FORRESTER®

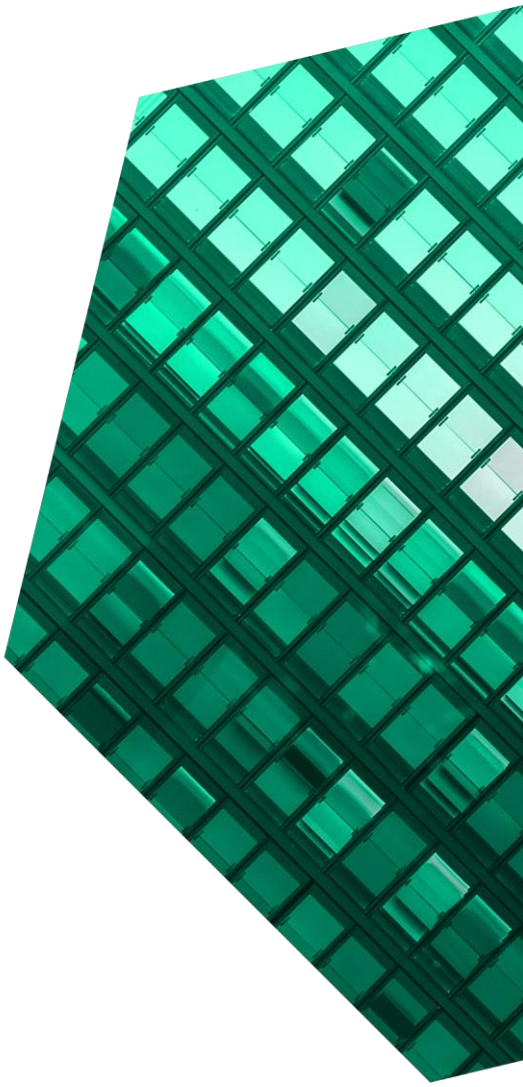
The Total Economic Impact™ Of ServiceNow Security Operations

Cost Savings And Business Benefits Enabled By Security Incident Response And Vulnerability Response

October 2020

Table Of Contents

Consulting Team: Sri Prakash Gupta
Henry Huang



Executive Summary

With the ever-growing complexity and volume of cyberattacks, organizations will become even more vulnerable to security threats. All companies — big or small — have critical assets to protect, including customer data that will cause business damage or market setback if violated. Therefore, organizations need security orchestration tools that can connect security and IT teams to respond faster and more efficiently to security incidents and vulnerabilities and to get a definitive view of their security posture.

ServiceNow commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying ServiceNow's Security Operations. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of investing in ServiceNow to improve security incident and vulnerability response processes for their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed three customers with experience of using Security Operations (consisting of Security Incident Response and Vulnerability Response). For the purposes of this study, Forrester aggregated the experiences of the interviewed customers and combined the results into a single composite organization.

The interviewees said that prior to investing in Service Now, their organizations spent several person-hours gathering security event and incident data from multiple sources for each incident, prioritizing and grouping them by criticality, identifying the locations of vulnerable infrastructure assets, and working across cross-functional teams to remediate issues. However, prior attempts yielded limited success, leaving customers exposed to bigger security risks and vulnerabilities, and unable to scale as the workloads continued to grow.

KEY STATISTICS

Return on investment (ROI)
238%

Net present value (NPV)
$4.4 million

PAYBACK
6 months

ServiceNow Security Operations helped these customers:

- Automate manually intensive security incident and vulnerability response workflows.
- Consolidate and prioritize alerts from multiple security tools onto a single platform.
- Quickly map security incidents and vulnerabilities to IT infrastructure for better impact analysis and accurate assignment.
- Prioritize and resolve the most critical security incidents and vulnerabilities first.

KEY FINDINGS

Quantified benefits. The composite organization experiences the following risk-adjusted present value (PV) quantified benefits over three years:

- **Increased efficiency of prioritization and resolution of security incidents, resulting in $4.9 million in benefits.** The composite organization sees a 40% improvement in the efficiency with which frontline security analysts handle tier 1 security incidents. It also realizes a 60% efficiency increase related to managing tier 2 and higher security incidents that require coordination across multiple IT and security resources. These efficiencies are gained by automating workflows that span security and IT, prioritizing security incidents based on business criticality, and tracking incidents and assigning tasks using a single platform
- **Improved vulnerability management and response times, resulting in $488,311 in benefits.** The interviewed customers now conduct routine weekly scans to identify, classify, and prioritize vulnerabilities in their environments. On average, they identify 30,000 vulnerabilities each week. Previously, they resorted to manually intensive processes to categorize vulnerabilities and have them analyzed by their security teams. ServiceNow Security Operations allows these customers to automatically pull all the data from a vulnerability scan into the solution and then apply rules and logic to identify critical vulnerabilities that need immediate action (for instance, map vulnerabilities and prioritize based on risk score, eliminate manual tasks / disjointed processes with automated workflows). It also links these vulnerabilities to existing assets to determine business relevance and impact. The composite organization sees a 70% improvement in the way in which it identifies and prioritizes vulnerabilities and assesses the impact on existing assets. In addition, it realizes a 30% improvement in vulnerability response times by speeding the application of patches and other remediation efforts with automated workflows.

> "We had multiple security tools. However, our inability to address vulnerabilities in a rapid fashion remained a huge concern for our organization. We wanted to get rid of manual process and automate the identification and remediation process. ServiceNow provides faster vulnerability response management, as well as additional context to fine tune the security posture."
>
> *Manager of cybersecurity, utilities*

> "ServiceNow provided 24x7 visibility into our security environment, which was much needed for our global business operations. It helped us to reduce the security response time and significantly improve vulnerability management."
>
> *Chief information security officer, financial services*

- **Realized opex savings by eliminating legacy security tools, resulting in $283,997 in benefits.** The composite organization is able to discontinue software licenses and support contracts for legacy tools it used to manage security incident response processes. Forrester estimates these tools cost the organization $200,000 each year and that it would be able to discontinue and realize these savings beginning in Year 2.
- **Improved security governance with real-time visibility and reporting, resulting in $430,862 in benefits**. The composite organization realizes labor and time savings with unified dashboards,

workflow automation, and easy reporting. It helps security and IT teams respond faster and more efficiently to incidents and vulnerabilities, and make use of time for improvements and innovation. The composite organization would have needed to have added 1.5 FTEs to produce real-time reports with the manually driven legacy environment and to match the reporting/visualization capabilities of ServiceNow.

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

- **Improved IT productivity.** Previously, the composite organization's IT resources assisted the security team by pulling data from multiple sources to identify security incidents and vulnerabilities. ServiceNow Security Operations provides the organization with a single platform to consolidate and integrate data across its environment and to route tasks to the right IT and security teams using automated workflows.
- **Better visibility into security posture.** Intuitive real-time dashboards allow security teams and executives to understand the composite organization's current security posture. These dashboards make it easy to track in-progress tasks, critical metrics, and KPIs to make business decisions and mobilize resources around the highest-priority security incidents.
- **Increased collaboration.** ServiceNow Security Operations lets both IT and security resources assign tasks and collaborate in real time using a common system. Better collaboration improves security incident and vulnerability response times and accuracy.

Costs. The composite organization experiences implementation costs and annual license fees as highlighted below. Risk-adjusted PV costs include:

- **ServiceNow Security Operations deployment, license, and professional services costs of $1.2 million.** The composite organization incurs an up-front initial deployment cost and annual license fee for ServiceNow Security Operations. It hires a professional services partner to help with the implementation, as well as with the process and system design of ServiceNow Security Operations within its environment. These costs are incurred on number of devices and its configuration. This gives it access to the ServiceNow security incident response application, vulnerability response application, threat intelligence applications, performance analytics, dashboards, and communication tools. The annual license fee also covers routine upgrades and maintenance
- **Due diligence and ongoing management costs of $589,169.** The composite organization's implementation is straightforward, and it requires minimal resource time for planning and testing. The organization dedicates internal support resources including project managers, security analysts, and IT staff members to gather requirements and collect the data required to transition to ServiceNow Security Operations. It also dedicates 75% of the time of two FTEs to support and administer the ServiceNow solution.

Annual license and implementation costs will vary depending on the size and scope of implementation. Readers are encouraged to reach out to ServiceNow for a more tailored quote based on specific requirements and planned business outcomes. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $1,832,013.

The customer interviews and financial analysis found that the composite organization would experience benefits of $6,199,517 over three years versus costs of $1,832,013, adding up to a net present value (NPV) of $4,367,504 and an ROI of 238%.

ROI
238%

BENEFITS PV
$6.2 million

NPV
$4.4 million

PAYBACK
6 months

Financial Summary

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 Security Operations.

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 the Security Operations can have on an organization.

DUE DILIGENCE

Interviewed ServiceNow stakeholders and Forrester analysts to gather data relative to the ServiceNow Security Operations products.

CUSTOMER INTERVIEWS

Interviewed three decision-makers at organizations using ServiceNow Security Operations to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

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

FINANCIAL MODEL FRAMEWORK

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

CASE STUDY

Employed four fundamental elements of TEI in modeling 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 ServiceNow Security Operations Customer Journey

Drivers leading to the Security Operations investment

Interviewed Organizations

Industry	Region	Interviewee	Total Security Operations Employees	Total Employees
Financial services	Headquartered in Europe	Chief information security risk officer (CISO)	150	40,000
Manufacturing	Headquartered in Europe	Manager of cyberdefense operations team	25	25,000
Utilities	Headquartered in North America	Manager of cybersecurity risk management	35	6,500

KEY CHALLENGES

Prior to investing in ServiceNow Security Operations, the composite organization struggled with common challenges, including:

- **Manual processes hindered security incident and vulnerability response times.** The composite organization's security team was inundated with alerts and information from multiple tools. Each incident required manual effort to determine the risk level, business context, and priority. Once the team established the criticality and priority of a security incident, coordinating a response across IT and security and tracking it through to resolution involved inefficient manual processes.
- **Limited visibility into security posture.** The composite organization had a number of security products that monitored its environment and alerted it to potential security threats and risks. Security analysts struggled to consolidate data and metrics across these multiple products to provide the management team with real-time visibility into the security posture of the organization.
- **High costs associated with manual security response.** The composite organization previously spent days assessing each security incident or vulnerability and then coordinating a remediation plan. In addition, frontline security analysts were burdened with working on incidents that could easily be addressed through automation.

> "With ServiceNow Security Operations, transparency and reporting became available instantly to everyone in management. Whereas before, it would take days or even weeks to produce any type of insight."
>
> *Manager of cyberdefense, manufacturing*

SOLUTION REQUIREMENTS/INVESTMENT OBJECTIVES

The interviewees said their organizations searched for a solution that could:

- **Improve security incident response times.** The composite organization increases the efficiency with which it manages both tier 1 security incidents as well as the more complex tier 2 and higher incidents after implementing ServiceNow.

- **Improve vulnerability management process.** The composite organization can automatically pull in data from vulnerability scans into ServiceNow Security Operations, group vulnerabilities by criticality, and automatically link a vulnerability to an enterprise asset.
- **Offer intuitive dashboards and reporting to deliver real-time visibility into the security posture.** All levels within the composite organization can track the status of its security and risk profile at any time.
- **Increase communication and coordination between IT, security, and risk teams.** A single platform lets the teams communicate, track, and coordinate security incident and vulnerability response efforts more effectively.
- **Increase automation.** The composite organization can now automate basic tasks, route incidents and vulnerabilities to appropriate resources, and save audit trails. This leads to improved security operations productivity.
- **Realize opex savings from a single enterprise security response solution.** The composite organization discontinues its legacy tools, which results in additional savings.

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 three companies that Forrester interviewed and is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

- The composite organization has global operations across multiple countries.
- The composite organization is a large enterprise with more than 10,000 employees and $2 billion in annual revenue.
- The composite organization has been using ServiceNow Security Operations for security incident response and vulnerability response management for more than two years. It has approximately 65 security operations FTEs (analysts and security engineers).

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 efficiency of security incident response process	$1,953,720	$2,012,332	$2,072,571	$6,038,623	$4,996,347
Btr	Improved vulnerability management and response times	$190,944	$196,672	$202,560	$590,176	$488,311
Ctr	Opex savings from discontinuation of legacy tools	$0	$180,000	$180,000	$360,000	$283,997
Dtr	Real-time visualization — cost savings for reporting	$168,480	$173,534	$178,729	$520,744	$430,862
	Total benefits (risk-adjusted)	$2,313,144	$2,562,538	$2,633,860	$7,509,543	$6,199,517

INCREASED EFFICIENCY OF SECURITY INCIDENT RESPONSE PROCESS

According to the interviewed customers, the implementation of ServiceNow Security Operations improved the efficiency of identifying, prioritizing, and resolving security incidents. ServiceNow Security Operations is a security orchestration, automation, and response (SOAR) solution that integrates with other security tools to consolidate all security incidents in one place and orchestrate investigations and response.

Access to business and threat context allows security analysts to quickly triage incidents and prioritize the most critical issues. Once they identify and classify a security incident, a number of next actions are available: They can initiate predefined automatic responses to analyze, contain, or resolve incidents, route others to frontline security analysts, and send more complex incidents to specialized teams to respond. All open threats are tracked using the ServiceNow solution, enabling quicker coordination around responding to and remediating security incidents.

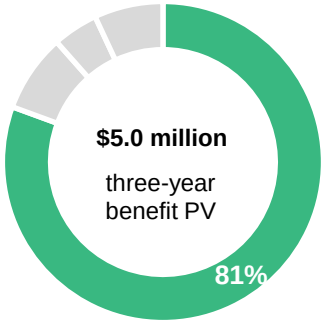
Modeling and assumptions. The composite organization deals with 900 qualified security incidents each month that require responses. On average, 95% of these incidents are classified as tier 1 or less complex incidents that frontline security analysts can handle and resolve. Prior to using ServiceNow, the composite organization's frontline analysts spent approximately 2.5 hours responding to each tier 1 incident. By implementing ServiceNow Security Operations, the organization estimates that response times for these incidents improves by 40%. Automating responses to recurring incidents allows security analysts to focus on investigating and remediating more complex threats.

Resolving the remaining 5% of security incidents requires greater coordination across IT and security teams. The composite organization realizes a 60% improvement in response times for these security incidents. ServiceNow Security Operations functionality allows organizations to easily assign tasks, hold teams accountable, and coordinate responses across security and IT teams. Out-of-the-box features of the ServiceNow solution help with prioritizing and routing security incidents and tasks to the right resources using automated workflows.

Risks. Forrester considered the following potential risks when assigning a risk adjustment:

- The number of security threats affecting an organization.
- The types of security threats affecting an organization.
- The skill sets of IT and security resources.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $4,996,347.



Increased efficiency of security incident response process: 81% of total benefits

Increased Efficiency Of Security Incident Response Process

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
A1	Average number of qualified monthly security incidents	Interviews	900	900	900
A2	Average annual number of qualified security incidents	A1*12	10,800	10,800	10,800
A3	Percentage of qualified security incidents that are tier 1 (can be managed by front line security analysts)	Interviews	95.0%	95.0%	95.0%
A4	Percentage of qualified security incidents that are tier 2 and above (need other teams' involvement to remediate)	Interviews	5.0%	5.0%	5.0%
A5	Number of annual tier 1 security incidents per year	A2*A3	10,260	10,260	10,260
A6	Average manhours to remediate tier 1 security incidents prior to ServiceNow	Interviews	2.5	2.5	2.5
A7	Improved efficiency to manage tier 1 security incidents after implementing ServiceNow	Interviews	40.0%	40.0%	40.0%
A8	Number of tier 2 and higher security incidents per year	A2*A4	540	540	540
A9	Average manhours to remediate tier 2 security incidents prior to ServiceNow	Interviews	80.0	80.0	80.0
A10	Improved efficiency to manage tier 2 security incidents after implementing ServiceNow	Interviews	60.0%	60.0%	60.0%
A11	Average hourly fully burdened rate of security FTE	Industry average. Assumption (incl. 3% YoY growth)	$60.00	$61.80	$63.65
At	Increased efficiency of security incident response process	(A5*A6*A7*A11)+(A8*A9*A10*A11)	$2,170,800	$2,235,924	$2,302,857
	Risk adjustment	↓10%			
Atr	Increased efficiency of security incident response process (risk-adjusted)		$1,953,720	$2,012,332	$2,072,571
	Three-year total: $6,038,623			**Three-year present value: $4,996,347**	

IMPROVED VULNERABILITY MANAGEMENT AND RESPONSE TIMES

ServiceNow Vulnerability Response provides risk-based vulnerability management (RBVM) to help organizations respond faster and more efficiently to vulnerabilities, connect security and IT teams, and provide real-time visibility.

Vulnerability Response management provides a comprehensive view of all vulnerabilities affecting a given asset or service through integration with ServiceNow Configuration Management Database (CMDB), as well as the current state of all vulnerabilities affecting the organization. The composite organization uses vulnerability scanning tools to identify vulnerabilities, risk assessment, and asset value management for contextualization and prioritization across its infrastructure.

Modeling and assumptions. On average, each weekly scan generates a list of 30,000 vulnerabilities that the composite organization may be susceptible to. Prior to using ServiceNow Security Operations, the organization spent 80 person-hours per week across its IT and security teams to classify and prioritize vulnerabilities and to find assets that could be impacted. Previously, this effort primarily involved manual processes and analysis. With ServiceNow Security Operations, these vulnerabilities get immediately imported into the solution. They are prioritized by criticality and linked to existing infrastructure assets. The composite organization estimates a 70% improvement to this vulnerability management process.

Improved Vulnerability Management And Response Times

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
B1	Average number of vulnerabilities identified per weekly scan	Interviews	30,000	30,000	30,000
B2	Number of weeks	52 weeks	52	52	52
B3	Average number of person-hours to classify, prioritize, and link vulnerabilities to assets, per 30,000 vulnerabilities scanned (prior to ServiceNow)	Interviews	80	80	80
B4	Improvement in classifying, prioritizing, and linking vulnerabilities to assets, per 30,000 vulnerabilities scanned (with ServiceNow)	Interviews	70.0%	70.0%	70.0%
B5	Average number of person-hours spent to remediate vulnerabilities per weekly scan	Interviews	40	40	40
B6	Improved efficiency to remediate vulnerabilities identified through weekly scan	Interviews	30.0%	30.0%	30.0%
B7	Average hourly fully burdened rate of FTE	Industry average (including 3% YoY growth)	$60.00	$61.80	$63.65
Bt	Improved vulnerability management and response times	{(B1*B2*B3*B4*B7)+(B1*B2*B5*B6*B7)}/B1	$212,160	$218,525	$225,066
	Risk adjustment	↓10%			
Btr	Improved vulnerability management and response times (risk-adjusted)		$190,944	$196,672	$202,560
	Three-year total: $590,176			**Three-year present value: $488,311**	

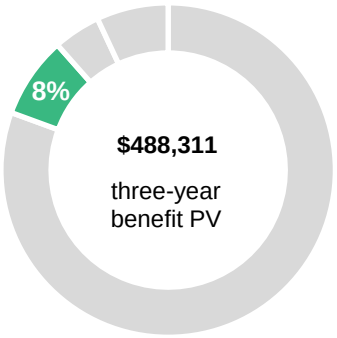
Once the organization identifies vulnerabilities, it develops response plans that include initiating the necessary software upgrades, activating controls, mitigation, and applying patches to remediate these threats.

The workflow automation and alerts functionality within ServiceNow encourages authorized administrators to adhere to the response plan and it speeds up processes. Prior to using ServiceNow Security Operations, this process took 40 person-hours per weekly vulnerability scan. The composite organization estimates a 30% improvement in vulnerability response times with ServiceNow Security Operations.

Risks. To be conservative, Forrester considered the following potential risks when assigning a risk adjustment:

- The number of vulnerabilities and subsequent remediation efforts affecting an organization.
- The type of vulnerabilities affecting an organization.
- The skillsets of IT and security resources

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $488,311.



Improved vulnerability management and response times: 8% of total benefits

OPEX SAVINGS FROM DISCONTINUATION OF LEGACY TOOLS

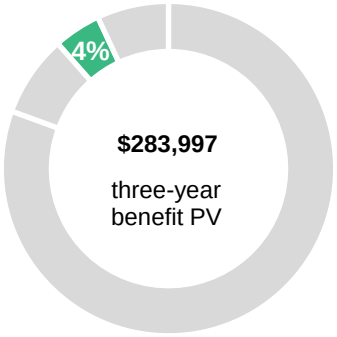
With the investment in ServiceNow Security Operations, the composite organization is able to discontinue its legacy tools. Initially, it runs both tools in parallel.

Modeling and assumptions. After the first year, when all the data and integrations with ServiceNow are in place, the organization discontinues the use of its legacy tools. It is estimated to save the organization $200,000 in Year 2 and Year 3.

Risks. Opex savings from discontinued tools could vary based on following factors:

- The number and types of legacy tools that are discontinued.
- The contract terms and agreements of legacy tools that are discontinued.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $283,997.



Opex savings from discontinuation of legacy tools:4% of total benefits

Opex Savings From Discontinuation Of Legacy Tools					
Ref.	**Metric**	**Calculation**	**Year 1**	**Year 2**	**Year 3**
C1	Opex savings related to discontinuation of security incident management tool	Interviews	$0	$200,000	$200,000
Ct	Opex savings from discontinuation of legacy tools	C1	$0	$200,000	$200,000
	Risk adjustment	↓10%			
Ctr	Opex savings from discontinuation of legacy tools (risk-adjusted)		$0	$180,000	$180,000
	Three-year total: $360,000			**Three-year present value: $283,997**	

REAL-TIME VISUALIZATION — COST SAVINGS FOR REPORTING

The implementation of ServiceNow SecOps results in labor and time savings for the composite organization in the following areas:

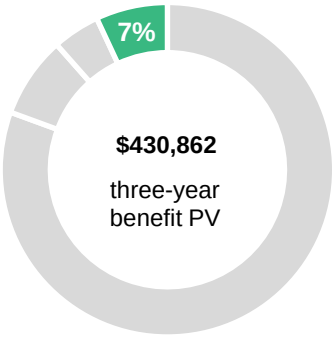
- Unified dashboard that consolidates data from all components and enables capabilities to create custom dashboards and set thresholds and targets for monitoring security operation processes.
- Easy visualization of enterprise security risk posture, vulnerabilities, threats, and technology stack capabilities.

Modeling and assumptions. The composite organization would have needed to have added 1.5 FTEs to produce real-time reports with the manually driven legacy environment and to match the current reporting/visualization capabilities of ServiceNow. Forrester used a fully loaded hourly cost of $60 for the one security analyst FTE with 3% year-over-year (YoY) increase for Year 2 and Year 3.

Risks. The average cost of the resource could vary, so there's some uncertainty as to the benefit amount.

Real-Time Visualization — Cost Savings For Reporting					
Ref.	**Metric**	**Calculation**	**Year 1**	**Year 2**	**Year 3**
D1	Resource savings (e.g., dashboards/reporting/visualization)	Interviews	1.5	1.5	1.5
D2	Average hourly fully burdened rate of FTE	Industry average (including 3% YoY growth)	$60.00	$61.80	$63.65
Dt	Real-time visualization — cost savings for reporting	D1*(D2*2,080 hours)	$187,200	$192,816	$198,588
	Risk adjustment	↓10%			
Dtr	Real-time visualization — cost savings for reporting (risk-adjusted)		$168,480	$173,534	$178,729
	Three-year total: $520,744			**Three-year present value: $430,862**	

To account for above risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $430,862.



Real-time visualization — cost savings for reporting: 7% of total benefits

UNQUANTIFIED BENEFITS

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

- **Improved IT productivity.** Previously, the composite organization's IT resources assisted the security team by pulling data from multiple sources to identify security incidents and vulnerabilities. ServiceNow Security Operations provides the organization with a single platform to consolidate and integrate data across its environment and to route tasks to the right IT and security teams using automated workflows.
- **Better visibility into security posture.** Intuitive, real-time dashboards allow security teams and executives to understand the organization's current security posture. These dashboards make it easy to track in-progress tasks, critical metrics, and KPIs to make business decisions and mobilize resources around the highest priority security incidents.
- **Increased collaboration.** ServiceNow Security Operations lets both IT and security resources assign tasks and collaborate in real time using a common system with a consistent user experience and data set. Better collaboration improves security incident and vulnerability response times.

FLEXIBILTY

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

- **Integrability and scalability.** Out-of-the-box configuration capabilities and features allow organizations to integrate ServiceNow Security Operations with other security solutions and to configure the system to meet their specific needs. Organizations can quickly add and scale users or modify forms and data tables. The underlying platform and optimized workflows let organizations easily leverage other ServiceNow cloud services (for IT service management, integrated risk management, IT operations management, and HR service delivery) and use prebuilt spokes to access third-party application and infrastructure data sources such as identity and access management. The platform's low code and no code developer tools also help organizations rapidly build other business applications with reusable components.
- **Governance.** ServiceNow provides enterprise-grade logging of all actions, alerts, and changes, and organizations can use it to reduce effort and improve efficacy of governance related to auditability, policy-driven controls, and adherence to organizational standards and guidelines. Integration with ServiceNow governance risk and compliance (GRC)/integrated risk management (IRM) products can notify risk teams of new vulnerabilities and security incidents that affect risk posture.

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	ServiceNow Security Operations deployment, license, and professional services costs	$381,150	$346,500	$346,500	$346,500	$1,420,650	$1,242,844
Etr	Due diligence and ongoing management costs	$86,486	$196,560	$202,457	$208,531	$694,034	$589,169
	Total costs (risk adjusted)	$467,636	$543,060	$548,957	$555,031	$2,114,684	$1,832,013

SERVICENOW SECURITY OPERATIONS DEPLOYMENT, LICENSE, AND PROFESSIONAL SERVICES COSTS

Fees for Security Operations include platform deployment, customization, and license costs. The model uses $330,000 as up-front platform deployment and professional services fees. License costs for Security Operations are $330,000 per year.

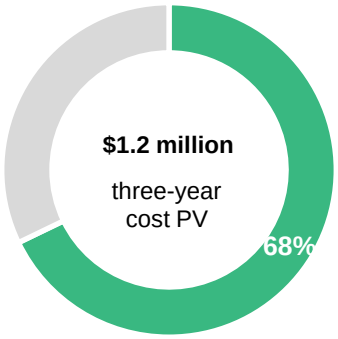
Also, Forrester included $33,000 (which is 10% of the initial cost) as a professional service partner cost to help through the implementation journey. This includes installation, post-installation support, configuration setup, analysis and modeling, and testing.

Please note that costs are based on high-level estimates and do not constitute a quote. For a more detailed business case, please request a tailored quote directly from ServiceNow.

Risks. Implementation costs will vary depending on:

- The number of devices and configuration.
- The size and scope of implementation.

To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1,242,844.



ServiceNow Security Operations deployment, license, and professional services costs: 68% of total costs

ServiceNow Security Operations Deployment, License, And Professional Services Costs						
Ref.	**Metric**	**Calculation**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	ServiceNow Security Operations initial deployment and license costs	Provided by ServiceNow	$330,000	$330,000	$330,000	$330,000
E2	Professional services	10% of Initial cost	$33,000			
Et	ServiceNow Security Operations deployment, license, and professional services costs	E1+E2	$363,000	$330,000	$330,000	$330,000
	Risk adjustment	↑5%				
Etr	ServiceNow Security Operations deployment, license, and professional services costs (risk-adjusted)		$381,150	$346,500	$346,500	$346,500
Three-year total: $1,420,650				**Three-year present value: $1,242,844**		

DUE DILIGENCE AND ONGOING MANAGEMENT COSTS

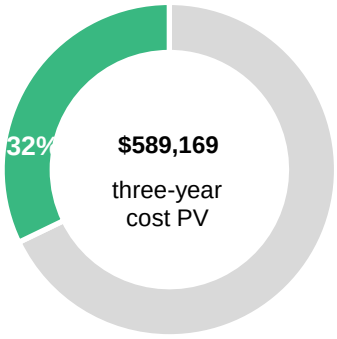
For the composite organization, ServiceNow deployment is straightforward, and the required resource time is minimal. Successful deployments require resource hours at project feasibility and an implementation/testing stage over a few weeks. Specific due diligence and implementation tasks include:

- Spending time with ServiceNow to understand how Security Operations could improve security postures and mitigate vulnerabilities faster.
- Working with ServiceNow on requirements, software setup, network and environment integration, configuration, testing, and customization.
- Once the solution is up and running, the organization dedicates 75% of two FTEs' time to oversee, manage, and monitor the ServiceNow deployment.

Risks. Costs might will vary depending on:

- The resource salary/costs.
- The size and scope of implementation.

To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $589,169.



Due diligence and ongoing management costs: 32% of total costs

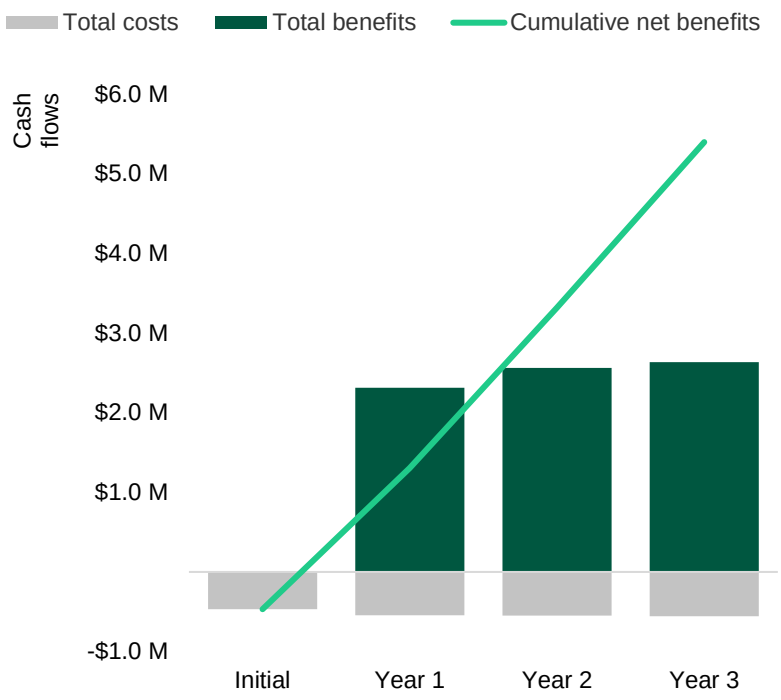
Due Diligence And Ongoing Management Costs

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
F1	Number of IT and security FTEs	Interviews	8	2	2	2
F2	Percentage of FTE time required during planning and implementation	Interviews	33%	0%	0%	0%
F3	Percentage of FTE time required for ongoing management and support	Interviews	0%	75%	75%	75%
F4	Number of months	Interviews	3	12	12	12
F5	Monthly burdened rate of FTE	Industry average (including 3% YoY growth)	$10,400.00	$10,400.00	$10,712.00	$11,033.36
Ft	Due diligence and ongoing management costs	(F1*F2*F4*F5)+ (F1*F3*F4*F5)	$82,368	$187,200	$192,816	$198,600
	Risk adjustment	↑5%				
Ftr	Due diligence and ongoing management costs (risk-adjusted)		$86,486	$196,560	$202,457	$208,531
	Three-year total: $694,034			**Three-year present value: $589,169**		

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	($467,636)	($543,060)	($548,957)	($555,031)	($2,114,684)	($1,832,013)
Total benefits	$0	$2,313,144	$2,562,538	$2,633,860	$7,509,543	$6,199,517
Net benefits	($467,636)	$1,770,084	$2,013,582	$2,078,830	$5,394,859	$4,367,504
ROI						238%
Payback						<6 months

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."

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.


FORRESTER®