket filing may vary depending on the number of tickets to file. For example, if the number of tickets is much higher, it may result in less time spent on research and validation of a ticket.

To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year risk-adjusted total PV of $26,471.

Snyk helps researchers avoid **45 minutes** of labor writing tickets on *each* uncovered vulnerability.

Savings From Automating The Filing Of Tickets On Vulnerabilities: Calculation Table					
Ref.	**Metric**	**Calculation**	**Year 1**	**Year 2**	**Year 3**
B1	Number of critical vulnerabilities recorded annually	Interviews	500	550	605
B2	Savings from not manually writing and validating tickets (hours)	45 min	0.75	0.75	0.75
B3	Average hourly rate for security researcher	$96,132/2,080 hours	$46.22	$46.22	$46.22
B4	Productivity recapture		70%	70%	70%
Bt	Savings from automating the filing of tickets on vulnerabilities	(B1*B2*B3*B4)	$12,133	$13,346	$14,681
	Risk adjustment	↓20%			
Btr	Savings from automating the filing of tickets on vulnerabilities (risk-adjusted)		$9,706	$10,677	$11,745

Savings From Reduced Time Spent Investigating And Remediating Vulnerabilities

The previous method for filing tickets led to further inefficiencies when developers set forth on remediation. Tickets were only as detailed as the security researchers' visibility into their system's infrastructure. The manual nature of filing tickets also led to occasions of human error where the wrong link or information was copied into the ticket.

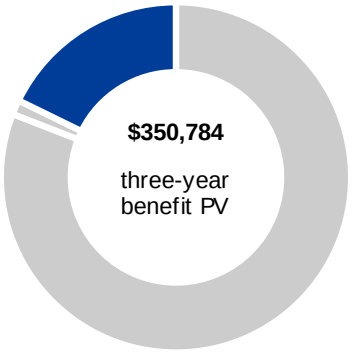
These factors often led to additional research time for the development team as they backtracked to locate the necessary information internally or on the web to remediate vulnerabilities. The cloud security manager shared: "Snyk helps the developer to do a lot less searching now; everything they need to know is on the ticket. We can now tell them, 'There's a vulnerability in this library; it was introduced through this library and here's all the background you need.'"

The interviewee attributed the depth of knowledge on threats to Snyk's internal database on vulnerabilities, which alerts the team to threats they would have otherwise missed if they only followed the National Vulnerability Database. Snyk gives developers the most relevant information to accelerate the time to fix vulnerabilities.

While some reported threats could be remediated quickly (in a couple hours), more severe threats can require multiple days of work toward remediation. Since the interviewed technology vendor uses Snyk to target critical threats, the time savings have been significant.

Modeling and assumptions:

- The number of critical vulnerabilities increases from 500 in Year 1 to 605 by Year 3.
- The reduced amount of time spent investigating and remediating each critical threat totals 8 hours or one workday. The time savings primarily reflect Snyk's help in gathering the basis of information for developers to get a head start on remediation.
- The average hourly rate for a developer is $57.42, with the annual salary totaling $119,445.



Savings from reduced time spent investigating and remediating vulnerabilities: 18% of total benefits

- As a result of the increased velocity to fix the vulnerabilities, the developer reallocates 70% of their time saved to additional work-related activities.

Variations to benefit result:

- The reduced amount of time spent investigating and remediating threats will vary based on current security analysis processes already in place and if they are saving time for the organization.
- Since the reported threats for the interviewed organization skewed toward more serious vulnerabilities, the time for investigation and remediation typically was longer because more work was required to patch the code. Lower-level threats often take less time to resolve and can reduce the average amount of time spent on resolving the issues.

To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year risk-adjusted total PV of $350,784.

Snyk helps developers save **8 hours** of time on investigating per bug, 70% of which is reallocated toward additional work-related activities.

Savings From Reduced Time Spent Investigating And Remediating Vulnerabilities: Calculation Table

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
C1	Number of critical vulnerabilities recorded annually	Interviews	500	550	605
C2	Avoided time to investigate and remediate vulnerabilities (hours)		8	8	8
C3	Average hourly rate for developers	$119,445/2,080 hours	$57.42	$57.42	$57.42
C4	Productivity recapture		70%	70%	70%
Ct	Savings from reduced time spent investigating and remediating vulnerabilities	C1*C2*C3*C4	$160,776	$176,854	$194,539
	Risk adjustment	↓20%			
Ctr	Savings from reduced time spent investigating and remediating vulnerabilities (risk-adjusted)		$128,621	$141,483	$155,631

Unquantified Benefits

In addition to the quantified benefits above, the interviewees experienced additional benefits that were not quantified, including:

- **Snyk's ability to integrate with the existing development tech stack.** The interviewed organization wanted to use a security intelligence platform that easily integrated with its existing DevOps pipeline and project tracking systems. As a result, Snyk seamlessly delivers alerts on vulnerabilities through a variety of different channels across development teams, drastically reducing the amount of email back-and-forth discussing details on a threat.

Snyk's flexibility for integration and its proprietary vulnerability database were key drivers of adoption for the tech vendor.

- **Improved confidence in security information.** The information provided by Snyk's internal database of vulnerabilities has helped engineers shorten time on research and remediation; it has also increased confidence among the team in trusting the information they are given. "Having access to Snyk's vulnerability database is so handy. There's a lot less friction now for fixing issues because developers aren't second guessing information being sent to them," the interviewee said.

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 Snyk and later realize additional uses and business opportunities, including:

- **Snyk's "fix" button automates remediation of threats.** Snyk offers an automated pull request "fix" button that seamlessly resolves threats. The interviewed technology vendor has not made significant use of this feature yet because it relies on Snyk to address critical threats. However, the interviewee did mention there were opportunities to use the feature when dealing with Java language in one of the organization's key products.

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

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

Total Costs

Ref.	Cost	Initial	Year 1	Year 2	Year 3	Total	Present Value
Dtr	Implementation and ongoing licensing costs	$827	$180,413	$180,413	$180,413	$542,067	$449,488
	Total costs (risk-adjusted)	$827	$180,413	$180,413	$180,413	$542,067	$449,488

Implementation And Ongoing Licensing Costs

The interviewed organization pays for Snyk based on the number of developers given access to the solution. Initial deployment costs were driven by time spent by developers to integrate the platform with other applications and to input scripts for identifying vulnerabilities. Regular review and upgrade of scripts produce recurring costs throughout the three years.

The organization incurs additional costs for servers to run Snyk Broker, a proxy between Snyk and on-premises hosted repositories. Since Snyk primarily automates its analysis, the organization does not need a full-time employee to manage the solution.

Risk:

- Depending on how many users an organization plans to grant access to use Snyk, the costs will decrease or increase accordingly.

To account for these risks, Forrester adjusted this cost upward by 20%, yielding a three-year risk-adjusted total PV of $449,488.

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 interviewed organization expects risk-adjusted total costs to be a PV of $449,488.

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.

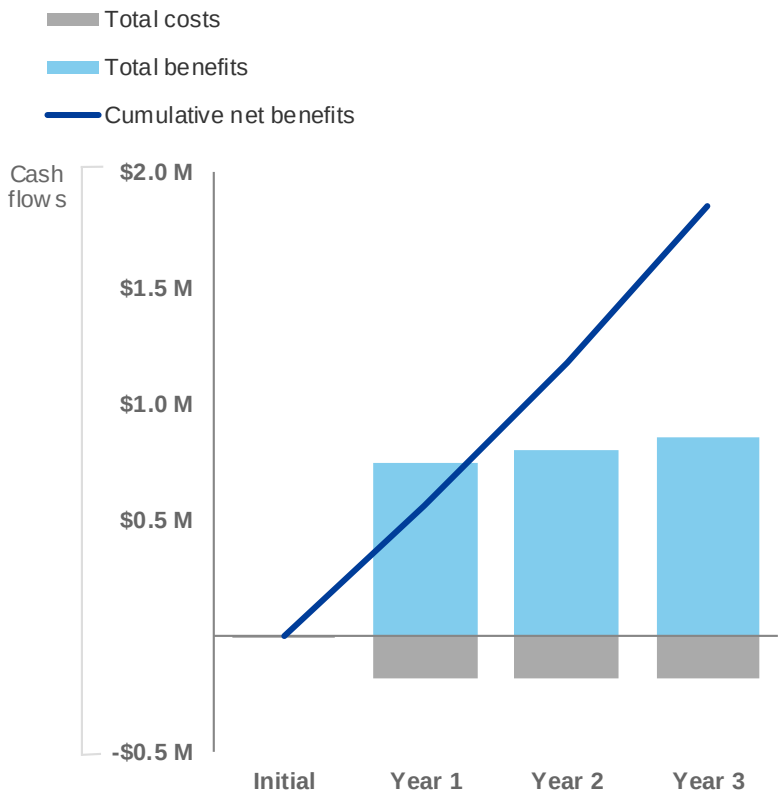
Implementation And Ongoing Licensing Costs: Calculation Table

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
D1	Time spent on integrating Snyk and building scripts (hours)		12	6	6	6
D2	Average hourly rate for security engineer		$57.42	$57.42	$57.42	$57.42
D3	Snyk license and subscription costs			$60,000	$60,000	$60,000
D4	On-premises server cost			$90,000	$90,000	$90,000
Dt	Implementation and ongoing licensing costs	Initial: D1*D2 Y1-Y3: D1*D2+D3+D4	$689	$150,345	$150,345	$150,345
	Risk adjustment	↑20%				
Dtr	Implementation and ongoing licensing costs (risk-adjusted)		$827	$180,413	$180,413	$180,413

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 interviewed 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	($827)	($180,413)	($180,413)	($180,413)	($542,067)	($449,488)
Total benefits	$0	$744,327	$796,944	$853,426	$2,394,697	$1,976,483
Net benefits	($827)	$563,914	$616,530	$673,012	$1,852,629	$1,526,995
ROI						340%
Payback period (months)						<3

FORRESTER®

Snyk: Overview

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

Snyk is a developer-first security company that helps organizations develop fast and stay secure. Snyk is the only solution that seamlessly and proactively finds and fixes vulnerabilities and license violations in open source dependencies and container images.

Snyk was built on the belief that security must be integrated into the development process and that, with the right solutions, this aspiration becomes a reality. Snyk combines developer tooling and user experience (UX) expertise with deep cybersecurity knowledge to deliver a developer-first solution companies can use every day to stay secure — without slowing down development. By using Snyk's flexible CLI, workflow integrations, and API, developers can easily add projects to be tested and quickly find vulnerabilities in their open source dependencies. With tight integration into existing source code tools (including GitHub, Bitbucket, and GitLab), Snyk enables developers to automatically test every commit to ensure the applications are secure through each checkpoint in their process.

Snyk enables users to quickly identify issues and drives action with automatically generating fix pull requests and patches. Snyk's goal is to automate vulnerability remediation so that issues are actually identified and fixed on an ongoing basis.

Snyk's dedicated security research team maintains a database of known and researched vulnerabilities, making it one of the best and most accurate databases available in the market today. By integrating this vulnerability data into the solution, Snyk alerts customers to security flaws in the code they're using and offers an automated solution to fix them. The team of Snyk expert researchers and analysts ensures the database maintains the highest level of accuracy with a low false-positive rate. All items in the database are analyzed and tested and include hand-curated content and summaries of the vulnerabilities, including code snippets where applicable.

Developers can start using Snyk for free in minutes at https://snyk.io.

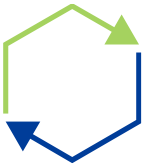
Appendix A: Total Economic Impact

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 Analytics Global Business Technographics® Security Survey, 2018.

[2] Source: "Cost of a Data Breach Report 2019," Ponemon Institute, LLC, sponsored by IBM, July 2019 (https://databreachcalculator.mybluemix.net/executive-summary).

[3] Source: "The State Of Application Security, 2018," Forrester Research, Inc., January 23, 2018.

[4] Source: "Cost of a Data Breach Report 2019," Ponemon Institute, LLC, sponsored by IBM, July 2019 (https://databreachcalculator.mybluemix.net/executive-summary).

[5] Source: Forrester Analytics Global Business Technographics® Security Survey, 2018.