A Forrester Total Economic Impact™ Study

Commissioned By Armor

Project Director:
Bob Cormier, Vice President And Principal Consultant

January 2017

The Total Economic Impact™ Of The Armor Complete And Armor Anywhere Solutions

Cost Savings And Business Benefits Attributed To The Armor Complete And Armor Anywhere Solutions

FORRESTER®

Table Of Contents

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®

Executive Summary

In late 2016, Armor commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study to examine the potential return on investment (ROI) enterprises may realize by deploying the Armor Complete and Armor Anywhere solutions. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of the Armor Complete and Armor Anywhere solutions within their organizations.

To better understand the benefits, costs, and risks associated with an investment in the Armor Complete and Armor Anywhere solutions, Forrester interviewed six Armor customers. We then created a composite or representative *Organization* to tell the ROI and benefit story of the Armor Complete and Armor Anywhere solutions. For a description of the six customers and the composite *Organization*, see the section titled Analysis.

The Armor Complete and Armor Anywhere solutions helped the *Organization* achieve the following benefits (risk- and present value [PV]-adjusted) over three years, totaling $1,663,095:

- **$471,507 — Armor Anywhere — security and compliance staff avoided.**
- **$278,527 — Armor Anywhere — security operations center staff avoided.**
- **$19,248 — Armor Anywhere — OS-level security tools cost avoidance.**
- **$507,318 — Armor Complete — security and compliance staff avoided.**
- **$334,233 — Armor Complete — security operations center staff avoided.**
- **$52,261 — Armor Complete — network-level and OS-level security tools cost avoidance.**

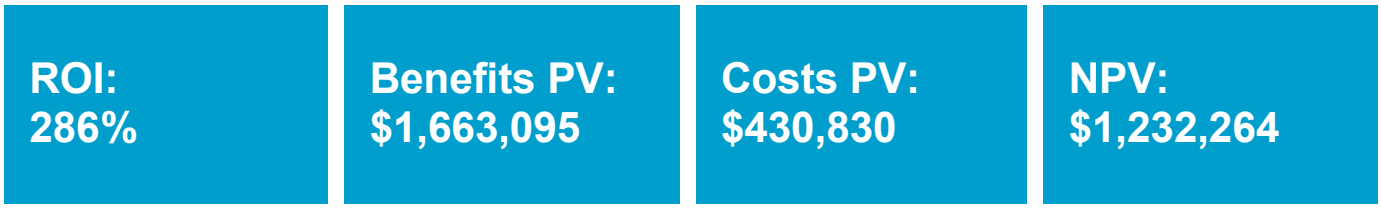
According to Armor, it delivers true and measurable security outcomes to organizations. Armor's proprietary, closed-loop secure cloud hosting approach unburdens businesses by reducing the risk and complexity associated with managing cyberthreats. For more details, see the section titled: The Armor Complete And Armor Anywhere solutions: Overview.

Prior to investing in Armor Complete, the *Organization* owned its hardware, which resided at a colocation facility. With Armor Complete, it rebuilt and redeployed new software instances and transferred data to Armor's secure cloud. Prior to investing in Armor Anywhere, the *Organization* was using basic security technologies and processes.

ARMOR COMPLETE AND ARMOR ANYWHERE SOLUTIONS DELIVER A 286% RETURN ON INVESTMENT

Our interviews and subsequent financial analysis found that the *Organization* experienced the risk-adjusted ROI, benefits, and costs shown in Figure 1. The analysis points to risk-adjusted benefits of $1,663,095 over three years versus costs of $430,830, equating to a net present value (NPV) of $1,232,264. The three-year risk-adjusted ROI was a favorable 286%, and the payback period was a quick four months.

FIGURE 1
Financial Summary Showing Three-Year Risk-Adjusted Results



Source: Forrester Research, Inc.

In our interviews, Forrester identified the following benefit categories of the Armor Complete and Armor Anywhere solutions. The *Organization* experienced the following benefits totaling $1,663,095 (risk- and present value-adjusted) over three years, further described in the Benefits: Quantified section:

- $471,507 — Armor Anywhere — security and compliance staff avoided.
- $278,527 — Armor Anywhere — security operations center staff avoided.
- $19,248 — Armor Anywhere — OS-level security tools cost avoidance.
- $507,318 — Armor Complete — security and compliance staff avoided.
- $334,233 — Armor Complete — security operations center staff avoided.
- $52,261 — Armor Complete — network-level and OS-level security tools cost avoidance.

In our interviews, Forrester also identified five cost categories. The *Organization* experienced the following costs totaling $430,830 (present value-adjusted) over three years, further described in the Costs section:

- $560 — Costs to plan and deploy Armor Anywhere.
- $21,818 — Costs to plan and deploy Armor Complete.
- $72,727 — Data and application migration for Armor Complete.
- $126,829 — Armor Anywhere fees.
- $208,896 — Armor Complete fees.

If the risk-adjusted ROI and NPV of costs and benefits still demonstrate a compelling business case, it raises confidence that the investment is likely to succeed because the risks that threaten the project have been taken into consideration and quantified. The risk-adjusted numbers should be taken as “realistic” expectations, as they represent the expected value considering risk. Assuming normal success at mitigating risk, the risk-adjusted numbers should more closely reflect the expected outcome of the investment.

“The Armor Complete solution allows us to spin up applications quicker, go after new business, and keep current clients. Armor allows faster time-to-market and at a lower cost.”

— Executive vice president; pharmaceutical consulting organization

Disclosures

The reader should be aware of the following:

- The study is commissioned by Armor and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.
- Forrester makes no assumptions as to the potential return on investment 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 Armor Complete and Armor Anywhere solutions.
- Armor reviewed and provided feedback to Forrester, but Forrester maintained editorial control over the study and its findings and did not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study.
- The customer names for the interviews were provided by Armor. Armor did not participate in the customer interviews.

TEI Framework And Methodology

INTRODUCTION

From information provided in the interviews, Forrester has constructed a Total Economic Impact (TEI) framework for those organizations considering investing in the Armor Complete and Armor Anywhere solutions. The objective of the framework is to identify the benefits, costs, flexibility, and risk factors that affect the investment decision.

APPROACH AND METHODOLOGY

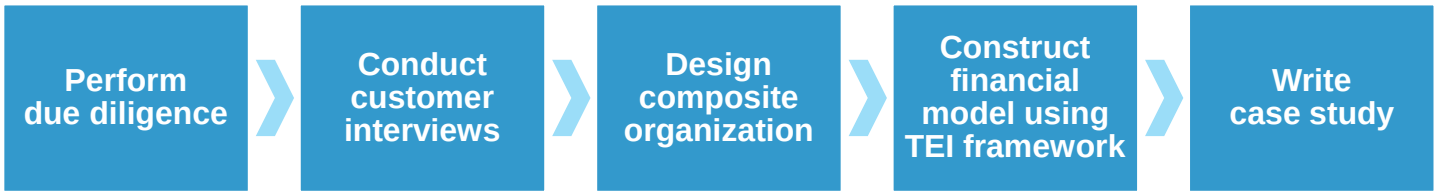
Forrester employed four fundamental elements of TEI in modeling the Armor Complete and Armor Anywhere solutions: benefits, costs, flexibility options, and risks.

Forrester took a multistep approach to evaluate the impact that the Armor Complete and Armor Anywhere solutions can have on the *Organization* (see Figure 2). Specifically, we:

- Interviewed Armor marketing, sales, and product management personnel to better understand the value proposition for the Armor Complete and Armor Anywhere solutions.
- Constructed a financial model representative of the interviews using the TEI methodology. The financial model is populated with the cost and benefit data obtained from the interviews.
- Risk-adjusted the financial model based on any issues or concerns the six customers highlighted in interviews. Risk adjustment is a key part of the TEI methodology. While the customers provided cost and benefit estimates, some categories included partial projections or a broad range of responses, or had a number of internal forces that might have raised or lowered the benefits. For that reason, each benefit has been risk-adjusted and is detailed in each relevant section.

Given the increasing sophistication that enterprises have regarding ROI analyses related to technology investments, Forrester's TEI methodology serves to provide a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

FIGURE 2
TEI Approach



Source: Forrester Research, Inc.

Analysis

INTERVIEWED CUSTOMERS

Forrester derived its conclusions in large part from information received in a series of in-depth interviews we conducted with personnel across six Armor customer organizations. The following is a brief description of the interviewed customers, all of which were promised anonymity:

- A healthcare payments technology company that has been using Armor Complete for nine months. Forrester interviewed the vice president of strategy.
- An organization that secures and protects digital content. It has been using Armor Complete for over two years. Forrester interviewed the CEO of this organization.
- A Midwestern US credit union that has been using Armor Anywhere for 11 months. Forrester interviewed its senior information security analyst.
- The parent company of several travel, hospitality, and restaurant businesses. It has been using Armor Anywhere for three months. Forrester interviewed the director of technology.
- A provider of regulatory compliance software for the entertainment industry. It has been piloting Armor Anywhere for seven months. Forrester interviewed the CEO of this organization.
- A consulting organization specializing in compliance and reporting aspects of pharmaceutical programs. It has been using Armor Complete for eight months. Forrester interviewed the executive vice president, chief product and technology officer.

THE COMPOSITE ORGANIZATION

The composite *Organization* is a small enterprise with revenues of about $1 billion. Organizations with revenues between $50 million and $2 billion can benefit from an investment in Armor Complete and Armor Anywhere, either deployed as individual solutions or deployed together as part of a multicloud strategy.

The composite *Organization* has invested in the Armor Complete and Armor Anywhere solutions for the following workloads:

Armor Anywhere workloads (25 virtual machines [VMs]):

- Nonproduction data.
- No personally identifiable information (PII) or company IP.
- Risk-based level of security performance and availability.
- Early-stage development.

Armor Complete workloads (six VMs):

- “Tier 0” applications.
- Applications/data with PII that require high-level access.
- Data and application security.
- Compliance with regulatory (HIPAA) mandates required.

The following Armor Complete add-ons were purchased or were included in the Armor Complete fees, some of which were mandatory for HIPAA and PCI compliance:

- Secure sockets layer (SSL), virtual private network (VPN), plus two-factor authentication (2FA).
- Vulnerability scanning.
- Log monitoring and management.
- Deployment planning.
- Health check and monitoring.
- Migration.
- Load testing.
- Encryption.
- Backup and recovery solution.

Prior to investing in Armor Complete, the *Organization* owned its hardware, which resided at a colocation facility. With Armor Complete, it rebuilt and redeployed new software instances and transferred data to Armor's facilities. Prior to investing in Armor Anywhere, the *Organization* was using basic security technologies.

With its investment in the Armor Complete and Armor Anywhere solutions, the *Organization*'s goals and objectives were to:

- Find a secure managed environment that it did not have to worry about.
- Support compliance with regulatory (HIPAA) mandates.
- Accommodate the new focus on software-as-a-service (SaaS) within healthcare.
- Avoid cost of hiring security staff.
- Avoid cost and complexity of purchasing security tools.
- Ensure 24x7 monitoring of threats to mission-critical systems and other systems.
- Avoid a poor security audit result.

"The people at Armor are very engaging; when you have a particular question there are several people on the call to help answer it. We meet about every other week, and there's a team of Armor people on these calls also. I feel very well supported by Armor."

— Director of technology, parent company of several travel, hospitality, and restaurant businesses

BENEFITS: QUANTIFIED

The *Organization* experienced quantified benefits in six major categories, which are further described below:

- Armor Anywhere — security and compliance staff avoided.
- Armor Anywhere — security operations center staff avoided.

- Armor Anywhere — OS-level security tools and services cost avoidance.
- Armor Complete — security and compliance staff avoided.
- Armor Complete — security operations center staff avoided.
- Armor Complete — network-level and OS-level security tools cost avoidance.

Armor Anywhere — Security And Compliance Staff Avoided

During Forrester's interviews, we asked Armor Anywhere customers to think about the level of security and compliance provided by Armor Anywhere. We then asked what additional security staff they would have to hire to provide the same level of security and compliance in-house. We provided interviewees with a list of security job functions that are provided and included with Armor Anywhere. The consensus among the customers was that at least two staff would have to be added: a cyberintelligence analyst and a threat intelligence analyst. Table 1 includes the security and compliance staff cost avoidance savings attributed to Armor Anywhere. Salaries represent average fully loaded costs provided by the interviewed customers.

There were a variety of responses from the customers both in terms of job functions needed and salaries. Due to this variability, this benefit was risk-adjusted (reduced) by 20% in Table 1. See the section on Risks for more detail.

TABLE 1
Armor Anywhere — Security And Compliance Staff Avoided

Ref.	Metric	Calculation/Source	Year 1	Year 2	Year 3
A1	Cyberintelligence analyst annual cost	Interviews	$111,000	$111,000	$111,000
A2	Threat intelligence analyst annual cost	Interviews	$126,000	$126,000	$126,000
At	Armor Anywhere — security and compliance staff cost avoided	A1 + A2	$237,000	$237,000	$237,000
	Risk adjustment	↓20%			
Atr	**Armor Anywhere — security and compliance staff avoided (risk-adjusted)**	**At – 20%**	**$189,600**	**$189,600**	**$189,600**

Source: Forrester Research, Inc.

Armor Anywhere — Security Operations Center Staff Avoided

During Forrester's interviews, we asked Armor Anywhere customers to think about the level of security and operations center (SOC) support provided by Armor Anywhere. We then asked what additional security staff they would have to hire to provide the same level of SOC support in-house. We provided interviewees with a list of security job functions that are provided and included with Armor Anywhere. The consensus among the customers was at least 1.5 FTE staff would have to be added: half a security engineer at an annual savings of $60,000 (half of the full-year cost of $120,000) and a systems administrator at an annual savings of 80,000. Table 2 includes the SOC staff cost avoidance savings attributed to Armor Anywhere. Salaries represent average fully loaded costs provided by the interviewed customers.

There were a variety of responses from the customers both in terms of job functions needed and salaries. Due to this variability, this benefit was risk-adjusted (reduced) by 20% in Table 2. See the section on Risks for more detail.

TABLE 2
Armor Anywhere — Security Operations Center Staff Avoided

Ref.	Metric	Calculation/Source	Year 1	Year 2	Year 3
B1	One-half security engineer annual cost	0.5 FTEs/interviews	$60,000	$60,000	$60,000
B2	Systems administrator annual cost	Interviews	$80,000	$80,000	$80,000
Bt	Armor Anywhere — security operations center staff cost avoided	B1 + B2	$140,000	$140,000	$140,000
	Risk adjustment	↓20%			
Btr	**Armor Anywhere — security operations center staff avoided (risk-adjusted)**	**Bt – 20%**	**$112,000**	**$112,000**	**$112,000**

Source: Forrester Research, Inc.

Armor Anywhere — OS-level Security Tools And Services Cost Avoidance

Interviewed customers reported being able to retire and/or avoid buying the following OS-level security tools and services upon their investment in Armor Anywhere: vulnerability monitoring, log management, malware protection, OS patch management, and integrity monitoring. Customers reported total cost avoidance savings between $7,200 and $10,000 annually, with Forrester using the average of $8,600 in savings per year. See Table 3.

Forrester risk-adjusted (reduced) these benefits by 10% to acknowledge the wide variety of security tool vendors, products, and prices.

TABLE 3
Armor Anywhere — OS-level Security Tools And Services Cost Avoidance

Ref.	Metric	Calculation/Source	Year 1	Year 2	Year 3
C1	OS-level security tools cost avoidance	Interviews	$8,600	$8,600	$8,600
Ct	Armor Anywhere — OS-level security tools and services cost avoidance	C1	$8,600	$8,600	$8,600
	Risk adjustment	↓10%			
Ctr	**Armor Anywhere — OS-level security tools and services cost avoidance (risk-adjusted)**	**Ct – 10%**	**$7,740**	**$7,740**	**$7,740**

Source: Forrester Research, Inc.

Armor Complete — Security And Compliance Staff Avoided

During Forrester's interviews, we asked Armor Complete customers to think about the level of security and compliance provided by Armor Complete. We then asked what additional security staff they would have to hire to provide the same level

of security and compliance in-house. We provided interviewees with a list of security job functions that are provided and included with Armor Complete. The consensus among the customers was that at least two staff would have to be added: a chief information security officer (CISO) and security incident manager. Table 4 includes the security and compliance staff cost avoidance savings attributed to Armor Complete. Salaries represent average fully loaded costs provided by the interviewed customers.

There were a variety of responses from the customers both in terms of job functions needed and salaries. Due to this variability, this benefit was risk-adjusted (reduced) by 20% in Table 4. See the section on Risks for more detail.

TABLE 4
Armor Complete — Security And Compliance Staff Avoided

Ref.	Metric	Calculation/Source	Year 1	Year 2	Year 3
D1	Chief security officer annual cost	Interviews	$175,000	$175,000	$175,000
D2	Security incident manager annual cost	Interviews	$80,000	$80,000	$80,000
Dt	Armor Complete — security and compliance staff avoided	D1 + D2	$255,000	$255,000	$255,000
	Risk adjustment	↓20%			
Dtr	**Armor Complete — security and compliance staff avoided (risk-adjusted)**	**Dt – 20%**	$204,000	$204,000	$204,000

Source: Forrester Research, Inc.

Armor Complete — Security Operations Center Staff Avoided

During Forrester's interviews, we asked Armor Complete customers to think about the level of security and compliance provided by Armor Complete. We then asked what additional security operations center staff they would have to hire to provide the same level of security and compliance in-house. We provided interviewees with a list of security operations center job functions that are provided and included with Armor Complete. The consensus among the customers was that at least 1.5 FTE staff would have to be added: a penetration tester at an annual savings of $108,000 and half a security engineer at an annual savings of $60,000 (half of the full-year cost of $120,000). Table 5 includes the security operations center staff cost avoidance savings attributed to Armor Complete. Salaries represent average fully loaded costs provided by the interviewed customers.

There were a variety of responses from the customers both in terms of job functions needed and salaries. Due to this variability, this benefit was risk-adjusted (reduced) by 20% in Table 5. See the section on Risks for more detail.

TABLE 5
Armor Complete — Security Operations Center Staff Avoided

Ref.	Metric	Calculation/Source	Year 1	Year 2	Year 3
E1	Penetration tester annual cost	Interviews	$108,000	$108,000	$108,000
E2	One-half security engineer annual cost	0.5 FTEs/interviews	$60,000	$60,000	$60,000
Et	Armor Complete — security operations center staff avoided	E1 + E2	$168,000	$168,000	$168,000
	Risk adjustment	↓20%			
Etr	**Armor Complete — security operations center staff avoided (risk-adjusted)**	**Et – 20%**	**$134,400**	**$134,400**	**$134,400**

Source: Forrester Research, Inc.

Armor Complete — Network-Level And OS-Level Security Tools Cost Avoidance

Interviewed customers reported being able to retire and/or avoid buying the following network-level security tools and services upon their investment in Armor Complete: a web application firewall, SSL VPN, and two-factor authentication. Customers reported total cost avoidance savings between $13,500 and $16,000 annually, with Forrester using the average of $14,750 in savings per year.

Customers reported being able to retire or avoid buying the following OS-level security tools: vulnerability monitoring, log management, malware protection, OS patch management, and integrity monitoring. Customers reported total cost avoidance savings between $7,200 and $10,000 annually, with Forrester using the average of $8,600 in savings per year. See Table 6.

Forrester risk-adjusted (reduced) these benefits by 10% to acknowledge the wide variety of edge security tool vendors, products, and prices.

TABLE 6
Armor Complete — Network-Level And OS-Level Security Tools Cost Avoidance

Ref.	Metric	Calculation/Source	Year 1	Year 2	Year 3
F1	Network-level security tools cost avoidance	Interviews	$14,750	$14,750	$14,750
F2	OS-level security tools cost avoidance	Interviews	$8,600	$8,600	$8,600
Ft	Armor Complete — network-level and OS-level security tools cost avoidance	F1 + F2	$23,350	$23,350	$23,350
	Risk adjustment	↓10%			
Ftr	**Armor Complete — network-level and OS-level security tools cost avoidance (risk-adjusted)**	Ft – 10%	**$21,015**	**$21,015**	**$21,015**

Source: Forrester Research, Inc.

Total Benefits

Table 7 shows the total of all benefits as well as present values (PVs) discounted at 10%. Over three years, the *Organization* expects risk-adjusted total benefits to be a PV of $1,663,095.

TABLE 7
Total Quantified Benefits (Risk-Adjusted)

Ref.	Benefit Category	Year 1	Year 2	Year 3	Total	Present Value
Atr	Armor Anywhere — security and compliance staff avoided	$189,600	$189,600	$189,600	$568,800	$471,507
Btr	Armor Anywhere — security operations center staff avoided	$112,000	$112,000	$112,000	$336,000	$278,527
Ctr	Armor Anywhere — OS-level security tools cost avoidance	$7,740	$7,740	$7,740	$23,220	$19,248
Dtr	Armor Complete — security and compliance staff avoided	$204,000	$204,000	$204,000	$612,000	$507,318
Etr	Armor Complete — security operations center staff avoided	$134,400	$134,400	$134,400	$403,200	$334,233
Ftr	Armor Complete — network-level and OS-level security tools cost avoidance	$21,015	$21,015	$21,015	$63,045	$52,261
	Total benefits (risk-adjusted)	**$668,755**	**$668,755**	**$668,755**	**$2,006,265**	**$1,663,095**

Source: Forrester Research, Inc.

BENEFITS: UNQUANTIFIED

The interviewed customers identified the following additional benefits of using the Armor Complete and Armor Anywhere solutions but were not able to quantify the benefits at the present time:

- According to the interviewed customers, Armor Complete eliminates noise and improves compliance and visibility. These were demonstrable outcomes.
- Dwell time is a leading metric in measuring the proficiency of a given security strategy and its related processes, policies, and controls. It's defined as the number of days a threat actor remains undetected within a given environment until remediation. Anecdotally, the interviewed customers believe that dwell time is improved with Armor Complete, but it did not have direct evidence to allow for quantification at interview time.
- Compliance audits take less time to perform, according to the interviewed customers. Armor's customers' auditors and assessors have access to tools that automate vulnerability scanning of internal and external networks, facilitating the compliance and assessment process and providing self-assessment tools including self-assessment questionnaires.

"It only took us only 16 hours to plan the implementation of Armor Anywhere. Instructions were very easy: Here's the executable file, here's where to deploy it, here are the firewall rules to allow outbound connection to Armor, and that's it!"

— Senior information security analyst, US credit union

COSTS

The *Organization* incurred costs in the following categories with its investment in the Armor Complete and Armor Anywhere solutions.

Labor Cost To Plan And Deploy The Armor Complete And Armor Anywhere Solutions

The internal labor associated with planning and deploying the Armor Anywhere solution totaled 16 hours. Tasks included a systems administrator following instructions to deploy the Armor Anywhere executable file and establish firewall rules to allow outbound connection to Armor. At a labor expense of $38.50 per hour, the cost to plan and deploy Armor Anywhere was $616 (16 hours * $38.50 per hour = $616).

The internal labor associated with planning and deploying the Armor Complete solution totaled 400 hours over five weeks and included work by the chief security officer, security engineer, and a systems administrator. At an average hourly labor rate of $60, the cost to plan and deploy Armor Complete was $24,000 (400 hours * $60 per hour = $24,000).

The *Organization* hired contractors in conjunction with Armor's professional servicers to migrate data from applications in its data center into the Armor environment, at a total cost of $80,000. Armor's onboarding services helped to expedite the process and eliminate concerns around application and data migration to Armor's secure cloud. Armor provided the following assistance: initial environmental configuration, data migration, final data sync and cutover, and resource dedication.

Armor Complete And Armor Anywhere Fees

The fee categories for the Armor Complete and Armor Anywhere solutions are listed in Table 8.

TABLE 8
Total Costs Associated With Armor Complete And Armor Anywhere Solutions

	Cost		Year 1	Year 2	Year 3	Total	Present Value
G1	Costs to plan and deploy Armor Anywhere	Interviews	$616	$0	$0	$616	$560
G2	Costs to plan and deploy Armor Complete	Interviews	$24,000	$0	$0	$24,000	$21,818
G3	Data and application migration for Armor Complete	Interviews	$80,000	$0	$0	$80,000	$72,727
G4	Armor Anywhere fees	Armor quote	$51,000	$51,000	$51,000	$153,000	$126,829
G5	Armor Complete fees	Armor quote	$84,000	$84,000	$84,000	$252,000	$208,896
Gt	Total costs associated with Armor Complete and Armor Anywhere	G1:G5	$239,616	$135,000	$135,000	$509,616	$430,830
	Risk adjustment	↓0%					
Gtr	**Total costs associated with Armor Complete and Armor Anywhere (risk-adjusted)**	Gt-0%	**$239,616**	**$135,000**	**$135,000**	**$509,616**	**$430,830**

Source: Forrester Research, Inc.

Table 8 shows the total of all costs as well as associated present values, discounted at 10%. Over three years, the *Organization* expects costs to total $509,616, with a present value of $430,830. Forrester chose to not risk-adjust costs because the *Organization* has already incurred these expenses, most of which were fixed fees from Armor.

FLEXIBILITY OPTIONS

Flexibility, as defined by TEI, represents an investment in additional capacity or capability that could be turned into business benefit for some future additional investment. This provides an organization with the "right" or the ability (or option) to engage in future initiatives but not the obligation to do so. In our case study, it answers this question: Now that the *Organization* has invested in the Armor Complete and Armor Anywhere solutions, what other things (flexibility options) can it do cheaper, better, and/or faster as a result of that initial investment?

Forrester's study results include all costs and benefits in the initial three-year period that the *Organization* used the Armor Complete and Armor Anywhere solutions. In addition, the interviewed customers are considering the following future flexibility options:

- For Armor Complete, its cloud solution is all about flexibility and agility to scale up and down in the future.
- According to Armor, its SOC has visibility into many companies' threats and attacks that are thwarted and then categorized within Armor's intelligence engine, which then benefits all customers in the future. It would be cost-prohibitive for individual customers to replicate a similar SOC in-house.

› When customers hand off their infrastructure and security to Armor, it allows them to concentrate on core competencies such as application development and managing the business.

The interviewed customers agreed with the flexibility benefits above, but they were not able to articulate and quantify these flexibility option benefits. Therefore, Forrester did not quantify them for this study.

Forrester encourages readers to learn more about the Armor Complete and Armor Anywhere solutions' capabilities to determine the potential quantifiable flexibility option benefits for their organizations. The value of the flexibility option, when calculated, is based on the Black-Scholes Option Pricing formula. (For information regarding the flexibility calculation, please see Appendix A.)

RISKS

Forrester defines two types of risk associated with this analysis: "implementation risk" and "impact risk." Implementation risk is the risk that a proposed investment in the Armor Complete and Armor Anywhere solutions may deviate from the original or expected requirements, resulting in higher costs than anticipated. Impact risk refers to the risk that the business or technology needs of the *Organization* may not be met by the investment in the Armor Complete and Armor Anywhere solutions, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for cost and benefit estimates. Note: Forrester chose to not risk-adjust costs because the *Organization* has already incurred these expenses, most of which were fixed fees from Armor.

TABLE 9
Benefit And Cost Risk Adjustments

Benefits	Adjustment
Armor Anywhere — security and compliance staff avoided	↓ 20%
Armor Anywhere — security operations center staff avoided	↓ 20%
Armor Anywhere — OS-level security tools cost avoidance	↓ 10%
Armor Complete — security and compliance staff avoided	↓ 20%
Armor Complete — security operations center staff avoided	↓ 20%
Armor Complete — network-level and OS-level security tools cost avoidance	↓ 10%

Costs	Adjustment
(Costs were not risk-adjusted)	↑ 0%

Source: Forrester Research, Inc.

Highlighting impact risk by adjusting the benefits results in more meaningful and accurate estimates and a more accurate projection of the ROI. In general, risks affect costs by raising the original estimates, and they affect benefits by reducing the original estimates. The risk-adjusted numbers should be taken as "realistic" expectations since they represent the expected values considering risk.

The following implementation risk that affects costs is identified as part of this analysis:

- The Armor Complete and Armor Anywhere solutions fees may vary. Although Forrester did not risk-adjust the Armor Complete and Armor Anywhere solutions fees, other organizations' costs may differ due to variable discounts.

The following impact risk that affects benefits is identified as part of the analysis:

- The onboarding process for new Armor customers has risks associated with it. The migration of applications and data to the Armor data center cloud should be done with the help of Armor professional services. Customers reported that Armor's onboarding processes helped to mitigate the risks around application and infrastructure migration to Armor's secure cloud.
- The interviewed customers were using the Armor Complete and Armor Anywhere solutions in different ways, and not all customers were taking advantage of each benefit described in this study. Forrester took into account this variability, and Table 9 shows the risk-adjustment (downward) percentages used to adjust the benefits values in this study.

The TEI model uses a triangular distribution method to calculate risk-adjusted values. To construct the distribution, it is necessary to first estimate the low, most likely, and high values that could occur within the current environment. The risk-adjusted value is the mean of the distribution of those points. Readers are urged to apply their own risk ranges based on their own degree of confidence in the cost and benefit estimates.

> *"We are definitely saving a lot of time. With Armor Anywhere, it's almost like having network security staff onsite. Armor has a team of security professionals watching over our servers and applications 24x7."*
>
> — Director of technology, parent company of several travel, hospitality, and restaurant businesses

Financial Summary

The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the *Organization*'s investment in the Armor Complete and Armor Anywhere solutions, as outlined in Table 10.

Table 10 shows the risk-adjusted ROI, NPV, and payback period values. These values are determined by applying the risk-adjustment values from Table 9 in the Risks section to the total benefit and cost numbers in Table 7 and Table 8.

TABLE 10
Cash Flow (Risk-Adjusted)

	Year 1	Year 2	Year 3	Total	Present Value
Costs	($239,616)	($135,000)	($135,000)	($509,616)	($430,830)
Benefits	$668,755	$668,755	$668,755	$2,006,265	$1,663,095
Net benefits	**$429,139**	**$533,755**	**$533,755**	**$1,496,649**	**$1,232,264**
ROI	**286%**				
Payback period	**Four months**				

Source: Forrester Research, Inc.

The ROI was a favorable 286% with a quick four-month payback period. If the risk-adjusted costs, benefits, and ROI still demonstrate a compelling business case, it raises confidence that the investment is likely to succeed because the risks that might threaten the project have been taken into consideration and quantified. The risk-adjusted numbers should be taken as "realistic" expectations, as they represent the expected value considering risk. Assuming normal success at mitigating risk, the risk-adjusted numbers should more closely reflect the expected outcome of the investment.

The Armor Complete And Armor Anywhere Solutions: Overview

According to Armor, it delivers true and measurable security outcomes to organizations. Armor's proprietary, closed-loop secure cloud hosting approach unburdens businesses by reducing the risk and complexity associated with managing cyberthreats.

ANALYZE, AUTOMATE, AND MITIGATE

Designed in-house, Armor's automation controls drive scalability to deliver real security outcomes. This process — analyze, automate, and mitigate — empowers Armor's cloud security professionals to defeat the threats that target businesses. We've fine-tuned the balance between managed security, automation, and proprietary processes in the secure cloud.

CLOSE THE SECURITY LOOP

Armor's proprietary closed-loop system of intelligence, defense, and control automates real-time updates and streamlines the effectiveness of our world-class security operations center (SOC) in defending our secure cloud.

COMPLIANCE WILL FOLLOW

Armor's security-first approach is built to deliver compliance as an outcome. Gain the compliant hosting that businesses need while concurrently complying with robust industry regulations, including PCI and HIPAA.

ARMOR ANYWHERE

Experience Armor's cloud security's talent, techniques, and technology on any secure cloud, including public clouds, private clouds, or your own IT environments. Platforms secured with Armor anywhere include: Amazon Web Services, Microsoft Azure, Google Cloud Platform, and SoftLayer.

ARMOR COMPLETE

Armor's managed secure Virtual Private Cloud is a cloud hosting solution for organizations that store, access, or manage sensitive data that requires the best in performance and security. For critical or highly sensitive data, Armor Complete delivers a compliant, fully managed environment with the lowest possible risk of data breach or loss. For example:

- "Tier 0" applications.
- Applications/data with PII that require high-level access.
- Data and application security.
- Compliance with industry (PCI) or regulatory (HIPAA) mandates.
- Intellectual property.
- High-availability architecture.
- Low-latency performance requirements.

ARMOR COMPLETE OR ARMOR ANYWHERE?

Depending on performance requirements and data workload sensitivity, select either Armor Complete or Armor Anywhere, which may be integrated as part of a secure multicloud strategy.

Appendix A: Total Economic Impact™ Overview

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 technology initiatives to both senior management and other key business stakeholders.

The TEI methodology consists of four components to evaluate investment value: benefits, costs, flexibility, and risks.

BENEFITS

Benefits represent the value delivered to the user organization — IT and/or business units — by the proposed product or project. Often, product or project justification exercises focus just on technology cost and cost reduction, leaving little room to analyze the effect of the technology on the entire organization. The TEI methodology and the resulting financial model place 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. Calculation of benefit estimates involves a clear dialogue with the user organization to understand the specific value that is created. In addition, Forrester also requires that there be a clear line of accountability established between the measurement and justification of benefit estimates after the project has been completed. This ensures that benefit estimates tie back directly to the bottom line.

COSTS

Costs represent the investment necessary to capture the value, or benefits, of the proposed project. IT or the business units may incur costs in the form of fully burdened labor, subcontractors, or materials. Costs consider all the investments and expenses necessary to deliver the proposed value. In addition, the cost category within TEI captures any incremental costs over the existing environment for ongoing costs associated with the solution. All costs must be tied to the benefits that are created.

FLEXIBILITY

Within the TEI methodology, direct benefits represent one part of the investment value. While direct benefits can typically be the primary way to justify a project, Forrester believes that organizations should be able to measure the strategic value of an investment. Flexibility represents the value that can be obtained for some future additional investment building on top of the initial investment already made. For instance, an investment in an enterprise-wide upgrade of an office productivity suite can potentially increase standardization (to increase efficiency) and reduce licensing costs. However, an embedded collaboration feature may translate to greater worker productivity if activated. The collaboration can only be used with additional investment in training at some future point. However, having the ability to capture that benefit has a PV that can be estimated. The flexibility component of TEI captures that value.

RISKS

Risks measure the uncertainty of benefit and cost estimates contained within the investment. Uncertainty is measured in two ways: 1) the likelihood that the cost and benefit estimates will meet the original projections and 2) the likelihood that the estimates will be measured and tracked over time. TEI applies a probability density function known as "triangular distribution" to the values entered. At a minimum, three values are calculated to estimate the underlying range around each cost and benefit.

Appendix B: Glossary

Discount rate: The interest rate used in cash flow analysis to take into account the time value of money. Although the Federal Reserve Bank sets a discount rate, companies often set a discount rate based on their business and investment environment. Forrester assumes a yearly discount rate of 10% for this analysis. Most organizations typically use discount rates between 8% and 16% based on their current environment. Readers are urged to consult their respective organizations to determine the most appropriate discount rate to use in their own environment.

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.

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.

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.

Return on investment (ROI): A measure of a project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits minus costs) by costs.

A NOTE ON CASH FLOW TABLES

The following is a note on the cash flow tables used in this study (see the example table below). The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1. Those costs are not discounted. All other cash flows in years 1 through 3 are discounted using the discount rate (shown in the Framework Assumptions section) at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations are not calculated until the summary tables are the sum of the initial investment and the discounted cash flows in each year.

TABLE [EXAMPLE]
Example Table

Ref.	Metric	Calculation/Source	Year 1	Year 2	Year 3

Source: Forrester Research, Inc.