

Forrester Consulting

HELPING BUSINESS THRIVE ON TECHNOLOGY CHANGE

Prepared for Lumension Security™

September 10, 2007

The Total Economic Impact™ of Lumension Security's Sanctuary Application And Device Control

Project Director: Jonathan Lipsitz

Contributor: Lauren Hughes

FORRESTER®

FORRESTER®

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	4
Purpose	4
Methodology.....	4
Approach.....	5
Key Findings	5
Disclosures.....	6
Sanctuary Application And Device Control: Overview	7
Analysis.....	8
Interview Highlights: John C. Lincoln Hospitals.....	8
TEI Framework	10
Introduction	10
Framework Assumptions.....	10
Costs	11
Planning And Implementation Costs: Device Control	11
License Fees: Device Control	11
Planning And Implementation Costs: Application Control	12
License Fees: Application Control	12
Yearly Maintenance Fees: Application And Device Control	13
Total Costs.....	13
Benefits	14
Reduced IT Effort To Enforce Endpoint Security Policy	14
Reduced Cost To Reimage Computers	15
Reduced Cost To Upgrade Computers	16
Reduced Cost To Replace Computers.....	17
Total Quantified Benefits.....	17
Reduced Security Risks: Data Leakage And/Or Malware Introduction.....	17
Improved IT Services To Organization	18
Increased User Productivity	18
Risk.....	19
Flexibility.....	20
TEI Framework: Summary	20
Study Conclusions.....	23
Appendix A: Total Economic Impact™ Overview	24
Benefits	24
Costs	24
Risk.....	24

Flexibility.....24
Appendix B: Glossary25
A Note On Cash Flow Tables25

© 2007, Forrester Research, Inc. All rights reserved. Forrester, Forrester Wave, RoleView, Technographics, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. Forrester clients may make one attributed copy or slide of each figure contained herein. Additional reproduction is strictly prohibited. For additional reproduction rights and usage information, go to www.forrester.com. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

Executive Summary

In June 2007, Lumension Security, then SecureWave, commissioned Forrester Consulting to examine the total economic impact and potential return on investment (ROI) that enterprises may realize by deploying Sanctuary Application and Device Control. Sanctuary (formerly SecureWave Sanctuary) Application and Device Control is an integrated application and device control solution providing enterprisewide endpoint security. This study illustrates the financial impact of moving from a difficult-to-enforce, "voluntary" compliance solution to an IT-driven solution that automatically enforces endpoint security policies.

In conducting in-depth interviews with John C. Lincoln Hospitals (JCL), an existing Sanctuary Application and Device Control customer, Forrester found that this organization achieved significant benefits, some easily measured for this ROI study and others that could not be measured but are likely to be more valuable. Specifically, the benefits fall into the following categories: 1) reduced effort required by the IT staff to enforce security policy; 2) reduced cost and effort to maintain, repair, and upgrade computers; 3) reduced number of new computers that need to be purchased each year; 4) reduced risk/cost of "data leakage," sensitive information being taken out on USB drives and other mobile storage devices; 5) reduced risk/cost of accidental or intentional malware introduction; 6) improved quality of life for the IT staff due to fewer late-night emergencies; 7) improved image of the IT department, as they can now provide more services and with a quicker response time across the entire healthcare system; and 8) increased user productivity from improved computer uptime and performance thanks to the prevention of access to non-work related applications.

JCL was able to provide metrics to quantify the first three benefits. For the interviewed customer, Forrester found an anticipated return on investment (ROI) of between 365% and 372% with Sanctuary Application and Device Control.

Purpose

The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Sanctuary Application and Device Control on their organizations. 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 Sanctuary Application and Device Control.

Methodology

Lumension Security (formerly SecureWave) selected Forrester for this project because of its industry expertise in IT security 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.

For this study, Forrester employed four fundamental elements of TEI in modeling Sanctuary Application and Device Control:

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. Please see Appendix A for additional information on the TEI methodology.

Approach

Forrester used a four-step approach for this study:

1. Forrester gathered data from existing Forrester research relating to the Sanctuary solution and the endpoint security market in general.
2. Forrester interviewed Lumension Security's marketing and sales personnel to fully understand the potential (or intended) value proposition of the Sanctuary solution.
3. Forrester conducted in-depth interviews with one organization currently using Lumension Security's Sanctuary solution.
4. Forrester constructed a financial model representative of the interviews. This model can be found in the TEI Framework section below.

Key Findings

Forrester's study yielded following key findings:

- **ROI.** Based on the interviews with an existing customer, Forrester constructed a TEI framework and the associated ROI analysis illustrating the financial impact areas. As seen in Table 1, the risk-adjusted ROI for this company is 365% with a breakeven point (payback period) of 19 months after deployment. The breakeven point would have been considerably shorter had Application Control been implemented with Device Control in Year 1, instead of in Year 2.
- **Benefits.** As discussed previously, many of the benefits associated with Sanctuary were difficult to quantify for this study. For the purposes of the ROI analysis, only benefits associated with reduced headcount required to enforce endpoint security, reduced effort and cost to maintain and repair end user computers, and reduced need to upgrade and replace end user computers were quantified. The risk-adjusted, present value of the benefits amount to \$632,966 over a four-year period.
- **Costs.** Implementing Sanctuary is a straightforward and quick process. Particularly in the case of Device Control, the customer found that very little implementation effort and almost no professional services were needed. Additionally, the interviewee indicated that there is almost no need for ongoing support of the product. Therefore, the bulk of the costs are comprised of license and maintenance fees. The risk-adjusted present value of costs amount to \$136,040 over a four-year period.

Table 1 illustrates the risk-adjusted cash flow for JCL, 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 risk adjustments used in this study, please see the "Risk" section.

Table 1: Company ROI, Original and Risk-Adjusted

Summary financial results	Unadjusted (best case)	Risk-adjusted
ROI (four year)	372%	365%
Payback*	16 month	19 months
Total four-year costs (PV)	(\$140,384)	(\$136,040)
Total four-year benefits (PV)	\$662,092	\$632,966
Total four-year net savings (NPV)	\$521,709	\$496,926

** Note: Payback would have been faster, had deployment not been spread out over two years.*

Source: Forrester Research, Inc.

Disclosures

The reader should be aware of the following:

- The study is commissioned by Lumension Security and delivered by the Forrester Consulting group.
- Lumension Security 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.
- The customer name for the interviews was provided by Lumension Security.
- 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 the Sanctuary solution.
- This study is not meant to be used as a competitive product analysis.

Sanctuary Application And Device Control: Overview

According to Lumension Security, Sanctuary offers unified policy enforcement for centrally managing and monitoring application and device control that proactively secures an organization from data threats, including data leakage, malware, and spyware. Sanctuary provides organizations with a comprehensive solution for endpoint security management by combining the proven capabilities of its comprehensive integrated application and device control modules — all from a single console. Offering the best of both worlds, Sanctuary gives control back to IT administrators, while giving end users the flexibility they demand.

- Sanctuary Application Control, a component of Sanctuary, provides policy-based enforcement of application use to secure endpoints from malware, spyware, zero-day threats, and unwanted or unlicensed software. By employing a whitelist approach, Sanctuary Application Control enables only authorized applications to execute on a network server, terminal services server, thin client, laptop, or desktop. Unauthorized applications are prohibited from executing.
- Sanctuary Device Control, a component of Sanctuary, provides policy-based enforcement of removable device use to control the flow of inbound and outbound data from your endpoints. By employing a whitelist approach, Sanctuary Device Control enables only authorized devices to connect to a network, laptop, thin client, or desktop. Unauthorized device access is prohibited by default.

Analysis

As stated in the Executive Summary, Forrester took a multistep approach to evaluate the impact that implementing Sanctuary can have on an organization:

- Interviews with Lumension Security marketing and sales personnel.
- In-depth interviews with one organization currently using Sanctuary Application and Device Control.
- Construction of a financial framework for the implementation of Sanctuary Application and Device Control.

Interview Highlights: John C. Lincoln Hospitals

JCL is a community-based not-for-profit healthcare system. The system consists of two hospitals, several physician practices, and multiple community outreach programs. More than 3,500 employees work throughout the system, and there are an additional 1,400 physicians affiliated with the system.

In 2005, when Sanctuary Device Control was implemented, there were approximately 2,500 PCs (desktop and laptop) used by employees in the performance of their jobs. Each of these computers represented an endpoint security risk for either malware introduction (i.e., viruses, keyloggers, etc.) or data leakage. Preventing data leakage of sensitive information, such as patients' medical records, is a particular concern because of HIPAA (Health Insurance Portability and Accountability Act of 1996).

Additionally, there are approximately 750 applications approved for use. Ensuring that all of these applications were properly installed and did not have any software conflicts was a serious undertaking for IT staff. This problem was compounded by the rogue installation of unapproved applications and files, including: games, mp3s, and instant messenger programs.

The interviews uncovered the following points that either impact the ROI analysis or may be of interest to the reader:

- Sanctuary was implemented as part of an overall client security strategy that included antivirus protection. The organization is using gateway antivirus, network firewalls, and other technologies that usually comprise an enterprise deployment.
- The primary reason that JCL's CIO, Rob Israel, chose to implement Sanctuary was because it represented a best practice solution to a known risk area, data leakage. The CIO had read about serious losses of sensitive data at other organizations, e.g., the Veterans Administration, and wanted to put the best solution in place before JCL was affected. JCL was not aware of any data leakage events within its organization, "but would not have really known if they did occur." Additionally, JCL felt that implementing Sanctuary would improve its customer response time and remove mundane, repetitive support tasks.
- JCL had two minor experiences that reinforced its known need for additional endpoint security measures:
 - In 2004, JCL was hit by the Slammer virus. It was most likely introduced via a floppy disk inserted into an insecure PC. The IT team responded excellently and prevented

any clinical systems or mission-critical applications from being taken offline. Email was down for approximately 8 hours and all external connections to the Internet were shut down. The entire IT team of 25 professionals worked through the night to keep systems up and get everything back to normal.

- Not long after that, a laptop computer was stolen from one of the hospitals. Fortunately, it was brand new and had no sensitive information on it. However, this further emphasized the need to have more control over where information was stored and what devices users had access to, and it highlighted the need for information protection to be taken more seriously.
- When selecting an application and device control solution provider, the customer considered several vendors. It eventually decided on Sanctuary because of the overall quality of the solution and because “nothing was easier to deploy and administer.”
- Implementation of Sanctuary was extremely easy, especially in the case of Device Control. Device Control took three days to implement and approximately one week of follow-up for fine tuning. Application Control took two months, primarily to build application catalogs and figure out the nuances at the patch and update level.
- The learning curve to use and fully realize the benefits of Sanctuary was very short. In the case of Device Control, benefits were realized almost immediately. For Application Control, full benefits were realized after approximately three months.
- The IT organization had very detailed, written security policies to address endpoint security, specifically around not attaching any unauthorized devices, installing applications or files, or removing any information from the premises. However, enforcement was largely based on the honor system and manual processes to perform audits. After implementing Sanctuary, policy enforcement became automatic, eliminating problems before they could arise.

TEI Framework

Introduction

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

Framework Assumptions

Table 2 lists the discount rate used in the PV and NPV calculations and time horizon used for the financial modeling.

Table 2: General Assumptions

Ref.	General assumptions	Value
A1	Discount rate	10%
A2	Length of analysis	Four 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 respective finance department to determine the most appropriate discount rate to use within their own organizations.

Four years was chosen as the length of analysis because Device Control was implemented in Year 1 and Application Control was implemented in Year 2. By using four years, there is enough time for all of the benefits associated with both implementations to fully come online. *It is important to note that had the customer implemented both Device and Application Control in Year 1, all of the benefits would have come online earlier, resulting in a shorter payback period.*

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

Table 3: Salary Assumptions

Ref.	Metric	Calculation	Value
B1	Loaded annual cost per IT employee (Year 1)	[Rises with inflation]	\$37,000
B2	Work days per year		200
B3	Loaded daily cost per IT employee (Year 1)	(B1/B2)	\$185

Source: Forrester Research, Inc.

Costs

The costs to implement and manage Sanctuary Application and Device Control included planning and implementation costs, software license fees, and software maintenance fees. The vast majority of the costs are for the initial license fees. There is no significant ongoing cost for administration for Sanctuary. Instead, the implementation of Sanctuary resulted in a headcount reduction for the customer, which is discussed in the benefits section below.

Planning And Implementation Costs: Device Control

The IT department spent several months investigating various options for their endpoint security needs. This was done on a part-time basis when time was available. After selecting Sanctuary, the actual implementation took less than one week, and approximately one more week for fine-tuning.

Any hardware needed to host the solution was repurposed, so the only implementation costs are the associated labor costs. The total customer labor cost to plan and implement Device Control is equal to the product of the number of employees on the project, the fully burdened salary per employee per day, and the number of days on the project. The fully burdened salary per IT administration employee in Year 1 of the study is equal to \$37,000. Assuming 200 work days per year, the daily burdened salary is equal to \$185. The resulting total cost equals \$3,700.

Table 4: Total Device Control Planning And Implementation Costs, Non-Risk-Adjusted

Ref.	Metric	Calculation	Value
C1	Number of people*		2.0
C2	Fully burdened IT resource cost per day		\$185
C3	Days of effort per person		10.0
Ct	Planning and implementation costs: Device Control	(C1 * C2 * C3)	\$3,700

**Only one person was involved in the actual implementation. The second person reflects research and planning efforts.*

Source: Forrester Research, Inc.

License Fees: Device Control

Sanctuary costs are based on a per-seat license. The license costs used in this study are the list price adjusted for volume discounts. Device Control was implemented in Year 1 of this study.

Based on the volume of Device Control licenses bought and that they were bundled with Application Control, the per-seat cost for Device Control is equal to \$35. The customer purchased 1,000 Device Control licenses, resulting in a total cost of \$35,000.

Table 5: Total Device Control License Fees, Non-Risk-Adjusted

Ref.	Metric	Calculation	Value
D1	Per-seat license fee - Device Control		\$35
D2	Number of seats		1,000
Dt	License fees: Device Control	(D1 * D2)	\$35,000

Source: Forrester Research, Inc

Planning And Implementation Costs: Application Control

JCL looked at Application Control while the decision was being made to implement Device Control; however, the IT department was busy with various projects and put off implementation of Application Control until the following year.

It took approximately two months to implement Application Control. Most of this time was spent building up the application catalogs. There were some difficulties at the patch and upgrade level of the catalog, but these challenges were overcome in discussions with Lumension Security and the appropriate application vendors. In total, the customer had 750 approved applications to be tested and added to the catalog.

A total of one-and-a-half full-time equivalents (FTEs) spent two months researching and implementing Application Control. The total burdened salary and benefits per day in Year two of the study is equal to \$192.40. One-and-a-half employees each working 60 days on the implementation results in a total implementation cost of \$17,316.

Table 6: Total Application Control Planning And Implementation Costs, Non-Risk-Adjusted

Ref.	Metric	Calculation	Value
E1	Number of People		1.5
E2	Fully burdened IT resource cost per day		\$192.40
E3	Days		60.0
Et	Planning and implementation costs: Application Control	(E1 * E2 * E3)	\$17,316

Source: Forrester Research, Inc.

License Fees: Application Control

The per-seat list license fee for Application Control, given license volume and bundling with Device Control, is equal to \$23.33 per seat. The customer purchased 3,000 licenses, resulting in a total cost of \$69,990.

Application Control was implemented the year after Device Control.

Table 7: Total Application Control License Fees, Non-Risk-Adjusted

Ref.	Metric	Calculation	Value
F1	Per-seat license fee: Application Control		\$23.33
F2	Number of seats		3,000
Ft	License fees : Application Control	(F1 * F2)	\$69,990

Source: Forrester Research, Inc.

Yearly Maintenance Fees: Application And Device Control

There is a standard 15% annual maintenance fee based on the total value of the licenses. Maintenance fees begin the year after the purchase.

The maintenance fees on Device Control started in Year 2 and on Application Control in Year 3.

Table 8: Total Maintenance Fees, Non-Risk-Adjusted

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3	Year 4
G1	Prior year license fees	(= Dt + Ft)		0	\$35,000	\$104,990	\$104,990
G2	Software maintenance percentage		15.0%	15.0%	15.0%	15.0%	15.0%
Gt	Software maintenance fees	(G1 * G2)			\$5,250	\$15,749	\$15,749

Source: Forrester Research, Inc.

Total Costs

Table 9 summarizes the total costs associated with this customer's implementation of Sanctuary Application and Device Control.

Table 9: Total Costs Of Sanctuary Application And Device Control, Non-Risk-Adjusted

Ref.	Costs	Initial Cost	Year 1	Year 2	Year 3	Year 4	Total	PV
Ct	Planning and implementation costs: Device Control	\$3,700					\$3,700	\$3,700
Dt	License fees: Device Control		\$35,000				\$35,000	\$31,818
Et	Planning and implementation costs: Application Control			\$17,316			\$17,316	\$14,311
Ft	License fees: Application Control			\$69,990			\$69,990	\$63,627
Gt	Software maintenance fees			\$5,250	\$15,749	\$15,749	\$36,747	\$26,927
	Total	\$3,700	\$35,000	\$92,556	\$15,749	\$15,749	\$162,753	\$140,384

Source: Forrester Research, Inc.

Benefits

The benefits that JCL's CIO, Rob Israel, sought and realized go beyond those that are easily quantified in this ROI analysis. Therefore, the first half of this section details the benefit calculations that go into the ROI analysis, and the second half describes the qualitative benefits that are not included in the ROI analysis. In many respects, the qualitative benefits are more valuable than the quantitative ones and should be taken into consideration when analyzing the total return on investment offered by the Sanctuary solution.

Reduced IT Effort To Enforce Endpoint Security Policy

Prior to the implementation of Sanctuary, enforcing specific endpoint security policy and fixing related problems that arose was a very manually intensive effort. The Sanctuary implementation reduced the FTE headcount dedicated to these tasks from 4.0 to 1.5. Additionally, JCL was able to avoid future headcount growth.

Headcount reduction began in Year 1 when Device Control was implemented. Headcount reduction grew as Application Control was implemented and future headcount growth was avoided, as well. It is worth noting that JCL has lower labor costs than many other companies. Readers are encouraged to input their own labor costs into the model as the corresponding financial benefit is likely to be higher than what is calculated in this study.

Table 10: Total Reduced IT Headcount, Non-Risk-Adjusted

Ref.	Metric	Calculation	Year 1	Year 2	Year 3	Year 4
H1	Number of workers (saved)		0.5	1.0	2.5	3.5
H2	Yearly total burdened cost per IT administrator		\$37,000	\$38,480	\$40,019	\$41,620
Ht	Reduction in headcount	(H1 * H2)	\$18,500	\$38,480	\$100,048	\$145,670

Source: Forrester Research, Inc.

Reduced Cost To Reimage Computers

Prior to the implementation of Sanctuary, servicing computers required a great deal of manual effort. This was needed to remove unauthorized applications and files, repair application conflicts, remove malware, etc. Sanctuary made it impossible for these applications and files to get on the computers in the first place, thereby reducing the number of computers that needed to be serviced annually.

Table 11 calculates how many fewer computers need to be serviced each year. The baseline assumes that 15% of all computers require service each year. This baseline is reduced in approximate proportion to the reduced headcount required to service these computers.

Table 11: Reduced Number Of Computers Needing Service Calls

Ref.	Metric	Calculation	Year 1	Year 2	Year 3	Year 4
I1	Number of computers		2,500	3,000	3,700	3,885
I2	Percent of computers needing service		15%	15%	15%	15%
I3	Number of computers needing service (baseline)	(I1 * I2)	375	450	555	583
I4	Percent reduction in computers needing service		5%	15%	40%	50%
It	Reduced number of computers needing service	(I3 * I4 [rounded])	19	68	222	291

Source: Forrester Research, Inc.

Of the total number of service calls, 30% require reimaging. The total activity-based cost to reimage a computer is \$250. Since headcount savings are accounted for in the above analysis, this value is reduced to avoid double counting. Forrester estimates that 30%, or \$83.33, of the total cost is attributable to user downtime while their computer is being serviced and other non-IT labor costs.

Table 12: Reduced Cost To Reimage Computers, Non-Risk-Adjusted

Ref.	Metric	Calculation	Year 1	Year 2	Year 3	Year 4
J1	Reduced number of computers needing service	(= It)	19	68	222	291
J2	Percent of serviced computers that are reimaged		30%	30%	30%	30%
J3	Reduced number of computers that are reimaged	(J1 * J2 [Rounded])	6.0	20.0	67.0	87.0
J4	Cost to reimage a computer		\$83.33	\$83.33	\$83.33	\$83.33
Jt	Reduced computer reimaging costs	(J3 * J4)	\$500	\$1,667	\$5,583	\$7,250

Source: Forrester Research, Inc.

Reduced Cost To Upgrade Computers

In addition to the reduced cost to reimage computers, fewer computers need to be upgraded each year. An upgrade consists of installing more RAM. Because the computers are not burdened with running unapproved memory-intensive applications, they can perform at a level necessary to meet the work requirements without the installation of additional memory.

Of the computers that would otherwise need to be serviced, 70% of the service calls are dedicated to the installation of more memory. The total activity-based cost to perform the upgrade is \$200. Again, this value is reduced since the IT labor component was previously accounted for in the headcount reduction benefit above. A value of \$100 is used to reflect the cost of the memory, user downtime, and other costs.

Table 13: Reduced Cost To Upgrade Computers, Non-Risk-Adjusted

Ref.	Metric	Calculation	Year 1	Year 2	Year 3	Year 4
K1	Reduced number of computers needing service	(= It)	19	68	222	291
K2	% of serviced computers that would be upgraded		70%	70%	70%	70%
K3	Reduced number of computers to be upgraded	(L1 * L2 [rounded])	13	48	155	204
K4	Cost to upgrade a computer		\$100	\$100	\$100	\$100
Kt	Reduced cost to upgrade computers	(L3 * L4)	\$1,300	\$4,800	\$15,500	\$20,400

Source: Forrester Research, Inc.

Reduced Cost To Replace Computers

The CIO estimates that once the full benefits of Application and Device Control came online, the healthcare system avoided buying 250 new computers per year. These are computers that otherwise would have been scrapped because they could not be fixed or the cost to fix them would have exceeded the replacement value. Since this situation represents a total write down of the asset and not a life-cycle extension, the total value of the computer is recognized in this ROI analysis.

Table 14: Reduced Cost To Replace Computers, Non-Risk-Adjusted

Ref.	Metric	Calculation	Year 1	Year 2	Year 3	Year 4
L1	Reduced number of computers to be replaced		0	100	250	250
L2	Cost to replace a computer		\$900	\$900	\$900	\$900
Lt	Reduced computer replacement costs	(K1 * K2)		\$90,000	\$225,000	\$225,000

Source: Forrester Research, Inc.

Total Quantified Benefits

Table 15 summarizes the total benefits JCL realized implementing Sanctuary Application and Device Control.

Table 15: Total Benefits From Sanctuary Application And Device Control, Non-Risk-Adjusted

	Benefits	Year 1	Year 2	Year 3	Year 4	Total	Present value
Ht	Reduction in headcount	\$18,500	\$38,480	\$100,048	\$145,670	\$302,698	\$223,282
Jt	Reduced computer reimaging costs	\$500	\$1,667	\$5,583	\$7,250	\$15,000	\$10,979
Kt	Reduced computer upgrade costs	\$1,300	\$4,800	\$15,500	\$20,400	\$42,000	\$30,728
Lt	Reduced computer replacement costs	\$ -	\$90,000	\$225,000	\$225,000	\$540,000	\$397,104
	Total	\$20,300	\$134,947	\$346,131	\$398,320	\$899,698	\$662,092

Source: Forrester Research, Inc.

Reduced Security Risks: Data Leakage And/Or Malware Introduction

The customer's principal motivation in the implementation of Sanctuary was to address endpoint security risks — malware introduction and/or data leakage. Indeed this is the case with most

Sanctuary customers. Quantifying security risks and their associated costs can be very difficult. A company often never knows that a leak has taken place, particularly in the case of data leakage.

As discussed previously, the customer who participated in this study had two endpoint security events transpire: 1) Slammer virus infection, and 2) stolen laptop computer. In both instances, the impacts were not terribly significant. But that offers no assurance that a future event would not have had major consequences. For this reason, the customer implemented a wide range of security solutions, of which Sanctuary was a major component.

A report often cited to estimate the cost of a security breach is the "CSI/FBI Computer Crime And Security Survey".¹ According to the 2006 survey, the average cost per security breach was \$167,713 — down 18% from 2005. One of the only areas that showed an increased cost from 2005 to 2006 was the loss associated with mobile hardware, i.e., laptops or USB drives. That cost increased by more than 50% to \$30,057 per incident. This is mostly attributable to the implications of the loss, and not the value of the hardware itself.

A Forrester study published in April 2007, "Calculating The Cost Of A Security Breach," provides metrics to calculate the potential cost of a security breach for any given company.² The study calculates the "cost per record" for three different company profiles:

- Low-profile breach in a non-regulated industry (\$90).
- Low-profile breach in a regulated industry (\$155).
- High-profile breach in a highly regulated industry (\$305).

As a major healthcare provider in a highly regulated industry, any significant breach is likely to be high profile. Given the thousands of patient records held, at \$305 per record, any security breach would result in a very significant cost to the customer.

Improved IT Services To Organization

This customer was able to free up 2.5 FTEs from the IT department to work on more strategic, value-add projects. This has resulted in better service to the entire organization and a better overall perception of the IT department since it is providing more services and has a quicker response time. Additionally, it has resulted in a better quality of life for members of the IT staff. They are now called in for fewer late-night emergencies and so are able to focus on activities that are more strategic and contribute to the overall success of the healthcare system.

Increased User Productivity

User productivity has increased for two reasons. First, there is improved uptime of end user computers. Second, JCL, like most companies, had employees using work computers for non-work-related activities. This varied from watching video clips to working on college term papers during overnight shifts. By keeping unauthorized applications and files off of the computers, employees can no longer pursue these outside activities. Not all of this time translates directly into additional productive work, but it has been a significant unquantified benefit for this customer.

¹ "2006 CSI/FBI Computer Crime And Security Survey". Lawrence A. Gordon, et al., Computer Security Institute, 2006.

² "Calculating The Cost Of A Security Breach." Khalid Kark, et al. , Forrester Research, April 2007.

Risk

Risk is the third component within the TEI model and is used as a filter to capture the uncertainty surrounding 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 since the risks that threaten the project have been taken into consideration and quantified. The risk-adjusted numbers should be taken as "realistic" expectations, since they represent the expected value considering risk. In general, risks impact benefits by reducing the original estimates and impact costs by raising the original estimates.

The main risks that were considered in this study are:

- The risk that implementation costs may be higher because of a higher fully burdened cost of an IT employee.
- The risk that an organization may not be able to save as much money through cost avoidance of buying new computers.

Other than these areas, all risks were deemed to be "low" or "none."

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. "Most likely" is always set at 100%. The risk-adjusted value is the mean of the distribution of those points.

For example, the cost of planning and implementation for Application Control is defined as "high" risk. This risk level was chosen because the customer has a lower total burdened cost for an IT resource than a lot of other companies. Therefore, it is very likely that someone reading this paper will experience a higher cost of implementation. The original estimated cost is \$17,316. To calculate the risk-adjusted cost, the "most likely" scenario was set at 100% of cost, the "high" scenario was assigned 125% of cost, and the "low" scenario was assigned 100% of cost. The rounded mean of these three values is 108%. The resulting cost used in the risk-adjusted tables is \$18,701, or 108% of \$17,316.

On the other hand, License Fees has a risk level of "none." Since list price with appropriate volume discounts are used, a reader may expect to receive similar pricing. Therefore, there is no inherent risk involved in this estimate.

The following tables show the values used to adjust for uncertainty in cost and benefit estimates. Readers are urged to apply their own risk ranges based on their own degree of confidence in the cost and benefit estimates.

Table 16: Risk Adjustments To Costs

Ref.	Risk adjustments to costs	Low	Most likely	High	Risk-adjusted
M1	Planning and implementation costs: Device Control (High)	100%	100%	125%	108%
M2	License fees: Device Control (None)	100%	100%	100%	100%
M3	Planning and implementation costs: Application Control (High)	100%	100%	125%	108%
M4	License fees: Application Control (None)	100%	100%	100%	100%
M5	Software maintenance fees (None)	100%	100%	100%	100%

Source: Forrester Research, Inc.

Table 17: Risk Adjustments To Benefits

Ref.	Risk adjustments to benefits	Low	Most likely	High	Risk-adjusted
N1	Reduction in headcount (Low)	90%	100%	105%	98%
N2	Reduced computer reimaging costs (Low)	90%	100%	105%	98%
N3	Reduced computer upgrade costs (Low)	90%	100%	105%	98%
N4	Reduced computer replacement costs (Medium)	80%	100%	103%	94%

Source: Forrester Research, Inc.

Flexibility

Flexibility, as defined by Forrester, 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).

In the case of this study, the customer does not use any additional services that were not included in the original licenses, nor are there any plans to do so in the immediate future. Therefore, the flexibility that the customer realizes is derived from Lumension Security's approach to security. Since application and device permissions are based on an approval whitelist, the customer has a good level of protection against future, unknown endpoint security threats that will develop.

TEI Framework: Summary

Considering the financial framework constructed above, the results of the costs, benefits, and risk and sections can be used to determine a return on investment, net present value, and payback period. Tables 18 and 19, below, show the risk-adjusted cost and benefit values, applying the risk-

TEI™ For Lumension Security's Sanctuary Application And Device Control

adjustment method indicated in the "Risks" section and the values from Table 16 and 17 to the numbers in Tables 9 and 15, respectively.

Table 18: Risk-Adjusted Costs

Ref	Total costs, risk-adjusted	Initial	Year 1	Year 2	Year 3	Year 4	Total	Present value
L1	Planning and implementation costs: Device Control	\$3,996					\$3,996	\$3,996
L2	License fees: Device Control		\$35,000				\$35,000	\$31,818
L3	Planning and implementation costs: Application Control			\$18,701			\$18,701	\$15,456
L4	License fees: Application Control			\$69,990			\$69,990	\$57,843
L5	Software maintenance fees (yearly)			\$5,250	\$15,749	\$15,749	\$36,747	\$26,927
Lt	Total	\$3,996	\$35,000	\$93,941	\$15,749	\$15,749	\$164,434	\$136,040

Source: Forrester Research, Inc.

Table 19: Risk-Adjusted Benefits

Ref	Total benefits, risk-adjusted	Year 1	Year 2	Year 3	Year 4	Total	Present value
M1	Reduction in headcount	\$18,130	\$37,710	\$98,047	\$142,756	\$296,644	\$218,816
M2	Reduced computer reimaging costs	\$490	\$1,633	\$5,472	\$7,105	\$14,700	\$10,759
M3	Reduced cost to upgrade computers	\$1,274	\$4,704	\$15,190	\$19,992	\$41,160	\$30,113
M4	Reduced computer replacement costs	\$ -	\$84,600	\$211,500	\$211,500	\$507,600	\$373,278
Mt	Total	\$19,894	\$128,648	\$330,209	\$381,353	\$860,104	\$632,966

Source: Forrester Research, Inc.

It is important to note that values used throughout the TEI Framework are based on in-depth interviews with one organization. Forrester makes no assumptions as to the potential return that other organizations will receive within their own environment. Forrester strongly advises that

readers use their own estimates within the framework provided in this study to determine the expected financial impact of implementing Sanctuary Application and Device Control.

Study Conclusions

Forrester's in-depth interviews with one Sanctuary Application and Device Control customer, John C. Lincoln Hospitals, yielded several important observations:

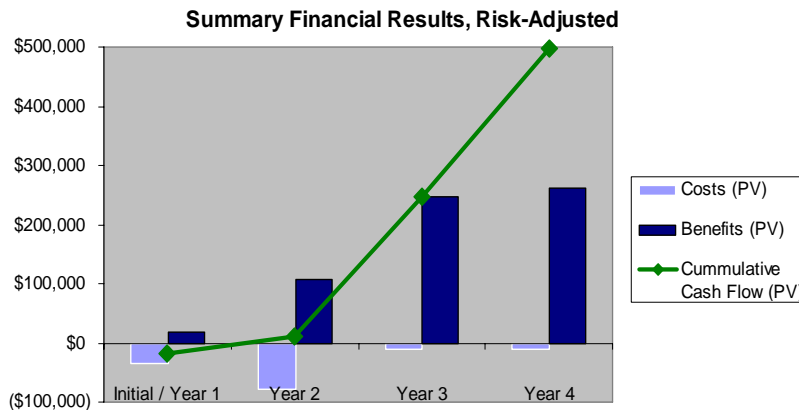
- Forrester found that organizations can realize quantitative benefits in the form of lower costs to manage endpoint security, lower costs to maintain and upgrade computers, and cost avoidance in purchasing new computers.
- Adoption of Sanctuary also reduces the risk of malware introduction and data leakage. Additional benefits include an improved perception of the IT department across the entire organization and increased job satisfaction among IT employees.

The financial analysis provided in this study illustrates the potential way in which an organization can evaluate the value proposition of Sanctuary Application and Device Control. Based on information collected from one customer, Forrester calculated a four-year risk-adjusted ROI of 365% with a payback period of 1.6 years. It is important to note that the payback period would have been shorter had the customer implemented both Device and Application Control in Year 1. All final estimates are risk-adjusted to incorporate potential uncertainty in the calculation of costs and benefits.

Table 20: ROI, Original And Risk-Adjusted

Summary financial results	Unadjusted (best case)	Risk-adjusted
ROI (four year)	372%	365%
Payback*	16 months	19 Months
Total four-year costs (PV)	(\$140,384)	(\$136,040)
Total four-year benefits (PV)	\$662,092	\$632,966
Total four-year net savings (NPV)	\$521,709	\$496,926

* Note: Payback would have been faster had deployment not been spread out over two years.



Source: Forrester Research, Inc.

Appendix A: Total Economic Impact™ Overview

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.

The TEI methodology consists of four components to evaluate investment value: benefits, costs, risks, and flexibility. For the purpose of this analysis, the impact of flexibility was not quantified.

Benefits

Benefits represent the value delivered to the user organization — IT and/or business units — by the proposed product or project. Often product or project justification exercises focus just on IT cost and cost reduction, leaving little room to analyze the effect of the technology on the entire organization. The TEI methodology and the resulting financial model place 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. Calculation of benefit estimates involves a clear dialogue with the user organization to understand the specific value that is created. In addition, Forrester also requires that there be a clear line of accountability established between the measurement and justification of benefit estimates after the project has been completed. This ensures that benefit estimates tie back directly to the bottom line.

Costs

Costs represent the investment necessary to capture the value, or benefits, of the proposed project. IT or the business units may incur costs in the forms of fully burdened labor, subcontractors, or materials. Costs consider all the investments and expenses necessary to deliver the proposed value. In addition, the cost category within TEI captures any incremental costs over the existing environment for ongoing costs associated with the solution. All costs must be tied to the benefits that are created.

Risk

Risk measures the uncertainty of benefit and cost estimates contained within the investment. Uncertainty is measured in two ways: the likelihood that the cost and benefit estimates will meet the original projections and the likelihood that the estimates will be measured and tracked over time. TEI applies a probability density function known as "triangular distribution" to the values entered. At a minimum, three values are calculated to estimate the underlying range around each cost and benefit.

Flexibility

Within the TEI methodology, direct benefits represent one part of the investment value. While direct benefits can typically be the primary way to justify a project, Forrester believes that organizations should be able to measure the strategic value of an investment. Flexibility represents the value that can be obtained for some future additional investment building on top of the initial investment already made. For instance, an investment in an enterprisewide upgrade of an office productivity suite can potentially increase standardization (to increase efficiency) and reduce licensing costs. However, an embedded collaboration feature may translate to greater worker productivity if activated. The collaboration can only be used with additional investment in training at some future point in time. However, having the ability to capture that benefit has a present value that can be estimated. The flexibility component of TEI captures that value.

Appendix B: 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 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 4 are discounted using the discount rate shown in Table 2 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.