The Total Economic Impact™ Of Skybox Security Posture Management Platform

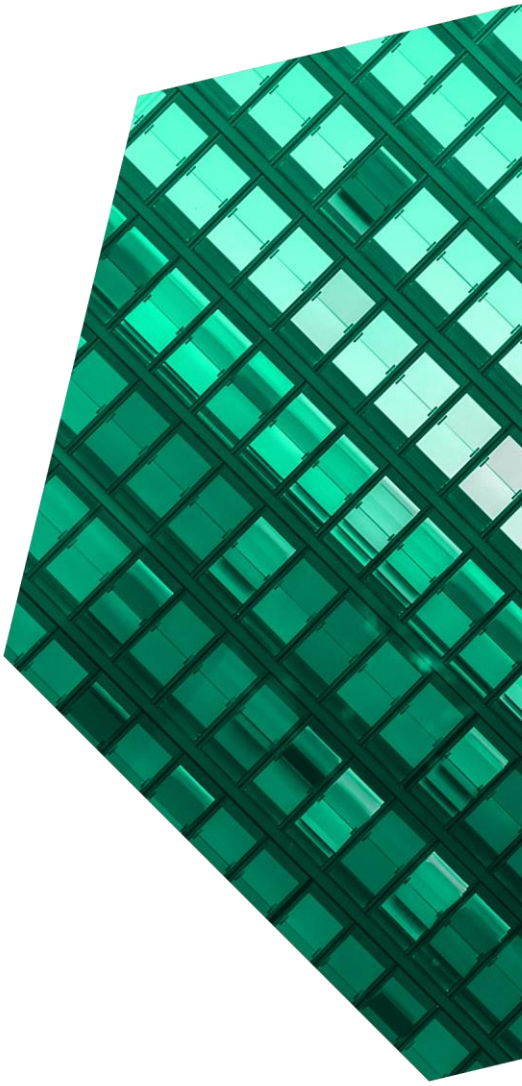
Cost Savings And Business Benefits Enabled By Skybox Security Posture Management Platform

SEPTEMBER 2022

A FORRESTER TOTAL ECONOMIC IMPACT™ STUDY COMMISSIONED BY SKYBOX

Table Of Contents

Consulting Team: Alexander Parsons



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

Keeping assets and data secure has become more difficult for companies operating complex internal networks on a global scale. These challenges are compounded by ever-increasing pressures from compliance and regulatory requirements. Implementing Skybox's suite of products enables companies to discover, prioritize, remediate, and report exposed vulnerabilities as well as improve security policy management while driving efficiencies and decreasing operational downtime.

Skybox Security Posture Management Platform (the Skybox Platform) combines infrastructure context with threat intelligence to unlock visibility into the attack surface spanning information technology (IT), hybrid cloud, and operational technology (OT) environments. This allows security and risk teams to comply with corporate and regulatory policies, reduce misconfigurations, securely automate changes, and prioritize remediation of the riskiest vulnerabilities. These capabilities help customers create a global framework across their network to decrease risk from external and internal sources while improving productivity for end-to-end security, audit, and compliance processes.

Reduced risk of a significant data breach

55%

KEY STATISTICS

Return on investment (ROI)	Net present value (NPV)
142%	**$2.21M**

Skybox commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying the Skybox Platform. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of the Skybox Platform on their organizations. To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four representatives from customers of Skybox with experience using the Skybox Platform. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization that is a global conglomerate with over $2 billion revenue that maintains 30,000 assets internally across its 15,000-employee base. The composite organization is representative of the interviewees' four different organizations and is used to present the financial analysis in the study.

Prior to using the Skybox Platform, interviewees noted that their organizations depended on a combination of outdated third-party solutions, spreadsheets, and homegrown tools that they pieced together to meet their security visualization needs. Without a centralized tool to help prioritize remediations and better understand their holistic IT and OT environments, companies faced internal and external threats while incurring inflated costs for compliance and security operations teams.

After investment in the Skybox Platform, the interviewees were quickly able to remediate the riskiest vulnerabilities and improve network segmentation to reduce risk more comprehensively and with more precision than with previous solutions. Organizations created cross-functional governance processes to prioritize work across teams supporting IT and OT, improving efficiencies. Expanded visibility and end-to-end audit processes reduced external audit costs while improving internal operational efficiencies.

> **"Skybox had the technical background [and were working with] some of the other vendors that we were already establishing relationships with. It makes it much easier when you are part of that ecosystem and they're already tried and tested."**
>
> *Director of cybersecurity, manufacturing*

KEY FINDINGS

The representative interviews and financial analysis found that a composite organization experiences benefits of $3.78 million over three years versus costs of $1.56 million, adding up to a net present value (NPV) of $2.21 million and an ROI of 142%.

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

- **A 55% reduction in the risk of a significant data breach.** By leveraging Skybox's capabilities to prioritize and remediate exposed vulnerabilities and address compliance concerns, the composite organization reduces risks from internal and external threats. Holistic security controls and improved visibility for applications and managed assets across both IT and OT environments leads to $1.15 million in savings.
- **A 50% decrease in downtime for mission-critical assets.** The composite organization streamlines and better plans maintenance cycles as understanding and managing critical threats improves. As open vulnerabilities are addressed, the company decreases operational downtime, which translates to $1.17 million in avoided revenue leakage.
- **A 20% increase in efficiencies for the security operations team.** With expanded visibility, automated workflows, and improved vulnerability prioritization versus legacy solutions, the composite organization can redeploy internal resources to higher-value tasks. Automation reduces the need for manual intervention, while analysts use improved data and intelligence to increase productivity over time. Overall, improved security operations efficiencies drive $393,000 in savings.
- **Improved processes, data, and reporting, leading to $733,000 in audit and compliance gains.** Companies can decrease compliance violations and reliance on external auditors with the Skybox Platform through improved data monitoring and reporting. Automation of processes and access to contextualized data decrease time spent internally for audit and compliance processes. The composite organization decreases reliance on external auditors by 50% and increases productivity for internal teams by 30%.

> **“Skybox has given us visibility across our network, and there’s no other tool that we’ve had in the past that allowed us to do that on a global scale.”**
>
> *Principal network engineer, IT security*

- **A $329,000 savings in an enhanced and streamlined security stack.** Companies can reduce their reliance on various regional and enterprise tools related to vulnerability, firewall, and network security policy management to meet their overall security needs. This leads to savings through decommissioning legacy solutions after deploying the Skybox Platform.

Flexibility benefits. Future supplemental value enabled by longer-term added investments or nearer-term investments and scenarios that are not factored into the composite organization analysis include:

- **Consolidating processes to reduce IT/OT convergence risk.** The Skybox Platform helps companies better manage their combined IT environment (used for data-centric computing) and OT environments (which detects or causes a change through control of industrial equipment, assets, and processes). Interviewees felt their organizations were able to decrease their risk exposure while creating visibility across teams to drive consensus on the prioritization of exposed vulnerabilities.
- **Decreasing external audit failures.** The impact of an external audit noncompliance can lead to massive fines and require considerable operational support. Organizations can decrease the occurrence of failures while protecting brand equity by leveraging improved data and reporting to satisfy auditors’ feedback and questions.
- **Future opportunities for topline revenue growth and improved efficiencies.** Organizations can see the potential to unlock future returns by leveraging Skybox’s capabilities to achieve federal compliance standards and increase revenues. Additionally, interviewees saw the potential for broader adoption of the tool to improve end-to-end compliance workflows.

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

- **Improved employee satisfaction.** The Skybox Platform helps decrease employee burnout, as individuals spend less time on menial tasks, freeing up more time to engage in higher-value work.

> **“Skybox is going to be part of the supporting infrastructure that allows us to get federal certification. Potentially, that’s a huge growth opportunity.”**
>
> *Principal network engineer, IT security*

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

- **Three-year licensing fees of $940,000, representing 60% of total costs.** Skybox licensing is based on the products and services purchased and may vary based on the number and type of managed assets. On an annual basis, the composite organization paid $378,000 in annual licensing costs.

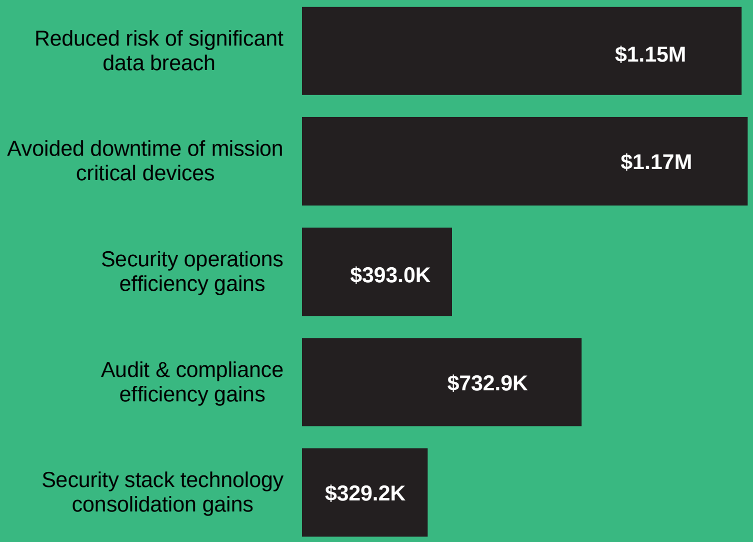
- **Implementation costs of just over $200,000 over a three-year period.** The composite organization utilizes a three-person internal implementation team along with Skybox professional services to complete planning, training, data integrations, migration, and industrialization tasks over a 16-week period to implement the Skybox Platform. Additional costs are incurred for hardware and software, including $50,000 upfront and $10,000 annually for upgrades.
- **Ongoing maintenance costs of $420,000.** The composite organization incurs ongoing maintenance and regular upkeep to ensure optimal performance of the tool. The company utilizes 20% to 30% of the time of five system administrators to sustain the Skybox Platform.

ROI
142%

BENEFITS PV
$3.78M

NPV
$2.21M

Benefits (Three-Year)



> **“Assets that are critical [are] tracked in Skybox, and the risk is assessed. If there is a vulnerability attached, we can fix it immediately. It’s reflected in Skybox, and we have evidence [for audits].”**
>
> — Information security manager, IT security

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 the Skybox Security Posture Management Platform.

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 Skybox Platform 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.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by Skybox and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the study to determine the appropriateness of an investment in the Skybox Platform.

Skybox reviewed and provided feedback to Forrester, but Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study.

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

DUE DILIGENCE

Interviewed Skybox stakeholders and Forrester analysts to gather data relative to their Security Posture Management Platform.

INTERVIEWS

Interviewed four representatives at organizations using the Skybox Platform 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 Skybox Security Posture Management Platform Customer Journey

Drivers leading to the Skybox Platform investment

Interviews

Role	Industry	Region	Revenue
Director of cybersecurity	Manufacturing	European headquarters, North and South America operations	$10 billion to $20 billion
Principal network engineer	IT security	North American headquarters, operating globally	$1 billion to $10 billion
Cybersecurity specialist	IT software and services	Mideast headquarters, operating globally	$1 billion to $10 billion
Information security manager	Financial services	North American headquarters, operating globally	$50 billion to $100 billion

KEY CHALLENGES

Before investing in the Skybox Platform, interviewees shared their experiences with using a combination of segmented, homegrown tools, spreadsheets, and antiquated third-party solutions to meet their needs for vulnerability and network security policy management.

The interviewees noted how their organizations struggled with common challenges:

- **Inability to prioritize vulnerabilities and extensive remedial work.** Interviewees discussed how their previous solutions to address threat and vulnerability management did not have the capabilities to distinguish or understand the criticality of threats across their IT and OT networks. This led to increased workloads across internal teams that were unable to keep pace with assessed vulnerabilities or with proper prioritization. Additionally, the potential threat of a significant data breach could have devastating consequences from a financial and brand standpoint.

- **Evolving needs for a centralized security system.** Prior solutions were focused on a smaller scope or regional security, which limited their visibility to enterprise level threats and gave rise to shadow IT internally. The principal network engineer at an IT security company discussed their company's previous issues and the Skybox Platform's influence: "Our challenge was to figure out visibility. One of the first products that we brought in after we did a bake-off was Skybox because it filled the void that we didn't have from our own products. There was no centralized group that was looking at these issues."

- **Inflated costs and inadequate data to support increasing audit and compliance needs.** Companies were forced to manage internal policies and firewalls through complex and manual processes. Disjointed or missing data and limited reporting led to longer external and internal audits while exposing the company to compliance risk or having to pay external fines for audit failures.

INVESTMENT OBJECTIVES

The interviewees' organizations searched for a solution that could enable their companies to:

- Establish an organization wide governance process for reviewing and prioritizing vulnerabilities and threats across IT and OT environments.

- Increase operational efficiencies through the reduction of menial work.

- Improve risk management and assessment.
- Prevent significant data breaches.
- Expand visibility, data, and critical audit logs to gain key government compliance standards and enable long-term growth.
- Utilize superior functionality and user experience.

After a request for proposal and business case process evaluating multiple vendors, the interviewees' organizations chose Skybox based on its capabilities and reputation:

- The information security manager in financial services discussed the decision-making process: "We did a bake-off, and the value of what the capabilities were with Skybox drove the decision … it was also because of the features that they offered, and [competitors] did not have those features."
- Customers felt Skybox would improve mean time to detection and drive efficiencies for internal resources.
- Skybox offered a comprehensive and centralized perspective of vulnerability and security policy management.

With Skybox, companies gain improved visibility and understanding of potential threats, enabling them to discover, prioritize, remediate, and report on vulnerabilities. At the same time, customers can collect, normalize, and optimize their network and security data to make complex policy management easier, faster, and more effectively. With Skybox, customers can easily detect access policy violations, rule conflicts, and misconfigurations, avoiding future exposure as policies and applications change. Moreover, companies can streamline their network policies and drive consistent management across their internal security stack.

"The team really liked the reporting showing what tests were run, what's in compliance, what's not in compliance, and what section of the PCI [payment card industry] compliance each test ran against."

Cybersecurity specialist,
IT software and services

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 based on the four interviewees' companies and is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. The composite organization is a global conglomerate that has seen growth through a series of mergers and acquisitions. The company has cross-functional operations across IT and OT generating over $2 billion in annual revenue, supported by 15,000 employees globally. A team of 20 security operations analysts support security and compliance processes.

Deployment characteristics. The composite organization completes data architecture, integration, and planning activities for Skybox using a three-person implementation team. In total, the process requires 50% of the time for the implementation team over a 16-week period to deploy Skybox's capabilities to 30,000 managed assets, including 50 firewalls and 200 network devices.

Key Assumptions

- **Over $2 billion revenue**
- **15,000 employees**
- **20 security operations analysts**
- **30,000 assets**

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	Reduced risk of significant data breach	$419,842	$466,492	$513,141	$1,399,475	$1,152,735
Btr	Avoided downtime of mission-critical devices	$320,000	$480,000	$640,000	$1,440,000	$1,168,445
Ctr	Security operations efficiency gains	$136,688	$159,469	$182,250	$478,407	$392,981
Dtr	Audit and compliance efficiency gains	$251,100	$297,675	$344,250	$893,025	$732,925
Etr	Security stack technology consolidation gains	$81,000	$162,000	$162,000	$405,000	$329,234
	Total benefits (risk-adjusted)	$1,208,630	$1,565,636	$1,841,641	$4,615,907	$3,776,320

REDUCED RISK OF A SIGNIFICANT DATA BREACH

Evidence and data. Interviewees shared that their companies were able to drastically reduce their exposure to significant data breaches resulting from internal and external threat actors. Using Skybox's capabilities, organizations could better prioritize and understand critical vulnerabilities while addressing compliance concerns on a global enterprise scale. Through increased visibility, interviewees' companies acted on critical items more quickly across IT and OT functions.

- The principal network engineer at an IT security company described his experience: "It was like the Wild West. We have thousands upon thousands or hundreds of thousands of vulnerabilities that show up in scans. What Skybox does is look at vulnerabilities in the context of all the other things in the network to [produce] a risk assessment, and that's what allows us to prioritize the vulnerabilities that need to be fixed."
- With a consistent framework for prioritizing exposed vulnerabilities, interviewees' companies created an internal governance process to centrally review and manage threats across IT and OT environments. This led to a massive reduction in the time to detect and remediate vulnerabilities. The manufacturing company saw a reduction from two months to a few days on the IT side of its business and from nine months to as low as two weeks for OT.

> **"We had endless streams or debt on vulnerability remedial work. Everything seemed extremely important. … We moved to Skybox because it gave us exactly the prioritization model that we needed."**
>
> *Director of cybersecurity, manufacturing*

- The director of cybersecurity at a manufacturing company discussed how Skybox helped reduce their company's risk of a significant security breach by 50%: "For a published threat, Skybox can tell you where to find it. There is no argument that the source of information is credible."

Reduction in mean time to detect vulnerabilities

67%

- Beyond the threat of an external attack, companies were able to leverage network segmentation strategies to limit the risk of internal dangers as well. The principal network engineer at the IT security company shared that they had realized a 200% improvement in their ability to address internal attack vectors: "We've been able to use Skybox as a tool to limit movement once a threat is inside the network, to limit where it can go."
- Overall, companies saw more than a 55% reduction in the risk of significant security breaches from most external and internal threats.

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

- Based on Forrester's proprietary research, an organization with $2 billion or higher revenue and 30,000 managed assets (the composite organization) will have 2.5 data breaches annually, at a cost of at least $655,300.[1]
- The composite organization sees an immediate 45% reduction in the risk of a significant data breach. The company sees subsequent gains in the future years due to compounding benefits from the prioritization and remediation of critical threats.
- Skybox's solutions cover 67% of potential types of data breaches, including external attacks, business partner/third-party attacks, and internal incidents.

Flexibility. Forrester traditionally views flexibility benefits as future supplemental value enabled by longer-term added investments. But flexibility can also be applied to nearer-term investments and scenarios that are not factored into the composite organization analysis but may be relevant to many readers. For example:

- Customers may reduce the risk of significant data breaches beyond the 55% benefit experienced by the composite organization. Several interviewees' organizations plan to implement Skybox Change Manager, which may reduce the risk of a data breach even more by automating rule lifecycle management and integrating change processes with existing ticketing systems to reduce their exposure to internal and external threats.
- Additionally, Skybox has the capability to test potential changes before implementing to ensure organizations can avoid misconfigurations and policy changes that would lead to noncompliance and exposed vulnerabilities. This can be measured in a risk reduction for potential customers for significant data breaches above and beyond what is measured with the composite organization.

Risks. The reduced financial impact of a significant data breach will vary with:

- The baseline security strength, exposure, and posture of the organization.
- The skill set and salary levels of the organization's security team.
- The organization's size, industry, and location.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.15 million.

Reduced Risk Of Significant Data Breach

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Number of significant data breaches per year prior to deploying Skybox	Forrester research	2.5	2.5	2.5
A2	Reduced risk of a significant data breach	Interviews	45%	50%	55%
A3	Number of significant data breaches per year after deploying Skybox	A1*(1-A2)	1.375	1.250	1.125
A4	Average cost per significant data breach	Forrester research	$655,300	$655,300	$655,300
A5	Percentage of data breaches covered with Skybox	Interviews	67%	67%	67%
At	Reduced risk of significant data breach	A1*A2*A4*A5	$493,932	$548,814	$603,695
	Risk adjustment	↓15%			
Atr	Reduced risk of significant data breach (risk-adjusted)		$419,842	$466,492	$513,141
	Three-year total: $1,399,475	**Three-year present value: $1,152,735**			

AVOIDED DOWNTIME OF MISSION-CRITICAL DEVICES

Evidence and data. Interviewed companies saw appreciable benefits from reducing downtime during operations for mission-critical assets based on their investment in Skybox. With a better understanding of the criticality of potential threats, companies were able to better plan maintenance cycles and remediate threats more quickly compared to previous solutions.

- As companies were able to clean up existing critical vulnerabilities and compliance risks within their internal networks, it decreased the necessity to bring down critical functions for remediation. Interviewees described how their organizations were focused on remediation strategies that minimized impacts for processes across IT and OT spaces.
- Operational downtime can be particularly critical for OT where productivity can have a direct impact on revenues. The director of cybersecurity at a manufacturing company shared: "We had server downtime on the OT side on a quarterly basis with crypto malware, things that would spend the CPU to try and do cryptocurrency mining or things like that. We used to have quite a number of those. That was one of the triggers for doing an OT cybersecurity program, and Skybox helped us to identify the most critical quite quickly."
- Organizations saw further reductions for mission-critical downtime as mission-critical threats were prioritized and remediated.
- Companies were able to decrease revenue leakage by as much as $1.2 million annually based on their investment in Skybox.

Modeling and assumptions. For the analysis, Forrester assumes the following:

- The composite organization reduces downtime in the first year by 8 hours, with additional improvements in subsequent years as unpatched vulnerabilities for critical assets are remediated.
- One hour of downtime costs the composite organization $50,000.

> **"OT downtime is measured in lack of production. We had a 4-hour incident every quarter and now we don't have that. We reduce quite significantly the risk surface by implementing Skybox."**
>
> *Director of cybersecurity, manufacturing*

Flexibility. Certain flexibility benefits may apply to some organizations that give them the opportunity for nearer-term investments and scenarios which were not factored into the composite organization. For example:

- Organizations could leverage Skybox to improve the IT/OT convergence process with reduced operational downtime**.** The Skybox Platform allows companies to consolidate and centralize their processes across IT/OT environments and drive improvements to their risk exposure efficiently. The director of cybersecurity at a manufacturing company shared their experience: "Skybox was the first convergence critical asset for both IT and OT, and that created a common framework for defining priorities and vulnerability visibility for the entire company."
- Organizations could measure the impact of reduced downtime for assets and resources that are not directly linked to driving revenues. Potential impacts could include the improvement

of end user productivity by reducing inefficiencies and driving value for operational processes.

- Organizations could avoid customer and employee frustration from interrupted processes and services. Better platform stability could be measured through improved employee and customer satisfaction in addition to driving improved business outcomes.

Risks. Several factors may affect the impacts organizations experience, including the following:

- The baseline security strength, exposure, and posture of the organization.
- The organization's size, industry, and location.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $1.17 million.

Avoided Downtime Of Mission-Critical Devices

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Downtime for mission-critical devices during operational hours before Skybox	Interviews	32	32	32
B2	Downtime for mission-critical devices during operational hours after Skybox	Interviews	24	20	16
B3	Decrease in downtime during operational hours after Skybox	B1-B2	8	12	16
B4	Revenue leakage for downtime per hour	Interviews	$50,000	$50,000	$50,000
Bt	Avoided downtime of mission-critical devices	B3*B4	$400,000	$600,000	$800,000
	Risk adjustment	↓20%			
Btr	Avoided downtime of mission-critical devices (risk-adjusted)		$320,000	$480,000	$640,000
	Three-year total: $1,440,000	**Three-year present value: $1,168,445**			

SECURITY OPERATIONS EFFICIENCY GAINS

Evidence and data. Gains from increased visibility and prioritization of unpatched vulnerabilities and threats had significant impacts from an operational standpoint. Interviewees' companies were able to redeploy internal cybersecurity analysts on higher-value tasks based on increased efficiencies in Skybox.

- The director of cybersecurity at a manufacturing company described how the tool reduced manual work for his team: "Skybox provides a prioritized list of vulnerabilities to remediate, leading to the reduction [of] time to do remedial work on the IT state primarily. So, we went from months to weeks to days depending on the criticality of the exposure."

  He continued by sharing the impact on his team: "The productivity gains were an effect of having better information. There is an indirect derivative of the mean time to detect and the mean time to remediate having improved significantly, and we have the risk better managed."

- Automation in processes decreased the necessity for manual intervention. Moreover, companies were able to use Skybox's straightforward interface and available data to optimize firewalls and internal policies more quickly than with their legacy solutions.

- Skybox users were able to improve their proficiency as they became more familiar with Skybox's features, which led to incremental improvements in efficiencies for interviewees' organizations.

- After deploying Skybox, interviewees' companies saw an average improvement in productivity of 20% over the course of their investment for their security operations teams.

Modeling and assumptions. For the financial analysis, Forrester assumes that:

- The composite organization has 15 security analysts who dedicate 50% of their time to vulnerability, threat, and firewall management.

- Security analysts see a 15% improvement in their overall productivity based on the deployment of Skybox's solutions in Year 1 and up to 20% by Year 3 based on increased proficiency in the tool.

- The average fully burdened salary of a security analyst is $135,000.

> **"Skybox is cumulative, so I don't have to reanalyze everything [each year]. It will do that analysis for me and then I can go straight to a table and work on that table. It's got a nice human interface and it's fast."**
>
> *Cybersecurity specialist,*
> *IT software and services*

Flexibility. Companies could see long-term benefits from increased adoption of Skybox's capabilities to drive incremental operational efficiencies as the holistic security operations team improves processes across their organization's end-to-end security stack. The information security manager at the financial services organization shared how the improved capabilities will continue to drive incremental value internally: "The policy team is slowly starting to look within the tool. That's one of the key things that [the prior solution] was never able to be adopted by people using the tool. I'm getting two to three requests a day for access into [the] Skybox system."

Risks. The value of this benefit may vary in other organizations based on the following:

- The baseline security strength, exposure, and posture of the organization.
- The organization’s size, industry, and location.
- The skill level, efficiency, and salaries of analysts within the organization.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $393,000.

Security Operations Efficiency Gains

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Security operations analyst FTEs	Composite	15	15	15
C2	Time spent on vulnerability management prior to Skybox	Interviews	50%	50%	50%
C3	Security operations analyst fully loaded salary	TEI standard	$135,000	$135,000	$135,000
C4	Increase in security operations productivity	Interviews	15.0%	17.5%	20.0%
Ct	Security operations efficiency gains	C1*C2*C3*C4	$151,875	$177,188	$202,500
	Risk adjustment	↓10%			
Ctr	Security operations efficiency gains (risk-adjusted)		$136,688	$159,469	$182,250
	Three-year total: $478,407		**Three-year present value: $392,981**		

AUDIT AND COMPLIANCE EFFICIENCY GAINS

Evidence and data. Organizations are facing increasing pressures to meet regulatory and compliance standards. Interviewees' companies significantly improved the end-to-end time required to manage processes based on their investment in the Skybox Platform. Through improved data and decreased compliance violations and human errors, companies were able to decrease their costs for external audits and time spent internally on compliance.

> **"The IT team spends less time on the audit; they used to handwrite a report and try to come up with explanations. Now they just take the information from Skybox and say, here's the proof."**
>
> *Principal network engineer, IT securitv*

- Improved data helped to decrease compliance violations, rework, and reliance on external auditors. The cybersecurity specialist in IT software and services explained: "The person who benefits the most from Skybox is actually [the external auditor] because they get their information quickly and they move on to other things."
- Internal teams were able to use improved data and reporting to decrease the time required on each internal and external process directly or indirectly related to audit and compliance. This allowed companies to do more with less as requirements have continued to increase from a regulatory standpoint.
- The information security manager in financial services discussed the impact of Skybox relative to their previous solution: "As firewalls get moved in and out of the ecosystem, with the prior solution, we had to go in, massage, and add those firewalls to start monitoring or stop monitoring. That's no longer needed, which saved half a day's worth of work every day just because Skybox does it automatically."
- Interviewees' companies were able to decrease their reliance on external auditors by 50% or more while seeing a 25% reduction in time that function teams were spending on audit and compliance activities.

Modeling and assumptions. This section explains how the modeling is done:

- The composite organization is required to conduct 40 security audits across multiple departments annually in the first year, which increases to 50 by the third year as the company faces increasing audit requirements.
- The organization decreases the amount of time external auditors spend on each audit from three days to 1.5 days. The composite organization pays $2,400 daily on the cost of an external auditor.
- The company has 20 security analysts who dedicate 25% of their time to audit and compliance activities.
- Security analysts see a 20% improvement in their overall productivity based on the deployment of Skybox's solutions in Year 1 and up to 30% in Year 3 based on increased proficiency in the tool.
- The average fully burdened salary of a security analyst is $135,000.

Flexibility. Companies could see long-term benefits from the reduced costs of external audit failures. Skybox can help reduce the potential risk of audit failures that drive significant operational costs and fines. Interviewees shared that they were expecting a decrease in failures while improving brand equity with partners and government agencies through clear audit trails, availability of data, and the ability to respond to audit feedback much quicker than with legacy toolsets.

Risks. The value of this benefit may vary in other organizations based on the following:

- The audit and compliance standards the company is held to are based on the organization’s size, industry, and location.
- The amount of time the company currently spends on audit and compliance processes.
- The skill level, efficiency, and salaries of analysts within the organization.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $733,000.

Audit And Compliance Efficiency Gains

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Average number of security audits per year	Interviews	40	45	50
D2	External auditor cost per day	TEI standard	$2,400	$2,400	$2,400
D3	Number of days per external audit prior to implementing Skybox	Interviews	3	3	3
D4	Number of days per external audit after implementing Skybox	Interviews	1.5	1.5	1.5
D5	Number of external audit days saved per year	D1*(D3-D4)	60.0	67.5	75.0
D6	Subtotal: external auditor savings after implementing Skybox	D2*D5	$144,000	$162,000	$180,000
D7	Security operations analyst FTEs	Composite	20	20	20
D8	Time spent internally on audit and compliance management prior to Skybox	Interviews	25%	25%	25%
D9	Security operations analyst fully loaded salary	TEI standard	$135,000	$135,000	$135,000
D10	Increase in audit and compliance management productivity	Interviews	20%	25%	30%
D11	Subtotal: Internal resource efficiency cost savings	D7*D8*D9*D10	$135,000	$168,750	$202,500
Dt	Audit and compliance efficiency gains	D6*D11	$279,000	$330,750	$382,500
	Risk adjustment	↓10%			
Dtr	Audit and compliance efficiency gains (risk-adjusted)		$251,100	$297,675	$344,250
	Three-year total: $893,025		**Three-year present value: $732,925**		

SECURITY STACK TECHNOLOGY CONSOLIDATION GAINS

Evidence and data. After implementing the Skybox Platform, companies were able to reevaluate their security stacks based on their investment. Companies decommissioned or downgraded their regional or enterprise tools related to vulnerability, firewall, and network policy management as well as reporting and analytics toolsets. The composite organization can retire legacy solutions six months after implementation. This saves the company half of the cost of Skybox thereafter.

- After deploying Skybox, interviewees reported that the capabilities and reporting available through Skybox replaced and improved on legacy solutions within their technology stacks. While each organization saw different impacts, most were able to retire at least one legacy system based on their investment.
- Interviewees' organizations generally ran Skybox concurrently with previous solutions until it was clear that their needs were met through Skybox.

Modeling and assumptions. For the financial analysis, Forrester assumes that:

- The composite organization can reevaluate and decommission annual spend on licensing for legacy vulnerability, firewall, and network policy management software resulting in savings of $6 per asset.
- The organization retires 15,000 legacy licenses in the first year and an additional 15,000 starting in the second year after deployment.

Flexibility. In addition to consolidating their security stacks, companies could see long-term benefits from unlocking value through efficiencies and insights across the security stack. Organizations felt that Skybox's capabilities offer the possibility of reevaluating end-to-end processes for their teams and driving efficiencies. The information security manager at a financial services organization shared: "Skybox is definitely doing what it was brought in to do, and I think there is potential in solving some of our other pain points that we have today. I think that would be a missed opportunity if we don't."

Risks. The total security stack consolidation gains benefit will vary based on the following:

- The existing security capabilities of the organization before implementing the Skybox Platform.
- The desired security posture, compliance requirements, and industry of the organization.
- The number of legacy tools.
- The cost of legacy tools.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $329,000.

Security Stack Technology Consolidation Gains

Ref.	Metric	Source	Year 1	Year 2	Year 3
E1	Number of retired third-party licenses	Composite	15,000	30,000	30,000
E2	Individual annual licensing cost	Composite	$6	$6	$6
Et	Security stack technology consolidation gains	E1*E2	$90,000	$180,000	$180,000
	Risk adjustment	↓10%			
Etr	Security stack technology consolidation gains (risk-adjusted)		$81,000	$162,000	$162,000
	Three-year total: $405,000		**Three-year present value: $329,234**		

UNQUANTIFIED BENEFITS

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

- **Improved employee satisfaction.** Interviewees' organizations saw a marked improvement in employee satisfaction, as the prioritization of vulnerabilities brought focus to ongoing work, reduced stress levels, and freed up time across security operations teams. Operational efficiencies for vulnerability and policy management also allowed employees to take part in higher-value tasks that were more engaging for the individual and drove more value for the organization.

> **"This has changed the life of at least one of my engineers. He actually has said it over and over: 'This is the best thing that's ever happened to me.'"**
>
> *Information security manager, financial services*

FLEXIBILITY

The value of flexibility is unique to each customer. Some flexibility opportunities have already been summarized for each benefit above but there are other scenarios in which a customer might implement the Skybox Platform and later realize additional uses and business opportunities, including:

- **Topline revenue growth as a result of achieving federal compliance standards.** Through the audit trail, data, and analytic capabilities of Skybox's solutions, companies see the potential for future growth through obtaining business certifications and opening the door to new potential customer segments. The principal network engineer at an IT security company shared: "Once we get the necessary certification, we can interact directly with the federal government. We'd be authorized to sell directly, so that's a big opportunity."

- **Consolidated and streamlined internal rulesets.** Companies can use Skybox's capabilities to fast-track decisions by eliminating redundant policies and consolidating firewall rulesets on a continual basis. With added processes and technology adoption, organizations can collect, normalize, and analyze data across integrated applications to automatically identify bad rules while improving internal visibility and efficiencies beyond what was modeled with the composite organization, leading to more straightforward processes for internal teams.

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
Ftr	Total annual license costs	$0	$378,000	$378,000	$378,000	$1,134,000	$940,030
Gtr	Implementation costs	$173,384	$11,500	$11,500	$11,500	$207,884	$201,983
Htr	Ongoing maintenance costs	$0	$200,475	$167,063	$133,650	$501,188	$420,731
	Total costs (risk-adjusted)	$173,384	$589,975	$556,563	$523,150	$1,843,072	$1,562,744

TOTAL ANNUAL LICENSE COSTS

Evidence and data. Interviewees' companies incurred annual licensing fees based on the Skybox products and services employed.

Modeling and assumptions. For the analysis, Forrester assumes the following:

- The composite organization has a three-year subscription license for Skybox Security Posture Management Platform.
- The organization has licensing costs based on 30,000 managed assets including 50 firewalls and 200 network devices.

Risks. The risks associated with Skybox's annual licensing costs include the number and mix of assets deployed by an organization as well as the actual product and service mix purchased.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $940,000.

Total Annual License Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	Internal assets	Composite		30,000	30,000	30,000
F2	Average annual cost per asset	Interviews		$12.00	$12.00	$12.00
Ft	Total annual license costs	F1*F2	$0	$360,000	$360,000	$360,000
	Risk adjustment	↑5%				
Ftr	Total annual license costs (risk-adjusted)		$0	$378,000	$378,000	$378,000
	Three-year total: $1,134,000			**Three-year present value: $940,030**		

IMPLEMENTATION COSTS

Evidence and data. Implementation costs include planning, training, data integrations, data migration, and industrialization specific to OT devices to deploy the Skybox Platform for the composite organization.

- Time frame of the implementation process varied for interviewees' organizations based on time dedicated to the process, features deployed, and how complex the existing infrastructure was. Companies averaged a four-month implementation for a small internal team.
- Companies incurred some upfront costs for Skybox professional service fees and training as part of the onboarding and implementation process.
- Interviewees' organizations incurred some upfront and ongoing expenses for updated CPU storage and memory as well as virtual and physical hardware.

Modeling and assumptions. Forrester assumes the following conditions surrounding implementation costs:

- Based on the composite organization's total employee base of 15,000 and managed assets of 30,000, the implementation takes 16 weeks to complete.
- Deployment of the Skybox Platform requires 50% of a three-person team's time with an aggregate fully loaded salary of $110,000.
- The company incurs upfront costs of $50,000 for Skybox professional service fees and training.
- The composite organization invests $50,000 upfront for hardware and software upgrades to support the implementation as well as an ongoing $10,000 annual cost for upkeep.

Risks. These costs may vary for their organizations based on several factors:

- The skillset and salary levels of the implementation team.
- The size and complexity of the organization's existing internal IT infrastructure.

Results. To account for these risks, Forrester adjusted this cost upward by 15%, yielding a three-year, risk-adjusted total PV of just over $200,000.

Implementation Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
G1	Number of people involved in implementation process	Interviews	3			
G2	Annual rate for aggregate implementation team	TEI standard	$110,000			
G3	Weeks spend on implementation tasks	Interviews	16			
G4	Percent of time allocated to implementation of Skybox	Interviews	50%			
G5	Subtotal: integrations, policy creation, and baselining	G1*G2*(G3/52)*G 4	$50,769			
G6	Professional service fees and training	Interviews	$50,000			
G7	Hardware and software investment	Interviews	$50,000	$10,000	$10,000	$10,000
Gt	Implementation costs	G5+G6+G7	$150,769	$10,000	$10,000	$10,000
	Risk adjustment	↑15%				
Gtr	Implementation costs (risk-adjusted)		$173,384	$11,500	$11,500	$11,500
	Three-year total: $207,884			Three-year present value: $201,983		

ONGOING MAINTENANCE COSTS

Evidence and data. Based on interviewee responses, organizations had ongoing costs related to their investment in Skybox to maintain the solution. Regular upkeep and tuning of Skybox's settings helped drive optimal performance and bring incremental value to the organization.

- The principal network engineer discussed why it was important to prioritize ongoing maintenance in Skybox: "It is more flexible than our previous solution; however, it requires that you keep at it. It's not one of these things where you just set it and forget it, but the more that you invest in it in terms of time and analytics, the more you're going to get back."
- Interviewed organizations were gradually able to decrease the time spent internally on maintenance as resources became more adept at the tool.

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

- Five system administrators spend 30% of their time on maintenance tasks in the first year. As the team gains proficiency in the tool, administrators can devote more time to other tasks and decrease maintenance time to 20% by the third year.
- The average fully loaded salary of a system administrator is $121,500.

Risks. Organizations may face varying maintenance costs dependent on:

- The complexity and support model of the organization's IT infrastructure.
- The skill level, efficiency, and salaries of the system administrators within the company.
- The security posture and exposure of the organization.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $421,000.

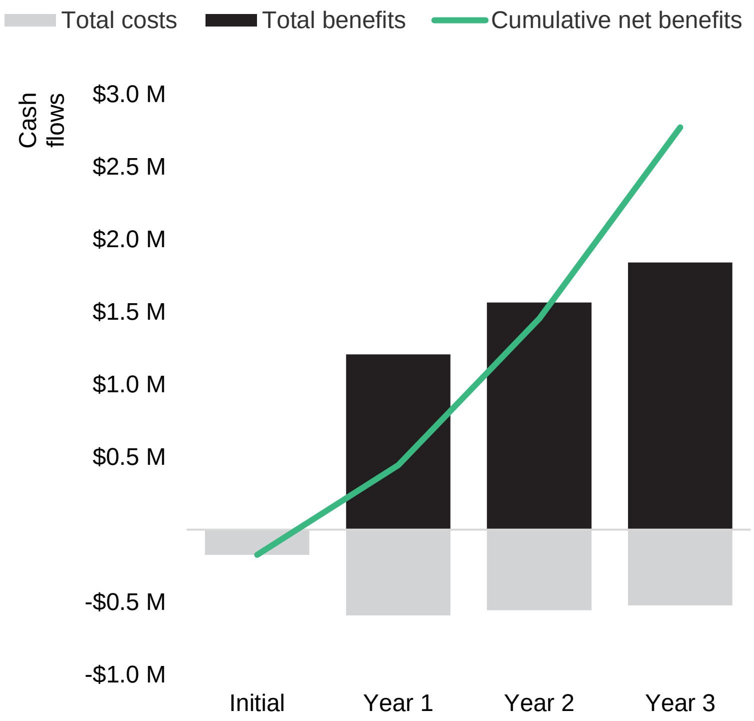
Ongoing Maintenance Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
H1	System administrator FTEs	Composite		5	5	5
H2	Time spent on maintenance and end-user support for Skybox	Interviews		30%	25%	20%
H3	System administrator's fully loaded salary	TEI standard		$121,500	$121,500	$121,500
Ht	Ongoing maintenance costs	H1*H2*H3	$0	$182,250	$151,875	$121,500
	Risk adjustment	↑10%				
Htr	Ongoing maintenance costs (risk-adjusted)		$0	$200,475	$167,063	$133,650
	Three-year total: $501,188			**Three-year present value: $420,731**		

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, and NPV values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

Cash Flow Analysis (Risk-Adjusted Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($173,384)	($589,975)	($556,563)	($523,150)	($1,843,072)	($1,562,744)
Total benefits	$0	$1,208,630	$1,565,636	$1,841,641	$4,615,907	$3,776,320
Net benefits	($173,384)	$618,655	$1,009,074	$1,318,491	$2,772,835	$2,213,576
ROI						142%

Appendix A: Total Economic Impact

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

TOTAL ECONOMIC IMPACT APPROACH

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

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

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

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

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

PRESENT VALUE (PV)

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

NET PRESENT VALUE (NPV)

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

RETURN ON INVESTMENT (ROI)

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

DISCOUNT RATE

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

PAYBACK PERIOD

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

Appendix B: Endnotes

[1] Source: Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q1 2021.

FORRESTER®