A Forrester Total Economic Impact™
Study Commissioned By Alert Logic
May 2019

The Total Economic Impact Of Alert Logic SIEMless Threat Management

FORRESTER®

Table Of Contents

Executive Summary 1
- Key Findings 1
- TEI Framework And Methodology 3

The Alert Logic Customer Journey 4
- Interviewed Customers 4
- Key Challenges 4
- Solution Requirements 5
- Key Results 5
- Composite Organization 6

Financial Analysis 8
- Security Staff Cost Avoided 8
- Compliance And Regulatory Staffing Costs Avoided 9
- Faster Client Acquisition: Incremental Gross Profit 11
- Security Infrastructure Cost Avoidance 12
- Unquantified Benefits 12
- Flexibility 13
- Fees Paid To Alert Logic 14
- Labor Expense To Set Up And Manage Alert Logic's Capabilities 15

Financial Summary 17

Alert Logic: Overview 18

Appendix A: Total Economic Impact 20

Appendix B: Endnotes 21

Project Directors:
Bob Cormier
Edgar Casildo

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®

Benefits And Costs

Security and compliance staffing costs avoided:
$954,489

Profit from faster sales cycles:
$93,259

Alert Logic services and management costs:
$207,771

Executive Summary

Alert Logic's SIEMless solution connects a security platform, threat intelligence, and expert defenders to provide better security for businesses 24/7. The Alert Logic offering is software-as-a-service (SaaS) based and includes vulnerability and asset visibility, extended endpoint protection, threat detection and incident management, along with web application firewall and assigned security operations center (SOC) analyst options. Alert Logic also helps companies comply with mandates such as PCI, HIPAA, GDPR, SOC 2, SOX COBIT; and standards such as NIST, ISO, and the CIS Benchmarks.

Alert Logic commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential ROI enterprises may realize by deploying Alert Logic's security-as-a-service solutions. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of the Alert Logic services on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed eight customers with experience using Alert Logic SIEMless services.

Prior to engaging Alert Logic, these customers struggled to assemble the right combination of tools and expertise to provide their own security as well as their clients' applications and data in public cloud and hybrid environments. Early attempts yielded limited success, leaving the customers with potential delays in achieving requisite certification and the ability to demonstrate compliance with a host of standards and an array of requirements, as well as delays in securing against breaches and achieving speed in application deployments. These limitations led to a search for an alternative approach to meet their needs more completely, and at a lower cost.

Based on the interviews, Forrester constructed a TEI framework, a composite *Organization*, and an associated ROI analysis that illustrates the areas financially impacted. The composite *Organization* is representative of the eight companies that Forrester interviewed. It's a midsize company servicing clients in multiple verticals from its 10 offices worldwide. The composite *Organization* is used to present the cost and benefit data in the *Financial Analysis* section below.

For interviewed customers and our composite *Organization*, Alert Logic emerged as the solution with demonstrated capabilities, strong reputation, and name recognition among auditors and prospective customers seeking secure environments, certification, and compliance.

Key Findings

Quantified benefits. The following risk- and present value-adjusted benefits total **$1,107,431** for the composite *Organization* and are representative of those experienced by the eight interviewed customers:

- **Security staffing costs avoided — $712,021.** The *Organization* found that it is more cost effective to pay Alert Logic than attempt to hire and retain scarce talent. With Alert Logic, it was also able to enhance its ability to spend time and resources on security alerts that matter while knowing which alerts do not matter.

FORRESTER®

ROI
433%

Benefits PV
$1,107,431

NPV
$899,659

Payback
<6 months

> "We would have needed multiple vendors on board to be able to do what we are doing with just Alert Logic. If I were talking to one of my colleagues in the industry who is looking for a cybersecurity solution, I would recommend Alert Logic, hands down."
> Lee Ramsey,
> Co-Founder of Pre-Fi

- **Compliance and regulatory staffing costs avoided — $242,468.** Compliance efforts require attention and expertise. If this capability is maintained in house, substantial and expensive resources must be hired and retained. Alert Logic helps companies comply with mandates such as PCI, HIPAA, GDPR, SOC 2, SOX COBIT; and standards such as NIST, ISO, and the CIS Benchmarks.
- **Faster client acquisition, as measured by incremental gross margin (profit) — $93,257.** For customers that require ISO 27001 certification, utilizing Alert Logic's services helps them to obtain ISO 27001 certification sooner, enabling them to accelerate sales and pull in more revenue earlier in the fiscal year. By overcoming the challenge of faster certification, the *Organization* was able to sign contracts with new clients three months earlier than initially expected.
- **Security infrastructure and log storage cost avoidance — $59,684.** An investment in Alert Logic has enabled the *Organization* to avoid costs for security infrastructure such as storage, servers, and software licenses with annual maintenance.

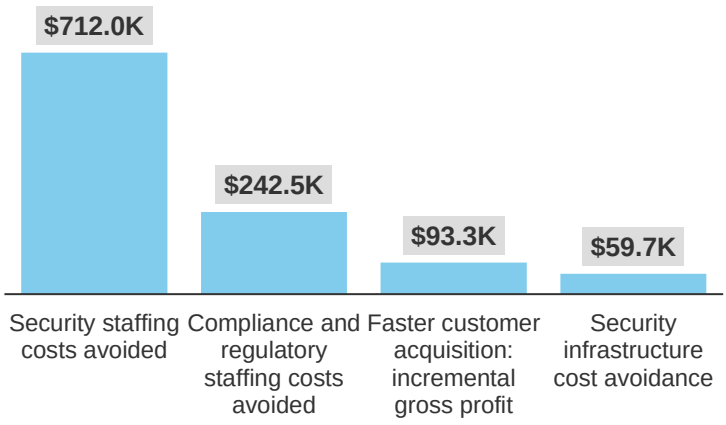
Costs. The *Organization* experienced the following risk- and present value-adjusted costs, which are representative of costs experienced by the eight interviewed customers; totaling **$207,771**:

- **Fees paid to Alert Logic — $136,463.** The main cost component of this analysis is the monthly services fee based on 50 nodes employed by the *Organization*.
- **Labor expense to set up and manage Alert Logic capabilities — $71,309.** Setup of the initial contract, relationship management, and the ongoing planning and coordination with Alert Logic.

Forrester's interviews with eight existing customers and subsequent financial analysis found that the composite *Organization* experienced benefits of $1,107,431 over three years versus costs of $207,771, adding up to a net present value (NPV) of $899,659 and an ROI of 433%.

Interviewed customers agreed that a DIY approach to security is quite costly and requires extensive ongoing investment in resources and expertise. Interviewed customers use Alert Logic's SIEMless Threat Management to deliver a security program that is simple to implement and maintain, easy to use, and provides a strong program ROI with a lower cost than other approaches.

Benefits (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 using Alert Logic.

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 Alert Logic's solutions 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 Alert Logic stakeholders and Forrester analysts to gather data relative to SIEMless Threat Management solutions.

CUSTOMER INTERVIEWS
Interviewed eight customers using Alert Logic security-as-a-service to obtain data with respect to costs, benefits, and risks.

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

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

CASE STUDY
Employed four fundamental elements of TEI in modeling Alert Logic's security-as-a-service 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.

The Alert Logic Customer Journey

BEFORE AND AFTER THE ALERT LOGIC INVESTMENT

Interviewed Customers

For this study, Forrester conducted interviews with eight Alert Logic customers. Interviewed customers include the following, each requesting anonymity:

INDUSTRY	REGION	INTERVIEWEE	SCOPE
Digital marketing agency	North America	Chief technology officer	Serving integrated marketing, advertising, and tech solutions to enterprise clients
Software-as-a-service (SaaS) tool provider	Worldwide	Solutions engineering manager	Providing software tools to the architecture and construction sectors in over 50 countries
SaaS provider – business continuity	North America	President	Integrated cloud-based platform for business continuity and disaster recovery planning
Higher education	North America	Chief information security officer	Specializing in design and fashion education
Retail	North America	Vice president, IT and data services	Consulting and marketing services
Platform-as-a-service (PaaS) provider	Worldwide	Chief information security officer	Development platform that accelerates creation of business applications
Automobile distributor	North America	Vice president, IT	Large, diversified company in vehicle distribution, finance and insurance, and dealer technology services
Retail consulting firm	North America	Vice president, IT	Serving Fortune 100 clients with custom reporting tools for big data analysis of retail sales via web interfaces

Key Challenges

The Alert Logic customers participating in this study described the following challenges related to their need to rapidly offer client services on public cloud infrastructure while assuring the security of their clients' data and applications.

- **Assume responsibility for clients' security whether in the cloud, hybrid, or on-premises.** Clients who were previously responsible for on-premises security of their data and web applications now need to secure their assets as part of their managed service on the public cloud infrastructure.
- **Inability to keep pace with an ever-changing threat environment.** The constantly changing nature of security threats and associated vulnerabilities made it difficult for the customers to learn of new threats to their networks, systems, and web applications, while also implementing adequate protection against these threats in a cadence that keeps pace with the attackers.

- **Need for 24x7 security monitoring on a global basis.** Because of the global nature of some of the companies and their clients, there was a need to provide 24x7 security monitoring to their geographically dispersed locations, reacting to security threats on a timely basis.
- **Certification and trust.** Obtaining ISO 27001 certification and demonstrating SOX, HIPAA, and PCI compliance is critically important to many of Alert Logic clients' business. It shows potential clients an effective security improvement in a cloud-based environment or an IT infrastructure in general, which results in a faster sales cycle. The demands of regulatory compliance on these customers required that they monitor their log files regularly, maintaining an audit trail of log-monitoring activities and providing the necessary audit reports.
- **Inability to actively monitor and review the hundreds or thousands of log files generated across their IT infrastructure daily.** Although some companies made previous attempts to monitor their log files with homegrown solutions, they could not keep pace with the sheer volume of data.
- **Challenges in recruiting and retaining skilled security engineers and analysts.** The companies used their IT staff to multitask a range of IT operation, including security activities. They realized that it would be difficult to recruit highly skilled security analysts on a global basis, and it would be expensive to train and certify existing IT staff. They also realized that they were unable to offer a career path to a skilled security analyst and that retention would become an issue in the future.

"When we move clients to a managed service, cloud security is a responsibility that we assume, and prior to every managed service project, whether it's a migration or a net-new one, there is an extensive discussion around our security practices and policies, our qualifications, and our track record. We have to put together a case as to how we are going to secure that user's data."

Solutions engineering manager, engineering tool services

Solution Requirements

In addition to meeting the challenges described above, the interviewed customers searched for a solution that could:

- **Scale up rapidly.** These companies required the ability to bring their clients onto public cloud infrastructure preferably without adding staff or infrastructure to meet growth as more managed service customers join their portfolios. "I don't have to exponentially scale that to support my volume of traffic," noted one interviewee. "It's just more traffic I send over to Alert Logic, and they essentially have the scale to support it."
- **Assure/reinforce brand integrity.** Providing SIEMless Threat Management to clients had to be done in a way that would enhance brand, trust, and client capital. Doing so via, "temporary solutions, experiments, and Band-Aids," or using an unknown partner would have diluted these key ingredients.

"Alert Logic was able to identify and resolve the vulnerabilities in our servers and stack. So now, we have a much cleaner stack. If I need to spin up a new server I do it a lot faster than before and in a much more secure fashion."

VP, IT and data services, retail industry

Key Results

The interviews revealed the key results — lower costs and higher revenues and profits from their Alert Logic investment including:

- **Security staffing costs avoided.** Interviewed companies found that it is more cost effective to pay Alert Logic than attempt to hire and retain scarce talent. With Alert Logic, they were also able to enhance their ability to spend time and resources on security alerts that matter while knowing which alerts do not matter.

- **Compliance and regulatory staffing costs avoided.** Compliance efforts require attention and expertise. If this capability is maintained in house, substantial and expensive resources must be hired and retained. Alert Logic helps companies comply with mandates such as PCI, HIPAA, GDPR, SOC 2, SOX COBIT; and standards such as NIST, ISO, and the CIS Benchmarks.
- **Faster customer acquisition**, **as measured by incremental gross margin (profit).** Obtaining ISO 27001 certification months sooner because of Alert Logic's reputation and capabilities pulled in more revenue sooner in the fiscal year. By overcoming the challenge of faster certification, they could sign contracts with new clients three months earlier.
- **Security infrastructure and log storage cost avoidance**. Investments in Alert Logic helped interviewees to avoid costs for security infrastructure such as storage, servers, and software licenses with annual maintenance.

"Before Alert Logic, this company was using temporary solutions, experiments, and Band-Aids."

Vice president, IT, digital strategic marketing

Composite *Organization*

Based on the interviews, Forrester constructed a TEI framework, a composite *Organization*, and an associated ROI analysis that illustrates the areas financially impacted. The composite *Organization* is representative of the eight 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:

Description of composite. The composite organization is a midsize company servicing clients in multiple verticals from their 10 offices worldwide.

Seventy-five percent of client workloads have been transitioned to public cloud infrastructure for data and applications formerly hosted on client premises or on several company data centers. Compliance requirements that the composite *Organization* must meet depend on the needs within the client's industry, including SOX, HIPAA, and PCI, in addition to the general security controls framework of ISO 27001. The *Organization* seeks to adhere to the Zero Trust Model.[1]

Deployment characteristics. The *Organization* has been using Alert Logic's security-as-as-service (SECaaS) platform for three years. The services include Alert Logic Professional, which is a security and compliance solution that provides various capabilities; a list of which are in the *Fees Paid To Alert Logic* section.

Previous environment. The *Organization* engaged Alert Logic as soon as early efforts made it clear that a collection of older, repurposed security products would be inadequate due to the lack of support for public cloud platforms or for key cloud functions like autoscaling or API addressability. Like the companies interviewed by Forrester, the *Organization* briefly experimented with unmanaged firewalls, intrusion and detection prevention systems, and/or security information and event management systems that were originally designed for on-premises security duties. These experiments quickly indicated that a native cloud security solution was needed.

In its new cloud environment, the *Organization* is moving existing clients to cloud from on-premises. New clients are typically set up directly onto public cloud infrastructure. Meanwhile, the *Organization* must continue to

Early lessons:
Human judgment and evolving expertise were needed for cloud security . . . in place of inadequate appliances and point solutions designed for on-premises infrastructure.

maintain or improve its on-premises security posture, which, when costly or uncertain, is further motivation to migrate clients to the public cloud offering. Further, the *Organization* looked for a set of capabilities that would be cloud-friendly across multiple public cloud providers, as well as private cloud providers. The *Organization* must maintain security and compliance in Microsoft Azure, Amazon Web Services (AWS), and with other private regional cloud providers.

Obviously, a solution that can work across all those environments is preferable, while avoiding multiple setups and redundancy.

Financial Analysis

QUANTIFIED BENEFIT AND COST DATA APPLIED TO THE *ORGANIZATION*

Total Benefits

REF.	BENEFIT	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Atr	Security staffing costs avoided	$195,000	$292,500	$390,000	$877,500	$712,021
Btr	Compliance staffing costs avoided	$97,500	$97,500	$97,500	$292,500	$242,468
Ctr	Faster client acquisition: incremental gross profit	$37,500	$37,500	$37,500	$112,500	$93,257
Dtr	Security infrastructure cost avoidance	$24,000	$24,000	$24,000	$72,000	$59,684
	Total benefits (risk-adjusted)	**$354,000**	**$451,500**	**$549,000**	**$1,354,500**	**$1,107,431**

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 $1.1 million.

One interviewee summarized the business case for an investment in Alert Logic's services this way:

"The business case is made on name recognition and reputation with external auditors, and not on having to hire extra people, and the ability to add customers quickly without needing to plan ahead and add security people by region. It makes a pretty good ROI case when you look at the monthly cost of Alert Logic. It's pretty black and white."

Security Staff Cost Avoided

One of the primary benefits of using Alert Logic instead of an in-house security solution is the avoidance of internal labor costs. "If our managed services [SaaS] grow in the way we expect it to," explained one interviewee, "and I had to bring staff in house to do IDS alert analysis 24x7 and log management at least once per day, and event log analysis, I would probably need to hire five to eight people over the next two years." It's important to note that the number of new hires depends on the company size, scope, and complexity of its cloud security responsibilities.

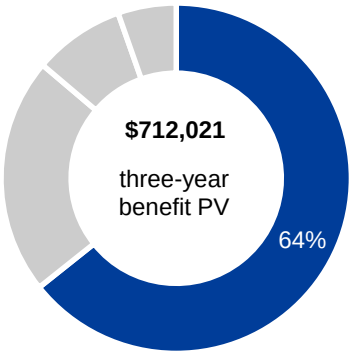
Cost savings for intrusion traffic analysis and log management, and event analysis: avoiding two, three, and then four new hires by Year 3 for the fast-growing composite *Organization*.

Another customer interviewee shared a common drawback to in-house solutions, “It’s a human resources challenge — finding the right skill sets, being able to afford and retain them especially after you train them to the specific needs of your business.”

Log management, log auditing, and log review is a perennial challenge for the interviewed companies because: 1) there is so much logged data and 2) knowing what data is important can either be done effectively with staff that do only that job, or it can be done inefficiently by staff who must chase and research a plethora of traffic that is not important or threatening.

Alert Logic’s per node pricing was cited by study participants as advantageous, one executive noted: “I don’t have to scale my staff to meet those growing needs. As we bring more and more managed service customers into our portfolio, I don’t have to exponentially scale to support the increased volume of traffic. I just send the traffic over to Alert Logic and they scale to support it. Our headcount does not have to increase as our number of customers increase. Having Alert Logic in the plan allows us to focus on the things that we can control with Alert Logic protecting our outside perimeter.”

Impact risk is the likelihood that benefit estimates will be higher than actual benefit results. To account for these risks, Forrester adjusted this benefit downward by 25%, yielding a three-year risk-adjusted total PV of $712,021.



Security staffing costs avoided: **64%** of total benefits

Security Staffing Costs Avoided: Calculation Table

REF.	METRIC	CALC./SOURCE	YEAR 1	YEAR 2	YEAR 3
A1	Security staffing new hires avoided	Interviews	2.0	3.0	4.0
A2	Yearly rate per person	Industry average	$130,000	$130,000	$130,000
At	Security staffing costs avoided	A1*A2	$260,000	$390,000	$520,000
	Risk adjustment	↓25%			
Atr	**Security staffing costs avoided (risk-adjusted)**		**$195,000**	**$292,500**	**$390,000**

Compliance And Regulatory Staffing Costs Avoided

Compliance efforts require attention and expertise. If this capability is maintained in house, substantial resources must be dedicated to assuring that the *Organization’s* managed services clients are kept from the harm that can befall organizations that fail to meet the rules and best practices mandated for their industry, as well as IT security in general.

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.

"Our partner introduced us to Alert Logic and said, 'Hey, if you're going to light up a solution like this, you probably need this level of security [and compliance] on it, right?' So, it's time to take it beyond the old school, of just a regular firewall or web application firewall, and into the realm of what we really need for compliance. We had seen Alert Logic out in the field before, when we've had things that needed either PCI or sometimes some type of SOX or HIPAA compliance, and we always thought it was a little bit too heavyweight for us until our partner introduced us, then we got hooked on Alert Logic."

The *Organization* must:

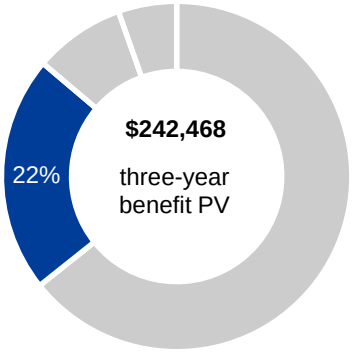
- **Meet regulatory requirements like SOX and PCI.** The demands of regulatory compliance on the interviewed customers required that they monitor their log files regularly, maintain an audit trail of log monitoring activities, and provide the necessary audit reports.
- **Address compliance requirements for log management for PCI and SOX.** Alert Logic solutions addressed PCI and SOX compliance requirements, including those for log management, vulnerability assessment, intrusion detection, and a web application firewall.

Companies have difficulty finding and retaining in-house staff who are charged with keeping up with the myriad of constantly changing government and industry-specific compliance requirements. "It is very difficult to keep up with standards and requirements," noted an interviewee, "even for somebody who's really good, really well trained, and really well paid." Another interviewee talked about skill, scale, and capacity mismatch, "It's difficult for a business of our size to assemble the compliance skills and capabilities that we really need to be successful." Alert Logic, by comparison, helped these organizations understand their customers' compliance needs — the interviewee went on: "They were really great when we were designing a HIPAA compliance solution for a medical device company. Alert Logic was on the phone with me three times a day answering questions or providing clarity on what was going to move the compliance needle with that company."

The reduction in labor costs for compliance will vary with:

- The number of resources required as the business grows.
- The time needed to develop in-house capabilities.
- The industry market compensation for compliance experts.

To account for these risks, Forrester adjusted this benefit downward by 25%, yielding a three-year risk-adjusted total PV of $242,468.



Compliance and regulatory staffing costs avoided: **22%** of total benefits

Compliance And Regulatory Staffing Costs Avoided: Calculation Table

REF.	METRIC	CALC./SOURCE	YEAR 1	YEAR 2	YEAR 3
B1	Compliance and regulatory specialist avoided	Interviews	1.0	1.0	1.0
B2	Yearly rate per person	Industry average	$130,000	$130,000	$130,000
Bt	Compliance and regulatory staffing costs avoided	B1*B2	$130,000	$130,000	$130,000
	Risk adjustment	↓25%			
Btr	**Compliance and regulatory staffing costs avoided (risk-adjusted)**		**$97,500**	**$97,500**	**$97,500**

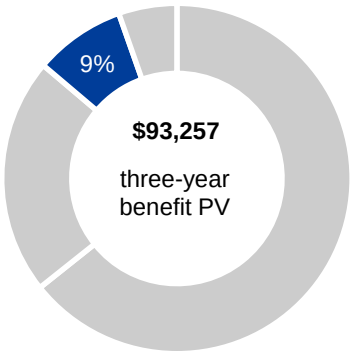
FORRESTER®

Faster Client Acquisition: Incremental Gross Profit

Prior to onboarding new clients, the *Organization* first had to achieve ISO 27001 certification. The interviewed customers wanted the process of achieving ISO 27001 certification and demonstrating industry-specific compliance to move ahead faster. By overcoming the challenges of faster certification, they could sign contracts with new clients three months earlier and move existing clients into the cloud environment earlier as well. The calculation in the table below is more for illustration than it is a complete quantification of the potential value of faster customer acquisition, which has large revenue and profit implications, and perhaps even larger market share and first mover advantages.

For the *Organization*, Forrester assumes that client contracts totaling $500,000 in annual revenue will be sold three months earlier with Alert Logic compared to without Alert Logic. This adds an incremental three months revenue and gross profit to the beginning of impacted contracts.

Risks. Even though the calculations below are *conservative*, Forrester nevertheless applied a risk adjustment factor of 25%; due to benefit assumptions being routinely optimistic. This risk adjustment mathematically removes any bias toward error due to optimism. The result is a risk-adjusted total PV of $93,257 in incremental gross profit over three years. Readers of this case study are encouraged to use their own estimates and timeline for accruing revenue and profits both with and without Alert Logic solutions.



Incremental gross profit:
9% of total benefits

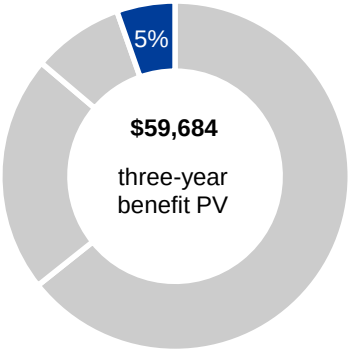
Faster Client Acquisition: Incremental Gross Profit: Calculation Table

REF.	METRIC	CALC./SOURCE	YEAR 1	YEAR 2	YEAR 3
C1	Incremental annual revenue	Interviews	$500,000	$500,000	$500,000
C2	Sales cycle time improvement	25% = 3 months faster	25%	25%	25%
C3	Gross profit	Average	40%	40%	40%
Ct	Faster client acquisition: incremental gross profit	C1*C2*C3	$50,000	$50,000	$50,000
	Risk adjustment	↓25%			
Ctr	**Faster client acquisition: incremental gross profit (risk-adjusted)**		**$37,500**	**$37,500**	**$37,500**

FORRESTER®

Security Infrastructure Cost Avoidance

Interviewed customers shared their experiences with net-new cloud infrastructure platforms for applications development and client services of applications, data, computational power, and engineering services. Forrester assumes the *Organization* needed to purchase $30,000 of security infrastructure (annually) such as storage, servers, and software licenses with annual maintenance, in order to store and handle log data. With a downward risk adjustment factor of 20%, this benefit category totals a three-year present value of $59,684. One interviewee described its pre-Alert Logic point solutions: “None of them were doing the IDS job, none of them were really doing the threat management job. Then we started to ramp up using the Alert Logic web application firewall and after a while it just didn’t make sense to have point solutions anymore.” Another interviewee explained: “Alert Logic replaced a lot of hodgepodge stuff. There’s still need for package-based firewall and whatever else, it’s just that those things are insanely difficult to manage from a logging perspective. So, having something that’s sniffing the exhaust and understanding what’s composing the exhaust is almost priceless.”



Security infrastructure cost avoidance: **5%** of total benefits

Security Infrastructure Cost Avoidance: Calculation Table

REF.	METRIC	CALC./SOURCE	YEAR 1	YEAR 2	YEAR 3
Dt	Security infrastructure cost avoidance	Interviews	$30,000	$30,000	$30,000
	Risk adjustment	↓20%			
Dtr	**Security infrastructure cost avoidance (risk-adjusted)**		**$24,000**	**$24,000**	**$24,000**

Unquantified Benefits

Examples of other benefits were expressed by study participants that Forrester did not quantify.

Incurring a security breach is of such potential negative impact that study participants mentioned it with trepidation. The value of avoiding such an incident is so large that it dwarfs other value calculations in this study. “I couldn’t even describe it,” explained one participant: “What would a breach cost me in time and materials? Six figures per day for the number of people I would have to have for audit, the number of project hours and opportunity cost hours lost. You are going to have your share of phone calls for next six or eight weeks, that are going to go 2 to 3 hours, where you're going to be talking to your client’s security people. And this is going to almost irreparably damage your brand. I can’t put a price tag on that.”

On the positive side, the Alert Logic interviewed customers described the concept of “client equity.” Having a solution that customers and their clients can trust allows Alert Logic customers to focus on the capabilities other than security and compliance that buy them client equity, like delivering applications on time. And as one customer notes, “I also have ‘hidden equity’ in the fact that for every day that goes by that we don’t have a breach, that’s another day.”

The cost of a breach, or a failed audit, would be a six-figure dollar amount.

FORRESTER®

Being a good corporate citizen (with ample security and compliance controls) might also be valuable to other organizations. “One of our clients gave us an award for being ‘security aware’ and noted, ‘When you participate in a neighborhood watch you make the whole neighborhood more valuable.’”

Flexibility

The value of flexibility is unique to each customer, and the measure of its value varies from organization to organization. There are scenarios in which a customer might choose to implement Alert Logic security-as-a-service and later realize additional uses and business opportunities, including:

- **“Hoteling” security and IT staff.** One interviewed customer described the potential for having staff function both in a security role and a development role, effectively straddling two or more domains. Because of the toolsets in the cloud and the interconnections, the opportunity to have multiskilled staff that are serving more than one team, or more than one purpose, is more viable in the cloud environment than it might be in a traditional data center.
- **The opportunity to develop new businesses and/or engage new segments** can be accomplished more quickly with: 1) a reputation for providing a secure environment; 2) scalability; and 3) when speed to industry-specific compliance can be achieved with the capabilities delivered by Alert Logic. An interviewee explained: “When you’re deploying in the cloud to be able to price it node by node you can achieve economies of scale. You can be very flexible. I can make this investment and protect our hosting property and have the power of [Alert Logic’s] SOC behind us, meaning we don’t have to train and retrain our staff.” Of note on compliance, an interviewed customer described their success in rapidly building a business in which clients require data and applications to be either fully HIPAA-compliant or at least attend to the rules of protected health information (PHI). The Alert Logic customer could focus on rapidly standing up the business because Alert Logic provided immediate expertise and practical capability for the compliance.

Flexibility might 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.

“In Alert Logic we have a partner that knows our environment very well. They help us make strategic decisions on how we should architect our security and how to tune alerts based on their knowledge of our industry.”

CISO, PaaS provider

Total Costs

REF.	COST	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Etr	Fees paid to Alert Logic	$0	$51,600	$56,760	$56,760	$165,120	$136,463
Ftr	Labor expense to setup and manage Alert Logic solutions and relationship	$22,815	$19,500	$19,500	$19,500	$81,315	$71,309
	Total costs (risk-adjusted)	**$22,815**	**$71,100**	**$76,260**	**$76,260**	**$246,435**	**$207,771**

Interviewed customers agreed that a DIY approach to security is quite costly and requires extensive ongoing investment in resources and expertise. Interviewed customers use Alert Logic's SIEMless Threat Management to deliver a security program that is simple to implement and maintain, easy to use, and provides a strong program ROI with a lower cost than other approaches.

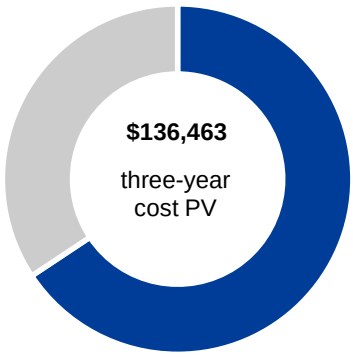
Fees Paid To Alert Logic

The *Organization* has invested in Alert Logic's security and compliance Professional offering, which includes the following capabilities:

- A 24x7 SOC with incident management, escalation, and response support.
- Intrusion detection.
- Attack prevention capabilities.
- Threat monitoring with frequency, severity, and status intelligence.
- Security analytics.
- Log collection, monitoring, and extensive search capabilities.
- Asset discovery and vulnerability scanning.
- Cloud configuration checks.
- Remediation guidance.
- PCI scanning and ASV support.
- 24x7 email and phone support.
- Extended endpoint protection.
- Reporting.

The main cost component of this analysis is the monthly services fee based on 50 nodes employed by the *Organization*. The Alert Logic fee is $4,300 monthly, or $51,600 annually. Note that pricing data was supplied by Alert Logic and was current at the time this study was written. We encourage readers to obtain pricing specific to their situation from Alert Logic.

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 $207,771.



Fees paid to Alert Logic: **66%** of total costs

FORRESTER®

Risks. Forrester does not risk-adjust Year 1 fees as these are contracted by Alert Logic. In subsequent years, however, services fees may vary, or changes in the business may bring about service fee changes. A modest risk adjustment of 10% is applied in years 2 and 3, yielding a three-year risk-adjusted PV of $136,463.

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.

Alert Logic Cloud Security And Compliance Solution: Calculation Table

REF.	METRIC	CALC./SOURCE	INITIAL	YEAR 1	YEAR 2	YEAR 3
E1	Monthly fee	Alert Logic	$0	$4,300	$4,300	$4,300
E2	Months	Months		12	12	12
Et	Alert Logic cloud security and compliance solution	E1*E2	$0	$51,600	$51,600	$51,600
	Risk adjustment	↑10%				
Etr	**Alert Logic cloud security and compliance solution (risk-adjusted)**		**$0**	**$56,760**	**$56,760**	**$56,760**

Labor Expense To Set Up And Manage Alert Logic's Capabilities

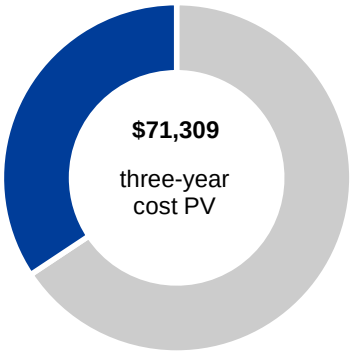
The interviewed customers described the labor effort needed to manage Alert Logic as modest. The labor effort included:

- Setup of the initial contract with Alert Logic, based on planning, discussions, service-level understanding, and initial relationship management.
- Business technology planning and coordination with Alert Logic as the traffic volume grows with the business, as more clients, existing and new, move from on-premises to cloud infrastructure for applications and data; also, managing the overall Alert Logic relationship.

For the *Organization*, three IT leaders (IT engineer, security analyst, and CISO) initially spent a total of 65 hours to analyze, plan, and scope the cloud security and compliance start-up requirements, and to work with Alert Logic to map the requirements against Alert Logic's capabilities and finalize contract terms.

For ongoing management of Alert Logic, we assume that 2.5 IT security FTEs will spend the equivalent of one week, twice a year (80 hours each) for business planning and coordination with Alert Logic.

We risk-adjusted this upwards by 30% to reflect variances in salary and uncertainty around the number of hours spent on these tasks. This yielded a three-year labor expense of a PV of $71,309.



Labor to set up and manage: **34%** of total costs

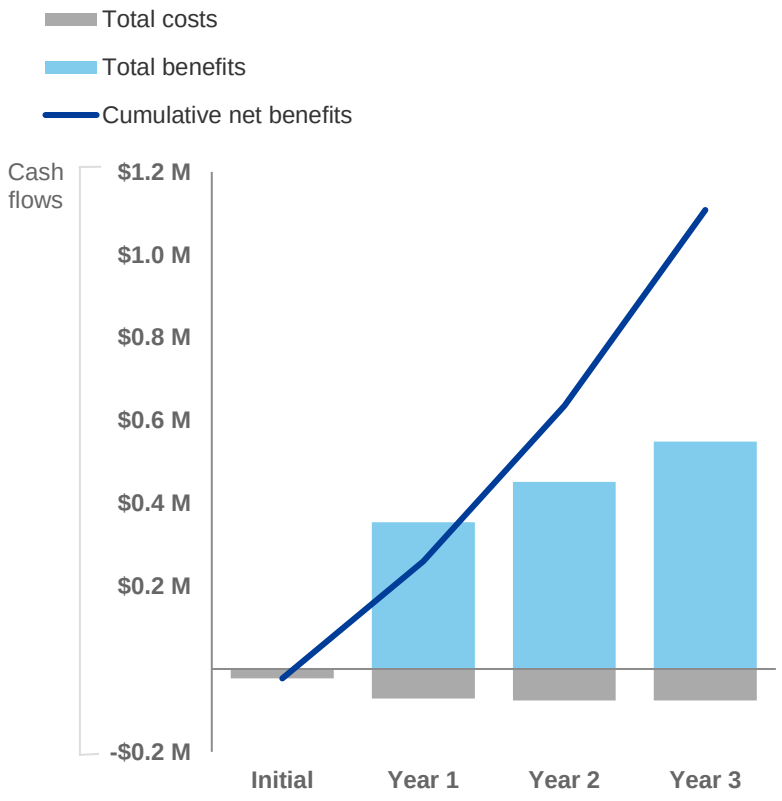
FORRESTER®

Labor Expense To Set Up And Manage Alert Logic's Capabilities: Calculation Table						
REF.	**METRIC**	**CALC./SOURCE**	**INITIAL**	**YEAR 1**	**YEAR 2**	**YEAR 3**
F1	Number of FTEs required	Interviews	3.0	2.5	2.5	2.5
F2	Hours required	Interviews	65	80.0	80.0	80.0
F3	Fully loaded hourly rate	Industry average	$90	$75	$75	$75
Ft	Labor expense to setup and manage Alert Logic capabilities	F1*F2*F3	$17,550	$15,000	$15,000	$15,000
	Risk adjustment	↑30%				
Ftr	**Labor expense to setup and manage Alert Logic's capabilities (risk-adjusted)**		**$22,815**	**$19,500**	**$19,500**	**$19,500**

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	($22,815)	($71,100)	($76,260)	($76,260)	($246,435)	($207,771)
Total benefits	$0	$354,000	$451,500	$549,000	$1,354,500	$1,107,431
Net benefits	($22,815)	$282,900	$375,240	$472,740	$1,108,065	$899,659
ROI						433%
Payback period						<6 months

FORRESTER®

Alert Logic: Overview

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

Alert Logic seamlessly connects a security platform, cutting-edge threat intelligence, and expert defenders to provide security and peace of mind for businesses 24/7, regardless of their size or technology environment. More than 4,000 organizations rely on Alert Logic SIEMless Threat Management to ensure the right level of security and compliance coverage for the right resources.

Alert Logic delivers the platform, intelligence, and expertise to help organizations build mature security programs and meet compliance mandates at a lower total cost than point solutions, SIEM tools, or traditional security outsourcing vendors.

That's the benefit of SIEMless Threat Management.

> "We would have needed multiple vendors on board to be able to do what we are doing with just Alert Logic. If I were talking to one of my colleagues in the industry who is looking for a cybersecurity solution, I would recommend Alert Logic, hands down."
>
> *Lee Ramsey,*
> *Co-Founder of Pre-Fi*

SIEMless Threat Management
Alert Logic provides three levels of offerings to give customers options when selecting their optimal coverage. This flexibility means that customers get the right coverage for the right resources and can tailor their approach to closely align their security programs to their business.

The Essentials Offering
The Essentials offering provides visibility for your environments and easily identifies the remediation steps required to eliminate exposure across platforms. Automatically track changes and posture status across your infrastructure and platforms, and intelligently block attacks through a combination of machine-learning and real-time behavior analysis.

The Essentials offering includes these capabilities:

- Asset discovery
- Vulnerability scanning
- Cloud configuration checks
- Extended endpoint protection
- Threat Risk Index
- Compliance scanning and reporting
- Support for multiple environments

The Professional Offering
At the Professional level, customers gain insight into the real threats in their environments, helping organizations make more informed security investment and resource decisions. Reduce network vulnerabilities and get verified security incidents without having to hire security experts to investigate alerts, remove noise, and analyze and prioritize threats.

The Professional offering provides these capabilities:

- 24/7 incident monitoring and management
- Security analytics and threat intelligence
- Log collection and monitoring
- Intrusion detection
- Security evet insights and analysis
- Office 365 log collection and search
- Cloud vendor security integrations
- User behavior anomaly detection
- Anti-virus integration

Plus all the capabilities of Essentials:

- Asset discovery
- Vulnerability scanning
- Cloud configuration checks
- Extended endpoint protection
- Threat Risk Index
- Compliance scanning and reporting
- Support for multiple environments

Enterprise:
Alert Logic Enterprise provides deeper security coverage for assets, vulnerabilities, and web applications for any environment with options for an assigned security analyst and managed Web Application Firewall. Access even greater protection to assist with incident response, security posture improvements, dark web scanning, and threat hunting. Get premium cybersecurity benefits and access to specialists at the right cost for your business.

Our Enterprise offering includes these options:
- Always-on managed WAF defense
- Assigned SOC analyst
- Threat hunting
- Dark web scanning

Plus all the strengths of our Professional and Essentials offerings:

- 24/7 incident monitoring and management
- Security analytics and threat intelligence
- Log collection and monitoring
- Intrusion detection
- Security evet insights and analysis
- Office 365 log collection and search
- Cloud vendor security integrations
- User behavior anomaly detection
- Anti-virus integration
- Asset discovery
- Vulnerability scanning
- Cloud configuration checks
- Extended endpoint protection
- Threat Risk Index
- Compliance scanning and reporting
- Support for multiple environments

Appendix A: Total Economic Impact

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

Total Economic Impact Approach

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

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

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

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

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

PRESENT VALUE (PV)

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

NET PRESENT VALUE (NPV)

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

RETURN ON INVESTMENT (ROI)

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

DISCOUNT RATE

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

PAYBACK PERIOD

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

Appendix B: Endnotes

[1] Source: Mark Western, “Developing a Framework to Improve Critical Infrastructure Cybersecurity,” The National Institute of Science and Technology, April 4, 2013 (http://csrc.nist.gov/cyberframework/rfi_comments/040813_forrester_research.pdf).