A Forrester Total Economic Impact™ Study Commissioned By Palo Alto Networks
October 2017

The Total Economic Impact™ Of Palo Alto Networks Traps

Cost Savings And Business Benefits Enabled By Traps Advanced Endpoint Protection

FORRESTER®

Table Of Contents

Project Director:
Bob Cormier
Vice President and Principal Consultant
Forrester Consulting

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®

Quantified Benefits

Opex labor savings:
$559,542

Opex headcount savings:
Two FTEs

Breach avoidance, cost savings: $1,691,059

(above are risk- and PV-adjusted)

Executive Summary

Palo Alto Networks Traps solution replaces legacy antivirus (AV) and secures endpoints with a multi-method prevention approach that blocks malware and exploits, both known and unknown, before they compromise endpoints, such as laptops, desktops, and servers. Palo Alto Networks commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and objectively examine the potential return on investment (ROI) enterprises may realize by deploying its Traps solution. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Traps on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four Palo Alto Networks Traps customers with a range of 11 to 36 months of experience using the Traps solution.

For this TEI study, Forrester created a composite *Organization* to illustrate the quantifiable benefits and costs of investing in Palo Alto Networks Traps. The composite *Organization* is a large global enterprise that has major operations in North America, Europe, and Asia Pacific with minor multisite operations globally. It has been using Palo Alto Networks Traps for three years to block malware and exploits, and currently has 25,000 endpoints protected by Traps. For more information, see the section titled Composite *Organization*.

Key Findings

Quantified benefits. The composite *Organization* experienced the following risk-adjusted present value (PV) quantified benefits totaling **$2,250,601** (see the Financial Analysis section for more details):

- **Breach avoidance, cost savings ($1,691,059).** Traps prevents security breaches by preemptively blocking known and unknown malware, exploits, and zero-day threats. Avoiding breaches results in less time and effort having to manage or mitigate breaches, thereby avoiding the cost of activating the Organization's incident response team.
- **Opex savings from Traps ($559,542).** The *Organization* has seen a dramatic reduction in malware incidents and false positives. Less staff resource time is spent trying to identify and isolate the malware to analyze the full scope of what occurred.

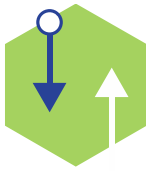
Unquantified benefits. The composite *Organization* experienced the following benefits, which are not quantified in this study:

- **System performance benefits.** One interviewed customer indicated that users aren't complaining as often about their systems being unusable due to performance issues caused by AV updating periods. Once Traps replaced AV software, system performance improved.
- **Palo Alto Networks WildFire.** Wildfire, included in the Traps subscription, is a cloud-based threat analysis service and prevention engine for highly evasive zero-day exploits and malware. The service employs a unique multi-technique approach, combining dynamic and static analysis, innovative machine learning techniques, and a bare metal analysis environment to detect and prevent the most evasive threats.

ROI
82%

Benefits PV
$2.3 million

NPV
$1.0 million



Payback
16 months

- **Panorama**. Traps sends security events from Endpoint Security Manager (ESM) to Panorama. Palo Alto Networks customers can analyze and correlate threat patterns using both network events and Traps security events to gain a unified picture of security events across the environment.

Costs. The *Organization* experienced the following present value costs totaling **$1,233,398**:

- **Labor to deploy and maintain Palo Alto Networks Traps solution ($43,003).** This includes labor that's necessary to perform technical development, pre-planning, implementation, support, and maintenance for the Palo Alto Networks Traps solution.
- **Palo Alto Networks Traps solution fees ($1,190,395).** This includes subscription licenses for 25,000 registered endpoint devices and Palo Alto Networks Premium Support; training and professional services are also included.

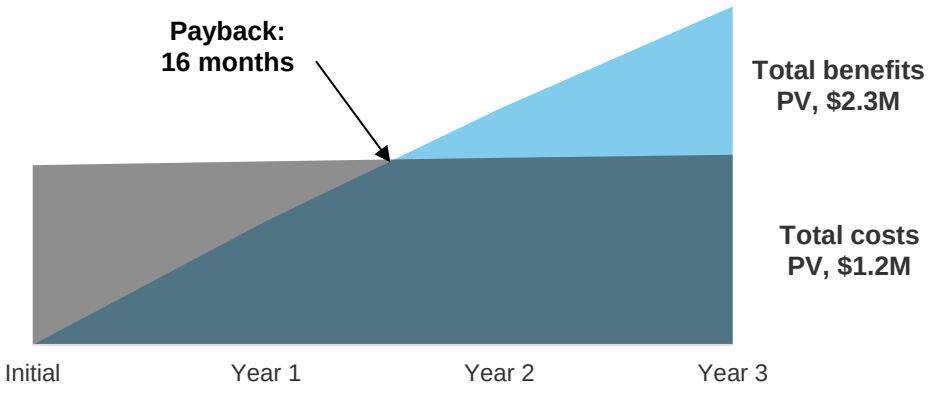
Forrester's interviews and subsequent financial analysis found that the *Organization* experienced benefits of $2,250,601 over three years versus costs of $1,233,398, adding up to a net present value (NPV) of $1,017,203, with a payback period of sixteen months and an ROI of 82%.

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

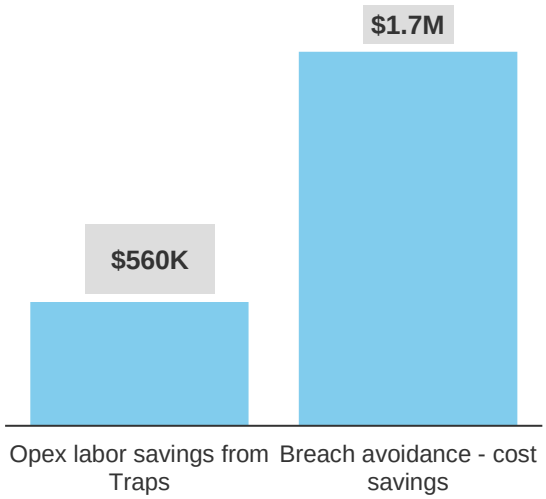
A note from Forrester:

Cybercriminals are using more sophisticated and targeted attacks to steal everything from valuable intellectual property to the sensitive personal information of your customers, partners, and employees. Their motivations run the gamut from financial to retaliatory, and your customers expect you to do everything in your power to not only protect their information, but to respond quickly and appropriately. A poorly contained breach and botched response have the potential to cost millions in lost business and opportunity, and ruin your organization's reputation.

Financial Summary



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 investing in the Palo Alto Networks Traps solution.

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 the Palo Alto Networks Traps solution 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 Palo Alto Networks stakeholders to gather data relative to the Traps solution.

CUSTOMER INTERVIEWS
Interviewed four customers using the Traps solution 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 composite *Organization*.

CASE STUDY
Employed four fundamental elements of TEI in modeling the Palo Alto Networks Traps solution's impact: benefits, costs, flexibility, and risks. Given the increasing sophistication that enterprises have regarding ROI analyses related to IT investments, Forrester's TEI methodology serves to provide a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

The Traps Customer Journey

BEFORE AND AFTER THE TRAPS INVESTMENT

For this study, Forrester conducted four interviews with Palo Alto Networks Traps customers. Interviewed customers are described as follows (each requesting anonymity):

INDUSTRY	INTERVIEWEE	MONTHS USING TRAPS	NUMBER OF ENDPOINTS
Healthcare	Senior security engineer	36	40,000
Retail	Manager, information security	11	10,000
Healthcare	Principal security analyst	13	32,000
Law firm	Chief security officer	12	2,200

Composite Organization

For this TEI study, Forrester created a composite *Organization* to illustrate the quantifiable benefits and costs of investing in Palo Alto Networks Traps. The composite *Organization* is a large global enterprise that has major operations in North America, Europe, and Asia Pacific, with minor multisite operations globally. It has been using Palo Alto Networks Traps for three years and currently has 25,000 endpoints protected by Traps.

Prior to its investment in Traps the *Organization* was using a legacy AV product. The AV product was replaced by Traps which includes malware and malicious executable functionality, exploit prevention capabilities, and protection against advanced attacks including fileless attacks and script-based attacks. In addition, it added incremental features and functionality, including: application whitelisting and restricted folders (which allowed the *Organization* to add a level of control to its endpoints that it didn't previously have), the ability to specifically state what is allowed to run on these systems, and the ability to block people from being able to execute files from their own user profiles.

> "After using Traps successfully for a week, it was concerning to not have the same level of prevention capability across our other environments. So, we accelerated our Traps implementation schedule to ensure the best level of prevention."
>
> *Principal security analyst, healthcare organization*

Key Challenges And High-Level Requirements

Endpoint security represents the *Organization's* last line of defense in its fight against cybercriminals. Breaches had become more frequent among employee endpoints and servers. The *Organization* recognizes that the effects from security breaches can be devastating, causing companies to lose revenue, market reputation, and market competitiveness. Unfortunately, in the past inadequate endpoint security left the doors open to a variety of attack techniques and tools, including malware, software exploits, and social engineering. The *Organization* feels that it's critical to have the right endpoint protection in place.

The *Organization* had the following challenges and high-level requirements, which were shared by the interviewed customers:

Challenges:

- **Inadequate detection techniques**. The legacy AV tools were inadequate in threat prevention and detection.
- **Inaccurate reporting protocols**. The previous AV tool was not accurately and clearly logging incidents.
- **Ransomware**. To avoid ransomware threats.
- **Prevention**. To prevent highly evasive zero-day exploits and malware.

High-level requirements:

- **Prevent malware and exploits from executing.** The solution should create an environment where malware isn't able to load into memory or an exploit is unable to take advantage of a running process.
- **Detect malicious activity post-execution.** The chosen endpoint security suite should monitor running memory to identify malware and exploited applications before they achieve their malicious goals.
- **Remediate and contain malicious activity and potential vulnerabilities.** Once the endpoint security solution identifies malicious endpoint activity or a potential vulnerability, it should be able to launch automated remediation without any significant involvement of an administrator.

Key Results

The customer interviews confirmed and revealed several key results attributed to the Palo Alto Networks Traps solution investment as follows:

- **Blocks malware and exploits.** Traps multi-method prevention blocks malware and exploits, known and unknown, before they compromise endpoints such as laptops, desktops, servers, and tablets.
- **High level of prevention.** Traps prevents over 90% of malware, compared to only 40% to 50% for traditional AV capabilities without having to add additional products.
- **A decrease in false positives**. As compared to the previous environment.
- **Local analysis.** Increased effectiveness of local analysis as machine learning model is trained.
- **Fewer reimaging.** Less infection incidents causing fewer reimage requests.
- **Staff efficiency**. Reduction in the number of hours of analyst/incident response staff.
- **WildFire**. An analysis and prevention engine for evasive zero-day exploits and malware that's included with Trap's.

> "Our Palo Alto Network sales rep is excellent. If he happens to be in the neighborhood, he'll swing by and come talk to us. He's not trying to sell us anything; he just wants to make sure that the environment is working the way we want it to, and lets us know about things that are going on within Palo Alto Networks. I really have not experienced that with any other vendor we deal with."
>
> *Manager, information security, retailer*

- Here's an example of positive results from a current customer using Traps with Wildfire. "Traps notified us that a suspicious executable had been blocked on one of our endpoints. In the meantime, two users received an email to a distribution list with a Word document and opened it. Traps prevented it from running, and sent it to Wildfire for analysis. I waited for the Wildfire verdict, and according to the analysis, a macro spawned a PowerShell command to download a file called troll1.jpg from an IP address. It detected that jpg file was actually an exe, which would have been renamed and executed, where it would have done some other really nasty damage. At any rate, I attempted to download the file from Wildfire but because I'm an SSL decrypt user, and I have Wildfire AV pattern files in use, I couldn't actually download the executable as my Palo Alto Networks firewall blocked it. The Palo Alto Networks platform approach proved itself here, and I'm about to present the business case for enabling SSL decryption across the entire enterprise, so this real world example will help!".

"From a compliance standpoint Traps allows our organization to be more confidently compliant, especially with HIPAA and the Breach Notification Rule (HITECH Act of 2009)."

Principal security analyst, healthcare organization

FORRESTER®

Financial Analysis

QUANTIFIED BENEFIT AND COST DATA

Total Benefits

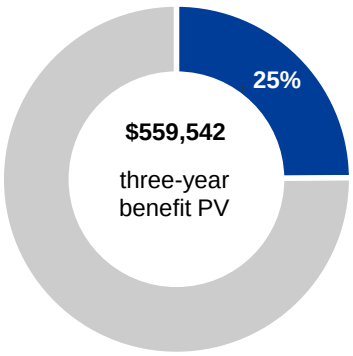
REF.	BENEFIT	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
A1	Opex savings from Traps	$225,000	$225,000	$225,000	$675,000	$559,542
Bt	Breach avoidance, cost savings	$680,000	$680,000	$680,000	$2,040,000	$1,691,059
	Risk adjustment	$905,000	$905,000	$905,000	$2,715,000	$2,250,601

Opex Savings From Traps

The interviewed customers confirmed that Traps advanced endpoint protection replaces AV solutions and secures endpoints against malware and exploit methods to preemptively block known and unknown threats from compromising systems. Less staff resource time is spent trying to identify and isolate the malware to analyze the full scope of what occurred. Labor hours are saved due to the following features and functionality:

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 nearly $2.3 million.

- Traps multi-method prevention blocks malware and exploits, known and unknown, before they compromise endpoints such as laptops, desktops, servers, and tablets.
- Traps prevents over 90% of malware.
- A decrease in false positives as compared to its legacy AV solutions.
- Increased effectiveness of local analysis as machine learning model is trained.
- Significantly less ransomware or infection incidents reducing reimage requests.
- Reduction in the number of hours of analysts' incident response time.
- Ability to build more automation around the logs received from Traps due to high confidence in the information Traps is providing.



Opex savings: 25% of total benefits

Modeling and assumptions. The *Organization* has seen a dramatic reduction in malware incidents and false positives. Less time is spent trying to identify and isolate the malware to analyze the full scope of what occurred. The desktop team has significantly fewer assets needing reimaging and fewer follow-up investigations which take an average of one week with multiple IT staff involved. The *Organization* is saving two FTEs; one IT security staff and one IT desktop staff.

FORRESTER®

Risks. Forrester considered the following potential when assigning a risk adjustment:

- Other organizations may experience slower rollout and adoption of the benefits of Traps.
- Some organizations may be slow in reassigning redundant staff to other value-added positions.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $559,542.

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.

Opex Savings From Traps: Calculation Table

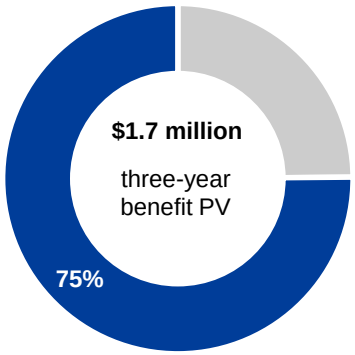
REF.	METRIC	CALC./SOURCE	YEAR 1	YEAR 2	YEAR 3
A1	IT security staff savings (FTE)	Interviews	1	1	1
A2	IT desktop staff savings (FTE)	Interviews	1	1	1
A3	Industry average fully loaded cost	Per FTE	$125,000	125,000	125,000
At	Opex labor savings from Traps	(A1+A2)*A3	$250,000	$250,000	$250,000
	Risk adjustment	↓10%			
Atr	Opex savings from Traps (risk-adjusted)	At-10%	$225,000	$225,000	$225,000

Breach Avoidance, Cost Savings

As with business continuity (BC) or IT disaster recovery (DR) plans, organizations need to have a comprehensive incident response plan for breaches. You don't want to develop your incident response plan in real time while cybercriminals are pilfering intellectual property. A well-defined incident management program provides a script to follow when incidents occur.

Here are the cross-functional roles, both internal and external that should be included in the *Organization's* incident response team, and where incident activation costs can be avoided.

- Information security staff. These individuals are responsible for handling the detailed investigation of the incident, and possessing the capabilities for advanced forensics. Many organizations also hire external consultants to assist with incident response and forensics.
- IT staff. System and network administrators will help with incident investigations because of their advanced knowledge of the applications and systems they support.
- Legal representatives. It's essential to engage legal staff during the incident response in order to provide guidance on the legality of potential searches and the requirements of evidence collection, as they will likely have to defend the incident response plan.



Breach avoidance, cost savings: 75% of total benefits

FORRESTER®

- Lines of business representatives**.** The information security team will need to partner with the business unit data owners to understand the data and its implications.
- A data champion or chief data officer (CDO). An individual who is responsible for the organization's use of data for business purposes is required, and thus they have an incentive to ensure that the data is protected and used appropriately.
- Corporate communications representatives. These are the individuals who will speak for the company and provide the message that the company wants to deliver to its customers, investors, and business partners. Poor communication can increase customer frustration and irreparably damage an organization's reputation.
- External investigators. An external investigator with the necessary skills to properly respond to an incident has the ability to leverage a company's incident response team out of a difficult situation when it is overwhelmed.

The *Organization* recognizes that the effects from security breaches can be devastating, causing the company to lose revenue, market reputation, and market competitiveness.

The customers Forrester interviewed all agree that Traps prevents security breaches by preemptively blocking known and unknown malware, exploits, and zero-day threats. With breach avoidance there's less time and effort involved in managing and mitigating breaches, thereby reducing the cost of activating the *Organization's* entire incident response team.

Modeling and Assumptions. Forrester's research supported an assumption that the *Organization* would incur a significant breach every year, and that most of the internal and external job roles listed above would have been activated to manage, mitigate, and control the breach. Interviewed customers estimated the cost of managing, mitigating, and controlling a breach to range between $600,000 to $1,000,000.

This amount does not take into account an inadequate or unsuccessful incident response (or no response) that leads to financial, operational, and/or reputational losses. Readers should consider and assess the ability of their own organizations to respond to incidents and prevent significant financial and reputational losses.

Interviewed customers reported a wide range of cost avoidance benefits using Traps, and Forrester will use an average of $800,000 per year before risks adjustments.

Risks. Forrester considered the following potential risks when assigning a risk adjustment:

- Since this is an estimate, it has been risk-adjusted.
- Readers of this study may have different savings outcomes.

To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year risk-adjusted total PV of $1,691,059.

> "We've seen dozens of executables prevented due to known Wildfire malware verdict; and local static analysis stopped confirmed ransomware which evaded our traditional AV solution"
>
> *Principal security analyst, healthcare organization*

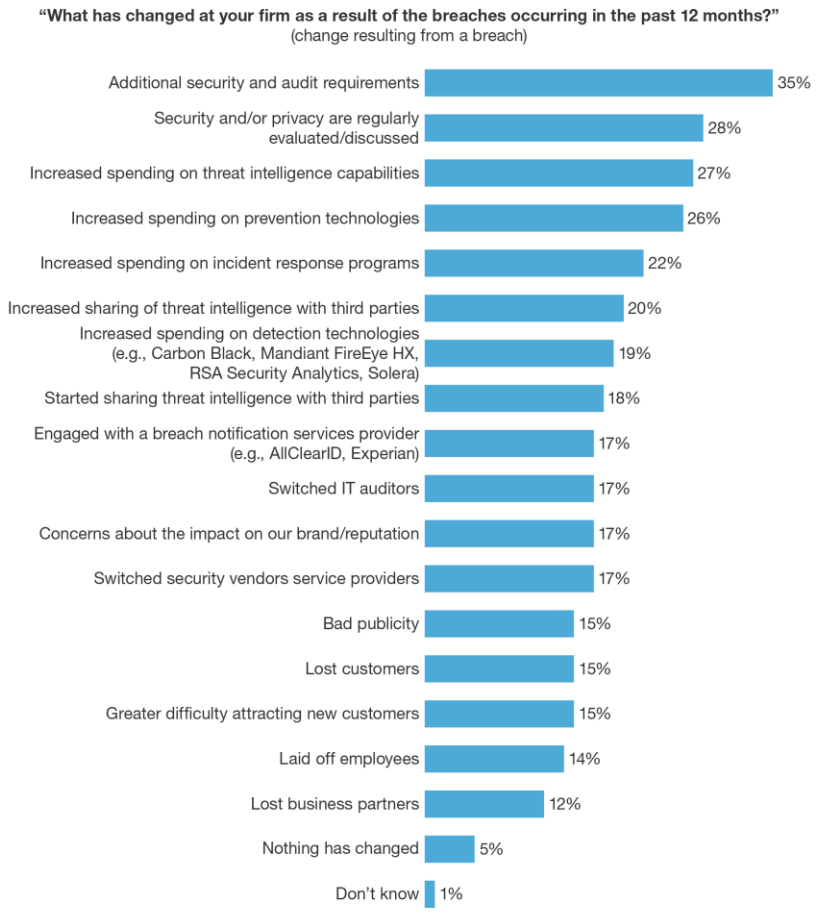
Breach Avoidance, Cost Savings: Calculation Table					
REF.	METRIC	CALC./SOURCE	YEAR 1	YEAR 2	YEAR 3
B1	Breach avoidance, cost savings	Interviews	800,000	800,000	800,000
Bt	Breach avoidance, cost savings	B1	$800,000	$800,000	$800,000
	Risk adjustment	↓15%			
Btr	Breach avoidance, cost savings (risk-adjusted)	Bt-15%	$680,000	$680,000	$680,000

The Forrester survey below asks the following question of companies that have experienced a breach in the past 12 months: “What has changed at your firm as a result of the breaches occurring in the past 12 months?”. Note that most if not all of the responses involve some increased spending on technology or increased time and effort (labor expense) as a result of a breach.

FORRESTER RESEARCH | SECURITY & RISK PROFESSIONALS

Strategic Change Resulting From Breach

Planning For Failure: How To Survive A Breach



Base: 332 global decision-makers responsible for network security at companies that have had a breach in the past 12 months (1,000+ employees) (multiple responses accepted)

Source: Forrester's Global Business Technographics® Security Survey, 2016

Unquantified Benefits

The interviewed customers experienced the following benefits, features, or functionality, which were not quantified for this study:

- **System performance benefits.** One interviewed customer indicated that users aren't complaining as often about their systems being unusable due to performance issues caused by AV updating periods. Once Traps replaced AV software, system performance improved.
- **Palo Alto Networks WildFire.** Wildfire, included in the Traps subscription, is a cloud-based threat analysis service and prevention engine for highly evasive zero-day exploits and malware. The service employs a unique multi-technique approach, combining dynamic and static analysis, innovative machine learning techniques, and a bare metal analysis environment to detect and prevent the most evasive threats.

FORRESTER®

- **Panorama.** Traps sends all security events from Endpoint Security Manager (ESM) to Panorama. Palo Alto Networks customers can analyze and correlate threat patterns using both network events and Traps security events to gain a unified picture of security events across the environment.

Flexibility

The value of flexibility is clearly 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 Palo Alto Network's Traps and later realize additional uses and business opportunities. There are two future flexibility options that the *Organization* is considering:

- **Securing different environments.** One interviewed customer stated that Traps gave them very stringent endpoint protection that it didn't previously have. This gave them a higher level of confidence in the future to move into remote businesses models where they don't fully have control of the environment; where employees, contractors, and partners would be working in a multitude of different spaces and environments.
- **Faster approval processes.** Another customer discussed how Traps and Wildfire will soon contribute to the faster flow of approvals for new software applications being introduced to the environment. Wildfire provides a return verdict quickly on newly introduced software which accelerates the approval process.

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

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

Total Costs

REF.	COST	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Ctr	Labor to deploy and maintain Palo Alto Traps	$5,760	$14,976	$14,976	$14,976	$50,688	$43,003
Dtr	Palo Alto Networks Traps fees	$1,190,395	$0	$0	$0	$1,190,395	$1,190,395
	Total costs (risk-adjusted)	$1,196,155	$14,976	$14,976	$14,976	$1,241,083	$1,233,398

Labor Costs To Deploy And Maintain Palo Alto Networks Traps

- **Pre-deployment costs and labor.** This cost includes 80 hours of labor to perform technical development, preplanning, proof of concept (POC), Traps training, implementation, and supporting and maintaining the Palo Alto Networks Traps solution:
- **Ongoing maintenance costs and labor.** The *Organization's* security staff spends an average of 4 hours per week (208 hours annually) supporting and maintaining the Traps solution and the relationships with Palo Alto Networks and partners.

Modeling and assumptions. Pre-deployment labor includes 80 hours of labor at $60.00 per hour or $4,800 for the initial period. Ongoing maintenance labor includes 208 hours per year or $12,480 annually.

Risks. Forrester risk-adjusted the implementation and ongoing maintenance costs downward by 20% to reflect the variability of experience held by security staff doing the deployment and ongoing maintenance.

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 *Organization* expects risk-adjusted total costs to be a PV of $1,233,398.

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.

Labor Costs To Deploy And Maintain Palo Alto Networks Traps: Calculation Table

REF.	METRIC	CALC./SOURCE	INITIAL	YEAR 1	YEAR 2	YEAR 3
C1	Pre-deployment costs and labor	Hours	80	0	0	0
C2	Ongoing maintenance costs and labor	Hours	0	208	208	208
C3	Labor cost per hour	Industry average	$60	$60	$60	$60
Ct	Labor costs to deploy and maintain Palo Alto Networks Traps	(C1+C2)*C3	$4,800	$12,480	$12,480	$12,480
	Risk adjustment	↑20%				
Ctr	Labor costs to deploy and maintain Palo Alto Network Traps (risk-adjusted)	Ct-20%	$5,760	$14,976	$14,976	$14,976

Palo Alto Networks Traps Fees

The *Organization* has 25,000 registered endpoint devices, with each having an active support license that includes Palo Alto Networks Premium Support (24x7 support with advance replacement four-hour delivery of parts). The *Organization* paid for a three-year license subscription, training and professional services in the initial period. Note: the Wildfire Threat Intelligence Cloud is included in the Traps subscription.

Modeling and assumptions. The fees in the table below are provided by Palo Alto Networks and confirmed by interviewed customers.

Risks. Forrester did not risk-adjust the Palo Alto Networks Traps fees, which were actual list price quotes (not discounted) from Palo Alto Networks.

16 month payback
Time to recover the initial investment in Palo Alto Networks Traps

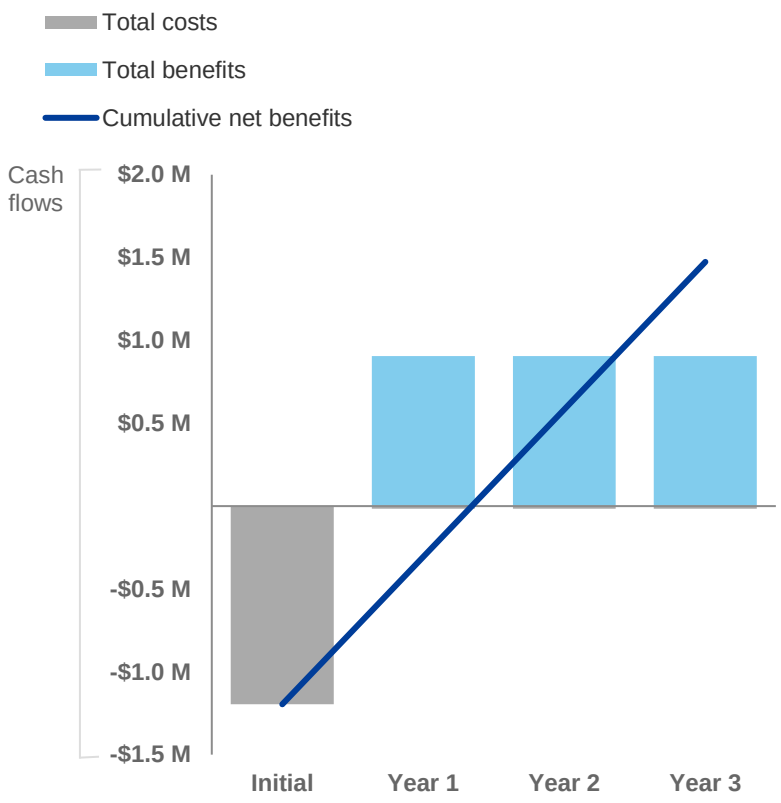
Palo Alto Networks Traps Fees: Calculation Table

REF.	METRIC	CALC./SOURCE	INITIAL	YEAR 1	YEAR 2	YEAR 3
D1	Number of endpoint devices	Composite *Organization*	25,000	25,000	25,000	25,000
D2	Traps license, training and partner professional services costs	Palo Alto Networks	$1,190,395	$0	$0	$0
Dt	Palo Alto Networks Traps fees	D2	$1,190,395	$0	$0	$0
	Risk adjustment	0%				
Dtr	Palo Alto Networks Traps fees (risk-adjusted)		$1,190,395	$0	$0	$0

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	($1,196,155)	($14,976)	($14,976)	($14,976)	($1,241,083)	($1,233,398)
Total benefits	$0	$905,000	$905,000	$905,000	$2,715,000	$2,250,601
Net benefits	($1,196,155)	$890,024	$890,024	$890,024	$1,473,917	$1,017,203
ROI						82%
Payback period						16 months

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

FORRESTER®

Palo Alto Networks Traps: Overview

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

Traps Advanced Endpoint Protection

Traps replaces legacy AV and secures endpoints with a multi-method prevention approach that blocks malware and exploits, both known and unknown, before they compromise endpoints, such as laptops, desktops, and servers.

Prevent Security Breaches With Light-Weight Agent

Preemptively block known and unknown malware, exploits and zero-day threats with the unique multi-method prevention approach of Traps advanced endpoint protection from a single and lightweight agent.

Automate Prevention

Automatically reprogram your endpoints to block known and unknown threats – without human intervention – using threat intelligence gained from our global community of customers and partners across endpoints, networks, and software-as-a-service applications.

Protect And Enable Users

Empower users to use web, mobile, and cloud-based applications without fearing cyberthreats. Protect users from inadvertently compromising their systems without depending on burdensome virus scans.

- **Multi-method malware prevention**. Traps prevents malicious executables rapidly and accurately with a unique, multi-method approach to prevention that maximizes coverage against malware while reducing the attack surface area and increasing the accuracy of malware prevention. This approach combines several prevention methods to instantly block known and unknown malware from infecting a system.

- **Multi-method exploit prevention.** Traps takes a unique approach to preventing exploits. Instead of focusing on the millions of individual attacks or their underlying software vulnerabilities, it focuses on the small set of techniques all exploit-based attacks use, which rarely change. Traps blocks these techniques, thereby preventing exploitation attempts before they can compromise endpoints.

Automatically Prevent Highly Evasive Zero-Day Exploits And Malware

Palo Alto Networks WildFire, included with Trap's is a cloud-based threat analysis service is an advanced analysis and prevention engine for highly evasive zero-day exploits and malware. The service employs a unique multi-technique approach, combining dynamic and static analysis, innovative machine learning techniques, and a groundbreaking bare metal analysis environment to detect and prevent the most evasive threats.

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.