WHITE PAPER

AN EXECUTIVE'S GUIDE TO BUDGETING FOR SECURITY INFORMATION & EVENT MANAGEMENT

COST ANALYSIS OF TWO DELIVERY MODELS: SELF-MANAGED SIEM VS. MANAGED SIEM SERVICES

Trustwave®

Smart security on demand

AN EXECUTIVE'S GUIDE TO BUDGETING FOR SECURITY INFORMATION & EVENT MANAGEMENT

COST ANALYSIS OF TWO DELIVERY MODELS:
SELF-MANAGED SIEM VS. MANAGED SIEM SERVICES

TABLE OF CONTENTS

INTRODUCTION

Security Information and Event Management (SIEM) solutions have been around for more than a decade. Yet, the industry is far from seeing the level of satisfaction and broad commitment to SIEM as in other security technologies at the same stage. However, SIEM must be a critical part of an organization's security strategy and toolset. Why? The driving problems still exist and are growing – how does one detect, analyze and remediate a breach to IT infrastructure? SIEM still addresses these problems better than other solutions. The frustration frequently comes from underestimating the costs and complexity of deployment and operation of a SIEM. To overcome these challenges, managed SIEM services have been introduced to address the unique needs and strategies for organizations of all sizes. But, how should an organization choose between self-managed and managed SIEM?

Ultimately, the goal of this paper is to provide an insightful tool to IT security buyers to understand the costs, options, and trade-offs of the two primary SIEM deployment models, self-managed (Do-It-Yourself) and managed security services. This paper compares the costs of SIEM under two delivery models, self-managed and managed SIEM for three different customer scenarios based on organizational size. The cost comparisons capture both capital expenses (upfront costs) and operating expenses (ongoing usage costs).

The three customer scenarios presented are:

- Large Enterprise
- Medium Enterprise
- Small Enterprise.

The value of these scenarios comes from applying and adjusting the appropriate scenario to an organization based on the descriptions and profiles provided within this analysis.

We understand that there are strategic considerations in addition to the financial ones. This paper briefly discusses three strategic issues due to the frequency in these discussions and their direct influence on costs.

COST METHODOLOGY

The cost models presented apply a total cost methodology by incorporating most indirect costs of buying a SIEM across a typical service time period of three years. For example, we include labor costs associated with operating the SIEM including:

- Training
- Deployment and implementation support
- Turnover and recruiting
- Fully-loaded labor rates (i.e., salary + overhead expense).

We intentionally exclude certain indirect costs, such as data center space, power and cooling that are included in many service provider total cost of ownership (TCO) models. The Trustwave Managed SIEM architecture requires a SIEM device on the customer's premises. Therefore, these indirect costs are the same for both delivery methods.

One indirect expense most companies do not capture when budgeting for their SIEM is staffing costs associated with recruiting, turnover and ongoing staff training and certification. These costs can be significant. This paper uses widely-published standards to capture these costs.

DEFINITIONS AND DESCRIPTIONS

In the information technology industry, terminology can vary between users leading to misunderstanding and incorrect conclusions. To ensure clarity, here are the definitions of the terms used in this paper.

Self-Managed

This is a delivery model for use of a security solution where the customer buys, deploys, and operates the SIEM solution on its premises – both software and hardware. Maintenance and support are included which follows standard purchasing practices for self-managed solutions. The customer's employees are responsible for the deployment and operation of the system. Success is dependent on the customer properly scoping and budgeting for the solution and maintaining necessary level of skilled staffing and training.

Managed SIEM delivered through Managed Security Services

As a managed security services provider (MSSP), Trustwave offers a broad portfolio of security services including different SIEM services. Under the managed security services model, the customer pays Trustwave a service fee (subscription) to deliver specific SIEM services.

Trustwave offers three types of managed SIEM services that align with the major operating components of a SIEM. These include:

1. Self-serve cloud log monitoring – Trustwave implements and maintains SIEM technology platform, covering basic system operations, including:
    - Device administration
    - Collection of logs into Trustwave global security operations centers (SOCs)
    - Presentation of data and device information through Trustwave TrustKeeper® portal based on settings created by customer or Trustwave services depending on service model
    - System heath check service (provided at an additional service fee).
2. Compliance monitoring service – Based on the collection and processing of the customer's log data by Trustwave SOCs, the daily compliance reporting service emails customers a log analysis report to help address compliance requirements. The compliance service can be tailored to report on a specific set of devices. Trustwave implements and maintains the SIEM technology platform.
3. Threat analysis monitoring service – Based on the collection and processing of the customer's log data by Trustwave SOCs, threat analysis monitoring service applies both machine and human analysis to detect and prevent security incidents and data breaches. The service can be tailored to report on a specific set of devices. SIEM threat analysis monitoring service includes:
    - Automated analysis of customer's data based on correlations created by Trustwave specific to customer's environment and risk profile
    - Human monitoring of SIEM activity, analysis of alerts, investigation of priority alerts
    - Notification to client about events of concern that require additional attention and on-site investigation and remediation by customer's security staff.

The customer and Trustwave agree upon the types of services that will enable the customer to meet their business and security objectives. This service model ties Trustwave more closely to the customer's success than traditional licensed technology models and helps eliminate the **shelfware problem**.

Capital Costs (CapEx) and Operating Costs (OpEx)

Many equipment purchases (e.g., servers, software, etc.) involve a CapEx and an OpEx component. Allocation of these expenditures into the “right” CapEx and OpEx buckets can quickly devolve into a technical accounting discussion based on individual accounting practices. This paper keeps the allocation simple and intuitive. Capital expenses are the upfront costs paid for the products (hardware and software) that the customer purchases. Ongoing costs associated with certain use of products (e.g., support and maintenance) are considered operating expenses. These expenditures are considered OpEx even if the customer pays in full at beginning of the use period.

Costs and Prices

Sources for all cost data are provided in Appendix 1.

COMMON STRATEGIC TRADE-OFFS

There are several strategic considerations when comparing self-managed and managed security services delivery models. Addressing all of these are beyond the scope of this paper. But, the strategic trade-offs that we most commonly hear about are:

- Cost allocation
- Strategic and tactical control
- Retention of in-house skills and expertise
- Risk management.

Cost Allocation

This trade-off is allocation of costs to either CapEx or OpEx. Most capital expenditures shift to operating expenses when the delivery model shifts from self-managed to managed security services like managed SIEM. This shift allows different accounting treatment of related expenses. For many companies, this shift is preferred, but depends on business, accounting and budgeting decisions made by individual organizations. The variety of accounting treatment policies is beyond scope of this paper.

Strategic and Tactical Control

Some organizations are concerned with turning information security over to a service provider because of fear they might lose control of their systems and capacity to respond to security issues. Based on general assumptions about the MSSP model, this may be a reasonable conclusion. An MSSP would have access to SIEM data and, depending on process design, could be the gatekeeper to alerts, analysis and response. But, with properly defined managed SIEM services and processes, organizations can retain the level of control of their systems to meet their security and business needs. In many situations, managed SIEM services can give the customer more control and better outcomes.

Customers control can improve along two factors – better visibility into systems and more intelligent control. These derive from several characteristics of the service provider model. First, managed SIEM services are based on proven best practices and delivered by security industry experts who continuously improve their tactics with the latest security insights. Many companies can’t bring this caliber of security intelligence in-house due to available resources and budget. Second, managed services are delivered 24/7/365. The cost of staff to deliver this service is cost prohibitive for many companies. With a managed security services provider, organizations can be confident that someone is always available to receive, analyze and respond to a security alert. In other words, when you don’t have someone to control your response, you have someone in control if necessary. Third, customer-centered services are transparent and collaborative. They provide organizations team with real-time access to all their SIEM data -- SIEM information is always available. Finally, customers can use a managed SIEM service that has a flexible approach to its services allowing customers to select the services it wants to retain. This co-managed model lets customers retain specific functions and expertise in-house.

Retention of in-house skills and expertise

Part of the control issue lies with retention of in-house skills. Every IT organization wants to maintain its capacity to define and deliver the services it provides. As technology and threats evolve, these skills and expertise help the organize adapt. But, does an IT organization need to maintain a staff that can deliver all of the services? Can they afford it? Based on IT strategy, environment, and risk profile, organizations will need to decide if the cost to retain certain IT capabilities is justified. Some of the key considerations in this decision include:

- Overhead requirements: Is there budget and headcount to hire and employ an in-house SIEM staff?
- Turnover and operational capacity: Recent surveys[1] indicate security staff members leave for a new position (in-house or external) approximately every two years*. On average it takes over three months to fill these positions with another four to six weeks to onboard these new employees. Organizations must decide if they can accept periods when their SIEM is under-staffed and unable to deliver on key security and business objectives.

Risk Management - 24/7 Monitoring?

The trade-off here is budget versus risk. Organizations will have to make a strategic, risk management decision about the acceptable service levels for monitoring and breach. Under the self-managed model, 24/7 security operations become expensive due to headcount requirements. (See Large Enterprise Scenario for details.) However, self-managed organizations can benefit from the flexibility to adjust staffing and service levels (i.e., coverage nights, weekends, holidays, etc.) to balance risk management, service levels and budget. But, lower staffing levels come at a cost, the increased risk from slower responses to alerts and breaches. Lower service levels must align with the company's risk management policies.

SCENARIO ANALYSIS

Below are three customer scenarios that compare the costs of self-managed and managed SIEM deployment models including:

- Large enterprise
- Medium enterprise
- Small enterprise.

These scenarios and related use cases are described in detail in the following sections.

Large Enterprise

The large enterprise scenario is representative of a large organization with at least 10,000 employees. The key characteristics for this analysis are the number of IT devices which are used for system sizing and service pricing. Workstation count is related to employee size but is not meant to equal it. Some organizations have more employees than workstations due to the industry and type of work.

Platform sizing – number and type of devices

- 10,000 workstations
- 30 policy devices (IDS, Firewall, etc.)
- 60 network devices
- 125 servers
- 15,000 events per second (~1 billion events per day)

[1] Sources: Ponemon Institute, "Understaffed and at Risk:Today's IT Security Department", February 2014.

Primary security use cases

- Securing the network
- Meeting compliance requirements
- Threat and risk analysis
- Breach containment and global incident response

Self-Managed solution description

- SIEM platform: Trustwave SIEM Enterprise (SIEM-E)
- Software and hardware support and maintenance: 3 years

Trustwave Managed SIEM solution description

- Subscription term: 3 years
- Platform management services (system administration)
  - Trustwave Managed Appliance service
  - Trustwave Health Check service (quarterly system performance analysis and updates)
- Compliance services: Trustwave Managed Compliance Monitoring services for workstations
- Threat analysis services: Trustwave Managed Threat Analysis Monitoring services for IDS, firewalls and servers
  - The Managed Threat Analysis Monitoring service also provides compliance reporting for these devices.

Training and implementation – 10-day training and implementation course

- Trustwave provides an on-site training and implementation course. The duration is based on the scope and complexity of the deployment.

Incident readiness and response

- Trustwave offers extensive readiness and response services which can be tailored to an incident response program based on a customer's goals, industry, and internal environment. This security service is not incorporated into this cost analysis.

Note that the staffing structure for the large enterprise scenario is different from the other scenarios. Two assumptions produce this difference:

1. A large enterprise would need service levels for monitoring, response times and remediation services of a 24/7 security operations center (SOC) to adhere to risk management policies. Staffing shortages have been identified as contributing factors at certain well-publicized breaches at large enterprises . 24/7 staffing requires at least 4.5 security analysts.
2. Since hiring half of a security analyst may be inefficient, this scenario assumes the organization would hire a fifth analyst. The remainder of the analyst's time would be allocated across other SIEM operations, specifically system administration and event remediation. Therefore, these costs are zero in this scenario.

These assumptions are applied in the cost table on the next page.

2. Source: RedLambda.com, "Is IT Security Being Impacted by Attrition?", November 2014.
http://www.redlambda.com/blog/is-it-security-being-impacted-by-attrition

LARGE ENTERPRISE

CapEx (One-Time Costs)		
	Self-Managed SIEM	**Managed SIEM**
SIEM appliance	$245,000	
End-user training • 10-day training + implementation	$24,000	$24,000
Deployment cost included in above		
Managed SIEM implementation fee • Set up data upstreaming to SOC • $1,000 if <3 years		$ 0
Total CapEx Year 1	**$269,00**	**$24,000**
OpEx (Ongoing Costs)	**Self-Managed SIEM**	**Managed SIEM**
Managed SIEM service		$64,000
System administration	$0*	
System administration service • Trustwave Health Check service		$10,900
Maintenance and support (hardware and software)	$8,320	
Compliance + Monitoring Analysts	$578,819	
SIEM Threat + Correlation Specialist	$130,340	
Managed compliance + threat analysis services		$428,930
Internal staff remediation of escalated events**	$0	$69,458
Recruiting	$89,232	
Annual training and certification	$21,000	
Total Annual OpEx	**$842,582**	**$573,288**
TOTAL COSTS YEAR 1	**$1,111,582**	**$597,288**

* Zero cost due to assumption that sysadmin tasks to be performed by reallocation off fifth security analyst time.

** For Self-Managed: zero cost due to assumption of allocation of excess time of fifth security analyst.
For Managed SIEM: This calculation is the hourly salary of an experienced IT employee times the hours spent on remediation. This would be in collaboration with Trustwave Managed Security Services experts, analysts and SOC teams. Time spent is based on an average of 6 events per week, with an average of 4 hours per event.

Costs over 3-Year Subscription Term*

	Year 1	Year 2	Year 3	Total Costs
Self-Managed SIEM	$1,114,120	$845,120	$845,120	**$2,804,359**
Managed SIEM	$597,288	$573,288	$573,288	**$1,743,865**

* Assumes no inflation of salaries or other costs which are standard within most organizations.

MEDIUM ENTERPRISE

The medium enterprise scenario is representative of a typical medium-sized enterprise with 1,000 or more employees. The key characteristics used for this analysis are the number of IT devices which are used for system sizing and service pricing. Workstation count is related to employee size but is not meant to equal it. Some organizations have more employees than workstations due to the industry and type of work.

Platform sizing – number and type of devices

- 1,000 workstations
- 18 policy devices (IDS, Firewall, etc.)
- 25 servers
- 1,500 – 3,000 events per second (130 – 260 million events per day)

Primary security use cases

- Securing the network
- Meeting compliance requirements
- Threat and risk analysis

Self-Managed solution description

- SIEM platform: Trustwave SIEM Enterprise (SIEM-E)
- Software and hardware support and maintenance: 3 years

Trustwave Managed SIEM solution description

- Subscription term:3 years
- Platform management services (system administration)
  - Trustwave Managed Appliance service
  - Trustwave Health Check service (quarterly system performance analysis and updates)
- Compliance services: Trustwave Managed Compliance Monitoringservice for workstations
- Threat analysis services: Trustwave Managed Threat Analysis Monitoring service for IDS, firewalls and servers
  - The Managed Threat Analysis Monitoring service also provides compliance reporting for these devices.

Training and Implementation – 5-day training and Implementation course

- Trustwave provides an on-site training and implementation course. The duration is based on the scope and complexity of the deployment.

MEDIUM ENTERPRISE

CapEx	Self-Managed SIEM	Managed SIEM
SIEM appliance	$86,500	
End-user training • 5-day training + implementation	$13,900	$13,900
Deployment cost included in above		
Managed SIEM implementation fee • Set up data upstreaming to SOC • $1,000 if < 3 years		$ 0
Total CapEx Year 1	**$100,400**	**$13,900**
OpEx	**Self-Managed SIEM**	**Managed SIEM**
Managed SIEM service		$38,000
System administration	$14,870	
System administration service • Trustwave Health Check service		$10,900
Maintenance and support (hardware and software)	$8,320	
Compliance + Monitoring Analyst • “near” 24/7 SOC support*	$347,292	
SIEM Threat + Correlation Specialist	$130,340	
Managed compliance + threat analysis services		$102,920
Internal staff remediation of escalated events**	$ 0	$34,729
Recruiting	$71,824	
Annual training and certification	$14,000	
Total Annual OpEx	**$581,689**	**$185,144**
TOTAL COSTS YEAR 1	**$682,089**	**$199,044**

* Assumption is that a medium-sized enterprise would accept a “partial” security operations center (SOC) of 3 full-time employees (FTEs) to provide coverage for an adequate level of service to meet risk management objectives. “Partial SOC” means that there will be time periods when the SOC is unstaffed. For example, on a weekly basis, the SOC will technically “unstaffed” for 48 hours based on 8-hour work shifts (i.e., ~7 hours per day). Using an average of 48 weeks worked per year per FTE, the SOC will be at 66% coverage for nearly one-third of the year.

** For Self-Managed: This position is a full-time SIEM security specialist. Based on the workload, this person will spend roughly 50-70% of his time on analysis and correlations and 20-30% of his time on incident response and remediation.
For Managed SIEM: This calculation is the hourly salary of an experienced IT employee times the hours spent on remediation. This would be in collaboration with Trustwave Managed Security Services experts, analysts and SOC teams. Time spent is based on an average of 3 events per week, with an average of 4 hours per event.

Costs over 3-Year Subscription Term*

	Year 1	Year 2	Year 3	Total Costs
Self-Managed SIEM	$682,089	$581,689	$581,689	**$1,845,468**
Managed SIEM	$199,044	$185,144	$185,144	**$569,332**

* Assumes no inflation of salaries or other costs which are standard within most organizations.

SMALL ENTERPRISE

The small enterprise scenario is representative of a typical small business with 250 to 500 employees. The key characteristics are the number of IT devices which are used for services pricing. Workstation count is related to employee size but is not meant to equal it. Some organizations have more employees than workstations due to the industry and type of work.

Platform sizing – number and types of devices

- 250 workstations
- 6 policy devices (IDS, Firewalle, etc.)
- 8 Servers
- 1,000 events per second (~86 million events per day)

Primary security use cases

- Log collection and management
- Compliance reporting
- Threat analysis on IDS

Self-Managed solution description

- SIEM platform: Trustwave Log Management Enterprise (LME)
- Software and hardware support and maintenance: 3 years

Trustwave Managed SIEM description

- Subscription term: 3 years
- Platform management services (system administration)
  - Trustwave Managed Appliance service
  - Trustwave Health Check service (quarterly system performance analysis and updates)
- Compliance services: Trustwave Managed Compliance Monitoring service for workstations
- Threat analysis services: Trustwave Managed Threat Analysis Monitoring service for IDS, Firewalls and Servers
  - The Managed Threat Monitoring service also provides compliance reporting for these devices.

Training and implementation – 3-day Trustwave on-site training and implementation course

- The duration is based on the scope of the deployment and complexity of the product.
- The period of training includes both in-class instruction and implementation of the SIEM system purchased. Instruction cost is per class, not per student.

Incident readiness and response

- Trustwave offers extensive readiness and response services which can be tailored to an incident response program based on a customer’s goals, industry, and internal environment. This security service is not incorporated into this cost analysis.

SMALL ENTERPRISE

CapEx		
	Self-Managed SIEM	Managed SIEM
SIEM appliance	$18,500	
End-user training • 3-day training + implementation	$7,500	$7,500
Deployment cost included in above		
Managed SIEM implementation fee • Set up data upstreaming to SOC • $1,000 if < 3 year subscription		$0
Total CapEx Year 1	**$26,000**	**$7,500**
OpEx	**Self-Managed SIEM**	**Managed SIEM**
Managed SIEM service		$12,456
System administration	$9,914	
System administration service • Trustwave Health Check service		$10,900
Maintenance and support (hardware and software)	$2,960	
Compliance + Monitoring Analyst	$115,764	
Managed compliance + threat analysis services		$33,873
Recruiting • 20% of salary of recruited FTEs	$23,153	
Annual training and certification	$3,500	
Internal staff remediation of escalated events*	$ 0	$11,596
Total Annual OpEx	**$166,886**	**$68,825**
TOTAL COSTS YEAR 1	**$192,886**	**$76,325**

* Assumption for escalated events is 1 event per week with an average of 4 hours spent per event.

For Self-Managed: The assumption is that due to resource contraints, small enterprise will use existing staff to respond to events; therefore, this cost is captured in above line items and entered as zero cost here.

For Managed SIEM: This calculation is the hourly salary of an experienced IT employee times the hours spent on remediation. It represents the opportunity cost to reallocate employee from their full-time commitment. This would be in collaboration with Trustwave Managed Security Services experts, analysts and SOC teams. Time spent is based on an average of 3 events per week, with an average of 4 hours per event.

Costs over 3-Year Subscription Term*

	Year 1	Year 2	Year 3	Total Costs
Self-Managed SIEM	$192,886	$166,886	$166,886	**$526,659**
Managed SIEM	$76,325	$68,825	$68,825	**$213,974**

* Assumes no inflation of salaries or other costs which are standard within most organizations.

MANAGED SECURITY SERVICES: NOT ALL OR NOTHING

While these scenarios present an either-or comparison, Trustwave doesn't believe the choice between self-managed or managed SIEM is binary. Every organization differs in their organizational resources, IT environment, and security strategy. When considering a SIEM solution, organizations should determine if and how the services can be customized for their IT strategy, organization and environment. Trustwave has designed its managed security services and delivery models to let customers choose the set of services that fit their needs. This approach provides for a hybrid model for managed SIEM services (co-managed). For example, a customer may want only compliance reporting services for its workstations and to perform all other threat analysis themselves. This approach allows customers to select components of the SIEM service almost à la carte.

SUMMARY

Based on this analysis, the managed SIEM option is the lower cost option in all three scenarios. However, an organization's choice should not be based on costs alone. They should also assess the strategic trade-offs between the self-managed and managed security services options. Reviewing the trade-offs listed in this paper, the managed SIEM option addresses key concerns for:

- **Cost allocation:** most companies have adopted tax strategies that values operating expenses over capital expenses, which favors the managed SIEM model.
- **Control:** organizations should select an experienced service provider with clearly defined roles and processes using a solution that makes SIEM operations transparent. By addressing these issues, a managed service provider will not obstruct your control.
- **Retention of expertise in-house:** by choosing a vendor with flexible services model, companies can customize their services portfolio retaining budget for in-house staff with expertise deemed strategically important.

These strategic and cost considerations provide the fundamental framework for choosing a delivery model. As companies start looking at vendor technologies (or evaluating a refresh of an existing SIEM), companies should focus on vendors who not only have experience with the delivery models discussed here, but also who offer the flexibility to customize services to meet their unique needs and provide migration from basic SIEM services to more advanced capabilities.

APPENDICES

Appendix 1: Scenario calculations and data sources

The table presents the formulas and data sources used for calculation of the costs for small enterprise scenario.

All prices of Trustwave products are our standard U.S. list prices at the time of orginal publication of this document. Prices are subject to change. Due to the pricing model for Trustwave products and services, prices quoted to customers will vary due to differences in types of services and number of devices being monitored.

CapEx		
	Self-Managed SIEM	**Managed SIEM**
SIEM appliance & data storage	Product price	
End-user training • 5-day training + Implementation	Standard service pricing	Standard service pricing
Deployment cost included in above		
Managed SIEM implementation fee • Set up data upstreaming to SOC • $1,000 if subscription one year or less		No implementation fee if customer subscribes for more than one year.
Total CapEx Year 1		

OpEx		
	Self-Managed SIEM	**Managed SIEM**
Managed SIEM service		Standard service pricing
System administration	10% of standard system administration using a fully-loaded salary of $99,136 and a burden rate of 33%. Base salary information from ComputerWorld 2015 IT Salary Survey. Large enterprise system administration has $0 cost because requirements covered by part of fifth information security analyst accounted for in “Compliance and Monitoring Analyst” costs.	
System administration service • Trustwave Health Check service		Standard service pricing
Maintenance and support (hardware and software)	Subscription price	

Compliance + Monitoring Analyst	Fully-loaded salary of $115,764 for an Information Security Analyst. Base salary information from ComputerWorld 2015 IT Salary Survey. FTE Staffing: • Small enterprise: 1 FTE • Medium enterprise: 3 FTEs • Large enterprise: 5 FTEs	
Security + Threat Correlation Analyst	Security Threat Correlation Specialist using a fully-loaded salary of $130,340 and applied burden rate of 33%. Assumes 10% premium over basic monitoring analyst. Base salary information from ComputerWorld 2015 IT Salary Survey.	
Managed Compliance + Security Service • Compliance + Monitoring • Threat Correlation		Standard service pricing
Internal staff remediation of escalated events	Requirements covered by monitoring and threat correlation analysts	Cost of time for IT specialist(s) to coordinate with Trustwave security services and perform on-site remediation. Time based on average number of events per week for the year times average time to remediate each event (4 hours). Scenario events: • Small enterprise: 1 event per week • Medium enterprise: 3 events per week • Large enterprise: 6 events per week Remediation with managed SIEM is assumed to be handled by existing staff. While it is not a new direct salary cost, it is still an opportunity cost to IT drawing resources from other IT projects and functions.

Recruiting	Recruiting costs are conservatively calculated at 20% of the first year's salary. There are varying reports on the costs to hire a new employee ranging from 10% to 100% of the employee's first year salary.	
Annual training and certification	This uses a cost of $3500 per employee per year to attend training and maintain appropriate certifications. This is only the direct cost of these activities (e.g., course costs, travel, certifications) and does not include the opportunity cost of the employee's time.	
Total Annual OpEx		
TOTAL COSTS YEAR 1		

Trustwave®

Smart security on demand