A Forrester Total Economic Impact™
Study Commissioned By Armor
August 2020

# The Total Economic Impact™ Of Armor Anywhere

## Cost Savings And Business Benefits Enabled By Armor Anywhere

FORRESTER®

# Table Of Contents




**Project Director:**
David Park

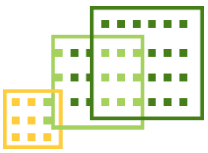

ABOUT FORRESTER CONSULTING

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



**$10,000,000**
Increase in addressable market

**64%**
Reduction in cost of security point solutions

**90%**
Reduction in rate of false positives

Armor Anywhere provides organizations with a comprehensive security and compliance solution that streamlines and optimizes security operations through an agent-based software that is deployed across on-premises, private, or public cloud computing environments. Armor commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Armor Anywhere. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Armor Anywhere on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four customers with years of experience using Armor Anywhere. Prior to adopting Armor Anywhere, customers leveraged a variety of security point solutions; with some being deployed either on-premises or in private clouds and others being deployed over the public cloud. Each of these deployments were fulfilling a specific security function such as log management or threat detection, and subsequently had varying levels of efficacy. However, as security and compliance requirements became more complex, these organizations faced steep licensing costs across their security stacks and struggled with managing, maintaining, and administering a diverse set of solutions. Consequently, these organizations sought out a partner that could quickly deliver the necessary security and compliance outcomes through a single platform, without the need for dedicated domain experts.

## Key Findings

**Quantified benefits.** The following risk-adjusted present value (PV) quantified benefits are representative of those experienced by the companies interviewed:

- **Incremental 5% addressable market, driven by adherence to additional compliance standards.** For organizations delivering products and services in highly regulated industries, achieving an additional set of compliance certifications meant being able to transact with a new pool of potential end customers. With Armor Anywhere, organizations conservatively estimated being able to do business with an additional 5% of their existing customer base, which over three years, resulted in a present-value benefit of $1.4M
- **Elimination of point solutions, reducing security technology costs by 64%.** Organizations decided not to engage with additional security vendors that offered solutions which were redundant, compared to features native to Armor Anywhere. Consequently, these organizations reduced their overall security TCO (total cost of ownership) by as much as 64%, or as a present value of $862K.
- **Streamlined compliance operations, reducing compliance FTEs needed by 60%.** Because Armor provided the technology and resources to instantly fulfill numerous compliance steps across a number of industrywide mandates, organizations needed fewer internal compliance officers to get and stay complaint throughout the year. Overall, organizations were able to reduce the number of back-office compliance personnel needed by approximately 60%, culminating in a three-year present value of $684K.

**ROI**
**774%**

**Benefits PV**
**$3.2 million**

**NPV**
**$2.8 million**

› **Optimized threat alerting, lowering the rate of false positives to 4% of all alerts.** Armor analyzes millions of security events and data logs collected from Armor Anywhere, network appliances, and cloud-native sources across a customer's environment. This data is correlated and analyzed against Armor's threat intelligence to identify genuine threats facing the organization. As a result, because of Armor's approach, these organizations experienced significant reductions in the percentage of false positive alerts they had experienced in the past. Over time, the operational burden on the security teams mitigating and responding to these threats diminished commensurately. Over three years, this improvement in alerting accuracy led to operational efficiencies totaling a present value of $264K.

**Unquantified benefits.** The interviewed organizations experienced the following benefits, which are not quantified for this study:

› **Reduced alert fatigue.** Since Armor Anywhere helped to minimize the rate of false positives, organizations felt empowered to address any security alerts knowing that alerting accuracy had improved significantly for their IT environments.

› **Improved security posture.** While unable to quantify the extent to which overall security posture had improved, organizations had more confidence in the safety of their workloads and data with Armor Anywhere.

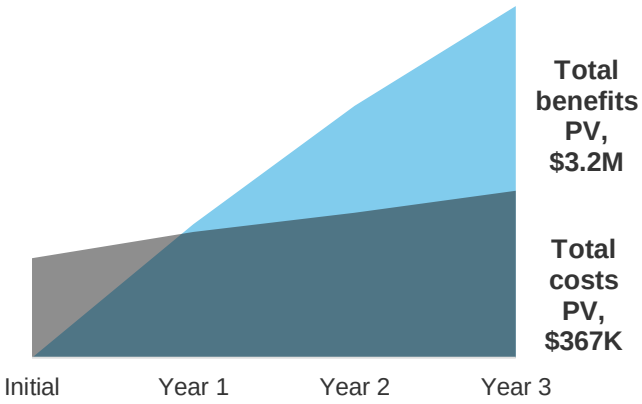
**Costs.** The interviewed organizations experienced the following risk-adjusted PV costs:

› Armor Anywhere platform fees reflect the cost of software agents deployed across an organization's infrastructure footprint, and those fees total a present value of $347K over three years.

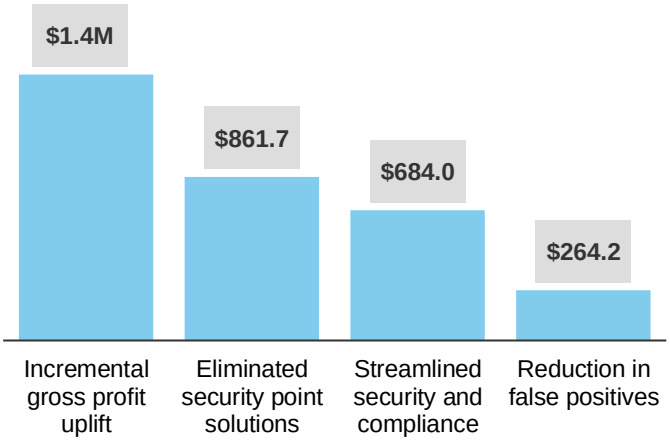
› Implementation and configuration costs include the time and resources required to configure software agents across an organization's endpoints and to gradually optimize log monitoring and threat alerting with Armor Anywhere. These costs total a three-year present value of $20K.

Forrester's interviews with four existing customers and subsequent financial analysis found that an organization based on these interviewed organizations experienced benefits of $3.2M over three years versus costs of $367K, adding up to a net present value (NPV) of $2.8M and an ROI of 774%.

**Financial Summary**




**(Three-Year)**






FORRESTER®

## TEI Framework And Methodology

From the information provided in the interviews, Forrester has constructed a Total Economic Impact™ (TEI) framework for those organizations considering implementing Armor Anywhere.

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 Armor Anywhere can have on an organization:

The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

**DUE DILIGENCE**
Interviewed Armor stakeholders and Forrester analysts to gather data relative to Armor Anywhere.

**CUSTOMER INTERVIEWS**
Interviewed four organizations using Armor Anywhere to obtain data with respect to costs, benefits, and risks.

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

**FINANCIAL MODEL FRAMEWORK**
Constructed a financial model representative of the interviews using the TEI methodology and risk adjusted the financial model based on potential variability across interviewed organizations.

**CASE STUDY**
Employed four fundamental elements of TEI in modeling Armor Anywhere's impact: benefits, costs, flexibility, and risks. Given the increasing sophistication that enterprises have regarding ROI analyses related to IT 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.





FORRESTER®

# The Armor Anywhere Customer Journey

**BEFORE AND AFTER THE ARMOR ANYWHERE INVESTMENT**

## Interviewed Organizations

For this study, Forrester conducted 4 interviews with Armor Anywhere customers. Interviewed customers include the following:

| INDUSTRY | OPERATING REGIONS | INTERVIEWEE | NUMBER OF ARMOR AGENTS DEPLOYED |
|---|---|---|---|
| Professional association | North America | Director of information security | 58 agents |
| Professional services | Global | Global IT director | 325 agents |
| Healthcare | North America | Vice president of security | 1,200 agents |
| Travel | Global | Security analyst | 55 agents |

## Key Challenges

Organizations faced a myriad of challenges prior to seeking a holistic security solution with Armor Anywhere. These challenges included:

- **Shortage of talent required to administer and run a cybersecurity program.** Due to the highly specialized skillsets required to administer specific security functions, interviewed organizations struggled to identify, recruit, and retain the talent that was needed to operate their security operations centers (SOCs). Consequently, these organizations often looked to third parties like security managed services partners to deploy and manage various components of the security framework, such as the organizations' SIEM (security information and event management) or log management processes. As one organization noted: "It's very difficult to find all of the right skillsets to manage a security program. Someone who knows firewalls is not necessarily going to be your incident response person, your risk management person, or your access control person."
- **Outdated and poorly understood security products and processes.** Several organizations struggled with legacy security systems and processes that did not deliver the required security outcomes or were otherwise underutilized or misused. Organizations with a cloud footprint, for instance, relied heavily on their cloud services partners to not only provide infrastructure but to also take care of security and compliance in the cloud, only to later find out that these providers were neither protecting their sensitive records nor guaranteeing compliance with common regulatory guidelines. As one organization remarked: "We thought our cloud partner was taking care of all of our security needs when in reality all they did was power on a web application firewall and hand it over to us to do the rest. We were collecting logs, but they were just sitting on a server with nobody looking at them."

> "It's very difficult to find all of the right skillsets to manage a security program. Someone who knows firewalls is not necessarily going to be your incident response person, your risk management person, or your access control person."
>
> *Vice president of security, healthcare*

> "We thought our partner was taking care of all of our security needs when in reality all they did was power on a web application firewall and hand it over to us to do the rest. We were collecting logs, but they were just sitting on a server with nobody looking at them."
>
> *Vice president of security, healthcare*



FORRESTER®

- **The high cost of security operations.** Costs associated with building a robust security operations center included both product licensing fees and personnel costs across both security and compliance. Further adding to these expenses, interviewed organizations leveraged a number of different point solutions to cover individual security functions, each requiring separate licensing and administration. One interviewed organization engaged three different point solutions to cover everything from threat detection, to threat response and mitigation, to log management.
- **The burden of achieving regulatory compliance.** Several organizations were subject to major compliance mandates, which are based on their specific industries or nature of their business operations.[1] This meant that security teams needed to seek out compliance-ready solutions, decipher where gaps, if any, existed, and provide the right tools, patches, and updates to fill those gaps. Because of the risks associated with failing compliance, organizations dedicated significant resources to processes such as ongoing scanning, monitoring, patching, and working with auditors to ensure completion of each compliance step. In reference to achieving PCI compliance before Armor Anywhere, one organization said, "Putting compliant systems in place and manually going through each of the 12 PCI steps is a huge recurring cost for us."

"Another vendor quoted us five times the price of Armor Anywhere for essentially the same features."

*Director of information security, professional association*

"Putting compliant systems in place and manually going through each of the 12 PCI steps is a huge recurring cost for us."

*Security analyst, travel*

## Key Results

The interviews revealed that key results from the Armor Anywhere investment include:

- **A lower security TCO.** By engaging Armor Anywhere, organizations were able to minimize their overall investments in cybersecurity by reducing both the technology and personnel expenses associated with building and managing a robust and compliant security program. Because of Armor's extensive coverage of various security functions, including intrusion detection and prevention, file integrity monitoring, malware protection, log and data management, vulnerability scanning, and SIEM, organizations could replace much of their existing security stacks with the Armor Anywhere platform which is comprised of a suite of security solutions. Consequently, these organizations simultaneously reduced the cost of redundant point solutions while simplifying security administration for these solutions.

"Armor Anywhere is a much more robust cloud solution than what we were using previously. We used to pay a lot more for just cloud monitoring and logging, and now we get that included with a bunch of other things like antivirus, vulnerability scanning, and more."

*Director of information security, professional association*

"Armor gave us an easy button to press to meet five or six checkboxes around features like intrusion detection and response, log correlation, and log retention, all with a single agent deployment. These are things I simply couldn't do by myself, whether because of lack of budget or just plain ignorance."

*Global IT director, professional services*

- **Easy access to security and compliance.** With the highly specialized skillsets associated with achieving both security and compliance in tandem, most organizations lacked the time, knowledge, or resources to build a program from the ground up. For these organizations, Armor offered an out-of-the-box solution that could meet both security and compliance requirements without significant software configurations and customizations. As one organization articulated: "Armor gave us an easy button to press to meet five or six checkboxes around features like intrusion detection and response, log correlation, and log retention, all with a single agent deployment. These are things I simply couldn't do by myself, whether because of lack of budget or just plain ignorance."
- **Expanded potential market.** Several interviewed organizations, particularly those in highly regulated industries such as healthcare, needed to achieve data and security compliance with specific mandates as a prerequisite prior to onboarding new customers. Because Armor Anywhere provided a suite of solutions compliant across the most common industry compliance standards such as PCI, HIPAA/HITECH, HITRUST, GDPR, and DFS, these organizations could easily prove compliance to auditors and ultimately expedite customer onboarding by referencing Armor documentation. One interviewed organization also commented on how Armor is an extension of their in-house security team: "We positioned Armor as our security partner, and they became an extension of our own security team. It was important to communicate this to our customers so we could say that our security team was more than just two people, but that it included the entire team at Armor too."
- **Enhanced security and control.** With their legacy SIEM solutions, organizations did not effectively optimize or categorize their alerts, allowing hundreds or even thousands of non-critical alerts to flood their systems each month. With Armor Anywhere, these organizations collaborated with Armor to continuously optimize, whitelist, and validate alerts, reducing alert fatigue and empowering security teams to address actual threats to their environments, instead of wasting valuable time and resources chasing false positives. As one organization stated: "Our false positives really died off within our first six months of using Armor. They worked closely with us to make sure that we were only getting alerts on issues that needed alerting."

"We positioned Armor as our security partner and they became an extension of our own security team. It was important to communicate this to our customers so we could say that our security team was more than just two people, but that it included the entire team at Armor too."

*Vice president of security, healthcare*

"Every alert was a coin flip in the past in the sense that there was a 50% probability that it was a false positive. Now, our rate of false positives is well under 5%."

*Global IT director, professional services*

## Composite Organization

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an associated ROI analysis that illustrates the areas financially affected. The composite organization is representative of the four companies that Forrester interviewed and is used to present the aggregate financial analysis in the next section. The composite organization that Forrester synthesized from the customer interviews has the following characteristics:

- Multinational organization in the healthcare industry with annual revenues of $200M. The organization is headquartered in North America with a satellite office in Western Europe.
- Hybrid infrastructure footprint consisting of 120 total servers and virtual machines (VMs) across on-premises and public cloud environments, with each endpoint configured with an Armor Anywhere agent.

**Key assumptions:**

- 120 agents
- $200M revenue
- 4 IT security FTEs



FORRESTER®

- Security team consists of two director-/VP-level FTEs managing cybersecurity across both offices, with one security and compliance officer at each location.
- Prior to Armor Anywhere, major security functions such as log management and correlation and threat intelligence and response were delivered by third-party point solution providers deployed on the public cloud.

# 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 | Incremental gross profit uplift | $562,500 | $562,500 | $562,500 | $1,687,500 | $1,398,854 |
| Btr | Eliminated security point solutions | $346,500 | $346,500 | $346,500 | $1,039,500 | $861,694 |
| Ctr | Streamlined security operations | $275,063 | $275,063 | $275,063 | $825,188 | $684,040 |
| Dtr | Reduction in false positives | $101,088 | $106,560 | $112,176 | $319,824 | $264,244 |
| | Total benefits (risk-adjusted) | $1,285,151 | $1,290,623 | $1,296,239 | $3,872,012 | $3,208,832 |

### Incremental Gross Profit Uplift

For organizations in regulated industries with strict data and compliance standards, meeting compliance is more extensive than simply filling a regulatory requirement. It is also a means to expand the top line. Each compliance mandate and certification that is met and achieved meant that these organizations could transact with an additional group of B2B customers that required adherence to specific mandates as a prerequisite to partnering. One organization said, “Armor helped us fulfill approximately 70 security controls, which allowed us to pursue RFPs that we previously were not able to bid on.” Evaluated organizations were able to unlock an additional 5% to 10% of their gross revenues by gaining additional compliance certifications with Armor Anywhere.

To model the incremental gross profit uplift for the composite organization, Forrester makes the following assumptions:

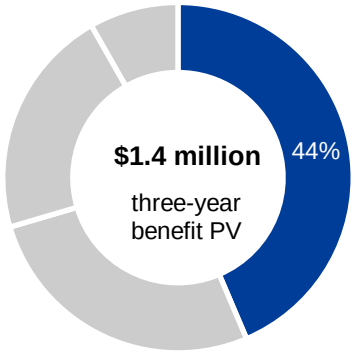
- The composite organization is able to increase its addressable market size by a conservative 5% of gross revenues, or $10M, after partnering with Armor.
- The composite organization is able to convert 15% of the new RFPs into deals.
- The gross margin on each deal is 50%.

Several factors can impact the degree of gross profit uplift that other organizations experience by unlocking new compliance certifications, including:

- Deal characteristics, such as average deal sizes, win and conversion rates, and cost of goods/services sold.
- Prior operating environment, including existing compliance standards met and gaps filled by Armor Anywhere.

Because of the potential for significant variance in outcomes given the aforementioned factors, Forrester adjusted this benefit downward by 25%, yielding a three-year, risk-adjusted total PV of $1.4M.

The table above shows the total of all benefits across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total benefits to be a PV of more than $3.2 million.




Gross profit uplift:
**44%** of total benefits

Impact risk is the risk that the business or technology needs of the organization may not be met by the investment, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for benefit estimates.



FORRESTER®

| Incremental Gross Profit Uplift: Calculation Table | | | | | |
|---|---|---|---|---|---|
| **REF.** | **METRIC** | **CALC.** | **YEAR 1** | **YEAR 2** | **YEAR 3** |
| A1 | New potential revenue streams unlocked by achieving compliance | | $10,000,000 | $10,000,000 | $10,000,000 |
| A2 | Average win rate | | 15% | 15% | 15% |
| A3 | Incremental revenue uplift from new deals | | 1,500,000 | 1,500,000 | 1,500,000 |
| A4 | Gross margin | | 50% | 50% | 50% |
| At | Incremental gross profit uplift | A3*A4 | $750,000 | $750,000 | $750,000 |
| | Risk adjustment | ↓25% | | | |
| Atr | Incremental gross profit uplift (risk-adjusted) | | $562,500 | $562,500 | $562,500 |

## Eliminated Security Point Solutions

Because of Armor's diverse coverage of security needs through Armor Anywhere and the flexibility of deployment across all computing environments, organizations found that they could replace much of their security stacks with the best-in-class solutions embedded within Armor Anywhere. Redundant solutions ranged from log monitoring and correlation software, threat intelligence tools, and malware protection. One organization said: "Cost was a major selling point of Armor, I have to admit. We were evaluating another major vendor that quoted us $2M a year for the same features we're getting with Armor. We're paying nowhere close to that."

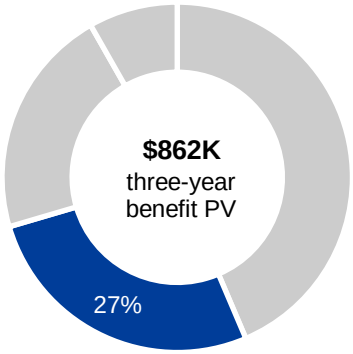
To calculate the security TCO reduction from eliminating redundant point solutions for the composite organization, Forrester conservatively assumes that:

- The composite organization replaces a threat intelligence software and a third-party SIEM software costing $290K and $60K, respectively.
- The composite organization also engaged the provider of the threat intelligence software to perform managed threat response at an add-on fee of $35K per year.
- The aforementioned point solutions and services are hosted on the vendor's own infrastructure (i.e., cloud), and therefore the TCO reduction is driven by reduced software licensing.

For other organizations, the magnitude of TCO reduction from eliminating point solutions will vary based on the following:

- Number and types of legacy point solutions for which Armor Anywhere provides redundancy.
- Deployment characteristics of legacy point solutions, which will determine if hardware and administration savings will factor into total cost savings.
- Vendor specific pricing and characteristics, which will determine how much cost is displayed through Armor Anywhere.

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




Eliminated security point solutions:
**27%** of total benefits



FORRESTER®

| Eliminated Security Point Solutions: Calculation Table | | | | | |
|---|---|---|---|---|---|
| REF. | METRIC | CALC. | YEAR 1 | YEAR 2 | YEAR 3 |
| B1 | Cost of threat intelligence software | | $290,000 | $290,000 | $290,000 |
| B2 | Cost of log management software | | $60,000 | $60,000 | $60,000 |
| B3 | Cost of managed threat response and mitigation | | $35,000 | $35,000 | $35,000 |
| Bt | Eliminated security point solutions | B1+B2+B3 | $385,000 | $385,000 | $385,000 |
| | Risk adjustment | ↓10% | | | |
| Btr | Eliminated security point solutions (risk-adjusted) | | $346,500 | $346,500 | $346,500 |

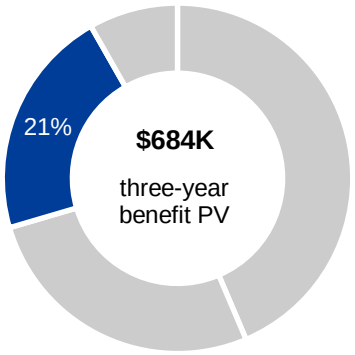
## Streamlined Security And Compliance

Due to the complexity of marrying cybersecurity with compliance across an extensive list of regulations and security protocols, most interviewed organizations did not have a robust back-office SOC, nor did they employ a full team of compliance experts to align their technology and controls to any number of compliance steps or to prepare for and successfully complete yearly audit cycles. Instead, these organizations relied heavily on Armor to act as a remote SOC and provide compliance expertise throughout the year and during audit seasons. Using a combination of Armor Anywhere's compliance-ready technology and ongoing alerting and reporting, organizations were informed of the necessary patches, updates, and fixes to run throughout the year to keep their workloads secure and compliant. Furthermore, during audits, security teams felt comfortable deferring much of their compliance checks to the Armor team, therefore reducing the need to employ a full SOC. One organization said: "With a new data center in Zurich and two in Europe looking to become certified, I was faced with the decision of whether to invest in a bunch of overhead to try to build a SOC or engage Armor and have immediate access to seven different compliance-ready technologies through a single pane of glass. It was a no-brainer."

To model the impact of streamlined security and compliance for the composite organization, Forrester assumes:

- Reaching full compliance by building an internal SOC would have required a minimum of five dedicated resources across the organization's North American and European offices. With Armor Anywhere, the organization maintains its existing team of one security officer per location without the need to hire additional resources.
- The fully burdened annual rate per IT security lead is $101,875, which includes base compensation plus a 25% benefits overhead rate.

The existing SOC characteristics of other organizations may vary significantly from those of the aforementioned composite organization. For example, some organizations may already have a robust SOC in place before engaging Armor or operating with a different pay scale. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $684K.




Streamlined security and compliance:
**21%** of total benefits



FORRESTER®

| Streamlined Security And Compliance: Calculation Table | | | | | |
|---|---|---|---|---|---|
| REF. | METRIC | CALC. | YEAR 1 | YEAR 2 | YEAR 3 |
| C1 | Number of security officers needed to manage data compliance, without Armor Anywhere | | 5 | 5 | 5 |
| C2 | Number of security officers needed to manage data compliance, with Armor Anywhere | | 2 | 2 | 2 |
| C3 | Reduction in FTEs required to manage IT security compliance | C1-C2 | 3 | 3 | 3 |
| C4 | Fully burdened annual salary per IT security and compliance FTE | | $101,875 | $101,875 | $101,875 |
| Ct | Streamlined security and compliance | C3*C4 | $305,625 | $305,625 | $305,625 |
| | Risk adjustment | ↓10% | | | |
| Ctr | Streamlined security and compliance (risk-adjusted) | | $275,063 | $275,063 | $275,063 |

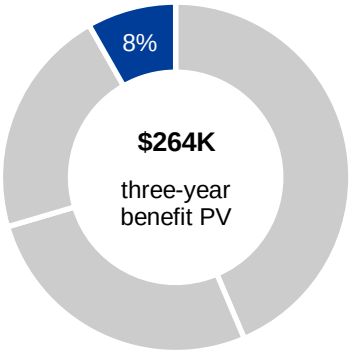
## Reduction In False Positives

In their previous environments, organizations were challenged with distinct and siloed point solutions that acted independently from one another, resulting in large quantities of potentially redundant reporting and log data, but without clear direction or actionability. For example, log monitoring systems would be poorly integrated with threat intelligence systems, resulting in poor correlation of log data and potential threats in the environment. As a result, organizations received dozens of alerts per week, or at times even per day, and only a handful of which warranted additional investigation. As one organization stated: "When you're constantly getting wake-up calls at 2:00 a.m. for a critical alert that turns out to be a false positive, the natural tendency is to become desensitized. And that's dangerous because out of one hundred wrong hurricane alerts, it only takes one Katrina to wipe out an entire city."

With Armor's synergistic combination of SIEM technologies such as log monitoring and correlation, threat and intrusion detection, and malware protection, all from a central point of access, organizations could reduce their rate of false positives to between 1% and 5%, reflecting a 90% overall reduction in false positives compared to their previous environments. As one organization put it: "If Armor sends us an alert at a medium, high, or critical level, we know that it's necessary to respond because these are often for something that has happened with a potential deletion or quarantine. When those types of alerts come in, we know that it's client data that is affected and we jump on it right away."

To quantify the financial impact of reducing the rate of false positives for the composite organization, Forrester makes the following assumptions:

- In its prior environment, the organization receives an average of 200 high-risk security alerts per year, 40% of which are false positives. With Armor Anywhere, the rate of false positives drops to 4% of total high-risk alerts in Year 1, 3% in Year 2, and 2% in Year 3, as the organization continues to collaborate with Armor to whitelist benign alerts and optimize the accuracy of alerting.
- Each alert requires an average of 20 security operations hours to fully investigate and remediate.




Reduction in false positives:
**8%** of total benefits

"If Armor sends us an alert at a medium, high, or critical level, we know that it's necessary to respond because these are often for something that has happened with a potential deletion or quarantine. When those types of alerts come in, we know that it's client data that is affected and we jump on it right away."

*Global IT director, professional services*



FORRESTER®

› The fully burdened hourly rate per IT security lead is $78, which includes base compensation plus a 25% benefits overhead rate.

Each organization's experience with threat alerting using Armor Anywhere will differ based on factors such as the organization's prior rate of false positives, the number and severity of alerts, and the average time to remediation or resolution. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $264K.

**Reduction In False Positives: Calculation Table**

| REF. | METRIC | CALC. | YEAR 1 | YEAR 2 | YEAR 3 |
|---|---|---|---|---|---|
| D1 | Total security alerts requiring manual intervention before Armor Anywhere, annually | | 200 | 200 | 200 |
| D2 | Percentage of false positives, before Armor Anywhere | | 40% | 40% | 40% |
| D3 | Percentage of false positives, with Armor Anywhere | | 4% | 3% | 2% |
| D4 | Reduction in number of alerts needing manual intervention, with Armor anywhere | | 72 | 74 | 76 |
| D5 | Average security operations hours needed to investigate and remediate security alerts | | 20 | 20 | 20 |
| D6 | Fully burdened hourly rate per IT security lead | | $78 | $80 | $82 |
| Dt | Reduction in false positives | D4*D5*D6 | $112,320 | $118,400 | $124,640 |
| | Risk adjustment | ↓10% | | | |
| Dtr | Reduction in false positives (risk-adjusted) | | $101,088 | $106,560 | $112,176 |

## Unquantified Benefits

Organizations experienced the following benefits, which were not quantified for the purposes of this study:

› **Reduced alert fatigue.** Organizations that historically experienced a high rate of false positive alerts began to disregard alerts over time, even before thoroughly investigating them. As a result, these organizations often allowed legitimate issues to slip by unaddressed, potentially compromising data and security, and causing workloads to run suboptimally. By significantly reducing the rate of false positives, these organizations felt empowered to address every alert, knowing that their logs were being actively managed and categorized based on Armor's extensive threat intelligence, the collective data lake, and the organization's own unique security environment.

- **Improved security posture.** With improved alerting and reporting and central control over the security stack on a single interface through the Armor Management Portal, security teams had greater visibility and transparency with respect to their logs and thus could address patches, updates, fixes, and other issues based on priority and risk to the environment. Furthermore, organizations collaborated with and leveraged Armor as an extension of their own security teams to increase the speed and accuracy of threat resolution. As one organization said, "If there's anything that comes up that we can't handle, we simply open a ticket with Armor, and so far there hasn't been anything they haven't been able to help with."

## Flexibility

The value of flexibility is clearly unique to each customer, and the measure of its value varies from organization to organization. There are multiple scenarios in which a customer might choose to implement Armor Anywhere and later realize additional uses and business opportunities, including:

- **Democratization of security administration.** With Armor's intuitive user interface, built-in analytics and dashboarding, and extensive product support, organizations could forego hiring expensive security domain specialists to run individual point solutions. Instead, even more junior security staff could administer Armor Anywhere as it abstracted out many of the complexities of running distinct facets of a security program, such as the SIEM or log management program, through a central front-end user interface. When more in-depth log analysis was required, admins could also use the Armor Anywhere platform to seamlessly search and dig through individual log data.

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

Flexibility, as defined by TEI, represents an investment in additional capacity or capability that could be turned into business benefit for a future additional investment. This provides an organization with the "right" or the ability to engage in future initiatives but not the obligation to do so.

# Analysis Of Costs

**QUANTIFIED COST DATA AS APPLIED TO THE COMPOSITE**

## Total Costs

| REF. | COST | INITIAL | YEAR 1 | YEAR 2 | YEAR 3 | TOTAL | PRESENT VALUE |
|---|---|---|---|---|---|---|---|
| Etr | Armor Anywhere platform fees | $0 | $139,680 | $139,680 | $139,680 | $419,040 | $347,363 |
| Ftr | Implementation and configuration | $0 | $21,528 | $0 | $0 | $21,528 | $19,571 |
| | Total costs (risk-adjusted) | $0 | $161,208 | $139,680 | $139,680 | $440,568 | $366,934 |

The table above shows the total of all costs across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total costs to be a PV of almost $367K.

### Armor Anywhere Platform Fees

Interviewed security teams unanimously agreed that the simplicity and transparency of Armor Anywhere's pricing made it easier to make the business case for the investment to executive decision makers. With a simple pricing scheme based on the number of agents deployed across an organization's hosts, security operations teams felt empowered to leverage the full breadth of features and services of Armor Anywhere, knowing that they would not incur additional charges without adding additional software agents. As one organization put it: "Armor doesn't care whether we have agents deployed on the private cloud, on-premises, a public cloud, or a combination of the above. It's still just a single bill."

To calculate Armor Anywhere platform fees for the composite organization, Forrester makes the following assumption:

- One hundred and twenty Armor Anywhere agents are deployed across the same number of servers and VMs in a hybrid computing environment.
- The organization does not add or remove any software agents over the analyzed three-year investment period.

Since list pricing was used to determine Armor Anywhere pricing as applied to the composite organization, Forrester made no risk adjustment. Over three years, risk-adjusted costs totaled a PV of $347K.

> "Armor doesn't care whether we have agents deployed on the private cloud, on-premises, a public cloud, or a combination of the above. It's still just a single bill."
>
> *Global IT director, professional association*

Implementation risk is the risk that a proposed investment may deviate from the original or expected requirements, resulting in higher costs than anticipated. The greater the uncertainty, the wider the potential range of outcomes for cost estimates.

**Armor Anywhere Platform Fees: Calculation Table**

| REF. | METRIC | CALC. | INITIAL | YEAR 1 | YEAR 2 | YEAR 3 |
|---|---|---|---|---|---|---|
| Et | Armor Anywhere platform fees | | | $139,680 | $139,680 | $139,680 |
| | Risk adjustment | 0% | | | | |
| Etr | Armor Anywhere platform fees (risk-adjusted) | | $0 | $139,680 | $139,680 | $139,680 |



FORRESTER®

## Implementation And Configuration

For all organizations, the deployment of Armor agents onto the organization's environment was completed within minutes. Organizations were able to get security outcomes immediately once the agents were turned on including the collection, correlation, and detection of threats in their environments.

For customers who also wanted Armor to correlate and analyze logs not native to the Armor agent, they worked closely with the Armor team to properly collect, store, and categorize those logs into Armor's platform. Once fully configured, the final step was to optimize the log management and correlation engines.

Typically, these additional steps took these organizations a combined two to four months, during which security teams collaborated with Armor's in-house experts. As one organization said, "We worked with Armor over several weeks to improve our log monitoring, but the actual Armor agents were deployed in less than 5 minutes per server."

To model the Armor Anywhere implementation and configuration costs for this type composite organization, Forrester makes the following assumptions:

- Configuration of Armor's Log and Data Management module for non-Armor agent logs takes place over a period of three months, during which two IT security leads spend an average of one week per month working to optimize the Log and Data Management module to collect, categorize, and correlate log data.
- The fully burdened hourly rate per IT security lead is $78, which includes base compensation plus a 25% benefits overhead rate.

While a total implementation time of two to four months was typical for the evaluated organizations, implementations for other organizations may vary based on factors such as the complexity of the organization's existing infrastructure and the scripting experience of the security team. Furthermore, salaries and pay rates for internal resources involved in implementation may vary by geography, industry, or individual organization. To account for these risks, Forrester adjusted this cost upward by 15%, yielding a three-year, risk-adjusted total PV of $20K.

"We worked with Armor over several weeks to improve our log monitoring, but the actual Armor agents were deployed in less than five minutes per server."

*Global IT director, professional association*



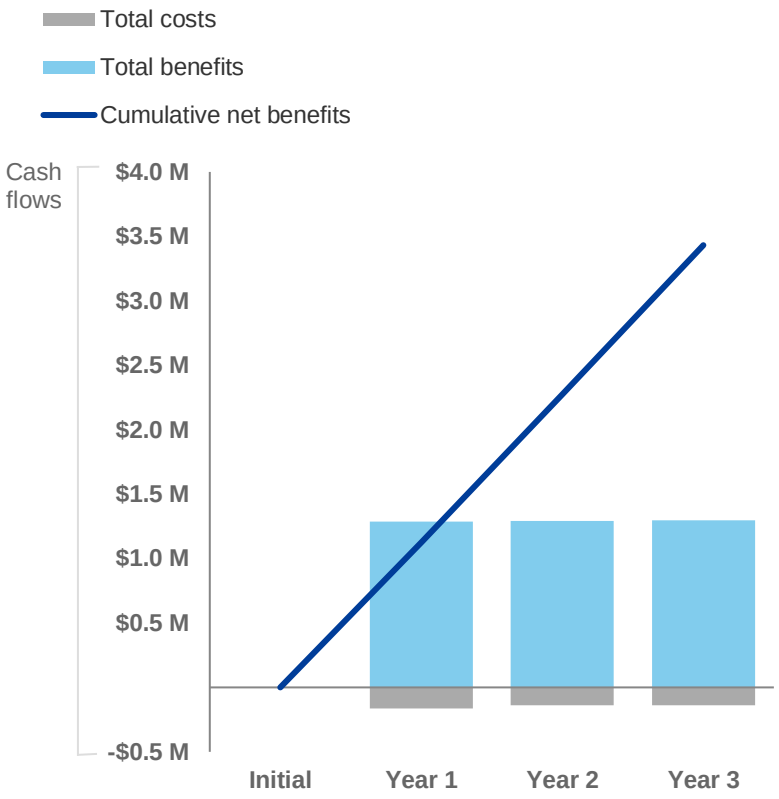
FORRESTER®

| Implementation And Configuration: Calculation Table | | | | | | |
|---|---|---|---|---|---|---|
| **REF.** | **METRIC** | **CALC.** | **INITIAL** | **YEAR 1** | **YEAR 2** | **YEAR 3** |
| F1 | Number of months to fully configure Armor's Log and Data Management module for non-Armor agent logs | | | 3 | | |
| F2 | Number of IT FTEs involved in implementation of Armor's Log and Data Management module for non-Armor agent logs | | | 2 | | |
| F3 | Number of hours dedicated to ongoing configuration of Armor's Log and Data Management module for non-Armor agent logs | | | 40 | | |
| F4 | Fully burdened hourly rate per IT security lead | | | $78 | | |
| Ft | Implementation and configuration of Armor's Log and Data Management module for non-Armor agent logs | F1*F2*F3*F4 | | $18,720 | $0 | $0 |
| | Risk adjustment | ↑15% | | | | |

# Financial Summary

**CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS**

## Cash Flow Chart (Risk-Adjusted)




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

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

**Cash Flow Table (Risk-Adjusted)**

| | INITIAL | YEAR 1 | YEAR 2 | YEAR 3 | TOTAL | PRESENT VALUE |
|---|---|---|---|---|---|---|
| Total costs | $0 | ($161,208) | ($139,680) | ($139,680) | ($440,568) | ($366,934) |
| Total benefits | $0 | $1,285,151 | $1,290,623 | $1,296,239 | $3,872,012 | $3,208,832 |
| Net benefits | $0 | $1,123,943 | $1,150,943 | $1,156,559 | $3,431,444 | $2,841,898 |
| ROI | | | | | | 774% |



FORRESTER®

# Armor Anywhere: Overview

The following information is provided by Armor.
Forrester has not validated any claims and does not endorse Armor or its offerings.

**ARMOR CLOUD SECURITY**

Armor is a global cybersecurity software company that simplifies protecting data and applications on-premises and in private, public, hybrid and multi- cloud environments. Armor Anywhere provides technology to detect and respond to threats and can be activated in minutes. Armor also helps organizations comply with major regulatory frameworks and controls. The company combines workload protection, analytics from cloud-native sources, and other security data to provide unparalleled insight into threats facing organizations.

Armor processes, analyzes and correlates **234 million** events a day to protect its global customer base. If an incident is identified, Armor's cyber experts promptly provide guidance and context to their customers, helping them respond quickly and effectively.

Organizations with mission critical applications and data can also choose Armor Anywhere with the secure hosting option.

Armor protects over 1,000 customers in over 40 countries.

**Armor Anywhere addresses the following use cases:**

**Threat Detection and Response**
Get advanced detection of threats in your applications and data. Go beyond alerting to receive a guided response from our cybersecurity experts.

**Audit-Ready Compliance**
Simplify compliance by meeting key controls in frameworks such as PCI DSS, HIPAA/HITRUST, and GDPR.

**Protection for Mission-Critical Applications and Data**
Offload the headaches of managing infrastructure while getting the industry's leading protection for your most sensitive workloads.

Armor Anywhere integrates robust security capabilities with 24/7/365 monitoring to deliver unified threat detection and response as well as compliance for your applications and data wherever they reside.

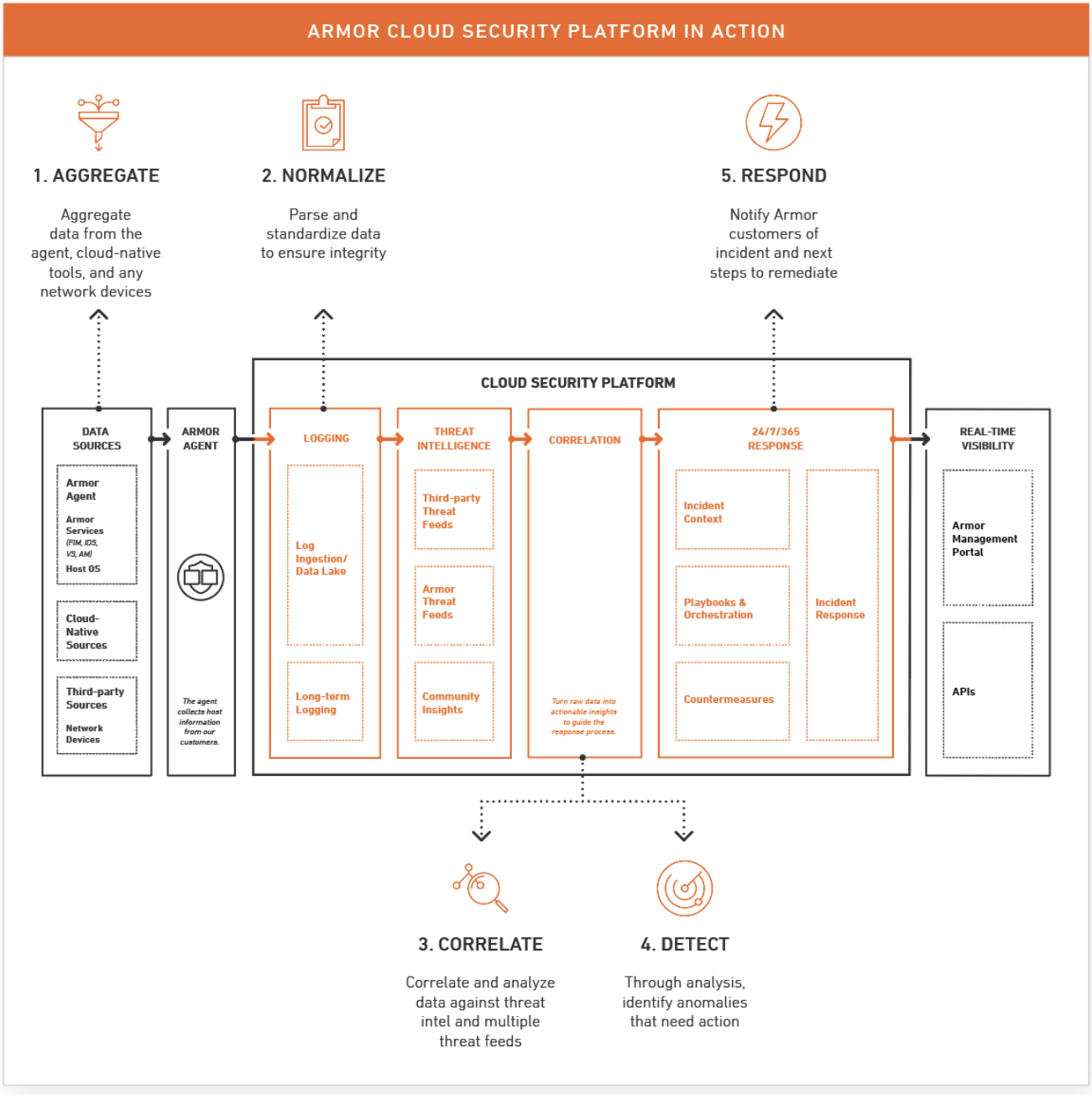
ARMOR AWS AZURE

GCP HYBRID PRIVATE



FORRESTER®

Armor integrates threat intelligence, advanced analytics, and incident response capabilities into a single platform that bolsters a company's defenses, uncovers threats, and prevents security breaches. Its modularity and interoperability allow Armor to deliver powerful security and compliance outcomes aligned to the unique use cases and consumption needs of its customers.




**ARMOR.COM**

Armor is a global cybersecurity software company. We simplify protecting data and applications in private, public, or hybrid clouds as well as help organizations comply with major regulatory frameworks and controls. We know security is complex; it doesn't have to feel that way.



FORRESTER®

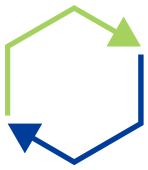
# Appendix A: Total Economic Impact

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.



FORRESTER®

# Appendix B: Endnotes

[1] Such compliance mandates for the interviewed organizations involve payment card industry compliance (PCI), HIPAA/Health Information Technology for Economic and Clinical Health Act (HITECH), Health Information Trust Alliance (HITRUST), and General Data Protection Regulation (GDPR).