FORRESTER®

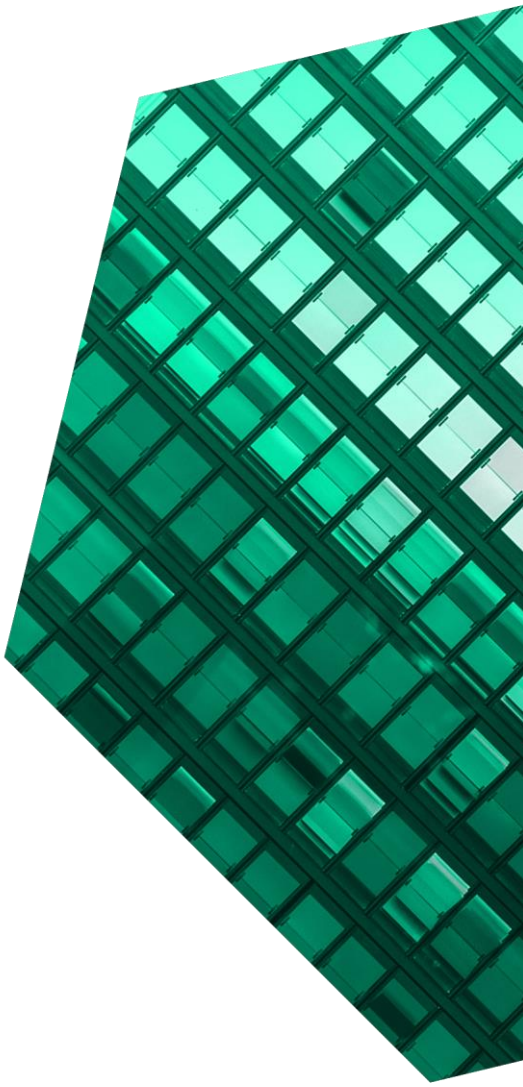
The Total Economic Impact™ Of Censys External Attack Surface Management

Cost Savings And Business Benefits Enabled By Censys External Attack Surface Management

APRIL 2023

Table Of Contents

Consulting Team: *Julia Fadzeyeva*
Claudia Heaney



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

As organizations move towards a multicloud infrastructure, attackers aim to exploit opportunities presented by unknown assets. According to Forrester Research, attack surface management tools can discover more than 30% more cloud assets that are unknown to security and IT teams.[1] Censys External Attack Surface Management equips firms with continuous attack surface discovery, cloud exposure management, risk management, and confidence with acquisitions and subsidiaries.

Censys External Attack Surface Management (EASM) is a tool that provides continuous internet asset discovery and inventory, risk detection, prioritization, and remediation; mergers and acquisitions (M&A) subsidiary risk analysis; and cloud security and governance. It equips organizations with near-real-time external attack surface visibility and comprehensive external asset data with the capability to connect organizations to public cloud infrastructure.

Censys commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Censys EASM.[2] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Censys EASM on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four representatives with experience using Censys EASM. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization that is a global, industry-agnostic organization with 15,000 employees and $4 billion in revenue.

KEY STATISTICS

Return on investment (ROI)
444%

Net present value (NPV)
$2.60M

Reduction in false positives

70%

Prior to using Censys EASM, these interviewees noted how their organizations relied on ad hoc, manual processes to understand and manage their attack surface. However, prior attempts yielded limited success, leaving them without a formal process to monitor their attack surface. These limitations led to inefficient manual effort, a lack of visibility into the attack surface, and vulnerabilities (particularly during M&A activity).

After the investment in Censys EASM, the interviewees utilized the solution as a formal process in external asset management to gain visibility into their attack surface. Key results from the investment

include increased efficiencies in discovering and monitoring assets; reduced likelihood and impact of security breaches; and improved processes in M&A due diligence.

KEY FINDINGS

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

- **Increased efficiencies in discovering and assessing assets by 30%.** With greater visibility of the attack surface, cybersecurity analysts can discover new assets and assess assets more quickly with Censys compared to the composite's previous environment, which required ad hoc, manual processes.
- **Reduced likelihood of a security breach by discovering unknown or unaccounted for assets.** Having an attack surface monitoring tool enables the composite organization to identify and investigate compromises more quickly. Censys EASM helped the organization discover 10,000 previously unknown assets, which constitutes 50% of the organization's total assets, thus reducing the likelihood of a security breach and avoiding related costs.
- **Reduction in employee productivity loss from a security breach by discovering the composite's vulnerable assets.** There is a reduction in employee productivity loss associated with downtime as the likelihood of security breaches is reduced. Censys equips the composite organization to reduce the likelihood of breach and, ultimately, the impact on employees across the entire composite organization.
- **Savings on security assessments for mergers and acquisitions of almost $283,000.** Censys enables the composite organization to eliminate special asset discovery projects during M&A due diligence phases, which took up to two months to complete before Censys.
- **Reduction in false positives by 70%.** Alerts are sent to the composite organization regarding any potential vulnerabilities in the attack surface. Censys's data accuracy reduces the number of false positives that the composite organization receives.
- **Faster remediation of security incidents by 15%.** With Censys, the composite organization remediates true security incidents faster compared to the prior environment.

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

- **Better control over shadow IT**. For interviewees, Censys helped identify and close down the assets that were created by employees and unknown (and therefore unmanaged) by the organization.
- **Outstanding collaboration.** According to the interviewees, Censys provided excellent partnership in solving issues and responding to their technical needs.
- **Suitability for cloud.** Censys's ability to connect to public cloud infrastructure with vendor-agnostic connectors provided additional value to the interviewees' organizations as the cloud presents challenges that make it difficult to navigate.
- **Peace of mind.** Censys delivered a sense of comfort by providing full visibility into the interviewees' organizations' attack surfaces, making reliable and timely information available, and offering proactive guidance on new vulnerabilities. Security professionals felt more in control and better prepared for reporting to C-level executives.
- **Growing use across the organization.** Departments beyond security became interested in obtaining access to external asset data and using Censys. The vulnerability management

team at one of the interviewees' organizations fed the Censys data into a security risk correlation tool, as it already incorporated any custom risk scoring, saving the analysts time on preparing the data and discovering zero-day vulnerabilities.

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

- **Licensing fees.** Licensing is dependent on the number of assets and is a flat fee across three years.
- **Internal implementation, integration, and training.** There are no direct fees from Censys related to implementation, integration, and training. These costs are dependent on the time needed from cybersecurity professionals at the composite organization.

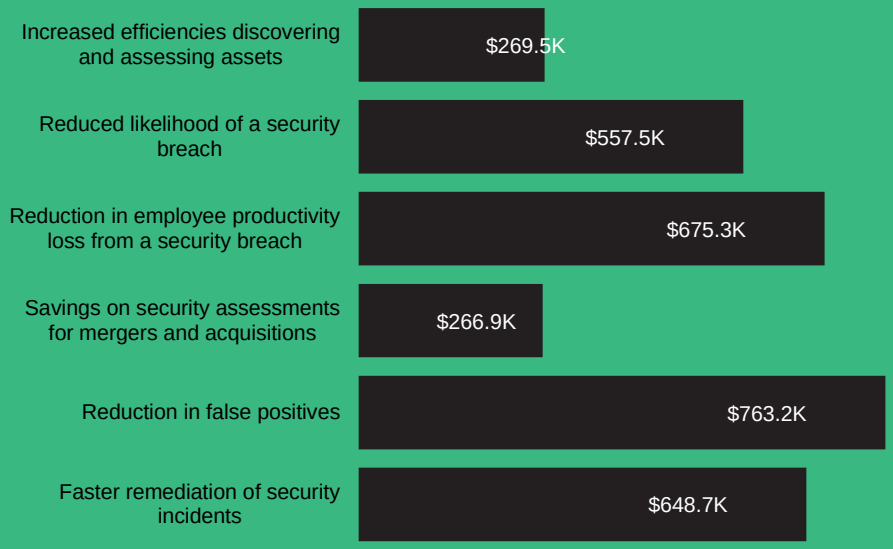
The representative interviews and financial analysis found that the composite organization experiences benefits of $3.18 million over three years versus costs of $584,000, adding up to a net present value (NPV) of $2.60 million and an ROI of 444%.

ROI
444%

BENEFITS PV
$3.18M

NPV
$2.60M

Benefits (Three-Year)



“Having the ability to see [our attack surface] and the changes in our posture … provides a unique sense of confidence. [Censys is] flexible and well-documented which makes a huge difference.”

— Director, cyber command center, technology insurance

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 Censys EASM.

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 Censys EASM can have on an organization.

DUE DILIGENCE

Interviewed Censys stakeholders and Forrester analyst to gather data relative to Censys EASM.

INTERVIEWS

Interviewed four representatives at organizations using Censys EASM 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 Censys External Attack Surface Management Customer Journey

Drivers leading to the Censys EASM investment

Interviews

Role	Industry	Region	Annual revenue and employees	Number of assets	Time with Censys EASM
Senior security engineer	Cloud communications	Global	$1.4 billion 2,000 employees	13,000	3.5 years
Technical director for security architecture and assurance	Aerospace and defense	Global	$67 billion 174,000 employees	89,500	2 years
Director, cyber command center	Technology insurance	Global	$8.5 billion 23,000 employees	50,000	16 months
Director of vulnerability management	Market research and consulting	Global	$3.3 billion 27,000 employees	Several thousand	7 to 8 months

KEY CHALLENGES

Before Censys EASM, the interviewees described ad hoc, manual processes as a solution to understanding and monitoring their organizations' attack surface. The techniques the organizations used included open-source reconnaissance, intelligence gathering, and spot research to discover and assess external assets. While technology insurance organization used another ASM tool prior to Censys, most did not have a formal program in place to manage their attack surface.

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

- **Manual processes that were point-in-time and required greater employee effort.** Interviewees described manual processes in which their organizations used spreadsheets and ran manual scripts to share external asset data. As this was a heavy manual lift, some organizations would only run these projects several times per year, which ultimately affected data accuracy as the attack surface could quickly change from one day to the next. The director of a cyber command center at a technology insurance organization, described that a manual effort, which took three to four days, was needed to cross-reference IP addresses and enter seed data into the previous tool.
- **Lack of visibility and comprehensiveness in mapping external assets.** Interviewees described the challenge to keep up with an ever-changing attack surface. Without tools that provided in-depth monitoring to review and identify external asset vulnerabilities, the interviewees' organizations were left susceptible to unknown and overlooked assets, such as cloud assets which are ephemeral in nature. This made it difficult for the interviewees' organizations to understand what they needed to

> **"We'd go out individually and query [the same sources as Censys], but the issue we were having was [that] we might do that once a year."**
>
> *Technical director for security architecture and assurance, aerospace and defense*

protect and where to prioritize detection and response.

- **Merger and acquisition activity exposing the company to shadow IT vulnerabilities.** Interviewees described the critical role of M&A activity in their organizations' growth strategies and the challenge of understanding the attack surface when merging and/or acquiring other companies. This exposed parent organizations to unknown assets and shadow IT risks as some of the acquired subsidiary companies came with IT departments that could never fully incorporate with the parent organization's IT department.

INVESTMENT OBJECTIVES

The interviewees' organizations searched for a solution that could:

- Provide a balanced trade-off between time and comprehensiveness on attack surface data.
- Reduce false positives and noise.
- Connect to public cloud infrastructure.

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 global, $4 billion industry-agnostic organization has 15,000 employees and about 10,000 known assets under management. The composite organization uses spreadsheets and open-source tools to discover external assets as it does not have an ASM or formal program in place to monitor external assets. The organization regularly acquires new businesses that need to be integrated into the parent organization, thus it is seeking a

Voice Of The Customer

"I think anybody that says shadow IT is not an issue at their organization maybe has their head in the sand a little bit."

Director, cyber command center, technology insurance

"The accuracy of the data was the number-one driving force behind [adopting] Censys."

Senior security engineer, cloud communications

KEY ASSUMPTIONS

- **$4 billion annual revenue**
- **15,000 employees**
- **10,000 known assets under management**
- **No prior ASM tool**
- **Regularly acquires new businesses**

solution to provide visibility into its growing attack surface.

Deployment characteristics. While the organization initially believes it has 10,000 assets under management, the deployment of Censys EASM provides visibility to the attack surface and discovers 20,000 assets under management in Year 1. The organization continues to grow after Censys deployment through acquisitions of four organizations and 22,050 assets under management in Year 3.

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	Increased efficiencies discovering and assessing assets	$108,360	$108,360	$108,360	$325,080	$269,475
Btr	Reduced likelihood of a security breach	$214,000	$224,700	$235,935	$674,635	$557,509
Ctr	Reduction in employee productivity loss from a security breach	$259,200	$272,160	$285,768	$817,128	$675,264
Dtr	Savings on security assessments for mergers and acquisitions	$73,100	$109,650	$146,200	$328,950	$266,917
Etr	Reduction in false positives	$292,950	$307,598	$322,977	$923,525	$763,189
Ftr	Faster remediation of security incidents	$249,008	$261,458	$274,531	$784,996	$648,710
	Total benefits (risk-adjusted)	$1,196,618	$1,283,925	$1,373,771	$3,854,314	$3,181,064

INCREASED EFFICIENCIES DISCOVERING AND ASSESSING ASSETS

Evidence and data. Interviewees described the impact that Censys had on improving visibility into their organizations' attack surface and discovering and assessing external assets, which led to an overall increase in analyst efficiencies.

- The senior security engineer at a cloud communications company compared asset discovery with Censys to their organization's prior ad hoc processes. The interviewee noted that it would have taken months in the prior environment because the organization had no formal asset discovery processes in place and no centralized way to collect external asset data. With Censys, the organization gathered external asset data within 30 minutes.
- The director of a cyber command center at the technology insurance company described the increase in speed to identify top common ports, protocols, new domains, and IPs; with Censys, the organization accomplished the task within a 24-hour period as compared to three to four days with a prior ASM tool.
- The director of vulnerability management at a market research and consulting organization attributed a 30% improvement in analyst efficiency to using Censys. Previously, analysts

> **"I can now get [data] in 30 minutes where I wouldn't have been able to get it all. I would have had to create a program to list every IP address owned, which is enormous."**
>
> *Senior security engineer, cloud communications*

were tasked to manually evaluate assets but stopped performing this task with Censys: "[Censys] is doing all sorts of scans every day so the data is updated every day. [This is] something less for the [analyst] team to do."

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

- Prior to Censys, two cybersecurity professionals engaged in discovering and assessing assets.
- Prior to Censys, there were four asset discovery projects per year (once every quarter). On average, these projects took two weeks to complete.
- With Censys, cybersecurity analysts increase efficiencies in assessing assets by 30%.
- The fully loaded annual salary for a cybersecurity analyst is $129,000. Their fully loaded monthly rate is $10,750.

Risks. Forrester recognizes that these results may not be representative of all experiences and results will vary depending on the following factors:

- An organization's prior attack surface monitoring practices and time to discover and assess external assets.
- Number of FTEs and specific roles working on asset discovery and assessment.
- Industry variations in salaries.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $269,000.

Increased Efficiencies Discovering And Assessing Assets

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Number of security professionals engaged in asset discovery prior to Censys	Composite	2	2	2
A2	Number of asset discovery projects run per year prior to Censys	Composite	4	4	4
A3	Average discovery project duration (months) prior to Censys	Composite	0.5	0.5	0.5
A4	Cybersecurity analyst fully loaded monthly rate	Composite	$10,750	$10,750	$10,750
A5	Subtotal: Increased efficiency discovering assets with Censys	A1*A2*A3*A4	$43,000	$43,000	$43,000
A6	Number of cybersecurity FTEs assessing assets	Composite	2	2	2
A7	Improved cybersecurity analyst efficiency assessing assets	Interviews	30%	30%	30%
A8	Cybersecurity analyst fully loaded annual salary	Composite	$129,000	$129,000	$129,000
A9	Subtotal: Increased efficiency assessing assets	A6*A7*A8	$77,400	$77,400	$77,400
At	Increased efficiencies discovering and assessing assets	A5+A9	$120,400	$120,400	$120,400
	Risk adjustment	↓10%			
Atr	Increased efficiencies discovering and assessing assets (risk-adjusted)		$108,360	$108,360	$108,360
	Three-year total: $325,080			**Three-year present value: $269,475**	

REDUCED LIKELIHOOD OF A SECURITY BREACH

Evidence and data. Interviewees described the impact that Censys had on reducing the likelihood of a security breach by providing greater visibility into the attack surface and alerting organizations on vulnerabilities in their attack surface.

- Censys enabled the interviewees' organizations to fully see their external attack surface and identify vulnerabilities across all assets. The director of a cyber command center at a technology insurance company stated, "[With Censys], we had less incidents with the root cause being a rogue or unknown asset living on the internet." According to the interviewee, the organization was likely preventing six to 12 infrastructure-related incidents annually, just from using Censys to learn what's out there.
- Censys helped the interviewees' organizations discover assets that were not previously known. The senior security engineer at a cloud communications company described that with Censys: "We found out we had a lot more externally visible assets. We thought, 'Oh, it's probably just under 5,000 [assets,]' and it was probably double that." Since implementing Censys, their organization closed over 5,000 high-risk issues. "A whole bunch of things that have been high risks no longer are. We made them not visible or had them upgraded," said the senior security engineer.
- The director of vulnerability management at a market research and consulting organization further described the speed at which Censys enabled their organization to identify and address potential vulnerabilities with more frequent scans of the attack surface rather than several ad hoc projects to review potential vulnerabilities throughout the year. Censys enabled the organization to "request things to be closed much more quickly if [they] see something wrong."

> **"I've seen the consequences of not knowing your assets. I can't defend what I don't know about, right? The benefit of knowing your assets is of course preventing a very, very serious issue from occurring."**
>
> *Director, cyber command center, technology insurance*

- Interviewees also considered vulnerability reports and notifications Censys's Rapid Response team delivered to be helpful tools for their security organization. Censys notified each of the interviewees of new vulnerabilities and provided recommendations for remediation. Knowing about new vulnerabilities ahead of time allowed the interviewees' organizations to be more proactive with their security and to feel more in control. "One of the nice things with Censys is that you don't have to be on the internet looking for that critical alert. They're going to let me know," said the senior security engineer at a cloud communications company.

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

- The total number of assets scales over the three years with 20,000 assets in Year 1, 21,000 assets in Year 2, and 22,050 assets in Year 3.
- Of total assets, 0.25% are vulnerable to security exploits.
- Forrester defines a breach as an incident resulting in the loss or compromise of data, accompanied by material remediation costs. According to Forrester TEI Consulting's Q4 2020 Cost Of A Security Breach Survey, an

organization with 15,000 employees incurs an average cost of $535,000 per security breach.[3]

- There is a 2% likelihood of a breach or an exploit impacting an asset.
- Censys EASM helped the organization discover 10,000 previously unknown assets, which constitutes 50% of the organization's total assets.

Risks. Forrester recognizes that these results may not be representative of all experiences and results will vary depending on the fact that Forrester applies a greater risk adjustment to security-related benefits to reflect the variability in organizations' digital footprints and respective experiences with security breaches.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $558,000.

"The public surface is our first line of defense, so we needed to understand what our public surface looked like."

Director of vulnerability management, market research and consulting

Reduced Likelihood Of A Security Breach

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Total assets	Composite	20,000	21,000	22,050
B2	Percent of assets vulnerable to hacks or exploits	Composite	0.25%	0.25%	0.25%
B3	Cost of a potential breach	Forrester research	$535,000	$535,000	$535,000
B4	Likelihood of breach or exploit per asset	Forrester research	2%	2%	2%
B5	Percentage of total assets found by Censys	Interviews	50%	50%	50%
Bt	Reduced likelihood of a security breach	B1*B2*B3*B4*B5	$267,500	$280,875	$294,919
	Risk adjustment	↓20%			
Btr	Reduced likelihood of a security breach (risk-adjusted)		$214,000	$224,700	$235,935
	Three-year total: $674,635			**Three-year present value: $557,509**	

REDUCTION IN EMPLOYEE PRODUCTIVITY LOSS FROM A SECURITY BREACH

Evidence and data. In addition to the cost of a security breach, interviewees recognized the impact that a security breach had on employee productivity due to downtime. With better awareness of their attack surface, the interviewees' organizations were more likely to protect their employees from an impact of a material breach.

A director of a cyber command center told Forrester that they saw the outcomes of security incidents on employee productivity: "Ransomware is a great example. If a piece of ransomware encrypts all your data, the integrity has been lost and then availability [becomes an issue]. So, if your data is encrypted, you can't use it or you face a denial of service that takes down an application or something else." With Censys, interviewees' organizations avoided these instances of downtime as a result of fewer security breaches.

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

- The organization experiences one security breach per year resulting from asset exploits. Potential number of breaches goes up slightly as the number of assets increases from Year 1 to Year 3.
- Censys EASM helped the organization discover 10,000 previously unknown assets, which constitutes 50% of the organization's total assets.
- According to Forrester TEI Consulting's Q4 2020 Cost Of A Security Breach Survey, a security breach impacts 30% of employees at an organization with 15,000 employees.[4]
- An average employee incurs 3.6 hours of downtime as a result of a breach.[5]
- The blended FTE fully loaded hourly rate is $40.

Risks. Forrester recognizes that these results may not be representative of all experiences and results will vary depending on the following factors:

- Organizations' digital footprints and respective experiences with security breaches.
- Number of employees and severity of a breach.
- Former security solutions in place to address asset-related vulnerabilities.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $675,000.

Reduction In Employee Productivity Loss From A Security Breach					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Total number of employees	Composite	15,000	15,000	15,000
C2	Average number of security breaches per year resulting from asset exploits	B1*B2*B4	1.0	1.05	1.1
C3	Percent of total assets found by Censys	Interviews	50%	50%	50%
C4	Percentage of employees impacted by security breach	Forrester research	30%	30%	30%
C5	Avoided employee downtime with Censys	Forrester research	3.6	3.6	3.6
C6	Blended FTE fully loaded hourly rate	TEI standard	$40	$40	$40
Ct	Reduction in employee productivity loss from a security breach	C1*C2*C3*C4*C5*C6	$324,000	$340,200	$357,210
	Risk adjustment	↓20%			
Ctr	Reduction in employee productivity loss from a security breach (risk-adjusted)		$259,200	$272,160	$285,768
	Three-year total: $817,128			**Three-year present value: $675,264**	

SAVINGS ON SECURITY ASSESSMENTS FOR MERGERS AND ACQUISITIONS

Evidence and data. Interviewees told Forrester that the ability to quickly find and categorize information around assets and vulnerabilities of new potential subsidiaries enabled by Censys was invaluable and instilled more confidence in their organizations' M&A endeavors. With Censys, interviewees no longer needed to run special asset discovery projects or risk stepping into a new agreement blindly.

- The technical director for security architecture and assurance at an aerospace and defense company described that the first step in due diligence assessments for M&A activity was to understand the external attack surface. Their organization used Censys to gain visibility into the attack surface of their acquired companies and thereby shortened the due diligence process by 25%.
- The senior security engineer at a cloud communications company described how the lack of a formal process to assess external attack surfaces from acquired companies created uncertainty over the accuracy of the data collected and subsequently shared with executive leaders and decision-makers. The interviewee stated, "I think it gives a lot of comfort to the executives, especially the CIO and the CSO,

"We have a much better understanding of the assets associated with us out there — with our subsidiaries, with our joint ventures."

Technical director for security architecture and assurance, aerospace and defense

when [they] see the [Censys] report of what I found."

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

- M&A activity scales over the period of three years with the composite organization acquiring two new subsidiaries in Year 1, three new subsidiaries in Year 2, and another four subsidiaries in Year 4.
- Two FTEs are required to work on M&A special asset discovery projects in the prior environment. These projects each take two months to complete.
- The security FTE supporting M&A has a fully burdened annual salary of $129,000.
- Censys requires no deployment or configuration to evaluate potential subsidiaries.

Risks. Forrester recognizes that these results may not be representative of all experiences and results will vary depending on the following factors:

- Number of mergers and acquisitions a company experiences.
- Labor related to M&A discovery projects.
- The type of FTE performing discovery projects.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $283,000.

> **"[Censys] definitely gives you a bit more comfort when you're acquiring [a company and know] what you're stepping into and what you're absorbing."**
>
> *Senior security engineer, cloud communications*

Savings On Security Assessments For Mergers And Acquisitions

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Mergers and acquisitions per year	Composite	2	3	4
D2	FTEs required to work on M&A in prior environment	Composite	2	2	2
D3	Number of months FTEs are required to work on an acquisition before Censys	Composite	2	2	2
D4	Fully burdened annual salary of security FTE supporting M&A	Composite	$129,000	$129,000	$129,000
Dt	Savings on security assessments for mergers and acquisitions	D1*D2*D3* (D4/12 months)	$86,000	$129,000	$172,000
	Risk adjustment	↓15%			
Dtr	Savings on security assessments for mergers and acquisitions (risk-adjusted)		$77,400	$116,100	$154,800
	Three-year total: $348,300			**Three-year present value: $282,618**	

REDUCTION IN FALSE POSITIVES

Evidence and data. Interviewees highlighted the accuracy of Censys data as it related to external assets in the attack surface. More accurate data led to fewer false positives, which saved analysis time for the security teams.

- The director of a cyber command center at a technology insurance company noted the importance of getting real and actionable data in front of their analysts. Prior to Censys, up to 25% of alerts were false positives that required analysts' attention and time that could have been spent handling real incidents. The interviewee stated: "I don't know that we have any false positives with Censys. The reason for that is how we've tuned those alerts prior to coming to our analysts."
- The senior security engineer at a cloud communications organization noted that prior to Censys, 30% of alerts were false positives versus 10% with Censys. The interviewee explained: "[Censys] had much less false positives for us. Censys was able to keep a lot of noise out of our attack surface and made my life easier because of that."

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

- 25% of assets experience an issue in a year, producing an alert. 30% of these alerts produced are false positives prior to Censys EASM.
- There is a 70% reduction in false positives with Censys.
- Cybersecurity analysts spend 5 hours investigating each false positive.
- The cybersecurity analyst fully loaded hourly rate is $62.

Risks. Forrester recognizes that these results may not be representative of all experiences and results will vary depending on the following factors:

> **"Every time I wanted to report on anything [before Censys], I'd have to double- and triple-check that it was really us. Because you lose a lot of credibility when you go out to someone and say, 'Look, I found this. It's insecure. It's ours.' And [then] it is not. Today, I can trust the data."**
>
> *Senior security engineer, cloud communications*

- The number of assets in an organization's attack surface.
- The number of alerts received per year and percentage of false positives within these alerts.
- The hours needed to investigate false positives.
- The type of FTE role that investigates false positives.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $763,000.

> **"Since we have more confidence in the tool, we can actually respond more quickly because we're not reaching out about [false] alerts nearly as much."**
>
> *Director, cyber command center, technology insurance*

Reduction In False Positives					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
E1	Total number of assets	Composite	20,000	21,000	22,050
E2	Percent of assets that experience an issue in a year	Composite	25%	25%	25%
E3	Number of incident alerts per year	E1*E2	5,000	5,250	5,513
E4	Percentage of false positives in prior environment	Composite	30%	30%	30%
E5	Reduction in false positives with Censys	Interviews	70%	70%	70%
E6	Number of false positives eliminated	E3*E4*E5	1,050	1,103	1,158
E7	Hours spent investigating each false positive	Composite	5	5	5
E8	Cybersecurity analyst fully loaded rate	Composite	$62	$62	$62
Et	Reduction in false positives	E6*E7*E8	$325,500	$341,775	$358,864
	Risk adjustment	↓10%			
Etr	Reduction in false positives (risk-adjusted)		$292,950	$307,598	$322,977
	Three-year total: $923,525			**Three-year present value: $763,189**	

FASTER REMEDIATION OF SECURITY INCIDENTS

Evidence and data. Interviewees explained that Censys contributed to time savings in issue assessment, which led to efficiencies in remediation of incidents.

- The senior security engineer at a cloud communications company described that the organization's prior environment required multiple data checks to ensure accuracy of alerts.
- The director of a cyber command center at a technology insurance company told Forrester that they relied on Censys's risk classification system for defining critical, high-, medium-, and low-risk events: "They also do a good job [with correlating findings]: take a single IP address. Maybe that IP address has three medium-severity findings. Well, three medium-severity findings could be correlated and then combined to maybe [be considered] a high-severity asset. So, [Censys] does that correlation which is really helpful."

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

- The total number of true issues scales as the attack surface grows. The total number of issues without false positives is 3,500 in Year 1, 3,675 in Year 2, and 3,859 in Year 3.
- Cybersecurity professionals spend 5 hours managing and reporting each security alert issue and 4 hours resolving each issue.
- 15% of time is saved with Censys.
- A security professional's fully loaded hourly rate is $62.

Risks. Forrester recognizes that these results may not be representative of all experiences and results will vary depending on the following factors:

- The number of false positives and time spent to manage, report, and resolve issue alerts.
- The salary of security professionals managing, reporting, and resolving alerts.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $649,000.

Faster Remediation Of Security Incidents

Ref.	Metric	Source	Year 1	Year 2	Year 3
F1	Total issues without false positives	E3-(E3*E4)	3,500	3,675	3,859
F2	Time spent on managing/reporting per issue (hours)	Composite	5	5	5
F3	Time spent on resolution per issue (hours)	Composite	4	4	4
F4	Total time on remediation process (hours)	F2+F3	9	9	9
F5	Time savings in remediation of incidents with Censys	Composite	15%	15%	15%
F6	Security professional fully loaded hourly rate	Composite	$62	$62	$62
Ft	Faster remediation of security incidents	F1*F4*F5*F6	$292,950	$307,598	$322,977
	Risk adjustment	↓15%			
Ftr	Faster remediation of security incidents (risk-adjusted)		$249,008	$261,458	$274,531
	Three-year total: $784,996			**Three-year present value: $648,710**	

UNQUANTIFIED BENEFITS

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

- **Better control over shadow IT**. For interviewees, Censys helped identify and close down the assets that were created by employees and unknown (and therefore unmanaged) by the organization. "I know for a fact we've identified domains that people have purchased outside of our approved process, which requires our marketing team and our legal team and my team security to review and sign off on," said the senior security engineer at a cloud communications organization. "[Censys] has helped us rein it in, without question."
- **Outstanding collaboration.** According to the interviewees, Censys provided excellent partnership in solving issues and responding to its customers' technical needs. The director of the cyber command center at a technology insurance organization said: "We've had a very good experience with being closely tied to their engineering and support teams. If we identify a bug or if there's a feature enhancement, we have near-real-time interactions via shared Slack integration where we can go back and forth, and they turn around ideas into features very quickly."

"When you begin to get more confidence in your detections, then you can build that trust with some of the other teams in the company."

Director, cyber command center, technology insurance

"They have a pretty unique capability where they actually hook into all of your public cloud infrastructure, and so they do both an outside-in and inside-out approach, which at least [since] the last time I was looking at tooling in the space, they're the only ones that do it in that manner."

Director, cyber command center, technology insurance

- **Suitability for cloud.** Censys's ability to connect to public cloud infrastructure with vendor-agnostic connectors was a key differentiator and selling point for interviewees to adopt the solution.
  - The director of a cyber command center at a technology insurance organization shared their perspective that, at the time when their organization was evaluating attack surface management tools, this capability was unique to Censys.
  - The director of vulnerability management at a market research and consulting firm stated, "The main differentiator from our perspective is the fact that there was [a] cloud connector, because I consider that the cloud environment is certainly one of the biggest challenge[s], maybe [even] the biggest challenge."
- **Peace of mind.** The interviewees spoke about the sense of comfort that full visibility into their attack surface provided to them via Censys EASM. Interviewees felt that they received reliable and timely information and proactive

guidance on new vulnerabilities. This made them feel more in control and better prepared for reporting to their management. The senior security engineer at a cloud communications organization said: "[Censys] lets you know if you have the issue so you can update management that, no, we're not susceptible. We don't have that one. You know, that definitely makes the CSO or the CIO more comfortable [and feel that,] 'Yeah, we're on it. My team is on their game.'"

FLEXIBILITY

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

- **Identification of unused or unnecessary assets.** Interviewees anticipated savings around maintenance of assets that the organizations did not know they were paying for before Censys.
- **Growing use across the organization.** Interviewees described that Censys may be primarily used by security teams within their organizations, but that other lines of business in their organizations have also been interested in obtaining access to external asset data. The director of a cyber command center at the technology insurance company described the usefulness of Censys EASM data to the vulnerability management team. At that organization, the analysts on the vulnerability management team fed the Censys data into a security risk correlation tool as it already incorporated any custom risk scoring, saving the analysts time on preparing the data and discovering zero-day vulnerabilities sooner.

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

"The other thing that it's starting to do for us [is] help us to identify the immaturity of some of our digital asset management processes."

Technical director for security architecture and assurance, aerospace and defense

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Gtr	Licensing	$0	$88,000	$92,400	$97,020	$277,420	$229,256
Htr	Implementation, integration, and training	$2,182	$141,900	$141,900	$141,900	$427,882	$355,067
	Total costs (risk-adjusted)	$2,182	$229,900	$234,300	$238,920	$705,302	$584,323

LICENSING

Evidence and data. Licensing costs were dependent on the number of external assets.

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

- Licensing costs are $80,000 per year.
- Pricing may vary. Contact the Censys team for additional details.

Risks. Forrester recognizes that these results may not be representative of all experiences and results will vary depending on the size of an organization's attack surface.

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 $229,000.

Licensing						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
G1	Licensing	Composite		$80,000	$84,000	$88,200
Gt	Licensing	G1		$80,000	$84,000	$88,200
	Risk adjustment	↑10%				
Gtr	Licensing (risk-adjusted)		$0	$88,000	$92,400	$97,020
	Three-year total: $277,420			**Three-year present value: $229,256**		

IMPLEMENTATION, INTEGRATION, AND TRAINING

Evidence and data. In addition to fees paid to Censys, interviewees described internal costs related to the implementation, integration, and training of the solution.

- Implementation efforts ranged from teams of one to five cybersecurity professionals of different levels, depending on the size of the organization and the size of the attack surface. All interviewees, however, said that working with Censys was easy. The technical director for security architecture at an aerospace and defense organization said, "It's [software as a service] (SaaS), they are turnkey."
- Interviewees described integration efforts as they related to cloud connectors to ensure that the tool was safely connected to the respective organization's interfaces.
- Interviewees described the basic training Censys provided as efficient and helpful. The senior security engineer at a cloud communications organization stated, "I've always been able to send an email off and have whoever my engineering rep is give me an answer quickly."

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

- Two cybersecurity FTEs are involved in the initial setup of the solution including 6 hours on implementation, 5 hours on integration, and 5 hours on training.
- One cybersecurity FTE is dedicated to ongoing management of Censys.
- The FTE fully loaded hourly rate of a cybersecurity FTE is $62.

Risks. Forrester recognizes that these results may not be representative of all experiences and results will vary depending on the following factors:

- The size of the organization's attack surface.
- The organization's prior environment and FTEs dedicated to attack surface monitoring.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $355,000.

> **"We had access one day [after] subscription, and I think it took [another] few days to finalize the searches — so this has been very rapid."**
>
> *Director of vulnerability management, market research and consulting*

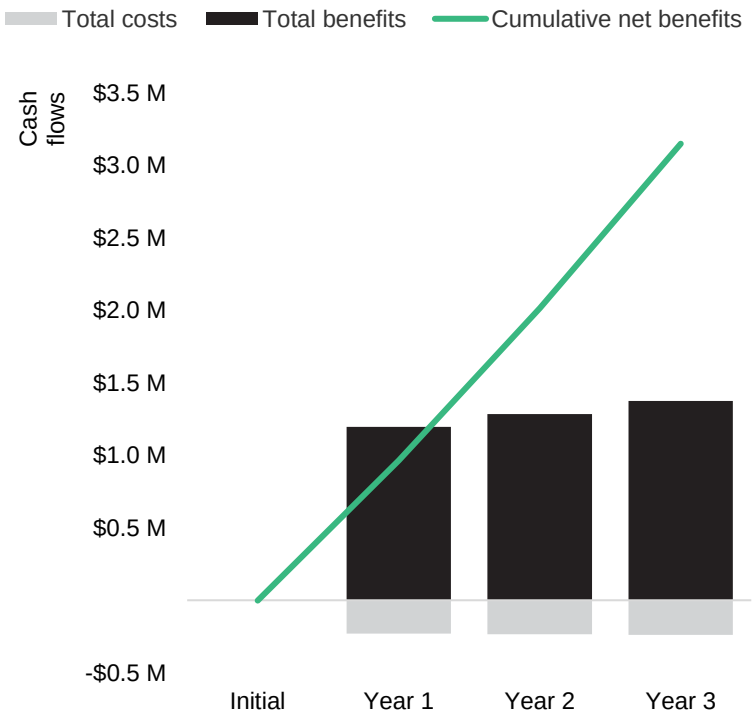
Implementation, Integration, And Training

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
H1	Implementation hours	Composite	6			
H2	Integration hours	Composite	5			
H3	Training hours	Composite	5			
H4	FTEs involved in implementation	Composite	2			
H5	Ongoing management effort (FTEs)	Composite		1	1	1
H6	Blended FTE fully loaded hourly rate	Composite	$62	$62	$62	$62
Ht	Implementation, integration, and training	(H1+H2+H3)*H4 *H6+H5*A8	$1,984	$129,000	$129,000	$129,000
	Risk adjustment	↑10%				
Htr	Implementation, integration, and training (risk-adjusted)		$2,182	$141,900	$141,900	$141,900
	Three-year total: $427,882			**Three-year present value: $355,067**		

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 and NPV for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI and NPV 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	($2,182)	($229,900)	($234,300)	($238,920)	($705,302)	($584,323)
Total benefits	$0	$1,196,618	$1,283,925	$1,373,771	$3,854,314	$3,181,064
Net benefits	($2,182)	$966,718	$1,049,625	$1,134,851	$3,149,012	$2,596,741
ROI						444%

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: “Find And Cover Your Assets With Attack Surface Management,” Forrester Research, Inc., January 6, 2022.

[2] 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.

[3] Source: Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q4 2020.

[4] Ibid.

[5] Ibid.


FORRESTER®