Forrester Consulting

MAKING LEADERS SUCCESSFUL EVERY DAY

Prepared for Trend Micro

June 2011

Total Economic Impact™ Of Trend Micro Enterprise Security

Project Directors: Jon Erickson and Sadaf Roshan Bellord

Headquarters
Forrester Research, Inc., 400 Technology Square, Cambridge, MA 02139 USA
Tel: +1 617.613.6000 • Fax: +1 617.613.5000 • www.forrester.com

TABLE OF CONTENTS

Executive Summary

Trend Micro commissioned Forrester Consulting to examine the total economic impact and potential return on investment (ROI) enterprises may realize by deploying Trend Micro Enterprise Security across their network. Trend Micro Enterprise Security is a line of products focusing on Web, messaging, server, and endpoint content security. These products leverage the Trend Micro Smart Protection Network – a cloud-client infrastructure that uses cloud-based threat and reputation technologies to deliver threat protection without the delays of conventional signature-based security downloads. This study illustrates the financial impact of an organization migrating to Trend Micro Enterprise Security and the benefits received from deploying Web, messaging, server, and endpoint security powered by a unique cloud-computing architecture that stops threats at their source before reaching the network.

In conducting in-depth interviews with seven existing Trend Micro customers, Forrester found these companies saw a reduced impact from malicious code infections across their network. For many of the clients interviewed, faster detection and protection of Web, messaging, server, and endpoint threats resulted in a lower overall number of infections, incidents (widespread infection) as well as reduced severity of incidents. This, in turn, resulted in improved IT operational efficiency through reduced administration and support costs as well as improved end user productivity through a reduction in the downtime due to incidents. The potential financial benefit from the reduced probability and severity of data breaches was not quantified due to its varying degree across industries and data types. The Trend Micro Enterprise Security products evaluated included:

- InterScan Messaging Security Suite Advanced
- InterScan Web Security Suite Advanced
- OfficeScan Client-Server Suite Standard

Most customers also used Trend Micro Control Manager for security management, however the product was not included in the formal evaluation.

The customers interviewed in this study deployed the Trend Micro Enterprise Security products as software solutions. However, Trend Micro provides these products as software or virtual appliances, enabling customers to realize the same financial benefits whether deployed in physical, virtual, or cloud environments.

Purpose

The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of choosing Trend Micro Enterprise Security for their complete content security protection. Forrester's aim is to clearly show all calculations and assumptions used in the analysis. Readers should use this study to better understand and communicate a business case for investing in Trend Micro Enterprise Security.

Methodology

Trend Micro selected Forrester for this project because of its industry expertise in the Enterprise security market and Forrester's Total Economic Impact™ (TEI) methodology. TEI not only measures costs and cost reduction (areas that are typically accounted for within IT) but also weighs the enabling value of a technology in increasing the effectiveness of overall business processes. Readers should note that numbers have been rounded throughout the study.

For this study, Forrester employed four fundamental elements of TEI in modeling Trend Micro Enterprise Security:

1. Costs and cost reduction
2. Benefits to the entire organization
3. Flexibility
4. Risk

Given the increasing sophistication that enterprises have regarding cost analyses related to IT investments, Forrester's TEI methodology serves an extremely useful purpose by providing a complete picture of the total economic impact of purchase decisions.

Approach

Forrester used a five-step approach for this study:

1. Forrester gathered data from existing Forrester research relative to the Enterprise security market in general.

2. Forrester interviewed Trend Micro marketing and sales management to fully understand the potential (or intended) value proposition of Trend Micro Enterprise Security solutions.

3. Forrester conducted a series of in-depth interviews with seven organizations currently using Trend Micro Enterprise Security solutions.

4. Forrester constructed a financial model representative of the interviews. This model can be found in the TEI Framework section below.

5. Forrester created a composite organization based on the interviews and populated the framework using data from the interviews as applied to the composite organization.

Key Findings

The composite organization that Forrester synthesized from these results represents a North America-based services organization with roughly 6,000 employees and 5,000 client devices located in 10 offices throughout North America and Europe.

Based on the characteristics of the representative customer, the key findings resulting from this analysis include:

- **ROI.** Based on the interviews with the seven existing customers, Forrester constructed a TEI framework for a composite organization and the associated ROI analysis illustrating the financial impact areas. As seen in Table 1, the risk-adjusted ROI for our composite company is 129% with a breakeven point (payback period) of 14 months after deployment.

- **Benefits.** The interviewed organizations adopted Trend Micro Enterprise Security solutions and Smart Protection Network to reduce the costs and severity of security incidents. These customers were able to reduce yearly endpoint infection rates by 73%. In addition, they reduced the total cost of ownership by moving from a multivendor strategy to a single-vendor environment. The present value (PV) of the risk-adjusted total benefits is equal to $605,927.

- **Costs.** The cost to implement includes software license costs for new services, annual software maintenance costs, testing and implementation costs, and administrative support. The software license and maintenance estimates are based on the most recent price list and do not include any discounts. In this study, we are evaluating an organization that is upgrading their Endpoint platform from a previous version as well as implementing the Web and Messaging solutions. The PV of the risk-adjusted total costs is $264,164.

Table 1 illustrates the risk-adjusted cash flow for the composite organization, based on data and characteristics obtained during the interview process. Forrester risk-adjusts these values to take into account the potential uncertainty that exists in estimating the costs and benefits of a technology investment. The risk-adjusted value is meant to provide a conservative estimation, incorporating any potential risk factors that may later impact the original cost and benefit estimates. For a more in-depth explanation of risk and the risk adjustments used in this study, please see the "Risk" section.

Table 1: Composite Company ROI, Risk-Adjusted

Summary Financial Results	Original Estimate	Risk-Adjusted
ROI	154%	129%
Payback period (months)	13	14
Total costs (PV)	$257,416	$264,164
Total benefits (PV)	$654,474	$605,927
Total (NPV)	$397,059	$341,763

Source: Forrester Research, Inc.

For the representative organization, benefits were realized by leveraging the Smart Protection Network through Trend Micro Web, Messaging, and Server and Endpoint solutions. While these solutions were used in parallel to control threats, the representative organization did see measureable improvements within each layer of the security infrastructure. These included:

- **Web Security:** a 15% reduction in network traffic spikes and a 20% reduction in infections caused by users accessing an external malware site.

- **Messaging Security:** an 18% reduction in malicious spam reaching the corporate network and a 25% reduction in infections caused by users opening infected files or messages.

- **Server and Endpoint Security:** a 30% reduction in infected server and client devices and a 40% reduction in the spread of infection if a server or client machine has been infected, yielding an overall infection reduction of 58%.

Each of these metrics was used as a base assumption to quantify the financial impact of using Trend Micro Enterprise Security.

Note that the collective result of using all three of these solutions is not a strict additive process because there is some overlapping protection provided. However, there is a significant increase in protection when all three solutions are used.

Each of these metrics was used as a base assumption to quantify the financial impact of using Trend Micro Enterprise Security. For the analysis, the following benefits were quantified:

- Effective Staff Allocation
- Reduction in the Cost of Protection
- IT Support Efficiency
- Reduced End-User Downtime
- Vendor Management Savings
- Annual Software Maintenance Cost Savings

In addition to the quantified benefits noted above, several organizations also noted additional qualitative benefits which played a factor in their investment decision. These included reduced probability of customer data breach, reduced probability of impact to enterprise systems, as well as the reduction in exposure from negative external publicity coming from an incident. Depending on industry and extent of a breach, the potential cost of these incidents can easily escalate to millions of dollars. For more information on data breach costs please see Table 10 on page 15 of this document

Disclosures

The reader should be aware of the following:

- Trend Micro commissioned the study, and it was delivered by the Forrester Consulting group.
- Trend Micro reviewed and provided feedback to Forrester, but Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study.
- Trend Micro provided the customer names for the interviews.
- Forrester makes no assumptions as to the potential return on investment that other organizations will receive. Forrester strongly advises that readers should use their own estimates within the framework provided in the report to determine the appropriateness of an investment in Trend Micro Enterprise Security.
- This study is not meant to be used as a competitive product analysis.

Trend Micro Enterprise Security: Overview

Trend Micro Enterprise Security is a tightly integrated offering of content security products, services and solutions powered by the Trend Micro Smart Protection Network™. Together they deliver immediate protection from emerging threats while greatly reducing the cost and complexity of security management.

Smart Protection Network
Combines cloud-based file, web and email reputation technologies, feedback loops and the expertise of TrendLabs security researchers to provide the continuous real-time threat detection and protection services that power Trend Micro Enterprise Security solutions.

Messaging Security
Provides cloud-client email security at the gateway and mail server to block spam, malware, phishing and data leaks. Includes robust email encryption and archiving and extended security for IM and SharePoint.

Web Security
Provides website protection for corporate sites as well as employee web security at the gateway via Smart Protection Network reputation services, content scanning, and URL filtering policies.

Endpoint & Server Security
Safeguards corporate and mobile endpoints and servers with anti-malware, web threat protection, intrusion defense and data protection solutions coupled with Smart Protection Network real-time Web and File Reputation. Includes advanced protection for physical and virtual servers, and unified security and systems management.

Operating Environments
Trend Micro Enterprise Security products protect any distributed physical/virtual/cloud-based environment; support a wide array of platforms and operating systems; and offer a full range of deployment options including hosted, software, and virtual appliance.

Security Management
Makes managing enterprise-wide security easier and more efficient by simplifying configuration and updates, providing powerful reporting and offering a unified platform for both security and systems management.

Solutions and Services
Includes solutions for key security initiatives such as data protection, server virtualization, cloud computing, and regulatory compliance. Trend Micro Threat Management Services deliver best-in-class threat discovery and remediation services, and Trend Micro Premium Support offers responsive service and direct access to technical expertise.

Analysis

Interview Highlights

Forrester conducted a total of seven interviews for this study, involving representatives from the following organizations:

1. A North America-based business services organization providing human resource functions to organizations around the world. The organization currently uses Trend Micro solutions for Messaging, Endpoint, Server and Web across roughly 8,000 client devices.

2. A North America-based manufacturing and services organization providing industrial support to companies throughout North and South America. The company currently uses Trend Micro Endpoint, Server, and Messaging solutions for its 2,500 client devices.

3. A North America-based nonprofit health services organization providing care and support to patients located within the US Midwest. The organization currently uses Trend Micro Server and Endpoint security across its roughly 17,000 client devices.

4. A North America-based food products organization providing commercial products and consumer foods to customers around the world. The company currently uses Trend Micro Server, Endpoint and Messaging to support its roughly 17,000 client devices.

5. A North America-based nonprofit health services organization providing care and support to patients located within the South-East of the US. The organization currently uses Trend Micro Server, Endpoint and Web security for security across its roughly 4,000 client devices.

6. A North America-based higher educational institution providing content security for 4,000 staff, students, and faculty through the use of Trend Micro Server, Endpoint, Messaging, and Web solutions.

7. A Europe-based consumer product goods packaging company employing roughly 24,000 employees within 20 countries around the world. The organization currently uses the Messaging solution for its roughly 10,000 internet-connected employees.

The seven in-depth interviews uncovered several key security challenges and common goals that drove the analysis:

- **The ability to detect and stop potential threats across entry points.** Several interviewed clients indicated the need to ensure an equal level of protection across the endpoint, messaging, and Web layers of their client environment. Organizations noted that users were generally increasing their access to information across multiple entry points – especially the web – and more often working remotely, raising the need to stop infections and potential threats early before they reached a client machine and expose the enterprise network to potential breach.

- **The increasing sophistication and exponential growth of threats is stretching IT resources and budgets.** Another common theme across those we spoke with was coping with the rapid growth in threats and complexities of security management without the

freedom to grow IT staff resources. As a result, organizations are looking for innovative ways to increase the level of protection while at the same time controlling IT costs.

- **The need for a way to detect and respond to threats in near-real time.** With the growth in threats, organizations noted that their security depended both on the speed of threat identification as well as the speed of response. Reducing the time-to-identify was a key metric of success that, for some organizations, directly translated to operational savings as well as top-line benefits.

These common challenges served as the basis of the creation of the analysis in this report.

TEI Framework

Introduction

From the information provided in the in-depth interviews, Forrester has constructed a TEI framework for those organizations considering an implementation of Trend Micro Enterprise Security. The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that impact the investment decision.

Composite Organization

Based on the interviews with the seven existing customers provided by Trend Micro, Forrester constructed a TEI framework, a composite or representative organization, and an associated ROI analysis that illustrates the areas impacted financially. The composite organization that Forrester synthesized from these results represents a North America-based services organization with roughly 6,000 employees and 5,000 client devices located in 10 offices throughout North America and Europe. End users access several key applications on a daily basis, including Microsoft Exchange for their messaging environment (with 5,500 email accounts) as well as an internal ERP application for HR and finance-specific functions as well as a CRM application primarily used for customer service and sales activities.

Prior to investing in Trend Micro Enterprise Security the organization used different point solutions to protect its messaging, Web, and server and endpoint environments. For their server and endpoint solution, the representative organization was using an earlier version of Trend Micro OfficeScan that did not leverage the benefits of the Smart Protection Network. In addition, the representative organization was using legacy solutions for both Web and messaging security, resulting in a multivendor security environment.

Prior to the investment in Trend Micro, the organization had seen an increase in the number of incidents as well as the severity of their impact within the organization. The organization did receive security and signature updates from their respective vendors on a regular basis; however, the increase in threat volume and severity resulted in the need to respond to threats sooner and more actively than conventional signature-based security would allow. The representative organization was especially concerned about the increasing volume of web and blended threats, and felt it required a solution that would offer the most up-to-date protection possible. As a result the representative organization decided to take advantage of Trend Micro's Smart Protection Network, replacing its existing legacy Web and messaging solutions with Trend Micro InterScan Web Security and Trend Micro InterScan Messaging Security as well as upgrading its endpoint and server security solution to the latest version of OfficeScan to take advantage of both File and Web Reputation to secure their clients and servers. All three products allowed the organization to improve protection and reduce costs with the cloud-client architecture of the Smart Protection Network. The products are centrally managed using Trend Micro Control Manager.

Framework Assumptions

Table 2 lists the discount rate used in the Present Value (PV) and Net Present Value (NPV) calculations and the time horizon used for the financial modeling.

Table 2: General Financial Assumptions

General assumptions	Value
Discount rate	10%
Length of analysis	Three years

Source: Forrester Research, Inc.

Organizations typically use discount rates between 8% and 16% based on their current environment. Readers are urged to consult with their finance department to determine the most appropriate discount rate to use within their own organizations.

In addition to the financial assumptions used to construct the cash flow analysis, Table 3 provides salary assumptions used within this analysis.

Table 3: Salary Assumptions

Ref.	Metric	Calculation	Value
A1	Hours per week		40
A2	Working weeks per year		50
A3	Hours per year (M-F, 9-5)		2000
A4	Junior IT administrator		$85,000
A5	Hourly	(A4/A3)	$43

Source: Forrester Research, Inc.

Costs

This section outlines the investment for the composite organization investing in Trend Micro Web and Messaging Security while upgrading to the latest version of Trend Micro Endpoint and Server Security Costs include software license fees, annual software maintenance costs, testing and implementation, and ongoing administrative support. Readers should measure the ROI for their own organization based on their negotiated price. These numbers do not include any vendor discount. We did not estimate any hardware increase costs because our interviewees either reduced the number of servers as a result of migrating from a multivendor environment to a single-vendor environment or used the number of resources currently available.

Software License Fees

This cost represents 48% of the overall investment and includes total software costs for perpetual licenses and Year 1 maintenance costs for the composite organization. For the composite organization, we assume that the organization is currently using Trend Micro Endpoint and Server Security and will be adding Web and Messaging solutions. There are no additional license costs required to upgrade the endpoint security or any legacy Trend Micro solution. (The list price of a new OfficeScan license equates to $15.40 per user for 5,000 users.) . For the purpose of this case study, we estimate that the composite organization will pay only for the additional new licenses in Web and Messaging solutions and will continue to pay maintenance costs on all three solutions. The total cost is $122.950 (5000*0+5000*$12.08+5000*$12.51). Readers who are considering implementing Trend Micro's Enterprise Security Solutions and do not have legacy Trend Micro solutions should calculate the license and maintenance costs for the entire implementation. Table 4 illustrates the calculation.

Table 4: Software License Fees

Ref.	Metric	Calculation	Initial
B1	Number of licenses for Endpoint and Server Security		5,000
B2	Cost per license (previously purchased)		0
B3	Number of licenses (InterScan Web Security Suite Advanced)		5,000
B4	Cost per license (new purchase)		$12.08
B5	Number of licenses (InterScan Messaging Security Suite Advanced)		5,000
B6	Cost per license (new purchase)		$12.51
Bt	Software license fees	B1*B2+B3*B4+B5*B6	$122,950

Source: Forrester Research, Inc.

Annual Software Maintenance Costs

The annual software maintenance costs represent 36% of the overall investment and cover the incremental maintenance costs of the Web and Messaging solutions assuming the cost of Endpoint and Server maintenance will remain the same within the upgrade scenario. Readers should note that maintenance will be paid prior to the period that it will support. For example, Year 2 maintenance will be paid at the end of Year 1. The annual maintenance rate is 30% of the overall software license costs. Table 5 illustrates this calculation.

Table 5: Annual Software Maintenance Costs

Ref.	Metric	Calculation	Per Period
C1	License fees for Messaging and Web Security		$122,950
C2	Yearly percent		30%
Ct	Annual software maintenance	C1*C2	$36,885

Source: Forrester Research, Inc.

Upfront Testing and Implementation Costs

This category represents 9% of the overall investment. The organizations interviewed allocated two full-time staff for a total of 80 hours to planning and testing the new solutions. With an average fully loaded hourly rate of $60, we estimate the total upfront costs to be $9,600 (2*$60*80). Table 6 demonstrates this calculation.

Table 6: Upfront Planning and Testing

Ref.	Metric	Calculation	Initial
D1	Number of people		2
D2	Fully loaded hourly rate		$60
D3	Hours		80
Dt	Upfront planning and testing	D1*D2*D3	$9,600

Source: Forrester Research, Inc.

In addition to planning and testing costs, the organizations interviewed allocated two full-time staff for a total of 100 hours to implement the solutions. With an average fully loaded hourly rate of $60, we estimate the total upfront costs to be $12,000 (2*$60*100). Table 7 illustrates the calculation used.

Table 7: Implementation Costs

Ref.	Metric	Calculation	Initial
E1	Number of people		2
E2	Fully loaded hourly rate		$60
E3	Hours		100
Et	Implementation costs	E1*E2*E3	$12,000

Source: Forrester Research, Inc.

Ongoing Administrative Costs

This cost category represents 8% of the overall investment and includes the daily and ongoing management costs for the system. The organizations interviewed explained that after implementing additional services, they allocated 10% of a full-time employee with a fully loaded salary of $85,000 to manage and monitor the additional solutions. Table 8 calculates the cost of $8,500 (1*10%*$85,000) for this category.

Table 8: Ongoing Administrative Costs

Ref.	Metric	Calculation	Per Period
F1	Number of people		1
F2	Percent of time allocated		10%
F3	Annual fully loaded salary		$85,000
Ft	Ongoing administrative costs	F1*F2*F3	$8,500

Source: Forrester Research, Inc.

Total Costs

Table 9 illustrates the total costs of implementing Trend Micro Enterprise Security for the composite organization.

Table 9: Total Costs – Non-Risk-Adjusted

Costs	Initial	Year 1	Year 2	Year 3	Total	Present Value
Software license fees	122,950				122,950	122,950
Annual software maintenance		36,885	36,885	$36,885	110,655	91,728
Upfront planning and testing	9,600				9,600	9,600
Implementation costs	12,000				12,000	12,000
Ongoing administrative costs		8,500	8,500	8,500	25,500	21,138
Total costs	$144,550	$45,385	$45,385	$45,385	$280,705	$257,416

Source: Forrester Research, Inc.

Benefits

The next component of the analysis examines the benefits associated with the investment in Trend Micro Enterprise Security. The organizations interviewed were able to quantify business as well as IT benefits, including a reduction in resources and software maintenance costs, a reduction in IT

support efforts by proactively meeting security challenges and lowering the costs of protection, and an improvement in end-user productivity thanks to a reduction in the number of security incidents that affected their ability to work on their PCs.

For the representative organization, benefits were realized in part by leveraging the Smart Protection Network through Trend Micro Web, Messaging, and Endpoint and Server Security solutions. While these solutions were used in parallel to control threats, the representative organization did see measureable improvements within each layer of the security infrastructure. These included:

- **Web Security:** a 15% reduction in network traffic spikes due to infections not reaching the network and a 20% reduction in infections caused by users accessing an external malware site.

- **Messaging Security:** an 18% reduction in malicious spam reaching the corporate network and a 25% reduction in infections caused by users opening infected files or messages.

- **Endpoint and Server Security:** a 30% reduction in infected client devices and a 40% reduction in the spread of infection if a client machine has been infected, yielding an overall infection reduction of 58%.

Each of these metrics was used as a base assumption to quantify the financial impact of using Trend Micro Enterprise Security.

Together these solutions provide a reduction in infections (explained in more detail in the Benefits section below). Note that the collective result of using all three of these solutions is not a strict additive process because there is some overlapping protection provided.

- Effective Staff Allocation – through near real-time protection of potential threats, organizations could reorganize IT staff, pushing tasks to lower cost resources.

- Reduction in the Cost of Protection – faster detection allowed organizations to reduce the overall number of incidents.

- IT Support Efficiency – reducing the number of incidents also results in a reduction in the number of calls to IT support, further improving IT costs.

- Reduced End-User Downtime – fewer incidents also avoids the impact of costly downtime on the organization.

- Vendor Management Savings – several of the organizations interviewed also saw cost savings by being able to standardize on a single Trend Micro platform.

- Annual Software Maintenance Cost Savings – for those organizations which had migrated either their messaging, Web, or endpoint and server security from a legacy platform, replacing it with Trend Micro resulted in elimination of maintenance costs of the previous platform.

In addition to the quantified benefits noted above, several organizations also noted additional qualitative benefits which played a factor in their investment decision. These included reduced probability of customer data breach, reduced probability of impact to enterprise systems, as well as

the reduction in exposure from negative external publicity coming from an incident. Depending on industry and extent of a breach, the costs can easily escalate to millions of dollars. While difficult to quantify, the table below presents Forrester's estimate of potential cost per record for three data loss scenarios.

Table 10: Data Breach Costs[1]

	Low-Profile Breach In a Non-Regulated Industry	Low-Profile Breach In a Highly-Regulated Industry	High-Profile Breach In a Highly-Regulated Industry
Cost Categories	**Cost Per Record**	**Cost Per Record**	**Cost Per Record**
Discovery, Notification, Response	$50	$50	$50
Lost Employee Productivity	$20	$25	$30
Opportunity Cost	$20	$50	$100
Regulatory Fines	$0	$25	$60
Restitution	$0	$0	$30
Other Security/Audit Requirements	$0	$5	$10
Other Liabilities	$0	$0	$25
Total Cost Per Record	$90	$155	$305

Source: Forrester Research, Inc.

Reduced Rate of Infection

A key driver for many of the benefits was seen through a reduced rate of infection. Reduced rate of infection can be seen in two ways: 1. A reduction in the number of documented incidents impacting multiple users or groups; and 2. A reduction in cases of infections to single users. For many of the organizations interviewed, the business case for investing in Trend Micro was primarily made through the reduction in high profile incidents, impacting both IT and end user resources. As a result, this analysis focuses on the impact of these incidents contributing to an overall reduced rate of infections.

To calculate the reduced rate of infections, the model assumes based on customer data the investment in Trend Micro reduces the overall number of incidents by 34% over the course of a year through the use of smart protection network and its cloud-computing architecture. In addition, the model assumes a 60% reduction of infection resulting from the decline in the overall spread of infection. Based on these percent reductions, it is possible to calculate a reduced overall rate of infection of 73%. Table 11 illustrates the calculation used.

[1] "Calculating The Cost Of A Security Breach", April 10, 2007 by Khalid Kark
http://www.forrester.com/Research/Document/0,7211,42082,00.html

Table 11: Reduced Rate of Infection

	Pre Investment	Post Investment
Total Infections	1500	400
Infection Reduction Rate		1- (400/1500) = 73%

Source: Forrester Research, Inc.

Reduction in Cost of Protection

In addition to reducing the cost of identifying and responding to incidents, reducing the overall number of incidents resulting from malware, spyware, or infected files reduces the overall burden to IT of repairing and restoring individual machines.

Prior to the investment, the representative organization experienced about 1500 infections per year and it takes the organization approximately 1 hour to clean an infected computer. At an hourly fully-loaded rate of $60, we estimate the total annual savings to be $66,000 (1500*$60*1*73%). Based on the interviews, we estimate that the organization captured 50% of the benefits in Year 1 and 100% in Year 2 and Year 3. Table 12 illustrates the calculation used.

Table 12: Reduction in Cost Of Protection

Ref.	Metric	Calculation	Per Period
A1	Number of infections		1500
A2	Fully loaded hourly rate		$60
A3	Time to clean an infected computer (hours)		1
A3	Reduced rate of infections		73%
At	Reduction in cost of protection	A1*A2*A3*A4	$66,000

Source: Forrester Research, Inc.

IT Support Efficiency

In additional to reducing the direct costs of repairing and restoring infected machines, organizations saw indirect cost savings through a reduction in calls to the tier one support team because of an outbreak. When the total incidents are reduced by 73%, IT can reduce the effort required to support infected users.

Based on the interviews with the referenced Trend Micro customers, we estimate that each IT support call will cost the composite organization approximately $25, leading to annual savings of $27,375(1500*$25*73%). To remain conservative, we estimate that the organization captured 50% of the benefits in Year 1 and 100% in Year 2 and Year 3. Table 13 illustrates the calculation used.

Table 13: IT Support Efficiency

Ref.	Metric	Calculation	Per Period
B1	Number of infections per year		1500
B2	Reduced rate of infection		73%
B3	Cost per call		$25
Bt	IT support efficiency	B1*B2*B3	$27,375

Source: Forrester Research, Inc.

Effective Staff Allocation

A key driver for the interviewed organizations' move to Trend Micro for client security was to reduce the burden on IT staff while increasing the protection across the client environment. In the interview process, several organizations noted that, as a result of migrating to Trend Micro Enterprise Security, they have been able to address security challenges proactively and reduce the amount of *ad hoc* resource allocation of their most expensive and experienced resources.

Table 14: Effective Staff Allocation

Ref.	Metric	Calculation	Per Period
C1	Total resources		5
C2	Makeup of security organization — junior (percent before)		60%
C3	Makeup of security organization — senior (percent before)		40%
C4	Average annual fully loaded salary — junior		$85,000
C5	Average annual fully loaded salary — senior		$145,000
C6	Makeup of security organization — junior (percent after)		80%
C7	Makeup of security organization — senior (percent after)		20%
Ct	Effective staff allocation	((C1*C2*C4)+(C1*C3*C5))-((C1*C4*C6)+(C1*C5*C7))	$60,000

Source: Forrester Research, Inc.

Prior to implementation, we estimate that the composite organization allocated a total of five staffers — distributed as 60% junior and 40% senior members — to manage ongoing security challenges as well as overall security file management. After the implementation, our interviewees were able to

shift the distribution of resources to 80% junior and 20% senior staff. The ability to proactively monitor security activities will allow the organization to use less expensive resources and further reduce the cost of support. We assume that the average annual fully loaded salaries are $85,000 and $145,000 for junior and senior staff, respectively. Based on the interviews, we estimate that the organization captured 50% of the benefits in Year 1 and 100% in Year 2 and Year 3. Table 14 above illustrates the calculation used.

Reduced End-User Downtime

The next component measures the improvement in end-user productivity when an organization can reduce the number of security incidents and prevent the spread of an infection.

A reduction of the rate of infection by 73% can have a significant impact on the end-user community. Our interviews also estimated average end-user downtime prior to the investment in Trend Micro was about 6 hours; this number could vary for remote workers or office-based employees who have dedicated IT staff locally. Based on the interviews, we estimate that, on average, end users experienced a productivity loss of about 30%. At a fully loaded hourly rate of $60, we estimate the annual savings of $118,260 (1500*$60*73%*6*30%). To remain conservative, we estimate that the organization captured 50% of the benefits in Year 1 and 100% in Year 2 and Year 3. Table 15 illustrates this calculation.

Table 15: Reduced End User Downtime

Ref.	Metric	Calculation	Per Period
D1	Number of yearly infections		1500
D2	Fully loaded hourly rate		$60
D3	Reduced rate of infection		73%
D4	Average downtime (hours)		6.00
D5	Reduced productivity during impact		30%
Dt	Reduced end user downtime — reduced severity of incidents	D1*D2*D3*D4*D5	$118,260

Source: Forrester Research, Inc.

Vendor Management Savings

Several of the organizations interviewed had seen the movement toward Trend Micro as a chance to consolidate their security solutions and standardize on a single vendor while at the same time leveraging the benefits of the Smart Protection Network. Consolidating on a single vendor provided the opportunity for organizations to realize vendor management cost savings by having a single point of contact for all of their content security infrastructure. Specific tasks include the cost of interfacing with the vendor for updates and product upgrades, vendor support, as well as overall account maintenance.

To calculate this benefit, the representative organization currently has two administrators spending roughly 20% of their time managing the vendor relationship. Based on the movement to a single-vendor environment, the organization can reduce the time spent on vendor management by roughly 30%, resulting in yearly savings of $14,400. Table 16 illustrates the calculation used.

Table 16: Vendor Management Savings

Ref.	Metric	Calculation	Per Period
E1	Number of administrators (FTE)		2
E2	Percent of time managing multiple security vendors		20%
E3	Hours per year		2,000
E4	Fully loaded hourly rate		$60
E5	Estimated percent reduction in time		30%
Et	Reallocation of resources	E1*E2*E3*E4*E5	$14,400

Source: Forrester Research, Inc.

Annual Software Maintenance Cost Savings

For the representative organization, moving to Trend Micro resulted in a cost impact of the Trend Micro licenses for the Messaging and Web Security solutions mentioned in Table 5. However, these investment costs are offset by the cost savings in maintenance of replacing the legacy solutions with Trend Micro.

For the composite organization, we estimate that the total software license value replaced was $120,000. We assume a 30% annual maintenance rate and calculate the cost saving for this category at $36,000 annually ($120,000*30%). Based on the interviews, we estimate that the organization captured 50% of the benefits in Year 1 and 100% in Year 2 and Year 3. Table 17 illustrates the calculation used.

Table 17: Annual Maintenance Cost Savings

Ref.	Metric	Calculation	Per Period
F1	Total license cost — pre-investment		$120,000
F2	Maintenance cost as a percent of license		30%
Ft	Annual maintenance cost savings	F1*F2	$36,000

Source: Forrester Research, Inc.

Total Benefits

Table 18 illustrates the total benefits resulting from the implementation of Trend Micro Enterprise Security for the representative organization. The potential financial benefit from the reduced probability and severity of data breaches was not quantified due to its varying degree across industries and data types.

Table 18: Total Benefits – Non-Risk-Adjusted

Benefits	Year 1	Year 2	Year 3	Total	Present Value
Reduced cost of protection	$33,000	$66,000	$66,000	$165,000	$134,132
IT support efficiency	$13,688	$27,375	$27,375	$68,438	$55,635
Effective staff allocation	$30,000	$60,000	$60,000	$150,000	$121,938
Reduced end user downtime	$59,130	$118,260	$118,260	$295,650	$240,341
Vendor management savings	$7,200	$14,400	$14,400	$36,000	$29,265
Annual maintenance cost savings	$18,000	$36,000	$36,000	$90,000	$73,163
Total benefits	$161,018	$322,035	$322,035	$805,088	$654,474

Source: Forrester Research, Inc.

Risk

Risk is the third component within the TEI model; it is used as a filter to capture the uncertainty surrounding different cost and benefit estimates. If a risk-adjusted ROI still demonstrates 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 values considering risk. In general, risks affect costs by raising the original estimates and they affect benefits by reducing the original estimates.

For the purpose of this analysis, Forrester risk-adjusts the cost and benefit estimates to better reflect the level of uncertainty that exists for each estimate. The TEI model uses a triangular distribution method to calculate risk-adjusted values. To construct the distribution, it is necessary to first estimate the low, most likely, and high values that could occur within the current environment. The risk-adjusted value is the mean of the distribution of those points. Forrester defines two types of investment risk associated with this analysis: implementation and impact risk. **Implementation risk** is the risk that a proposed technology investment may deviate from the original resource requirements needed to implement and integrate the investment, resulting in higher costs than anticipated. **Impact risk** refers to the risk that the business or technology needs of the organization may not be met by the technology investment, resulting in lower overall benefits. The greater the

uncertainty, the wider the potential range of outcomes for cost and benefit estimates. Quantitatively capturing investment risk by directly adjusting the financial estimates results in a more meaningful and accurate projection of the ROI.

The following *general* management and process risk was considered in this study:

- Organizations that are planning to implement Trend Micro Enterprise Security may require additional testing time depending on their infrastructure and the magnitude of the rollout.

The following risks specific to Trend Micro were considered in this study:

- The gains associated with the use of the Smart Protection Network may not be as great as anticipated due to the reduced growth of potential threats.

- Overall IT costs savings may be lower than anticipated.

Different cost and benefit estimates have different levels of risk adjustments. Forrester used list prices for all software licensing and maintenance fees. Below is the summary table showing the ROI result for the composite company with both the original and risk-adjusted results.

Table 19: Composite Company ROI, Risk-Adjusted

Summary Financial Results	Original Estimate	Risk-Adjusted
ROI	154%	129%
Payback period (months)	13	14
Total costs (PV)	$257,416	$264,164
Total benefits (PV)	$654,474	$605,927
Total (NPV)	$397,059	$341,763

Source: Forrester Research, Inc.

Readers are urged to apply their own risk ranges based on their own degree of confidence in the cost and benefit estimates.

Flexibility

Flexibility, as defined by TEI, represents an investment in additional capacity or capability that could be turned into business benefit for some future additional investment. Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix A).

While Forrester believes that organizations purchasing the Trend Micro solution can take advantage of these flexibility options, quantification (using the financial industry standard Black-Scholes or the binomial option pricing models) of the additional value associated with these options for this customer would require scenario development and forward-looking analysis that is not available at this time.

The value of flexibility is unique to each organization, and the willingness to measure its value varies from company to company.

While the value of flexibility has not been quantified for this analysis, Forrester does see several additional cases of additional benefit as a result of faster detection of threats within the enterprise. These include the reduction in the potential impact on transactional revenues if incidents affect transactional systems, such as ERP or CRM enterprise solutions. In addition, there are other intangible benefits resulting from reduced exposure, including a reduction in the risk associated with the loss of brand value, a reduction in the potential for customer data exposure, as well as a reduction in the third-party impact of external organizations that rely on an organization's internal systems. While the value of reduced exposure is not quantified for the report, readers should consider its impact as part of the overall value of investing in a more robust security solution.

Study Conclusions

Forrester's in-depth interviews with Trend Micro's customers yielded several important observations:

- These customers were able to improve malware detection and reduce infection to end users by taking advantage of the Smart Protection Network cloud-client architecture. In addition, they reduced the total cost of ownership by moving from a multivendor strategy to a single-vendor environment.

- Of the customers interviewed, several factors contributed to the difference in ROI. These factors included the reduction and severity of incidents across the enterprise compared with the pre-investment state, the size and complexity of the IT organization, as well as the number of client-specific endpoints within the organization.

The financial analysis provided in this study illustrates the potential way that an organization can evaluate the value proposition of Trend Micro Enterprise Security. Based on information collected in the seven in-depth customer interviews, Forrester calculated a three-year risk-adjusted ROI of129% for the composite organization with a payback period of 14 months. All final estimates are risk-adjusted to incorporate potential uncertainty in the calculation of costs and benefits.

All products in this study were deployed as software solutions. However, Trend Micro offers these products as virtual appliances as well, and provides messaging and endpoint SaaS solutions. Data centers are evolving to include server and endpoint virtualization and cloud-computing. Trend Micro security can protect these new environments and provides deployment options to further virtualization and cloud-computing efforts. Although not quantified in this study, Trend Micro customers may realize additional vendor management savings deploying Trend Micro Enterprise Security across physical, virtual, and cloud environments, providing an integrated approach to security across platforms.

Based on this study's findings, companies looking to migrate to Trend Micro can see tangible improvements to operational efficiency and effectiveness. Using the TEI framework, many companies may find the potential for a compelling business case to make such an investment.

Customized Results

For the purposes of this case study, Forrester created a composite or representative organization based on the results of the Trend Micro customer interviews. However, each organization's individual ROI will vary. To provide more customized results, Trend Micro has commissioned

Forrester to build a tool that presents the financial impact of implementing Trend Micro Endpoint Security. This tool is designed to include data specific to an individual company and produce a customized ROI estimate. This tool:

- Identifies the appropriate Trend Micro Endpoint Solution for an organization
- Includes a 3-year risk-adjusted, profit-loss analysis to illustrate the distribution of total costs, benefits, and ROI
- Offers the information needed to make an educated purchasing decision

To use this tool and receive information on the financial impact Trend Micro Endpoint Security would have on their business, companies should contact a Trend Micro sales representative for a free analysis.

Appendix A: Glossary

Discount rate: The interest rate used in cash flow analysis to take into account the time value of money. Although the Federal Reserve Bank sets a discount rate, companies often set a discount rate based on their business and investment environment. Forrester assumes a yearly discount rate of 10% for this analysis. Organizations typically use discount rates between 8% and 16% based on their current environment. Readers are urged to consult their organization to determine the most appropriate discount rate to use in their own environment.

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.

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 net present value of cash flows.

Payback period: The breakeven point for an investment. The point in time at which net benefits (benefits minus costs) equal initial investment or cost.

Return on investment (ROI): A measure of a project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits minus costs) by costs.

A Note On Cash Flow Tables

The following is a note on the cash flow tables used in this study (see the Example Table below). The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1. Those costs are not discounted. All other cash flows in Years 1 through 3 are discounted using the discount rate shown in Table 1 at the end of the year. Present value (PV) calculations are calculated for each total cost and benefit estimate. Net present value (NPV) calculations are not calculated until the summary tables and are the sum of the initial investment and the discounted cash flows in each year.

Example Table

Ref.	Category	Calculation	Initial cost	Year 1	Year 2	Year 3	Total

Source: Forrester Research, Inc.