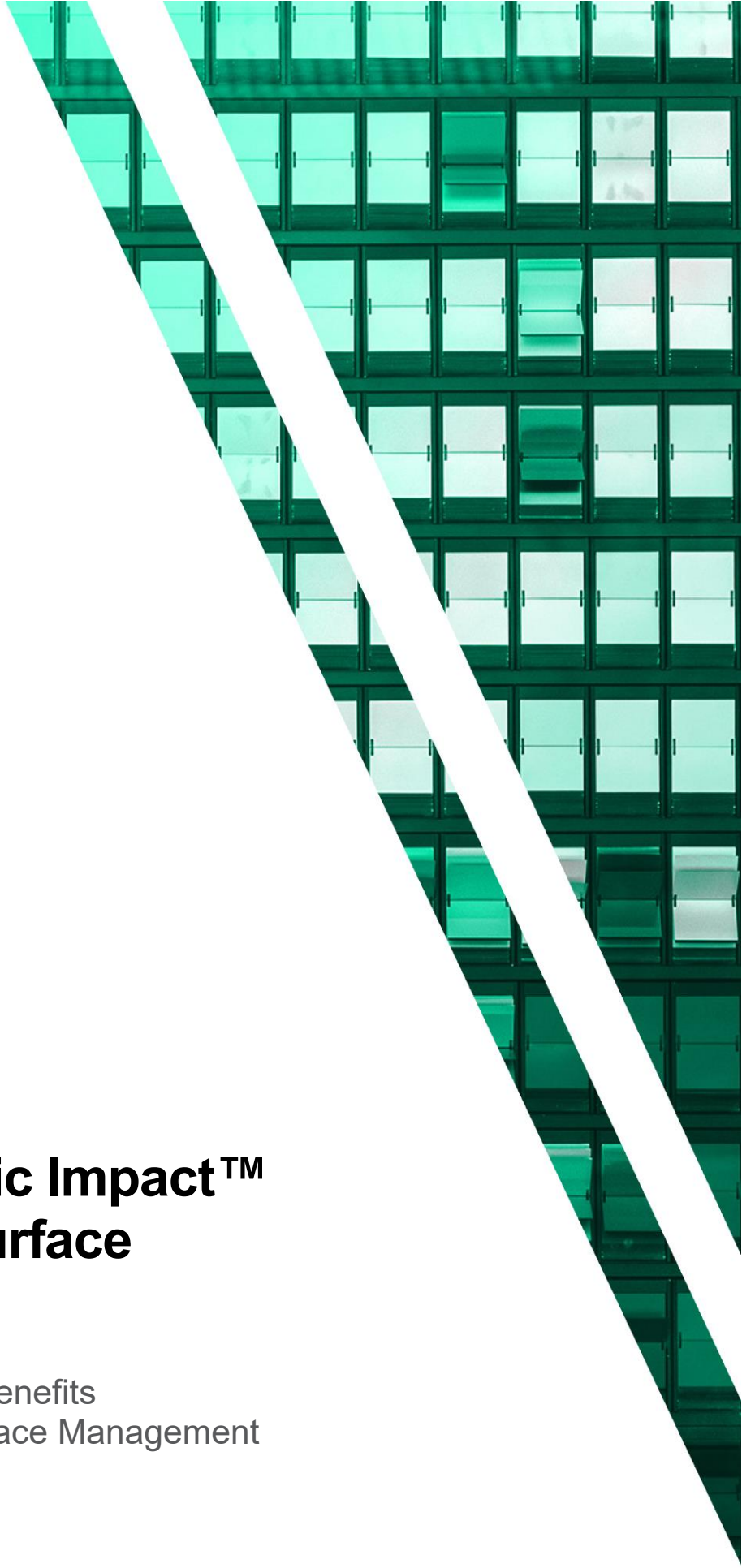
FORRESTER®



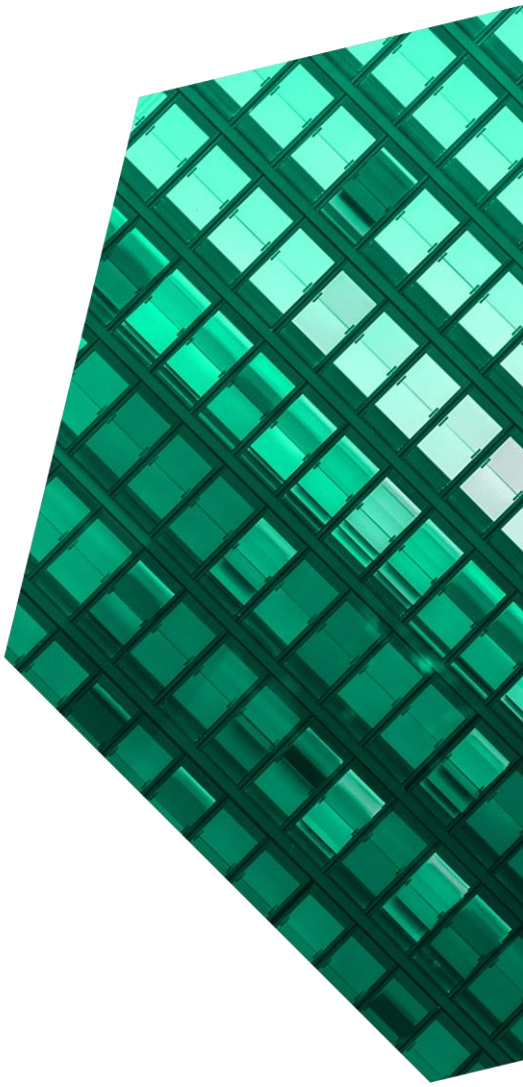
The Total Economic Impact™ Of Cisco Attack Surface Management

Cost Savings and Business Benefits Enabled By Cisco Attack Surface Management

JANUARY 2023

Table Of Contents

Consulting Team: Courtenay O'Connor
Nahida Nisa



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

With digital transformation headwinds pushing more organizations to the cloud at breakneck speeds, companies often sacrifice governance and security at the expense of speedy data migration. Organizations must protect cloud access and workloads with effective governance to mitigate cloud data breach risks and assure the vital backbone of trusted business. Solutions that confer cyber asset visibility help an organization de-risk its cloud journey while opening new pathways to value.[1]

Cisco Attack Surface Management is a cyber asset attack surface management (CAASM) software solution that leverages a comprehensive relationship graph for advanced and accelerated visibility into an organization's digital footprint and security posture.[2] Cisco ASM provides a single source of truth for locating cyber assets and their interrelationships, helping organizations limit the blast radius of a cybersecurity breach.

JupiterOne and Cisco ASM commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Cisco ASM.[3] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Cisco ASM on their organizations. This study was also published by JupiterOne as The Total Economic Impact™ Of JupiterOne.

Reduction in attack surface

150%

KEY STATISTICS

Return on investment (ROI)
332%

Net present value (NPV)
$3.07M

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four representatives from four organizations with experience using Cisco ASM. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization with a B2B and B2C approach, 50,000 customers, and annual revenue of $500 million.

Prior to using Cisco ASM, interviewees noted their organizations were handcuffed to outdated, inaccurate spreadsheets that were rarely updated to reflect the organizations' real cyber footprints. This led the interviewees' security organizations to spend vast amounts of time on rote, manual, and error-ridden processes. In addition to operational inefficiencies, several interviewees' organizations were exposed to security vulnerabilities due to ungoverned assets that were difficult to locate.

After the investment in Cisco ASM, the interviewees shifted a majority of the security operations (SecOps) incident response time devoted to manual identification of cyber assets to higher-value vulnerability management activities. Key results from the investment include a 150% reduction in the composite organization's attack surface.

KEY FINDINGS

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

- **Reduction in security risk from diminished attack surface worth $2 million over three years.** With Cisco ASM, the composite organization uncovers and decommissions a trove of ungoverned and misconfigured cyber assets. In doing so, it reduces its attack surface by 150% in the first year, thereby reducing the organization's exposure to the inherent data security risks to vendors and regulatory compliance institutions.
- **Reduction in business risk associated with a severe security breach worth more than $1 million over three years.** Cisco ASM reduces the hours the SecOps team needs to manually identify cyber assets during a severe security breach, further de-risking the composite organization. This shortened response time has cascading impacts on organizational end users' uptime, while simultaneously reducing the risk to customers and brand reputation with each breach.
- **SecOps incident response efficiencies from improved cyber asset visibility worth $496,000 in over three years.** With Cisco ASM, the composite experiences an 85% reduction in the number of SecOps resource hours devoted to manual investigation and identification of cyber assets.
- **Enhanced compliance and certification posture worth $462,000 over three years.** With Cisco ASM, the composite organization avoids the need to purchase a separate compliance solution; significantly reduces the amount of IT and SecOps hours dedicated to compliance and certification; and facilitates the attainment of a new certification that opens up a new market to it.

Unquantified benefits. Benefits that are not quantified in this study include:

- **Time to value.** Several interviewees noted how Cisco ASM allowed their organizations to shorten the time to release revenue-generating features and updates and permitted organizations to accelerate mergers and acquisitions due to the transparency it conferred to an IT organization's balance sheet.
- **Customer experience.** Interviewees also noted that their organizations delivered on their brand promise better through more secure and consistent engagement with their customers and customer data.

Cyber assets are granular software-defined entities that expand beyond endpoints, IP addresses, users, and devices to include code commits, security controls, applications, access policies, cloud configurations, and more.

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

- **Cisco ASM subscription fees, totaling $609,000.** Subscription fees are assessed primarily as a function of the total number of cyber assets captured within Cisco ASM digital infrastructure. In Year 1, the composite organization protects 250,000 cyber assets through Cisco ASM' Premier subscription tier. The composite organization's cyber footprint protected by Cisco ASM grows by 20% year-over-year.
- **Internal deployment and administration costs of $316,000.** Three SecOps resources are 80% dedicated to deployment for three months. All 20 SecOps resources undergo initial training on Cisco ASM upon deployment with ongoing training and enrichment throughout the three-year period. One resource dedicates one day a month to the ongoing administration of the Cisco ASM platform.

The representative interviews and financial analysis found that a composite organization experiences benefits of $3.99M over three years versus costs of $925K, adding up to a net present value (NPV) of $3.07M and an ROI of 332%.

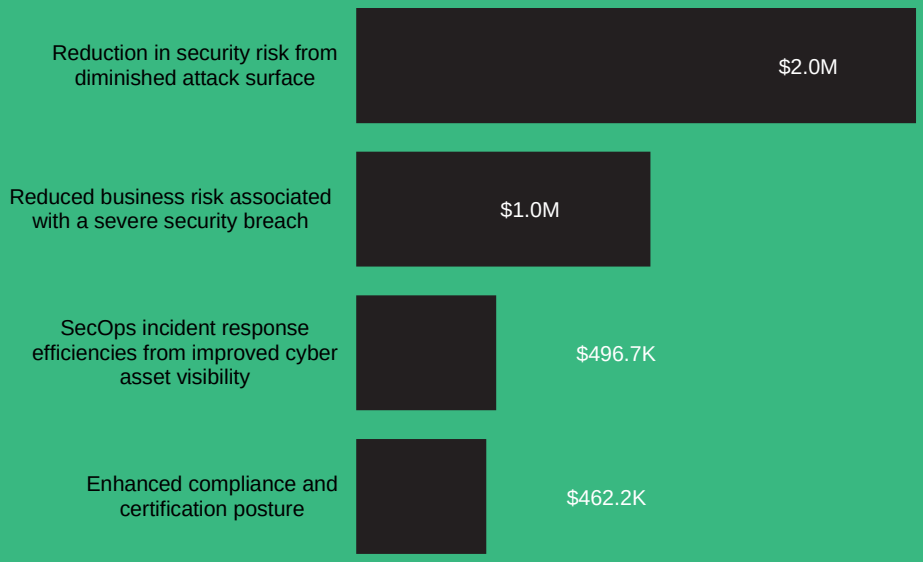
ROI
332%

BENEFITS PV
$3.99M

NPV
$3.07M

PAYBACK
<6 months

Benefits (Three-Year)



“With Cisco ASM, we can focus on strategy to solve security problems. It enables us to transition to a more analytic position and focus on best practices, rather than on scripting and in spreadsheets.”

— Director of information security, martech

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 Cisco ASM.

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 Cisco ASM can have on an organization.

Forrester Consulting conducted an online survey of 351 cybersecurity leaders at global enterprises in the US, the UK, Canada, Germany, and Australia. Survey participants included managers, directors, VPs, and C-level executives who are responsible for cybersecurity decision-making, operations, and reporting. Questions provided to the participants sought to evaluate leaders' cybersecurity strategies and any breaches that have occurred within their organizations. Respondents opted into the survey via a third-party research panel, which fielded the survey on behalf of Forrester in November 2020.

DUE DILIGENCE

Interviewed Cisco ASM stakeholders and Forrester analysts to gather data relative to Cisco ASM.

INTERVIEWS

Interviewed four representatives at organizations using Cisco ASM 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 Cisco Attack Surface Management Customer Journey

Drivers leading to the Cisco ASM investment

Interviews

Role	Industry	Region	Revenue
Director of information security	Martech	USA headquarters, global reach	$185 million
Chief information security officer	Data management	USA headquarters, global reach	$150 million
Information security manager	Fintech	USA headquarters, global reach	$150 million
Director of digital security and resilience	Telecommunications	UK headquarters, UK reach	$14.1 billion

KEY CHALLENGES

Before Cisco ASM, interviewees' organizations used homegrown tools that required intensive SecOps engagement to develop and run queries in order to identify cyber assets. Security and compliance processes often took days to complete and were subject to inaccuracies. Half of the interviewees had an inaccurate understanding of their cyber footprint by an order of magnitude.

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

- **Inadequate coverage of cyber footprint.** Interviewees suffered from inadequate solutions in the cloud and on-prem that lacked the ability to adequately scan and detect assets. Often little more than a set of spreadsheets, some interviewees' organizations' approaches covered only production environments or lacked the observability into cloud assets. Because of this, interviewees often lacked confidence in the accuracy of the findings their legacy discovery processes uncovered. Furthermore, a lack of visibility made interviewees susceptible to ungoverned critical areas of their cyber footprint and at risk of noncompliance with several standard drivers.
- **Time-consuming, manual processes for high-value SecOps resources.** With data mainly sequestered in spreadsheets and virtual machines, discovery processes for incident response, compliance, and certification required time-intensive — yet often rote — activities to pull, clean, and present data.
- **The ad hoc nature of response and reporting.** Critical processes lacked standardization in key areas, particularly related to data hygiene, risking myriad "ghost assets" lurking in the cloud, costing the organizations money while adding to their risk profiles.

"We didn't know how many actual instances we had running and their configuration posture. Every time we had to gather information, we ran scripts and did ad hoc analysis."
Director of information security, martech

SOLUTION REQUIREMENTS

The interviewees' organizations searched for a solution that could:

- Improve security posture through immediate visibility, particularly to enhance the ability to act quickly and at scale in the face of mounting security challenges.
- Enhance observability of the attack surface to secure SaaS and ephemeral assets.
- Streamline compliance posture, including automated evidence collection, easier certifications and attestations, better-met enterprise customer security requirements, and assistance in certification achievement.
- Deliver software development business insights derived from dashboards and reports.
- Reduce the cost and complexity of their prior cyber asset management.

Interviewees were drawn to Cisco ASM for several reasons. The asset discovery graph was a key differentiator. For interviewees, it was dynamic, providing:

- A consolidated view of the organizations' environment with solid data on asset inventory across multiple cloud service providers.
- Cloud-ready (or cloud-native) easy integration capabilities out of the box.
- Status of endpoints and real-time data on what's happening.
- Fast refreshes of organizational cyber footprints.

More broadly, it expanded how the organizations thought about asset inventory from just endpoints to CSPs, SaaS apps, code repos, IAM policies, security controls, vulnerability findings, and more.

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, multibillion-dollar B2B and B2C organization is cloud-first with 100% of its data in the cloud. The composite organization has a customer base of about 50,000 customers and 1,500 employees, including 450 developers. Its SecOps team of 20 includes four power users of Cisco ASM. Compliance and certification drivers for the composite organization include General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), Insurance Service Office (ISO), and governance, risk, and compliance (GRC).

The composite organization has 250,000 cyber assets to secure in its digital footprint with Cisco ASM and anticipates that number to grow by 20% each year.

Deployment characteristics. The composite organization deploys Cisco ASM to inventory and query assets, ensure compliance with drivers, and enforce and improve its security posture.

Key Assumptions

- **$500 million annual revenue**
- **250,000 cyber assets**
- **1,500 employees**
- **20 SecOps FTEs**

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	Reduction in security risk from diminished attack surface	$808,274	$794,944	$794,528	$2,397,746	$1,988,714
Btr	Reduced business risk associated with a severe security breach	$417,294	$420,635	$423,297	$1,261,226	$1,045,019
Ctr	SecOps incident response efficiencies from improved cyber asset visibility	$189,312	$200,448	$211,584	$601,344	$496,728
Dtr	Enhanced compliance and certification posture	$178,514	$186,395	$194,138	$559,046	$462,189
	Total benefits (risk-adjusted)	$1,593,394	$1,602,422	$1,623,546	$4,819,362	$3,992,650

REDUCTION IN SECURITY RISK FROM DIMINISHED ATTACK SURFACE

Evidence and data. Interviewees described several ways in which Cisco ASM diminished their organizations' attack surface and, consequently, reduced the risk associated with formerly ungoverned cyber assets.

- In one case, the information security manager in the fintech industry shared that Cisco ASM detected more digital identities in its multifactor authentication (MFA) solution than the solution itself detected.
- The director of digital security and resilience in the telecommunications (telecom) industry shared an example of how their organization recouped millions of dollars from a vendor: "We had a misconfiguration incident. One system was missing MFA enforcement for the users. The vendor responsible for the SaaS app credited $9 million back to us after we demonstrated that it was fraud. If we had visibility on the users and their configuration on that system, we could have been aware of the risk or maybe prevented it."

> **"Almost none of the unmanaged assets were being patched for vulnerabilities. By reducing the footprint for unmanaged assets, our security risk was reduced."** *Chief information security officer, data management*

Modeling and assumptions. The composite organization reduces its security risk as follows:

- Before Cisco ASM, the composite organization had 250,000 known cyber entities across its digital footprint in Year 1, and experienced 20% cyber asset growth year-over-year (YOY).
- Upon deployment of Cisco ASM, the composite organization identifies 250% more cyber assets in the cloud in Year 1, 106% in Year 2, and 102%

Customer Voice

The chief information security officer at the data management company shared the impact of Cisco ASM's visibility onto the attack surface, which experienced a wave of Russian malware hitting the production firewall prior to the Russian invasion of Ukraine in 2022.

The interviewee noted that the prior environment had issues with low standardization, but with Cisco ASM, they had:

- Real-time situational awareness for what needed to be deprovisioned and what was added in the last 48 hours with the resource count by type, mapped resources by type, and billable entities by type.
- Means for querying resources and infrastructure, and continuous security modeling on a daily basis with significant reductions in the organization's attack surface. The chief information security officer stated the following:
  - "We found lots of neglected or forgotten assets — they were actually costing us money and yet weren't doing anything."
  - "We deprovisioned millions of newly identified information assets ranging from outdated proof of concepts (POCs), technical demo assets, and training assets. They could have been used to launch other attacks to our production firewall."

in Year 3. This previously hidden subset of cyber assets includes:

  - Assets in new asset classes Cisco ASM discovers, such as proofs of concepts for sales pitches and collaboration that are not decommissioned after active use.
  - Ghost assets containing unencrypted customer and employee personal information.
- Within the newly discovered assets, the composite organization has a misconfiguration that brings them out of compliance with customer data regulations. Those assets are identified and then decommissioned in Year 1. It continues to identify and decommission a small number of ungoverned assets as needed. Over time, the number of these ungoverned assets is further reduced due to improved policies and cyber asset awareness.
- Forrester assumes that the Year 1 impacts of decommissioning a large volume of previously undetected cyber assets has slight balance sheet impacts to the organization's IT budget related to cyber assets. The composite experiences:
  - A reduction of 1% on capital expenditures related to purchasing licenses and subscriptions for cyber assets.
  - A reduction of 0.01% on the IT budget's operational expenditures related to managing cyber assets.
- Although the organization avoids a massive data breach, the cloud misconfiguration leaves the composite organization exposed to various levels of security risk:
  - Due to the misconfiguration, the organization exposed personal identifiable information for approximately 300 customers, violating key data privacy and security requirements with

vendors and state, federal, and international standards.

- According to the Ponemon Institute, ungoverned data records at risk could cost organizations $180 each if included in an actual breach.[4]
- Without Cisco ASM, the organization faces fines of $5,000 per individual record in violation of privacy standards.

- With Cisco ASM, the composite organization:
  - Decommissions the ghost assets and thereby neutralizes the potential risk of ungoverned assets.
  - Proves that this breach was unintentional rather than a purposeful violation of privacy laws, reducing the cost of the violation by 67% with a key regulator.
- By the end of the three-year period, the composite organization:
  - Reduces its total attack surface, including both known and unknown cyber assets, by over 150%.
  - Avoids almost $2.4 million in security risk and balance sheet inefficiencies.

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

- The amount of an organization's IT budget dedicated to costs related to cyber asset capital and operational expenditures. Companies should adopt a capital and operational cost saving approach that makes sense for their security organizations.
- Organizations should consider their own security context, including the number of severe-level cloud security incidents and the hours per investigation.

Results. To account for these risks, Forrester adjusted this benefit downward by 25%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $2.0 million.

Reduction In Security Risk From Diminished Attack Surface					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Number of known cyber assets before Cisco ASM	20% cyber asset growth YOY	250,000	300,000	360,000
A2	Percent of actual cyber footprint detected with Cisco ASM	Interviews	250%	106%	102%
A3	Number of obsolete cyber assets identified and decommissioned with Cisco ASM	Composite	375,000	17,500	8,750
A4	IT budget dedicated to purchasing and maintaining all cyber assets	Composite	$1,851,360	$1,851,360	$1,851,360
A5	IT budget efficiencies from decommissioned obsolete cyber assets identified with Cisco ASM	Composite	1.01%	0.05%	0.02%
A6	Subtotal: Cost savings from decommissioned cyber assets	A4*A5	$18,698.74	$925.70	$370.28
A7	Number of customers with PII found in decommissioned cyber assets	<1% of 50,000 customers	300	300	300
A8	Per record cost of PPI data security risk	Ponemon Institute	$180	$180	$180
A9	Fine received for an intentional violation of privacy standards	Composite	$5,000	$5,000	$5,000
A10	Reduction in fines with proof from Cisco ASM that breach was unintentional	Interviews	67%	67%	67%
A11	Subtotal: Reduction in risk associated with misconfigured and vulnerable assets	(A7*A8)+ (A7*A9*A10)	$1,059,000	$1,059,000	$1,059,000
A12	Reduction in attack surface with Cisco ASM	A3/A1	150%	6%	2%
At	Reduction in security risk from diminished attack surface	A6+A11	$1,077,699	$1,059,926	$1,059,370
	Risk adjustment	↓25%			
Atr	Reduction in security risk from diminished attack surface (risk-adjusted)		$808,274	$794,944	$794,528
	Three-year total: $2,397,746			**Three-year present value: $1,988,714**	

REDUCED BUSINESS RISK ASSOCIATED WITH A SEVERE SECURITY BREACH

Evidence and data. All interviewees reported time savings related to SecOps incident response:

- The director of information security in the marketing industry shared that Cisco ASM improved their organization's security posture through continuous monitoring, fast detection of cyber assets, and a faster overall response to security breaches.
- The director of digital security and resilience in the telecom industry characterized Cisco ASM's relationship graph as "priceless." He expanded: "In our legacy environment, incident response could take three to four days and an army of people to find the needle in the haystack … With Cisco ASM, I have comprehensive access, visibility, maximum security coverage, and automated policy enforcement. In case of a major incident, the linked data is pure gold. Recently, the team was able to quickly pinpoint to me what happened, whereas prior to Cisco ASM, it took the organization two to three days, and they couldn't find out what happened."

Modeling and assumptions. The composite organization reduces business risk associated with a severe security breach in the following ways:

- Breaches happen, and they sometimes go unnoticed. Forrester defines a breach as an incident resulting in the loss or compromise of data, accompanied by material remediation costs. According to Forrester's Cost Of A Cybersecurity Breach survey, an organization with 1,500 employees experiences an average of approximately three severe security breaches per year.[5]
- The SecOps team devotes half of its resources to severe vulnerability management and breach response. Each SecOps resource devotes 16 hours per breach to incident response and remediation, using manual cyber asset identification processes before ASM.
- With Cisco ASM, the composite organization reduces the number of hours spent on cyber asset identification by 85% in Year 1, 90% in Year 2, and 95% by the end of Year 3.
- The average fully burdened hourly rate per SecOps resource is $58.
- Forrester assumes a SecOps productivity recapture of 50% in Year 1, 65% in Year 2, and 75% in Year 3 to reflect the reality that some regained hours may not be used productively.
- Over the three-year period, the composite organization sees a reduction in SecOps hours to manually identify cyber assets during a severe breach, time savings valued at nearly $48,000.
- The composite achieves further cascading efficiencies across the organization's end users:
  - A serious breach impacts 80% of employees.
  - Forrester research revealed that the average downtime per employee per breach is 3.6 hours.[6]
  - The average fully burdened hourly rate per end-user employee is $42.
  - Forrester assumes a productivity recapture for each end user of 50% as regained hours are less likely to be used productively than the SecOps team.
  - With Cisco ASM, the composite organization further avoids an additional $816,000 in avoided end-user employee downtime.

- Finally, the organization avoids several risks to customers and brand reputation with Cisco ASM. Forrester values these additional costs of a material breach at over $817,000 by factoring in the following variables:
    - Regulatory fines; additive audit, legal, and security compliance costs; and response and notification to affected parties.
    - Customer compensation, lawsuits, and punitive damage; customer churn, the cost to acquire near customers, and lost revenue from loss of customers.
    - Lost revenue from system downtime and the cost to rebuild brand equity.[7]

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

- Forrester assumes a higher productivity capture for the SecOps team compared to general end users due to the closer impact on day-to-day job function.
- Forrester applies a steep risk adjustment to these security-related benefits to reflect the vast variability in organizations' digital footprints and respective experiences with security breaches.
- Organizations should consider a range of inputs to the downside risk of ungoverned assets in their security environment in a way that makes sense for their digital footprint. Inputs may include:
    - The number of hours spent in incident response and manual cyber asset identification prior to investing in Cisco ASM.
    - The level of SecOps expertise and querying training using Cisco ASM.
    - The fully burdened rate of SecOps FTEs.

Results. To account for these risks, Forrester adjusted this benefit downward by 25%, yielding a three-year, risk-adjusted total PV of $1.0 million.

Reduced Business Risk Associated With A Severe Security Breach					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	Number of severe security breaches per year	FORR TEI Research	3	3	3
B2	Number of SecOps resources dedicated to severe vulnerability management and breach response	Composite	10	10	10
B3	Number of hours of manual asset identification per breach before Cisco ASM	2 days per SecOps resource	16	16	16
B4	Percent reduction in hours of investigation and intervention per breach with Cisco ASM	Interviews	85%	90%	95%
B5	Average fully burdened hourly rate per SecOps resource	$121,000 / 2080 hours	$58	$58	$58
B6	SecOps productivity recapture rate	FORR TEI Assumption	50%	65%	75%
B7	Subtotal: Reduction in SecOps hours to manually identify cyber assets during a severe breach	(B1*B2*B3)*B4 *B5*B6	$11,832	$16,286	$19,836
B8	Total employees impacted by serious breach	80% of all employees	1,200	1,200	1,200
B9	Number of hours of downtime per employee per breach	FORR TEI Research	3.6	3.6	3.6
B10	Average fully burdened hourly rate for end user FTEs	$87,750 / 2080 hours	$42	$42	$42
B11	End user productivity recapture rate	FORR TEI Assumption	50%	50%	50%
B12	Subtotal: Avoided end-user employee downtime with Cisco ASM	B1*B8*B9*B10* B11	$272,160	$272,160	$272,160
B13	Avoided risk to customers and brand reputation with Cisco ASM per breach	FORR TEI Research	$90,800	$90,800	$90,800
B14	Subtotal: Avoided business risk with Cisco ASM	B1*B13	$272,400	$272,400	$272,400
Bt	Reduced business risk associated with a severe security breach	B7+B12+B14	$556,392	$560,846	$564,396
	Risk adjustment	↓25%			
Btr	Reduced business risk associated with a severe security breach (risk-adjusted)		$417,294	$420,635	$423,297
	Three-year total: $1,261,226			**Three-year present value: $1,045,019**	

SECOPS INCIDENT RESPONSE EFFICIENCIES FROM IMPROVED CYBER ASSET VISIBILITY

Evidence and data. Interviewees reported that Cisco ASM's cyber asset visibility significantly reduced the amount of time it took to manually identify cyber assets:

- The director of information security in the marketing company pointed to the ways in which Cisco ASM improved the organization's cyber asset visibility: "We can map application users to entities and can, for example, ask if a terminated employee is seen as active in any applications. We are able to point to the root cause and escalate it, and that's quite good for risk reduction."
- The information security manager noted that Cisco ASM provided their fintech organization with the ability to quickly make sense of its digital footprint when needed. The interviewee shared, "The data is formulated to make sense; my team can define and retrieve data quickly, while providing better visibility on spend and users."
- The director of digital security and resilience in the telecom industry was struck by the degree of visibility Cisco ASM provided into the digital environment: "Today, we have visibility into our environment and can see where the needle dropped. Seeing everything we have is an unexpected eye-opener."

"ASM' data automation answers complex questions around the context of assets, collects data in elegant way."

Information security manager, fintech

Modeling and assumptions. The composite organization experiences SecOps incident response efficiencies from improved cyber asset visibility in the following ways:

- The composite organization experiences an average of 200 minor to moderate security incidents requiring manual investigation of cyber assets per year.[8]
- The SecOps team fully dedicates four of its resources to this day-to-day incident response. Each SecOps resource devotes 8 hours to manually identify assets connected to an incident before Cisco ASM.
- With Cisco ASM, the composite organization experiences an 85% percent reduction of cyber asset investigation hours in Year 1, 90% in Year 2, and 95% by the end of Year 3.
- The average fully burdened hourly rate per SecOps resource is $58.
- Forrester assumes a SecOps productivity recapture of 75% to reflect the reality that some regained hours may not be used productively.

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

- The number of security incidents requiring manual investigation of cyber assets per year and duration of incident response timeframe.
- The number and hourly rate of SecOps resources dedicated to incident response

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $497,000.

SecOps Incident Response Efficiencies From Improved Cyber Asset Visibility					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Number of security incidents requiring manual investigation of cyber assets per year	FORR Research	200	200	200
C2	Number of SecOps resources dedicated to incident response	Composite	4	4	4
C3	Hours per SecOps resource to manually identify assets connected to an incident before Cisco ASM	Composite	8	8	8
C4	Percent reduction in hours of cyber asset investigation of per year with Cisco ASM	Interviews	85%	90%	95%
C5	Average fully burdened hourly rate per SecOps resource	$121,000 / 2080 hours	$58	$58	$58
C6	SecOps productivity recapture rate	FORR TEI Assumption	75%	75%	75%
Ct	SecOps incident response efficiencies from improved cyber asset visibility	(C1*C2*C3)*C4 *C5*C6	$236,640	$250,560	$264,480
	Risk adjustment	↓20%			
Ctr	SecOps incident response efficiencies from improved cyber asset visibility (risk-adjusted)		$189,312	$200,448	$211,584
	Three-year total: $601,344			**Three-year present value: $496,728**	

ENHANCED COMPLIANCE AND CERTIFICATION POSTURE

Evidence and data. Cisco ASM's instant insight into an organization's cyber assets conferred many benefits related to interviewees' certification experiences and compliance organizations:

- Three of the interviewees described positive impacts to their organizations related to compliance and certification time savings. In particular, the director of information security in the marketing industry described significant time savings to both SecOps and engineering when it came to certifications: "Previously, I would have to summon engineers from each team to provide information and scripts to show auditors. With Cisco ASM, I can run queries by myself to show lists of security groups with certain conditions without asking the engineer."
- The chief information security officer at the data management company noted that the Cisco ASM investment helped their organization achieve Federal Risk and Authorization Management Program (FedRAMP®) authorization, opening new business and revenue opportunities with the federal government.[9]
- For the director of digital security and resilience in the telecom industry, Cisco ASM's compliance functionality was so strong, their organization avoided purchasing an additional software solution that had been budgeted for compliance objectives.

Modeling and assumptions. The composite organization enhances its certification and compliance infrastructure in the following ways:

- With Cisco ASM, the composite organization avoids the annual cost of an additional compliance solution valued at $51,000.
- Cisco ASM also confers time savings to both SecOps and IT resources with its certification processes:
  - The composite organization conducts two certification processes per year. It fully dedicates two SecOps resources to managing certifications with each dedicating 520 hours to each certification process at an average fully burdened SecOps hourly rate of $58.
  - With Cisco ASM, these SecOps recourses reduce the number of hours dedicated to each certification by 75% in Year 1, 85% in Year 2, and 95% in Year 3.
  - In addition to the two managing SecOps resources, 10 IT resources were involved in certification efforts before the Cisco ASM investment.
  - Each IT resource dedicates at least 2 hours per certification at an average fully burdened IT hourly rate of $50.
  - With Cisco ASM, IT resources experience an 80% decrease in hours participating in certification processes, ramping to a 99% reduction by the end of Year 3.
  - Forrester assumes an IT productivity recapture of 85% to reflect the reality that some regained hours may not be used productively.
  - Total IT and SecOps certification time savings Cisco ASM confers are valued at over $266,000 over three years.
- Cisco ASM also facilitates the composite organization's successful application for FedRAMP Certification in Year 1, resulting in two new deals with the federal government valued at over $326,000 over three years after a 13% gross margin is considered.
- The composite organization attributes 50% of this new revenue to its investment in Cisco ASM.

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

- Organizations considering a separate compliance solution should consider how Cisco ASM aligns with compliance needs compared to other dedicated solutions.
- The number, frequency, and duration of certifications and the various compliance drivers to which an organization is beholden will directly impact this benefit. Organizations should consider the current and future compliance and certification drivers that make sense for their security and organizational growth goals.
- SecOps and IT time savings ramp up over a three-year period with a steeper ramp for IT, the role of which has diminished in the process.
- Forrester assumes a productivity recapture to reflect the reality that some regained hours may not be used productively.

Results. To account for these risks, Forrester adjusted this benefit downward by 25%, yielding a three-year, risk-adjusted total PV of $462,000.

Enhanced Compliance And Certification Posture

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Subtotal: Avoided cost of additional compliance solution	Interviews	$51,000	$51,000	$51,000
D2	Number of certifications per year	Interviews	2	2	2
D3	Number of SecOps resources managing certifications	Composite	2	2	2
D4	Average fully burdened hourly rate per SecOps resource	C5	$58	$58	$58
D5	Number of hours dedicated to each certification per SecOps resource before Cisco ASM	2,080 hours / 4	520	520	520
D6	Reduction in SecOps hours involved in certification	Composite	75%	85%	95%
D7	Number of IT resources involved in certification efforts before Cisco ASM	Composite	10	10	10
D8	Average Fully burdened hourly rate per IT FTE	C5	$50	$50	$50
D9	Number of hours per IT resource dedicated to each certification	Composite	2	2	2
D10	Reduction in IT hours involved in certification	Composite	80%	95%	99%
D11	Productivity capture	Assumption	85%	85%	85%
D12	Subtotal: IT And SecOps certification time savings	((D2*D3*D4*D5* D6)+(D2*D7*D8* D9 *D10))*D11	$78,268	$88,777	$99,100
D13	Revenue potential from FedRamp Certification with Cisco ASM	Two deals of $125k per year	$250,000	$250,000	$250,000
D14	Gross margin	Composite	13%	13%	13%
D15	New revenue resulting from FedRamp Certification	D13-(D13*D14)	$217,500	$217,500	$217,500
D16	Attribution to Cisco ASM	Composite	50%	50%	50%
D17	Subtotal: Increased incremental revenue from Fedramp certification with Cisco ASM	D15*D16	$108,750	$108,750	$108,750
Dt	Enhanced compliance and certification posture	D1+D12+D17	$238,018	$248,527	$258,850
	Risk adjustment	↓25%			
Dtr	Enhanced compliance and certification posture (risk-adjusted)		$178,514	$186,395	$194,138
	Three-year total: $559,046			**Three-year present value: $462,189**	

UNQUANTIFIED BENEFITS

Additional benefits that customers experienced but were not able to quantify include:

- **Time to value.** Several interviewees noted how Cisco ASM allowed their organizations to shorten the time to release revenue-generating features and updates and permitted organizations to accelerate mergers and acquisitions due to the transparency it conferred to an IT organization's balance sheet:
  - The director of digital security and resilience in the telecom industry described how the prior environment introduced delays in software releases due to the organization's software development security policies. With Cisco ASM, however, the interviewee shared that the organization fast-tracked software releases, accelerating the ability to cross-sell and upsell customers.
  - The information security manager in the fintech industry described what time to value with Cisco ASM meant for their organization: "It provides a consolidated view of the digital environment. With Cisco ASM, the time to value in visibility was immediate: within the first 30 days with integrations.
- **Customer experience.** Interviewees also noted that their organizations delivered on their brand promise better through more secure and consistent engagement with their customer and customer data.

FLEXIBILITY

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

- **Expanded organizational reach.** Most interviewees indicated that Cisco ASM was deployed to their organization in a phased, land-and-expand approach. As the solution demonstrated value towards its intended objectives, other areas of the organization were sensitized to the broad benefits conferred by its enhanced cyber-asset visibility. The director of digital security and resilience in the telecom organization stated, "Our head of operations was very impressed with the understanding we currently have of our cloud asset environment with Cisco ASM and wants to integrate it further to cover our legacy estate business units, so that we can have a single pane of glass."
- **Expanded functionality.** Not all organizations had implemented Cisco ASM's continuous security monitoring but noted it as a longer-term objective for the solutions. The information security manager in the fintech industry intended to leverage more of Cisco ASM's automation, stating: "Everything feeds into our data lake. With more streams of information from cyber assets, we can ask more complex questions about the current configuration."

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

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**
Etr	Cisco ASM subscription fees	$0	$244,800	$244,800	$244,800	$734,400	$608,781
Ftr	Internal deployment and administration costs	$282,854	$17,818	$12,250	$9,466	$322,387	$316,287
	Total costs (risk-adjusted)	$282,854	$262,618	$257,050	$254,266	$1,056,787	$925,068

CISCO ASM SUBSCRIPTION FEES

Evidence and data. Interviewees' Cisco ASM enterprise subscription fees were assessed as a function of:

- The total number of cyber assets included within the Cisco ASM digital infrastructure.
- The subscription tier selected, of which options include Base, Plus, and Premier.

Modeling and assumptions. Forrester assumes the following for the composite organization:

- The composite organization spends $204,000 annually on a Cisco ASM Premier subscription. This cost is based on the composite protecting 250,000 cyber assets.
- The composite organization's cyber footprint grows by 20% annually. To learn more about costs, speak to a Cisco ASM representative.

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

- The number of cyber assets protected. Organizations may have different taxonomies for assets and asset classes Cisco ASM protects.
- To accurately estimate the number of cyber assets included within Cisco ASM's CAASM solution, speak to a Cisco representative.

Results. To account for these risks, Forrester adjusted this cost upward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $609,000.

Cisco ASM Subscription Fees						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
Et	ASM subscription fees	Composite	$0	$204,000	$204,000	$204,000
	Risk adjustment	↑20%				
Etr	ASM subscription fees (risk-adjusted)		$0	$244,800	$244,800	$244,800
	Three-year total: $734,400			**Three-year present value: $608,781**		

INTERNAL DEPLOYMENT AND ADMINISTRATION COSTS

Evidence and data. In addition to fees paid to Cisco ASM, interviewees described the following internal costs related to the setup and ongoing management of the Cisco ASM platform:

- **Initial deployment costs**. Interviewees described an initial deployment process that required multiple resources mostly dedicated to deployment for approximately one quarter. This followed an initial proof-of-concept period in which Cisco ASM conducted a read-only scan of the customers' cyber footprints.
- **Ongoing administration costs**. Ongoing management costs were minimal. The director of information security in the marketing industry indicated that their organization maintained the Cisco ASM platform with just one resource checking in once per month

Modeling and assumptions. The composite organization deploys and manages the Cisco ASM platform as follows:

- Three SecOps resources are 80% dedicated to deployment for three months.
- All 20 SecOps resources receive two days of initial training on Cisco ASM upon deployment. These resources receive ongoing training and enrichment throughout the investment, though the total number of hours of ongoing training ramps down over the three-year period.
- One resource is dedicated to the ongoing administration of the Cisco ASM platform, allocating one hour a month to maintenance.

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

- The number and composition of cyber assets and asset classes Cisco ASM protects.
- The organization's prior environment and cloud journey.
- An individual resource's experience with querying languages. Interviewees noted that resources that were more experienced with querying languages had a faster onboarding time and higher confidence level when using Cisco ASM.

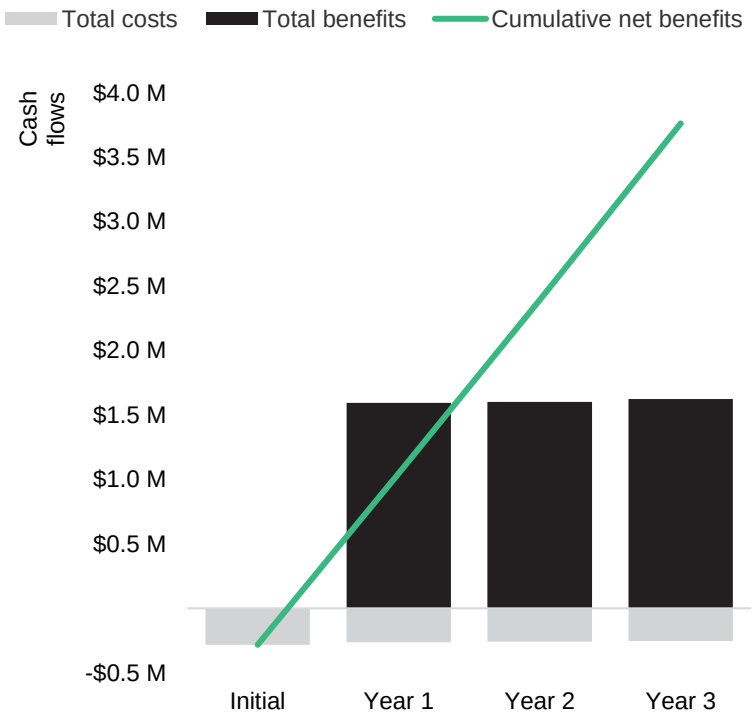
Results. To account for these risks, Forrester adjusted this cost upward by 20%, yielding a three-year, risk-adjusted total PV of $316,000.

Internal Deployment And Administration Costs						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
F1	Hourly rate per SecOps resource	$121,000 / 2,080 hours	$58	$58	$58	$58
F2	Number of SecOps resources dedicated to deployment	Composite	3	0	0	0
F3	Total deployment hours	80% for three months	1,248	0	0	0
F4	Number of SecOps resources trained on Cisco ASM	Composite	20	20	20	20
F5	Average number of training hours per SecOps resource	Assumption	16	8	4	2
F6	Total initial internal costs	(F1*F2*F3)+ (F1*F4*F5)	$235,712	$9,280	$4,640	$2,320
F7	Number of SecOps resources dedicated to Cisco ASM administration	Interviews	0	1	1	1
F8	Total administration hours	One hour per month	0	96	96	96
F9	Total Cisco ASM administration costs	F1*F7*F8	$0	$5,568	$5,568	$5,568
Ft	Internal deployment and administration costs	F6+F9	$235,712	$14,848	$10,208	$7,888
	Risk adjustment	↑20%				
Ftr	Internal deployment and administration costs (risk-adjusted)	F6*F7*F8)+ (F6*Ft*	$282,854	$17,818	$12,250	$9,466
	Three-year total: $322,387			**Three-year present value: $316,287**		

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	($282,854)	($262,618)	($257,050)	($254,266)	($1,056,787)	($925,068)
Total benefits	$0	$1,593,394	$1,602,422	$1,623,546	$4,819,362	$3,992,650
Net benefits	($282,854)	$1,330,776	$1,345,372	$1,369,281	$3,762,575	$3,067,582
ROI						332%
Payback period (months)						<6

Appendix A: Total Economic Impact

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

TOTAL ECONOMIC IMPACT APPROACH

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

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

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

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

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

PRESENT VALUE (PV)

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

NET PRESENT VALUE (NPV)

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

RETURN ON INVESTMENT (ROI)

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

DISCOUNT RATE

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

PAYBACK PERIOD

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

Appendix B: Endnotes

[1] Source: “Top Recommendations For Your Security Program, 2021,” Forrester Research, Inc., August 2, 2021.
[2] According to Forrester’s June 2022 article, “The ASM Landscape Is Shifting Under Our Feet — As Are The Acronyms,” cyber asset ASM (CAASM) is a tool or capability that delivers unified visibility across all known assets (internal, external, cloud, on-premises) for better identification of vulnerabilities and insufficient security controls.
[3] 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.
[4] Source: “Cost of a Data Breach 2022,” Ponemon Institute and IBM, July 2022.
[5] Source: Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q4 2020.
[6] Ibid.
[7] Ibid.
[8] Ibid.
[9] The Federal Risk and Authorization Management Program (FedRAMP®) was established in 2011 to provide a cost-effective, risk-based approach for the adoption and use of cloud services by the federal government. FedRAMP empowers agencies to use modern cloud technologies with an emphasis on security and protection of federal information.


FORRESTER®