Total Economic Impact

The Total Economic Impact™ Of Airlock Digital

Cost Savings And Business Benefits Enabled By Airlock Digital

A FORRESTER TOTAL ECONOMIC IMPACT STUDY COMMISSIONED BY AIRLOCK DIGITAL, DECEMBER 2025

Executive Summary

Allowlisting represents a shift from reactive to proactive security, focusing on protecting known-good resources rather than trying to identify every possible threat. This approach aligns with Zero Trust architecture and defense-in-depth strategies. Organizations that handle sensitive data or critical infrastructure are increasingly adopting allowlisting to meet strict security and compliance standards and to strengthen defenses as cyberthreats grow more sophisticated. The simple principle of denying everything except what's explicitly approved remains effective across evolving attack methods, which makes allowlisting a consistently valuable component of comprehensive cybersecurity programs.

Airlock Digital commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Airlock Digital.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Airlock Digital on their organizations.

224%

Return on investment (ROI)

$3.8M

Net present value (NPV)

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four decision-makers with experience using Airlock Digital. For the purposes of this study, Forrester aggregated the experiences of the interviewees and combined the results into a single composite organization, which is a B2B organization with annual revenue of $10 billion and 20,000 endpoints.

Interviewees noted that before using Airlock Digital, their organizations had determined that a reactive security approach was insufficient. Previous proactive solutions had limited success that led to incomplete endpoint coverage, performance issues, and high maintenance costs for complex solutions. These challenges prompted the organizations to look for a new solution, and they conducted proof-of-concept (POC) trials with multiple allowlisting providers.

The interviewees reported that after investing in Airlock Digital, their organizations achieved 100% coverage of all endpoints on their networks with little or no performance-related user impact and far better visibility into network activity than they had before. Key results from the investment include an improved security posture, lower overall maintenance costs, and improved software inventory management.

Key Findings

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

- **Strengthened security.** Using Airlock Digital reduces the composite's overall risk of a breach by more than 25%, which allows it to meet its compliance goals for strengthened security. Over three years, this saves the composite $4.1 million.
- **Reduced administrative overhead.** Maintaining Airlock Digital requires one security analyst at the composite to spend about 2.5 hours per week reviewing logs and creating any necessary tickets for needed changes to protocol and policies. This is a reduction that translates to $1.3 million over three years.
- **Improved software inventory management.** By eliminating license fees for idle applications and reducing maintenance by consolidating redundant applications, the composite organization saves $186,000 over three years.

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

- **Enterprisewide user productivity improvements.** The composite organization has fewer outages, which leads to fewer work disruptions. Airlock Digital also enforces application control for the organization without introducing latency or blocking legitimate work.
- **The ability to customize the solution by user group.** While the enhanced security provided by Airlock Digital partially addresses this benefit, it doesn't fully encompass the flexibility required for different users to access customized allow-lists.

- **On-demand exceptions and transparent logging.** The composite organization values that users can swiftly request a one-time pass to deploy a previously unapproved app when necessary, which helps secure organizational buy-in for the allow-listing solution.

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

- **Enterprise license fees.** Airlock Digital license fees are based on the number of endpoints. Because the composite has 20,000 endpoints, it pays $1.2 million in license fees over three years.
- **Technical implementation and maintenance.** One security analyst at the composite spends a total of 40 hours on the initial deployment of Airlock Digital and then 2.5 hours per week once under enforcement. In total, the organization's technical implementation and maintenance costs are $35,000.
- **Policy and protocol development.** The composite organization imports policies and protocols for 10,000 endpoints from its previous solution to Airlock Digital. This requires a 12-week audit and rules development period before transitioning to Airlock Digital enforcement. Over three years, the composite pays $422,000 for policy and protocol development.

The financial analysis that is based on the interviews found that a composite organization experiences benefits of $5.5 million over three years versus costs of $1.7 million, adding up to a net present value (NPV) of $3.8 million and an ROI of 224%.

>25%

Overall reduction to the risk of a security breach

> *"Our previous solution was fragile and difficult to manage at scale. It lacked centralized control and created operational overhead, especially during emergency response scenarios."*
>
> **CSO, equipment rental**

> *"We're very happy with the product, support, roadmap, and the leadership We plan to stay with Airlock as long as they will have us."*
>
> **SVP of network security, financial services**

Key Statistics

224%

Return on investment (ROI)

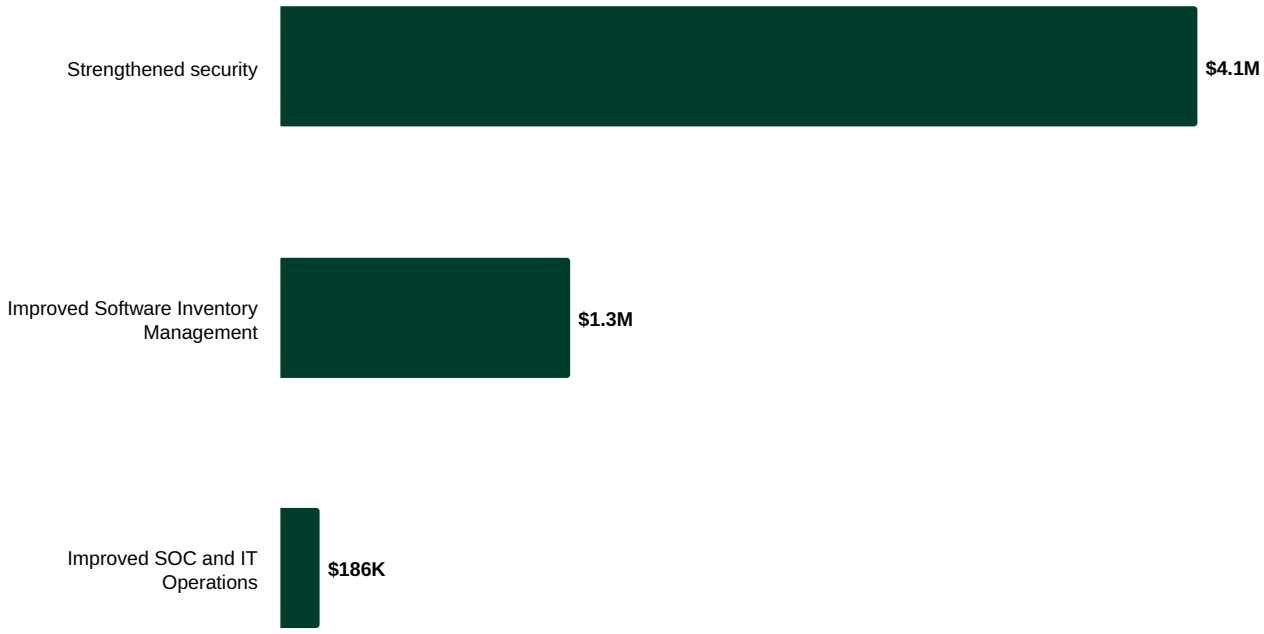
$5.5M

Benefits PV

$3.8M

Net present value (NPV)

Benefits (Three-Year)



The Airlock Digital Customer Journey

Drivers leading to the Airlock Digital investment

Interviews				
Role	**Industry**	**Region**	**Annual revenue**	**Endpoints**
SVP of network security	Financial services	US	$3B	11,000
System administrator	Vehicle sales, rental, and leasing	US and Canada	$10B	30,000
CSO	Equipment rental	North America and the UK	$11B	10,000
Technical lead of cybersecurity	Insurance	Australia and New Zealand	$10B	20,000

Key Challenges

Interviewees said that before implementing Airlock Digital, their organizations had fragmented or fragile security environments and solutions that left them struggling with performance issues and working with brittle systems that required extensive maintenance and could not scale with business growth. Interviewees noted how their organizations struggled with common challenges, including:

- **Inability to scale.** The system administrator at a vehicle sales, rental, and leasing organization said: “As my company grew, the complexity of the needs of our endpoints and the software we use and applications grew, and we found that [our previous solution] was just not scalable for our environment. It wasn’t adaptable. It wasn’t flexible. It was disruptive.”
- **Inability to provide complete endpoint coverage.** The same interviewee said: “We weren’t able to get to 100% coverage with our previous solution. It just didn’t scale well across our environment, and there were always exceptions or systems that couldn’t be brought under control.”
- **Complexity of the solutions in place.** The technical lead of cybersecurity at an insurance organization said: “Before switching, we were juggling multiple endpoint agents and still struggling with performance and visibility. It felt like we were constantly patching holes rather than securing the environment.”
- **Performance issues.** The same interviewee said: “Our previous solution caused significant performance degradation on endpoints, especially during updates and scans. The agent footprint was heavy, contributing to system slowdowns and user complaints.”
- **High maintenance requirements.** The cybersecurity lead for an insurance organization said: “We did a lot of baseline load testing of all the combinations of solutions, and the Airlock deployment added negligible overhead compared to the other combinations we used, including [our previous solution].”

Solution Requirements/Investment Objectives

The interviewees searched for a solution that could:

- Scale without disruption.
- Provide 100% endpoint protection across Windows, Mac, and Linux operating systems.
- Provide flexibility for different users and user groups across the organization.
- Reduce the amount of IT effort needed to maintain the solution.
- Provide a secure and efficient way to temporarily allow legitimate access to assets not previously approved, and to adapt the rule set when appropriate.

> *"We were able to reset all of our application controls and then manage the entire enterprise from a single product install."*
>
> **SVP of network security, financial services**

> *"We spun up 20,000 instances to stress test Airlock Digital's performance at scale. That gave us confidence it could handle our environment without introducing latency or instability."*
>
> **Technical lead of cybersecurity, insurance**

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 interviewees' organizations, and it is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

- **Description of composite.** The composite organization operates globally and has annual revenues of $10 billion. It's the product of a merger between two entities, each with 10,000 endpoints. One of the pre-merger organizations had previously implemented an allowlisting solution in enforcement mode with a well-developed set of policies and protocols in place. The second organization was new to allowlisting.
- **Deployment characteristics.** Prior to full deployment, the composite rolls out Airlock Digital across both 10,000-endpoint environments. The business unit with an existing allowlisting solution deploys Airlock Digital in audit mode during the technical implementation to align policies and protocols with the new standard before moving into enforcement. The second unit that is new to allowlisting begins in audit mode to develop policies and protocols and ramp users into the allowlisting model before enforcement.

KEY ASSUMPTIONS

- $10 billion revenue
- 20,000 endpoints under enforcement

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total						
Ref.	**Benefit**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Atr	Strengthened security	$1,632,442	$1,632,442	$1,632,442	$4,897,325	$4,059,641
Btr	Improved software inventory management	$510,000	$510,000	$510,000	$1,530,000	$1,268,295
Ctr	Improved SOC and IT operations	$74,610	$74,610	$74,610	$223,829	$185,543
	Total benefits (risk-adjusted)	$2,217,051	$2,217,051	$2,217,051	$6,651,153	$5,513,479

Strengthened Security

Evidence and data. Interviewees said the primary advantage of Airlock Digital is that it reduces the attack surface. They explained that by blocking everything except known-good entities, Airlock Digital's allowlisting eliminates most zero-day exploits, unknown malware, and unauthorized access attempts. Interviewees also noted that even sophisticated attacks often fail because they rely on executing unauthorized code or communicating with external command-and-control servers. This approach provides strong protection against advanced persistent threats (APTs) that might evade traditional signature-based detection and is particularly effective against fileless malware, living-off-the-land attacks, and other evasive techniques that exploit legitimate system tools. Each interviewee said that after implementing Airlock Digital, their organization has not experienced a breach.

- The system administrator at the vehicle sales, rental, and leasing organization said: "Airlock gave us full visibility and control over all 10,000 endpoints. We went from having blind spots to knowing exactly what's running, and that's a huge leap in security posture."
- Th SVP of network security at the financial services organization said: "Airlock helped us tighten controls across 11,000 licenses. We've seen a measurable drop in security incidents, and our auditors are much happier with the level of endpoint hygiene."
- The CSO at the equipment rental organization said: "Before [using] Airlock, we had visibility gaps and inconsistent enforcement. Now every endpoint is locked down, and we've dramatically reduced our exposure to malware and shadow IT."
- The technical lead of cybersecurity at the insurance organization said: "We're now in full enforcement mode on over 90% of our endpoints. That means no unauthorized software can run, and we've eliminated a whole class of threats that used to slip through."

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite has all 20,000 endpoints, and each is under enforcement with Airlock Digital.
- The composite's total risk exposure to security breaches is $3,149,000 per year.[2]
- For the composite organization, 81% of breaches originate from external attacks targeting organizations, external attacks targeting remote environments, internal incidents, or attacks or incidents involving the external ecosystem.[3]
- Based on this percentage and because Airlock Digital addresses 80% of those breaches for the composite, the solution reduces the organization's overall risk of a breach by more than 25%.
- The value of this benefit incorporates the full cost of a breach, including labor, direct expenses, and lost revenue while accounting for savings from breach remediation and improvements to mean time to identify (MTTI) and mean time to resolve (MTTR).

Risks. Factors that may affect the benefit of strengthened security may include the following:

- The extent to which the organization keeps endpoints in enforcement mode.
- The organization's annual revenue.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $4.1 million.

0

Breaches interviewees' organizations have had since implementing Airlock Digital

> *"Since we rolled out Airlock, we haven't had a single breach. That's a big deal for us, especially given the size of our environment and the sensitivity of the data we handle."*
>
> **System administrator, vehicle, sales, rental, and leasing**

Strengthened Security					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Total annual risk exposure to security breaches for the composite organization	Forrester research	$3,149,000	$3,149,000	$3,149,000
A2	Percent of breaches originating from external attacks targeting organizations, external attacks targeting remote environments, internal incidents, or attacks or incidents involving the external ecosystem	Forrester research	81%	81%	81%
A3	Percent of those attacks addressable with Airlock Digital	Interviews	80%	80%	80%
At	Strengthened security	A1*A2*A3	$2,040,552	$2,040,552	$2,040,552
	Risk adjustment	↓20%			
Atr	Strengthened security (risk-adjusted)		$1,632,442	$1,632,442	$1,632,442
	Three-year total: $4,897,326			**Three-year present value: $4,059,641**	

Improved Software Inventory Management

Evidence and data. Interviewees said the following about how Airlock Digital improved their organizations' software inventory management:

- The technical lead of cybersecurity at the insurance organization said, "We don't actually have to do much with it day-to-day on those machines that are running in enforcement mode. … The actual effort on a daily basis would be probably less than 30 minutes just to check that everything's going smoothly and there are no unexpected errors or blocks or anything like that. It's pretty low-touch. If we do see something we can quickly remediate, [it's] a couple-minute job to fix."
- The CSO at the equipment rental organization said, "We did a lot of baseline load testing of all the combinations of solutions, and the one with Airlock had negligible overhead compared to the other combinations that we used, including the incumbent."

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite has one security analyst who spends about 30 minutes per day maintaining Airlock Digital.
- The hourly rate for a security analyst (including overhead) is $81.

Risks. The actual benefit may vary due to the amount of times an exception must be made to allow a new permission.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.3 million.

2.5 hours

Weekly time security analysts need to maintain Airlock Digital

> *"Before Airlock, we had multiple tools and manual processes to track software, enforce policies, and respond to incidents. Airlock consolidated all that. We're spending less time managing endpoints and more time focusing on strategic initiatives."*
>
> **CSO, equipment rental**

Improved Software Inventory Management					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	Annual software spend on license and maintenance	Composite	$12,000,000	$12,000,000	$12,000,000
B2	Percent saved from improved software inventory management	Interviews	5%	5%	5%
Bt	Improved software inventory management	B1*B2	$600,000	$600,000	$600,000
	Risk adjustment	↓15%			
Btr	Improved software inventory management (risk-adjusted)		$510,000	$510,000	$510,000
	Three-year total: $1,530,000			**Three-year present value: $1,268,295**	

Improved SOC And IT Operations

Evidence and data. Interviewees reported an unexpected benefit during the initial audit phase of Airlock Digital's deployment. When reviewing the logs of applications running on the network, IT managers found licensed applications that were never executed, as well as duplicate applications serving the same function in different departments. By eliminating idle tools and consolidating overlapping ones, the organizations reduced software licensing costs and associated maintenance overhead.

- The technical lead of cybersecurity at the insurance organization said: "We can see exactly what's running on every endpoint. That level of visibility just wasn't possible before."
- The SVP of network security at the financial services organization said: "We now have a real-time view of what's running across the network. That's helped us catch unauthorized applications and tighten our controls."
- The system administrator at the vehicle, sales rental and leasing organization said: "Airlock gave us full visibility and control over all 10,000 endpoints. We went from having blind spots to knowing exactly what's running."

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite previously spent $12 million on software licenses and management each year.
- The composite reduces that spend by 5% beginning in Year 1.
- The composite continues to monitor its software inventory through Airlock Digital logs to prevent redundant installations and eliminate applications that are no longer needed through in Years 2 and 3.

Risks. The actual benefit may vary due to:

- The amount the organization spends on software licenses.
- The extent to which the organization has already implemented an allowlisting solution.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $186,000.

5%

Software cost reduction

> *"We found inefficiencies in our software spend. For example, we had two tools that do the same thing that two different teams were using. We had some instances where we were paying a per-asset license, and we'd find those assets in a base image for machines that never used them. Our savings by consolidating or eliminating those redundant and idle apps could amount to millions over the next three years."*
>
> **CSO, equipment rental**

Improved SOC And IT Operations					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Time saved on maintenance (hours)	Interviews	520	520	520
C2	Average fully loaded hourly cost of a security analyst	Composite	$81	$81	$81
C3	Operational efficiency from reduced solution maintenance	C1*C2	$42,120	$42,120	$42,120
C4	Application support analysts	Composite	10	10	10
C5	Percent of reduced application management time from improved software inventory management	Interviews	5%	5%	5%
C6	Time saved on application management (hours)	C4*C5*2,080	1,040	1,040	1,040
C7	Average fully loaded hourly cost of an application support analyst	Composite	$65	$65	$65
C8	Operational efficiency from improved software inventory	C6*C7	$67,600	$67,600	$67,600
C9	Productivity recapture	Research data	80%	80%	80%
Ct	Improved SOC and IT operations	(C3+C8)*C9	$87,776	$87,776	$87,776
	Risk adjustment	↓15%			
Ctr	Improved SOC and IT operations (risk-adjusted)		$74,610	$74,610	$74,610
	Three-year total: $223,830			**Three-year present value: $185,543**	

Unquantified Benefits

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

- **Enterprisewide user productivity improvements.** Interviewees explained that fewer outages mean fewer work disruptions and noted that Airlock Digital enforces application control without introducing latency or blocking legitimate work.
- **On-demand exceptions and transparent logging.** The assurance that users could swiftly request a one-time pass to run previously unapproved applications when necessary enabled teams adopt a deny-by-default posture without disrupting productivity. In addition to flexible exception handling, Airlock's logging capabilities were highlighted as a major benefit. These detailed, customizable logs helped IT teams monitor and audit exception periods by user or event type, simplifying oversight and reducing administrative burden.
- **The ability to customize the solution by user group.** Interviewees emphasized that Airlock Digital provides flexibility to tailor application control policies to specific user groups. They said this capability goes beyond general security improvements and demonstrates granular control over application access. This group-level customization made it easier for their organizations to

adopt a deny-by-default posture without disrupting workflows. By segmenting users based on their operational needs, teams could enforce strict controls while still supporting flexibility for developers, power users, or other exception groups.

> *"We can query user activity to find out exactly what was run on a given machine, which is incredibly helpful when someone is in audit mode or running something outside the allow list. The logs that Airlock generates are much easier to translate and dig through compared to [those generated by] our previous solution, which makes it far simpler to investigate and validate exceptions."*
>
> **SVP of network security, financial services**

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**
Dtr	Enterprise license fees	$0	$500,000	$500,000	$500,000	$1,500,000	$1,243,426
Etr	Technical implementation and maintenance	$3,888	$244	$244	$244	$4,624	$4,494
Ftr	Policy and protocol development	$421,848	$0	$0	$0	$421,848	$421,848
	Total costs (risk-adjusted)	$425,740	$500,244	$500,244	$500,244	$1,926,467	$1,669,768

Enterprise License Fees

Evidence and data. Interviewees reported their organizations pay enterprise license fees based on the number of endpoints under protection.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite has a total of 20,000 endpoints under Airlock Digital enforcement.
- The composite's license fees are $25 per endpoint per year.

Risks. Forrester applies no risk adjustment to this cost.

Results. Enterprise License Fees for the composite amount to a three-year total PV (discounted at 10%) of $1.2 million.

$25

License fee per endpoint per year

> *"The cost is low, and the effectiveness of the tool is incredibly high."*
>
> **CSO, equipment rental**

Enterprise License Fees						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
D1	Airlock license fee per endpoint	Airlock Digital	$0	$25	$25	$25
D2	Total endpoints	Composite	0	20,000	20,000	20,000
Dt	Enterprise license fees	D1*D2	$0	$500,000	$500,000	$500,000
	Risk adjustment	0%				
Dtr	Enterprise license fees (risk-adjusted)		$0	$500,000	$500,000	$500,000
	Three-year total: $1,500,000			**Three-year present value: $1,243,426**		

Technical Implementation And Maintenance

Evidence and data. Interviewees reported that technical implementation was very straightforward, and there were no significant complications or challenges. The technical lead of cybersecurity for the insurance organization said: "Once we had the initial policy built, we could have rolled out Airlock across the Zero Trust laptop fleet in a single day if we wanted to be aggressive. The actual build took about two weeks, but the deployment itself was fast and straightforward."

Modeling and assumptions. Based on the interviews, Forrester assumes the composite organization requires 40 hours of effort from one security analyst to deploy Airlock Digital.

Risks. This cost may vary due to:

- The time the organization spends on technical implementation.
- The average hourly wage (including overhead) of a security analyst.

Results. To account for these risks, Forrester adjusted this cost upward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $35,000.

$35K

3-year NPV of technical implementation and maintenance cost

> *"It took us about three to four months to develop the policies and roll out Airlock across our environment. That timeline included not just the technical setup, but also the internal coordination, testing, and ensuring we had the right controls in place. For a security product, that's a pretty fast turnaround."*
>
> **System administrator, vehicle sales, rental, and leasing**

Technical Implementation And Maintenance						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	Average fully loaded hourly cost of a security analyst	Composite	$81	$81	$81	$81
E2	Security analyst time to configure (hours)	Composite	40	0	0	0
E3	Security analyst time to maintain and monitor (hours)	Composite	0	130	130	130
Et	Technical implementation and maintenance	E1*(E2+E3)	$3,240	$10,530	$10,530	10,530
	Risk adjustment	↑20%				
Etr	Technical implementation and maintenance (risk-adjusted)		$3,888	$12,636	$12,636	$12,636
	Three-year total: $41,796			**Three-year present value: $35,312**		

Policy And Protocol Development

Evidence and data. Interviewees indicated that before implementing Airlock Digital, their organizations spent approximately 12 weeks in Audit mode to define the policies and protocols that would govern Enforcement mode.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- A team of two managers and three security analysts work on policy and protocol development.

- The fully loaded hourly cost of a manager is $111.
- The fully loaded hourly cost of a security analyst is $81.
- The composite runs Airlock Digital in Audit mode for one full quarter before switching to Enforcement mode.
- After the Audit phase, the composite handles all additional policy and protocol development as a part of regular maintenance.

Risks. This cost may vary due to:

- The number of team members assigned to policy and protocol development.
- The average hourly wage (including overhead) of a security analyst.
- The average hourly wage (including overhead) of a manager.
- The time needed to develop policies and protocols.

Results. This yields a three-year total PV of $422,000.

$422K

3-year NPV cost of policy and protocol development

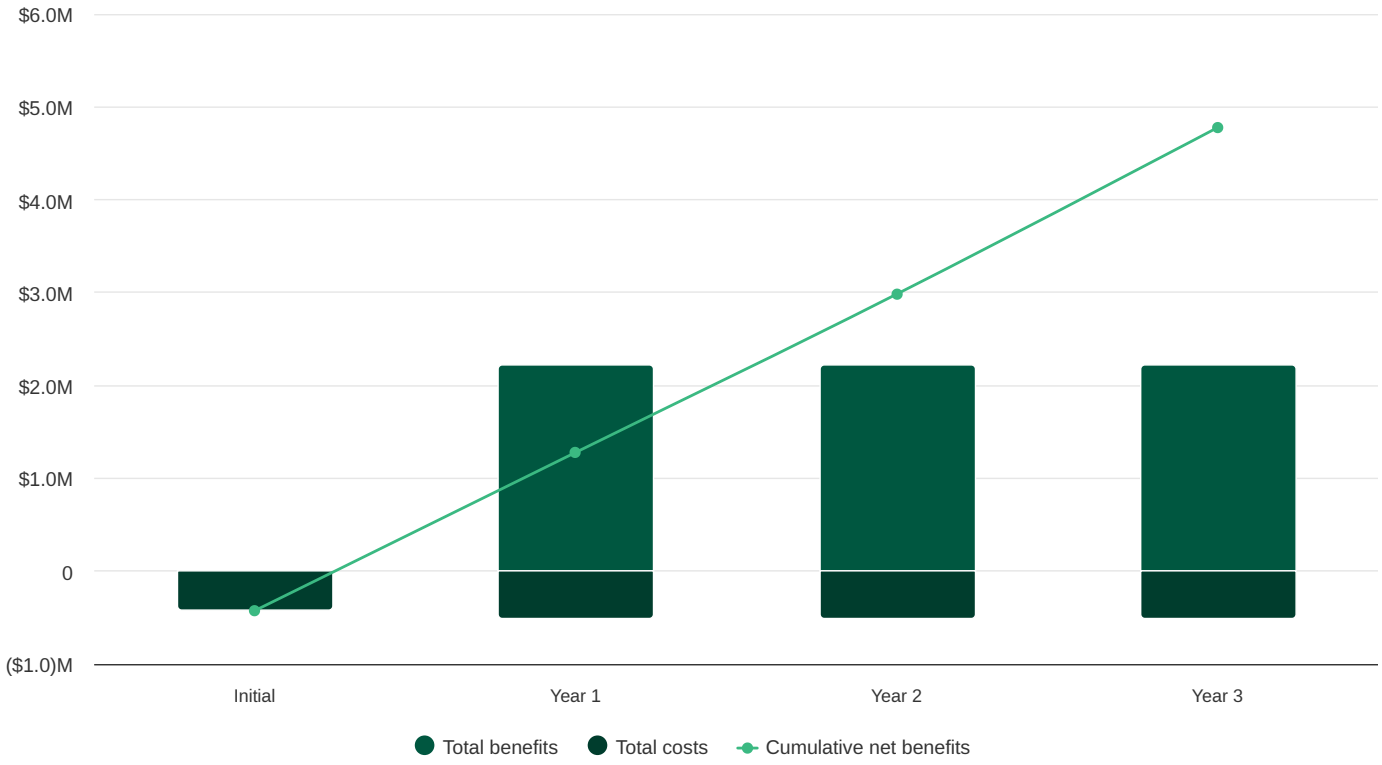
> *"We probably saw a 5% to 10% reduction in software spend just by removing things that were redundant or not being used."*
>
> **SVP of network security, financial services**

Policy And Protocol Development						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
F1	Time to enforcement status (weeks)	Composite	12			
F2	Average fully loaded hourly cost of a team member	Composite	$93			
F3	Weekly time spent developing policies and protocols (hours)	Composite	30			
F4	Team members	Composite	12			
Ft	Policy and protocol development	F1*F2*F3*F4	$401,760	$0	$0	$0
	Risk adjustment	↑5%				
Ftr	Policy and protocol development (risk-adjusted)		$421,848	$0	$0	$0
		Three-year total: $421,848			**Three-year present value: $421,848**	

Financial Summary

Consolidated Three-Year, Risk-Adjusted Metrics

Cash Flow Chart (Risk-Adjusted)



Cash Flow Analysis (Risk-Adjusted)						
	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($425,736)	($512,636)	($512,636)	($512,636)	($1,963,644)	($1,700,586)
Total benefits	$0	$2,217,051	$2,217,074	$2,217,074	$6,651,222	$5,513,479
Net benefits	($425,736)	$1,704,415	$1,704,145	$1,794,145	$4,687,510	$3,812,893
ROI						224%

Please Note

The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, and NPV for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

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

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.

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 Airlock Digital.

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 Airlock Digital can have on an organization.

Due Diligence

Interviewed Airlock Digital stakeholders and Forrester analysts to gather data relative to Airlock Digital.

Interviews

Interviewed four decision-makers at organizations using Airlock Digital to obtain data about 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.

Glossary

Total Economic Impact Approach

Benefits

Benefits represent the value the solution delivers to the business. The TEI methodology places equal weight on the measure of benefits and costs, allowing for a full examination of the solution's effect on the entire organization.

Costs

Costs comprise all expenses necessary to deliver the proposed value, or benefits, of the solution. The methodology captures implementation and ongoing costs associated with the solution.

Flexibility

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

Risks

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."

Financial Terminology

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%.

Appendixes

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 solution providers in communicating their value proposition to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of business and technology initiatives to both senior management and other key stakeholders.

APPENDIX B

Endnotes

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

[2] Cumulative breach costs are computed using the composite organization's size (revenue or number of employees) as an input to a regression analysis of reported total cumulative costs for all breaches for organizations that experienced at least one breach in the past 12 months. Source: Forrester's Security Survey, 2025, "Using your best estimate, what was the total cumulative cost of all breaches experienced by your organization in the past 12 months?" Base: 1,740 global security decision-makers whose organization has experienced a breach in the past 12 months. The cumulative breach cost is then multiplied by a 67% likelihood for organizations to experience one or more breaches in a given year. Source: Forrester's Security Survey, 2025, "How many times do you estimate that your organization's sensitive data was potentially compromised or breached in the past 12 months?" Base: 2,643 global security decision-makers.

[3] Percent of breaches by primary attack vector, as reported by security decision-makers whose organizations experienced at least one breach in the last 12 months. Source: Forrester's Security Survey, 2025, "Of the times that your organization's sensitive data was potentially compromised or breached in the past 12 months, please indicate how many of each fall into the categories below." Base: 1,766 global security decision-makers who have experienced a breach in the past 12 months.

Disclosures

Readers should be aware of the following:

This study is commissioned by Airlock Digital 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 Airlock Digital. For any interactive functionality, the intent is for the questions to solicit inputs specific to a prospect's business. Forrester believes that this analysis is representative of what companies may achieve with Airlock Digital based on the inputs provided and any assumptions made. Forrester does not endorse Airlock Digital or its offerings. Although great care has been taken to ensure the accuracy and completeness of this model, Airlock Digital and Forrester Research are unable to accept any legal responsibility for any actions taken on the basis of the information contained herein. The interactive tool is provided 'AS IS,' and Forrester and Airlock Digital make no warranties of any kind.

Airlock Digital 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.

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

Consulting Team:
Mary Barton

PUBLISHED
December 2025