A Forrester Total Economic Impact™ Study
Commissioned By AT&T Cybersecurity
March 2018

The Total Economic Impact™ Of AlienVault® Unified Security Management® (USM)

Cost Savings And Business Benefits Enabled By AT&T Cybersecurity

FORRESTER®

Table Of Contents

Project Director:
Sean McCormick

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

Reduced risk of a breach:
$449,822

Compliance reporting efficiency:
$639,073

AlienVault® USM Anywhere™ license cost (three-year PV):
$185,477 (based on 1 TB of monthly data consumption)

Executive Summary

AT&T Cybersecurity provides a unified security management solution that helps its customers improve threat detection, reduce incident response time, reduce risk, and simplify meeting compliance standards. AT&T Cybersecurity commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) organizations may realize by deploying the AlienVault® Unified Security Management® (USM) platform. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of the AT&T Cybersecurity solution on their organizations.

The AT&T Cybersecurity solution, AlienVault® USM Anywhere™, is a cloud-based security monitoring platform that integrates security information and event management (SIEM) and log management with asset discovery, vulnerability assessment, intrusion detection, behavioral monitoring, and threat intelligence in one unified solution. AT&T Cybersecurity sells its platform to direct customers, who use the product to monitor their own environments, as well as to managed security service providers (MSSPs) who use the platform to monitor their customers' environments. To better understand the benefits, costs, and risks associated with an investment in the AT&T Cybersecurity platform, Forrester interviewed four customers, two direct and two MSSPs who have multiple years of experience using these products.

For direct customers, the USM platform helped to improve productivity in security operations while meeting and maintaining compliance with regulations. Prior to deploying USM Anywhere, it was difficult for these organizations to meet compliance standards, to dedicate time for audits, and to proactively monitor log files and identify threats — these challenges prevented the organizations from expanding into new customer markets. One CEO said, “AlienVault played an enormous role in enabling us to maintain PCI Level 1 compliance, which allowed us to compete with the large enterprises and grow our business.”

For MSSPs, the USM platform was a critical component to improving productivity in the security operations center (SOC) while enabling growth in a new line of business. Previously, these organizations struggled with piecing together point solutions that led to manual processes and inefficiencies throughout the SOC. For others, the USM platform became the platform on which a managed security services business was built. One MSSP said: “We were looking for a platform that we could use as our core MSSP platform. After performing a buy versus build analysis, we quickly realized that the cost of staffing developers for nearly 10 open-source products would be costlier than AlienVault’s unified security solution.” See the **USM Anywhere Managed Security Service Provider (MSSP) Journey** section for more information.

Key Findings

Direct customer benefits. The following risk-adjusted quantified benefits are representative of those reported by the direct customers interviewed:

FORRESTER®

ROI
6x

Benefits PV
$1.4 million

NPV
$1.1 million

Payback
<3 months

80% faster threat detection and incident response time

Reduction in compliance reporting effort, 94%

- **AlienVault USM Anywhere made compliance reporting considerably easier for companies, resulting in nearly 6,000 hours of time savings each year.** Prior to adopting AlienVault USM Anywhere, key pieces of information had to be pulled from many different systems and consolidated into reports for the auditor. This process took nearly four months, but with the USM platform, onsite audits could be completed in one week as the compliance information and reports were readily available in real time. This resulted in approximately 2,000 hours of time savings per audit and, on average, three audits were being held each year.
- **AlienVault USM Anywhere reduces the cost of incidents through improving threat detection and incident response time by 80%.** Based on a 2017 study conducted by the Ponemon Institute, the probability that an organization will experience a breach greater than 1,000 records is 14%. However, with the deployment of USM Anywhere, the time to detect incidents was dramatically reduced, helping organizations identify and respond to attacks much faster. With 80% faster detection and response time, the impact and probability of a breach could be reduced.[1]
- **AlienVault USM Anywhere provided an 80% security operations staff productivity improvement.** Prior to adopting this AT&T Cybersecurity solution, organizations didn't dedicate much time to daily monitoring tasks. On average, two to three investigations arose each week, which took the combined effort of two dedicated resources. After the deployment of the USM Anywhere platform, the security operations team was able to monitor and detect issues in real time. This reduced the manual effort involved in investigative activities by 80% and allowed the resources to focus their time on more value-added tasks. "We are still responsible for monitoring alerts and logging, but it's gone from hours per day to minutes. It allows us to focus on things like serving our customers, writing new code, and ultimately bringing more business in the door."
- **Threat intelligence saves time and money.** With AT&T Alien Labs™ threat intelligence, organizations no longer have to dedicate resources to sifting through multiple sources of information and bulletins to keep up with the latest intelligence. Now they can rely on the Alien Labs Security Research Team for continuous updates to threat correlation rules and directives. With the added benefit of not having to pay for an alternative threat intelligence subscription, the overall annual cost savings for the composite organization resulted in more than $40,000 per year.

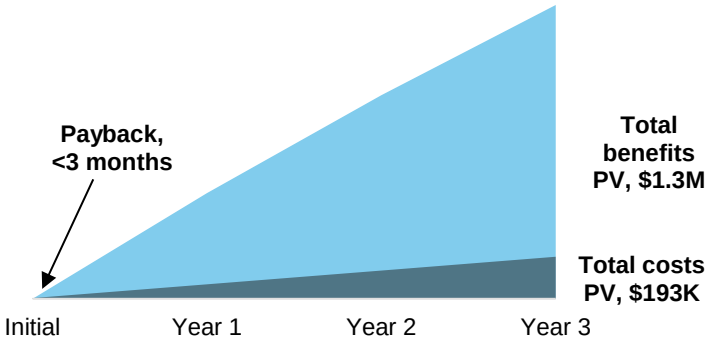
Direct customer costs. The following risk-adjusted quantified costs are representative of those reported by the direct customers interviewed:

- **AlienVault® USM Anywhere™ annual subscription costs of $65,000 to $80,000.** The platform's license and support costs are based on monthly consumption (GB) and the number of sensors deployed across an organization's environment.
- **$7,000 in implementation and training costs incurred.** The initial effort involved in the integration and setup of AlienVault USM Anywhere was five hours and could be done in less than a day. Additionally, security staff received two two-day training sessions to learn the depth and breadth of the USM platform.

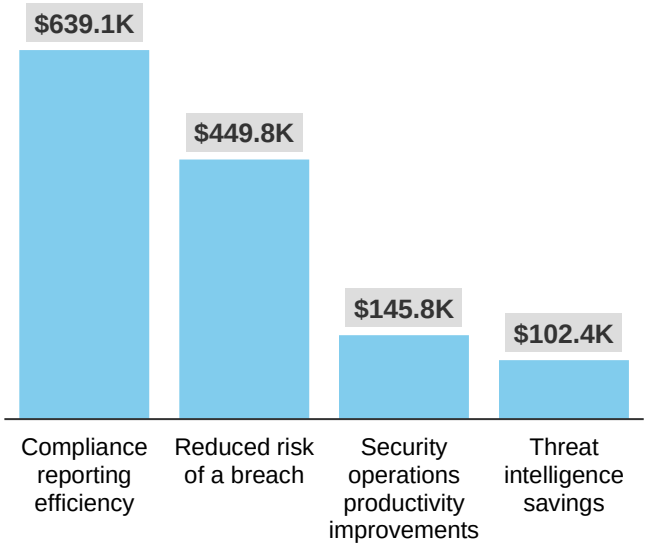
Forrester's interviews with two direct customers and subsequent financial analysis found that an organization based on these interviewed

organizations experienced benefits of $1,337,048 over three years versus costs of $192,729 adding up to a net present value (NPV) of $1,144,319 and a six-times return on investment.

Financial Summary



Benefits (Three-Year)



MSSP benefits. The interviewed managed security service providers experienced the following benefits, which are not quantified for this study:

- **AlienVault USM enables faster time to profit.** For MSSPs, adopting the Unified Security Management® (USM) platform shortened the time it took to break even on their initial investment and resource costs. As one interviewed MSSP stated, "We were profitable in about 15 months, but if we had to build the platform on our own, it would have cost $500,000 more in resources and delayed our profitability by nearly two and a half years."
- **AlienVault USM allows MSSPs to focus on customers' needs and innovate in key service areas.** With the USM platform, MSSPs don't have to worry about having an integration team trying to figure out how to integrate the messaging between critical pillars of an MSSP platform. Instead, they can focus their team on innovation in key service and solution areas such as reporting, communication, enhanced threat intelligence, and other additive areas.

MSSP costs. AT&T Cybersecurity offers specialized "pay-as-you-grow" subscription-based pricing bundles for managed security service providers (MSSPs).

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 AlienVault® USM 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 AlienVault USM 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 AT&T Cybersecurity stakeholders and Forrester analysts to gather data relative to the Unified Security Management® platform.

CUSTOMER INTERVIEWS
Interviewed four organizations using USM 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 issues and concerns of the interviewed organizations.

CASE STUDY
Employed four fundamental elements of TEI in modeling AlienVault USM Anywhere's impact: benefits, costs, flexibility, and risks. Given the increasing sophistication that organizations 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 USM Anywhere Direct Customer Journey

BEFORE AND AFTER THE UNIFIED SECURITY MANAGEMENT® PLATFORM INVESTMENT

Interviewed Organizations

For this study, Forrester conducted two interviews with AlienVault® USM Anywhere™ direct customers with the following characteristics:

Direct Customers

INDUSTRY	REGION	INTERVIEWEE	NUMBER OF SYSTEMS
Financial services	Atlanta, GA	CEO/founder	250 systems, 1 sensor
Healthcare	Seattle, WA	Director, information technology operations	80 systems, 3 sensors

Key Challenges

The interviewed direct customers were lacking a proper SIEM which made them susceptible to attacks and breaches. They did not have the tools or ability to detect intrusions or the resources and time to sift through log files and identify threats. These organizations invested in AlienVault to meet the following needs:

- **Identifying threats was too manual of a process.** Without a proper SIEM, it was tedious to manually sift through thousands of log files in order to identify threats or intrusions. One customer said: "We didn't have a proactive process related to observing activity in the system. If we had concerns, we would have to spend hours looking into it." Another customer said, "Before AlienVault, it was very intense to parse data." In addition to identifying threats manually, the time to detect and respond to incidents put the organization at high risk of a very costly breach. The director of information technology operations for a healthcare company said, "Prior to AlienVault, it would have taken us days, even weeks before something was detected."
- **Compliance audits were time consuming and overwhelming.** Because they operate in the financial services and healthcare industries, the interviewed organizations had to meet industry-specific regulations. After going through the audit process, it became apparent that they could not sustain the level of effort required to complete future audits. One company said, "Audits are becoming more sophisticated and if we didn't have AlienVault, we would be failing the audits." They went on to say that if they couldn't remediate the audit issues, they would likely lose customers. Another customer said it took them five months to gather all the information required to satisfy the auditor's needs. Achieving compliance is critical to these organizations, so it was imperative that they find a better way to meet the needs of auditors.

> "Prior to AlienVault, it would have taken us days, even weeks before something was detected."
>
> *Director of information technology operations, healthcare company*

FORRESTER®

- **Resources were scarce and difficult to obtain.** The interviewed organizations were lean companies with small understaffed security teams. Recruiting skilled cybersecurity resources to either build out or manage a security platform would be difficult. They needed a solution that was easy to use and could be run by general IT professionals. The CEO said, "There is a skills shortage, but AlienVault allows less experienced resources to gather information quickly."

Solution Requirements

The interviewed direct customers searched for a solution that could:

- **Combine the critical aspects of security into one package.** While implementing a SIEM and log management system was important for the interviewed companies, being able to improve their overall security solution and reduce the risk of a breach was critical. The director of information technology operations for a healthcare company said, "Vulnerability scans on the assets became very important overnight, and with AlienVault®, we could immediately see which servers were missing patches and show proof of patching to our customers." Managing multiple security systems also would have been time consuming and required more resources than these companies could spare. Another customer said, "For an organization our size, every resource makes the difference."
- **Be an easy-to-use system that allowed companies to train general IT resources on cybersecurity.** Given the scarcity of experienced cybersecurity professionals, it was difficult for midsize organizations to recruit the necessary skilled resources. Thus, it was critical to find a security solution that was easy to use and could give IT generalists the ability to operate it without a lot of specialized training. With AlienVault USM, most IT staff could learn the tool in less than a week. They could then focus on more value-added work like improving and satisfying customer needs, rather than being fully dedicated to security tasks. One customer said: "One direct impact that we saw was a much more rapid release cycle. We release a new version of software every 60 days; which is unheard of in our industry. This wouldn't be possible if we had to take two or three resources offline half the time to focus on security."
- **Be a cost-effective solution in meeting their security needs.** An important component for direct customers was to ensure the security solution they chose was cost effective. While no organization has money to waste, affordability and capital play an important role for midsize companies when making investment decisions. This was no different for the customers interviewed. With multiple solutions available in the marketplace, choosing one that provided all the key aspects of a unified security management platform and still had low upfront costs was vital. AlienVault USM met the needs of these organizations with low upfront costs, quick deployment, and minimal training required. In addition, the monthly license and support fees were based on consumption and therefore scaled with the size of the organization.

> "Vulnerability scans on the assets became very important overnight, and with AlienVault, we could immediately see which servers were missing patches and show proof of patching to our customers."
>
> *Director of information technology operations, healthcare company*

> "AT&T Cybersecurity understood that we were a small business and that we didn't have infinite resources in terms of human capital and money; they have a solution for that. There are lots of companies like us trying to make it on a shoestring budget and we have these enormous obligations to live up to in terms of compliance. AT&T Cybersecurity gets it."
>
> *CEO, financial services*

Key Results

The interviews revealed the following key results from the AlienVault USM Anywhere investment:

- **Enabling business growth by meeting compliance.** One of the reasons for adopting the AlienVault® USM platform was to help meet or maintain compliance. Historically, this had been challenging for customers since they would have to piece together and search for data through multiple systems and consolidate it into reports. However, beyond efficiency, the interviewed companies noted just how important meeting compliance was for their business. For example, one interviewee was able to achieve PCI Level 1 compliance which in turn increased their growth trajectory and allowed them to compete with the larger players in the market. In fact, after achieving compliance, they signed some large global and national customers. By maintaining and achieving compliance, these organizations were able to improve customer confidence and increase customer retention. "Without AlienVault, we would have failed our audits, and been fired by customers. AlienVault enabled our organization to continue growing."
- **Reduced cybersecurity risk by detecting and responding to incidents more quickly.** Prior to adopting the AlienVault USM platform, the customers interviewed didn't have a proactive way to monitor log files and identify areas of concern. One customer, using a pieced together set of tools, said the monitoring process was still very manual and, unless the customer knew what he or she was looking for, it proved difficult to identify threats in a timely manner. With the USM platform, threat monitoring was done effortlessly. IT teams could focus their efforts on other value-added work and if a threat was detected, an alert would be sent out. One customer, who relayed an event that occurred shortly after adopting AlienVault USM said, "We had an alarm hit that looked concerning, so we reached out to our development team, and then to AlienVault directly. Altogether, it took 15 minutes to get ahold of the teams and remediate the situation." Before AlienVault, this same situation would have taken days or weeks to detect. The customer would have had to see something in the behavior of the servers, research and try to identify if the behavior was threatening, and only then could they start remediating the issue.

  Threat intelligence is another valuable component in the Unified Security Management® platform from AT&T Cybersecurity. The AT&T Alien Labs Security Research Team provides continuously updated threat intelligence which allows organizations to stay up to date with the latest threats without spending hours of time on research and thousands of dollars on multiple sources of intelligence. One company said, "AlienVault threat intelligence is a huge time saver. We no longer have to read and understand five to ten bulletins across five to six different sources just to keep up with the latest threats." However, time wasn't the only thing being saved. Threat intelligence helped keep their USM platform deployment up to date ensuring threats didn't go unnoticed. The CEO of a financial services company said, "Our time to detection can be measured in minutes now, whereas before it was measured in hours or even days."

> "Now anyone of us with access to AlienVault can quickly retrieve the information the auditor is asking for. It doesn't take a specialized resource to do that."
>
> *CEO, financial services*

> "Threat detection has gone down to minutes. There's this constant real-time information from Amazon. AlienVault pulls that information and parses it. If it hits one of our triggers, or one of theirs, we get an alert within minutes.
>
> *Director of information technology operations, healthcare company*

> "Our time to detection can be measured in minutes now, whereas before it was measured in hours or even days."
>
> *CEO, financial services*

- **Efficiencies experienced across security operations.** Prior to adopting AlienVault USM, organizations lacked the necessary tools to maintain a secure environment, detect threats, and respond to incidents. Most security activities were prioritized based on urgency and took a considerable amount of time and effort to complete. The USM platform, with its SIEM and log management, threat intelligence, and intrusion detection system, alerted security teams of issues and gave them the tools to quickly classify and act on malicious activity. One company said, "We used to need one to two FTEs to help support daily monitoring activities, now we can do it in 1 to 2 hours per day."
- **Customer service and partnership.** One of the resounding remarks by the interviewed organizations was the quality of service provided. "The support team is fantastic, the response time is very short, and the engineers are knowledgeable."

Composite Organization

Based on the interviews with direct customers, 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 two direct 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 direct customer interviews has the following characteristics:

Description of composite. The composite company is a national midsize company with two locations. They are responsible for sensitive customer data and are subject to multiple data compliance regulations which require three audits per year. They have three IT analysts who have responsibility for security as well as other IT functions. The organization historically hasn't paid much attention to security, but due to recent developments with cybersecurity threats in the news, they decided to improve their security strategy and ensure they meet compliance standards.

Deployment characteristics. With two locations and a cloud-based environment, the organization deployed three sensors. Having 1,000 systems, including network devices, firewalls, routers, and servers, they needed to license up to one terabyte of data consumption in the AlienVault USM platform each month. The effort to implement AlienVault USM took 40 hours of total time with three IT staff members spending four days in training. All components of AlienVault USM Anywhere™ were utilized by the composite organization.

Key assumptions

1,000 systems

3 sensors

1 TB monthly consumption

FORRESTER®

Financial Analysis

QUANTIFIED BENEFIT AND COST DATA AS APPLIED TO THE COMPOSITE

Total Benefits

REF.	BENEFIT	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Atr	Compliance reporting efficiency	$251,567	$257,292	$263,188	$772,047	$639,073
Btr	Reduced risk of a breach	$180,880	$180,880	$180,880	$542,640	$449,822
Ctr	Security operations productivity improvements	$57,000	$58,710	$60,471	$176,181	$145,772
Dtr	Threat intelligence savings	$40,331	$41,217	$42,130	$123,678	$102,381
	Total benefits (risk-adjusted)	**$529,779**	**$538,099**	**$546,669**	**$1,614,547**	**$1,337,048**

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 $1.3 million.

Compliance Reporting Efficiency

Interviewed organizations experienced the following benefits in achieving and maintaining compliance standards.

- Reduced time to gather data across multiple systems.
- AlienVault® USM reporting consolidated the information necessary to meet compliance reporting needs.
- Audits became much more efficient since the reporting was available in real time and could be emailed directly to auditors. With AlienVault USM, organizations experienced a net 94% reduction in effort to complete audits.

For the composite organization, Forrester assumes that:

- Prior to adopting AlienVault USM, it took three full-time resources a total of four months to gather and consolidate information into reports, and supply it to auditors.
- After adopting AlienVault USM, these same three full-time resources were able to satisfy the requirements of the audit in one week.
- The average hourly rate for a full-time equivalent (FTE), fully loaded, was $36.06 and steadily increased 3% each year.
- On average, three external audits were completed each year by the composite organization.[2]
- The average cost of an external audit was approximately $75,000. This cost decreased by 30% with AlienVault USM.

Risks that can affect this benefit include:

- The industry in which an organization operates and the compliance standards they need to meet.
- The number of audits required each year may be different for every organization based on their specific compliance standards.

Audits became **94%** more efficient since reporting was available in real time and could be emailed directly to auditors.

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®

› The amount of time and effort required to satisfy an audit, both before and after AlienVault USM, can vary based on the complexity of the audit and its specific requirements.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $639,073.

Compliance Reporting Efficiency: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
A1	Internal effort required to satisfy audits before AlienVault	Hours	2,080	2,080	2,080
A2	Internal effort required to satisfy audits with AlienVault	Hours	120	120	120
A3	Average cost per resource, fully loaded (rounded)	$75,000/2080	$36.06	$37.14	$38.25
A4	Number of compliance audits per year		3	3	3
A5	Internal effort audit savings	(A1-A2)*A3*A4	$212,019	$218,380	$224,931
A6	Average cost for external audit		$75,000	$75,000	$75,000
A7	Percentage savings with AlienVault		30%	30%	30%
A8	External audit cost savings	A6*A7*A4	$67,500	$67,500	$67,500
At	Compliance reporting efficiency	A5+A8	$279,519	$285,880	$292,431
	Risk adjustment	↓10%			
Atr	Compliance reporting efficiency (risk-adjusted)		$251,567	$257,292	$263,188

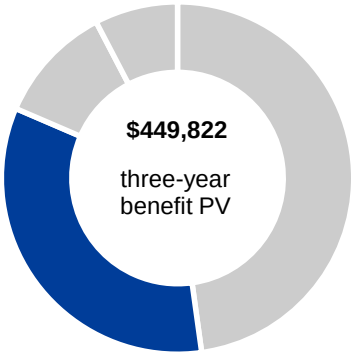
Reduced Risk Of A Breach

A primary need for all the interviewed organizations was to improve their cybersecurity practices and tool sets in order to reduce the risk of a potential breach. To satisfy this need, they sought to improve their ability to detect malicious activity and intrusions. The AlienVault® Unified Security Management® (USM) platform gave companies the tool set to monitor log files and activities, detect intrusions, and alert security teams if action was needed. Not only were organizations able to dramatically improve their time to detection, but they were able to investigate and take action much more quickly than before. By adopting the USM platform from AT&T Cybersecurity, organizations were able to lower their risk of costly data breaches and improve their incident response time in order to lower the cost of any incidents.

For the composite organization, Forrester assumes that:

› The average cost of a breach or large incident involving 1,000 records or more is $1,900,000. This is based on the low end of the range published by Ponemon in their 2017 study.[3]

› The probability for an average organization of experiencing a breach or large incident involving 1,000 records or more is 14% in a given year.[4]



Reduced risk of a breach: **34%** of total benefits.

FORRESTER®

› By adopting AlienVault USM, the composite organization saw an 80% improvement in threat detection and incident response time. This helped organizations lower the probability of an incident becoming a breach and reduced the average cost of an incident.

The reduced risk of a breach will vary with:

› The industry in which an organization operates as some industries have higher probabilities and costs to a breach.

› The effectiveness of a security operations team and their ability to respond to incidents.

To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year risk-adjusted total PV of $449,822.

Improvement in threat detection and incident response time, **80%**.

Reduced Risk Of A Breach: Calculation Table

REF.	METRIC	CALC./SOURCE	YEAR 1	YEAR 2	YEAR 3
B1	Average cost of breach or large incident	IBM data	$1,900,000	$1,900,000	$1,900,000
B2	Average probability of breach or large incident	IBM data	14%	14%	14%
B3	Improved time to detect incident and respond		80%	80%	80%
Bt	Reduced risk of a breach	B1*B2*B3	$212,800	$212,800	$212,800
	Risk adjustment	↓15%			
Btr	Reduced risk of a breach (risk-adjusted)		$180,880	$180,880	$180,880

Security Operations Productivity Improvements

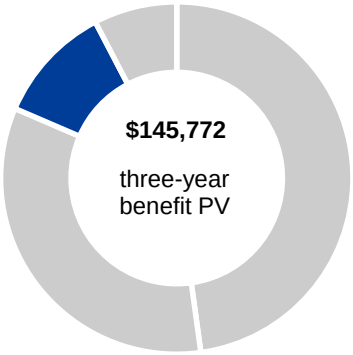
Based on the information provided by the interviewed organizations, productivity improvements were experienced in both daily monitoring activities and in investigations. Prior to adopting AlienVault® USM Anywhere™, companies were struggling to monitor log files and felt overwhelmed with the effort required to proactively identify threats. Resources dedicated more time than they could afford to sifting through log files and searching for incidents that required further investigation. With scarce IT resources, this was heavily taxing for these companies. AlienVault helped to solve these issues by reducing the monitoring effort to mere hours per week. One customer said, “For an organization my size, without a tool like AlienVault, it would take at least one full-time employee just to monitor the environment to make sure it's healthy, to review the logs. With AlienVault, we don’t even need just one, it's really just an hour or 2 split amongst the team.”

For the composite organization Forrester assumes that:

› Two FTEs were required for daily monitoring and investigation activity in security operations.

› An average of 130 incidents per year required investigation.

› Productivity for monitoring and investigative activities was improved by 80%, with 50% of that time savings being reallocated to other valuable activities.



Security operations productivity improvements: **11%** of total benefits.

FORRESTER®

› The average hourly rate for a fully-loaded FTE was $36.06 and increased by 3% each year.

Productivity improvements for security operations staff will vary based on:

› The amount of effort that was originally being dedicated to log monitoring.

› The percentage of time that could be captured and reallocated to other activities.

To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year risk-adjusted total PV of $145,772.

Productivity improved by 80% for security operations.

Security Operations Productivity Improvements: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
C1	Number of FTEs required for daily monitoring prior to AlienVault		2	2	2
C2	Average # of investigations per year		130	130	130
C3	Productivity improvement percentage		80%	80%	80%
C4	Percent of productivity captured		50%	50%	50%
C5	Average hourly rate, fully loaded (rounded)	$75,000/2080	$36.06	$37.14	$38.25
Ct	Security operations productivity improvements	C1*2080*C3*C4*C5	$60,000	$61,800	$63,654
	Risk adjustment	↓5%			
Ctr	Security operations productivity improvements (risk-adjusted)		$57,000	$58,710	$60,471

Threat Intelligence Savings

With AlienVault USM Anywhere, customers have access to the most up-to-date research, threat vectors, and attacker techniques as well as ways to defend against them. Intelligence like this can take a lot of time and money to gather, and it can require the use of multiple intelligence sources. One interviewed organization said, “Without somebody’s third-party tool, I think it would have been impossible to do threat intelligence on our own.” Another company said, “The threat intelligence network is a time saver.” These companies didn’t have the resources to dedicate to obtaining threat intelligence. Therefore, they would have incurred further costs and had to purchase it elsewhere if it were not already included with USM Anywhere. The AT&T Alien Labs™ Threat Research team improves the efficiency of a security-monitoring program by delivering continuously updated threat intelligence to identify new and emerging threats.

For the composite organization, Forrester assumes that:

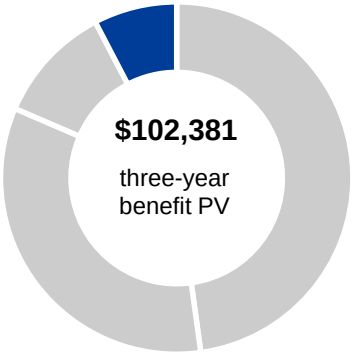
Threat intelligence ensures the most up-to-date threats can be detected while saving valuable time.

- Forty hours a week or one FTE was dedicated to gathering threat intelligence prior to adopting AlienVault USM.
- The amount of time required after AlienVault USM was deployed decreased to 5 hours a week with 50% of that time savings being reallocated to other valuable activities.
- The average hourly rate for a FTE, fully loaded, was $36.06 and increased by 3% each year.
- The average annual subscription cost avoided for outsourcing threat intelligence was $12,000.

Threat intelligence time savings will vary based on:

- The amount of effort that was originally being dedicated to threat intelligence.
- The percentage of time that could be captured and reallocated to other activities.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $102,381.



Threat intelligence savings: **7%** of total benefits.

Threat Intelligence Savings: Calculation Table

REF.	METRIC	CALC./SOURCE	YEAR 1	YEAR 2	YEAR 3
D1	Amount of time spent on gathering threat intelligence before AlienVault USM	Hours per week	40	40	40
D2	Amount of time spent on gathering threat intelligence with AlienVault USM	Hours per week	5	5	5
D3	Average hourly rate, fully loaded (rounded)	$75,000/2080	$36.06	$37.14	$38.25
D4	Percent of productive time captured		50%	50%	50%
D5	Threat intelligence time savings	(D1-D2)*52*D3*D4	$32,760	$33,743	$34,755
D6	Average threat intelligence subscription service cost avoidance, annual		$12,000	$12,000	$12,000
Dt	Threat intelligence savings	D5+D6	$44,813	$45,797	$46,811
	Risk adjustment	↓10%			
Dtr	Threat intelligence savings (risk-adjusted)		$40,331	$41,217	$42,130

Flexibility

The value of flexibility is unique to each customer, and the measure of its value varies across organizations. There are multiple scenarios in which a customer might choose to implement AlienVault® USM Anywhere™ and later realize additional uses and business opportunities, including:

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.

FORRESTER®

- **AlienVault USM Orchestration capabilities enable automated response actions.** An investment in USM Anywhere™ includes AlienApps™, modular software components that interact with other IT security and operations products, and business-critical applications, which help unify security architecture in a single platform, and centralize the orchestration of incident response activities. Once set up, automated ticketing and response actions can be applied based on predetermined parameters. This further reduces the time it takes to respond to incidents and enables security operations teams to be more productive and effective.
- **AlienVault USM Asset Discovery provides visibility into everything connected on the network and resident in the cloud.** For companies that have numerous devices logging onto their network, more assets in the cloud, or a hybrid environment, it can be difficult to know what's connected and what's not. USM Anywhere™ includes a built-in asset discovery capability that provides visibility into every IP-enabled device on the network, giving you information on the software and configurations as well as helping to discover any vulnerabilities or known threats. Organizations subject to compliance mandates require internal vulnerability scans and USM Anywhere makes that easier.

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

Total Costs

REF.	COST	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Etr	AlienVault USM license fee	$0	$67,536	$74,038	$83,709	$225,283	$185,477
Ftr	AlienVault implementation and training	$4,006	$1,269	$1,307	$1,347	$7,929	$7,252
	Total costs (risk-adjusted)	**$4,006**	**$68,805**	**$75,345**	**$85,056**	**$233,212**	**$192,729**

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 more than $193 thousand.

AlienVault USM License Fee

The monthly cost for AlienVault® USM Anywhere™ was based on the amount of data sent to the platform and the number of sensors deployed across locations and environments. AlienVault USM Anywhere requires a minimum one-year contract.

- The number of systems, including servers, network devices, firewalls, and routers, among others, impacts the amount of data consumed monthly. On average, each device consumes about one GB every month.
- In addition to systems, a virtual sensor will be deployed in each environment. A monthly fee of $200 per sensor will be incurred beyond the first two sensors.

For the composite organization, Forrester assumed:

- An average one TB of data per month, across 1,000 systems, is sent to the USM platform.
- Three environments, one cloud based and two on-premises environments, required sensors.
- Two sensors are initially included in the standard pricing. The amount of systems increased by 10% per year and a new sensor would be required in Year 3.

The cost for USM Anywhere licensing can be impacted by:

- The amount of data consumed on average by each system.
- Multiproduct discounting and other negotiated terms.

To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year risk-adjusted total PV of $185,477.

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.

AlienVault License Fee: Calculation Table						
REF.	METRIC	CALC./SOURCE	INITIAL	YEAR 1	YEAR 2	YEAR 3
E1	Monthly consumption	GB		1,000	1,100	1,210
E2	# of sensors deployed			3	3	4
E3	Monthly subscription cost	(E1*$5.16)+ (E2-2)*$200		$5,360	$5,936	$6,570
Et	AlienVault USM license fee	E3*12	$0	$64,320	$70,512	$79,723
	Risk adjustment	↑5%				
Etr	AlienVault USM license fee (risk-adjusted)		$0	$67,536	$74,038	$83,709

AlienVault USM Implementation And Training

The implementation process for AlienVault® USM Anywhere™ is simple and efficient. Minimal training is required for security team members and the overall cost for implementation and training is seen as a benefit by keeping upfront costs low and removing investment barriers. One interviewee said: “It's actually very straightforward to roll out. We're talking a couple of hours, and that's probably high.” This is compared to point solutions, where security staff would have to be trained separately on each system, which could take up to five to ten times the amount of effort upfront.

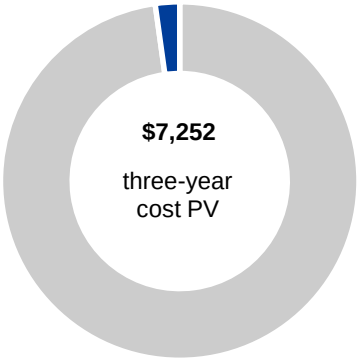
Forrester assumed the following for the composite organization:

- Five hours of effort required for implementation.
- Thirty hours of training for each security staff working with AlienVault USM. This includes a two-day course for deployment and configuration and a two-day course for security analysis.
- The security operations team had three dedicated security team members to begin with and annual growth and turnover requiring the hiring of one new analyst each year.
- The average hourly rate for a FTE, fully loaded, was $36.06 and increased by 3% each year.

Risks that could impact the cost of deployment and training include:

- The skill level of security resources and the degree to which they will be utilizing USM Anywhere™.
- The complexity of the environments, including the number of systems.
- The degree to which automated activities will be setup.

To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year risk-adjusted total PV of $7,252.



AlienVault implementation and training: **3%** of total costs.

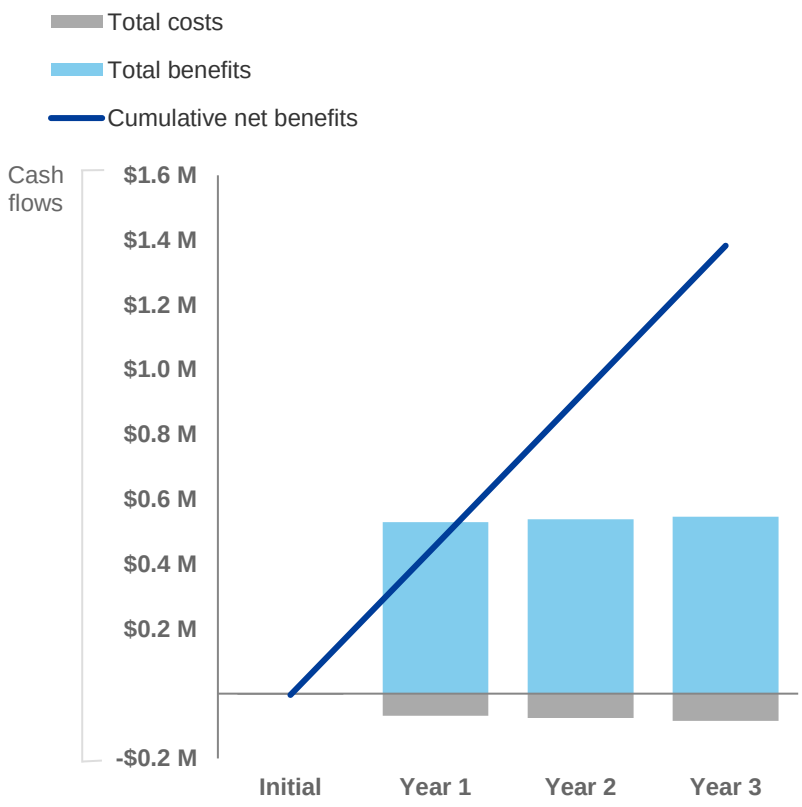
FORRESTER®

AlienVault Implementation And Training: Calculation Table						
REF.	**METRIC**	**CALC./SOURCE**	**INITIAL**	**YEAR 1**	**YEAR 2**	**YEAR 3**
F1	Effort required for implementation	Hours	5			
F2	# of security analysts requiring training		3	1	1	1
F3	Amount of training time per security analyst	Hours	32	32	32	32
F4	Average hourly rate, fully loaded (rounded)	$75,000/2080	$36.06	$36.06	$37.14	$38.25
Ft	AlienVault USM implementation and training	(F1+F2*F3)*F4	$3,642	$1,154	$1,188	$1,224
	Risk adjustment	↑10%				
Ftr	AlienVault USM implementation and training (risk-adjusted)		$4,006	$1,269	$1,307	$1,347

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 return on investment, NPV, and payback period for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

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

Cash Flow Table (Risk-Adjusted)

	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Total costs	($4,006)	($68,805)	($75,345)	($85,056)	($233,212)	($192,729)
Total benefits	$0	$529,779	$538,099	$546,669	$1,614,547	$1,337,048
Net benefits	($4,006)	$460,973	$462,754	$461,613	$1,381,335	$1,144,319
ROI						6x
Payback period						<3

FORRESTER®

The USM Anywhere MSSP Journey

BEFORE AND AFTER THE UNIFIED SECURITY MANAGEMENT® (USM) PLATFORM INVESTMENT

Interviewed Organizations

While the financial model presented above was based on the findings from interviews with direct AT&T Cybersecurity customers using AlienVault USM, MSSP customers were also interviewed as part of this study. The following section outlines the benefits described by these MSSP customers. For this study, Forrester conducted two interviews with AlienVault USM managed security service providers (MSSPs) with the following characteristics:

MANAGED SECURITY SERVICE PROVIDERS

INDUSTRY	REGION	INTERVIEWEE	SIZE OF COMPANY
MSSP	Phoenix, AZ	CEO/co-founder	60 employees, 50 customers
MSSP	USA	Leadership	10 employees, 15 customers

Key Challenges

- **For MSSPs, the biggest challenge was differentiating themselves in a profitable way.** The interviewed MSSPs were both operating consultative services prior to becoming a MSSP. However, they quickly realized that in order to differentiate themselves and meet the demands of their customers, they would need to extend their businesses to provide managed security services. Given the risk involved in building out a new business line, the MSSPs were looking for an affordable way to get to market quickly and speed up their payback period. One customer said, "Our break-even was two years and 15 clients. If we were using a different tool set, it would have absolutely taken longer. I would estimate closer to four years with more than 20 customers."

Solution Requirements

The MSSPs interviewed searched for a solution that could:

- **Reduce the effort involved in adoption by only training SOC analysts on one platform.** Having a unified security solution was also important for MSSPs. AlienVault USM allowed them to train and focus their security operations center (SOC) on a single security monitoring platform rather than operate multiple platforms and products. This created efficiencies and meant they could spend more time focusing on innovation and providing greater value to customers. One MSSP said, "AlienVault allowed us to innovate with different go-to-market strategies, and different portfolio offerings, and different enhancements that better service our end customers."

> "The cost structures and cost points for us to provide our service to our customers are drastically different as a result of not having to worry about trying to integrate things together. AT&T Cybersecurity does that for us under their USM [platform]."
>
> *CEO, MSSP*

FORRESTER®

- **Be a cost-effective solution in meeting their security needs.** An important component for both direct customers and MSSPs was to ensure the security solution they chose was cost effective. While no organization has money to waste, affordability and capital play an important role for MSSPs when making investment decisions. This was no different for the interviewed companies. With a variety of solutions in the marketplace, choosing one that provided all the key aspects of a unified security management platform and still had low upfront costs was vital. Ultimately, the AlienVault® Unified Security Management® platform met the needs of these organizations with low upfront costs, quick deployment, and minimal training required. In addition, the monthly license and support fees were based on consumption and therefore scaled with the size of the organizations they were serving. This allowed MSSPs to get to market faster, invest more in resources and innovation, and reduce the time to profit. One MSSP said: "We thought we would lose money in Year 1 and projected to break-even in Year 2 and be profitable by Year 3. Once we introduced AlienVault, we became profitable in 15 months."

"Those of us who had built out security programs all looked at this and said, "this is a terrific platform." So, we went all in and built our MSSP division around AlienVault."

CEO, MSSP

Key Results

The interviews revealed that an investment in AlienVault USM Anywhere™ included these key results:

- **AlienVault USM enabled MSSPs to get to market faster.** Timing is always a critical part of starting any new business. For the interviewed MSSPs, it was no different. They knew they had plenty of opportunities within their current customer base to extend existing services to managed security services, however, it was going to take a lot of time to design and build out the business. With AlienVault, these MSSPs were able to mobilize quickly and adopt the technology in a matter of weeks. One MSSP said: "We did a buy versus build analysis, wanting to either tie together open-source tools or buy a platform. And through this analysis a high degree of value was found in AlienVault." They went on to say that AlienVault USM saved them $2.5 to $3 million.
- **Increased value for their customers.** Providing managed security services was a natural extension for the interviewed organizations as it was a service their customers had been asking for. One MSSP reported, "We were approached by customers and asked if we could get into the managed security business?" With AlienVault USM, the MSSPs were able to deploy the solution in one to two weeks and detect issues right away for each customer. Another MSSP said: "A customer was concerned something was happening in the environment. We deployed AlienVault to the customer environment and in 15 minutes there was command and control messaging and lack of patching identified in the environment." By demonstrating quick wins with AlienVault USM, MSSPs were able to build trust and long-term business with their customers.

AlienVault® USM Anywhere™: Overview

The following information is provided by AT&T Cybersecurity. Forrester has not validated any claims and does not endorse AT&T Cybersecurity or its offerings.

AlienVault® USM Anywhere™, from AT&T Cybersecurity, is a unified security platform for early threat detection, rapid incident response, and simplified compliance management across cloud and on-premises environments.

With USM Anywhere, you can eliminate the time, expense, and resources required to deploy, integrate, and maintain a stack of point security solutions in your data center. The AlienVault USM platform delivers everything you need to detect threats and respond to threats on Day One, including continuous, curated threat intelligence from the AT&T Alien Labs Security Research Team.

Discover why 7000+ organizations worldwide trust AlienVault USM for their security and compliance needs.

Prevent a Security Breach with Early Threat Detection

AlienVault USM includes multiple, coordinated security capabilities to detect threats and vulnerabilities early and from all angles, including:

- Visibility across cloud and on-premises environments as well as cloud applications
- Built-in capabilities for vulnerability assessment, intrusion detection, user activity monitoring, SIEM event correlation, and much more
- Continuous, curated threat intelligence from the Alien Labs Security Research Team in the form of correlation rules, IDS signatures and incident response guidance

Get Security Insights on Day One

USM Anywhere fully deploys in minutes (not months) and automates asset discovery and data collection from your devices, cloud apps, networks and cloud infrastructure. With it, IT security teams can be more effective faster.

- Gives complete and accurate threat context on every prioritized alarm
- Includes built-in security analytics, interactive dashboards, and compliance reports

With USM Anywhere, you can focus on what matters most — protecting your critical IT infrastructure against the latest cyber threats.

Simplify Achieving and Maintaining Compliance

AlienVault USM Anywhere combines the essential security technologies needed to demonstrate compliance with today's most challenging regulatory standards:

- Automated log collection, analysis, and event correlation in a single console
- Secure storage of log data in the AlienVault Secure Cloud for up to 90 days online, and 12 months or more in cost-effective cold storage
- Continuous asset discovery and vulnerability scanning
- Simplified compliance reporting with out-of-the-box, predefined compliance reports and highly customizable data search and analytics

Learn more:

- 2-minute Product Overview Video
- Pricing Packages
- Online Demo

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] Source: Ponemon Institute's 2017 Cost of Data Breach Study: Global Overview (https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN).
[2] Source: The True Cost of Compliance with Data Protection Regulations (https://www.ponemon.org/news-2/80).
[3] Source: Ponemon Institute's 2017 Cost of Data Breach Study: Global Overview (https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN).
[4] Ibid.