



**Lumension**  
SECURITY

# Total Economic Impact™ -Analyse der Sanctuary- Lösung von Lumension Security

Application And Device Control

Projektleiter: Jonathan Lipsitz  
Referent: Lauren Hughes

Friday, August 29, 2008

[www.lumension.com](http://www.lumension.com)



## INHALT

<b>Einführung</b> .....	<b>3</b>
Ziel .....	3
Methodologie.....	4
Konzept.....	4
Ergebnisse im Überblick .....	5
Wichtige Hinweise.....	6
<b>Sanctuary Application And Device Control:Einführung</b> .....	<b>8</b>
<b>Analyse</b> .....	<b>9</b>
Ergebnis der Gespräche: John C. Lincoln Hospitals .....	9
TEI-Framework .....	11
Kosten .....	12
Nutzen.....	18
Risiken .....	25
Flexibilität .....	28
<b>Bilanz der Studie</b> .....	<b>31</b>
<b>Anhang A: Total Economic Impact™ im Überblick</b> .....	<b>32</b>
Nutzen.....	32
Kosten .....	32
Risiken .....	33
Flexibilität .....	33
<b>Anhang B: Glossar</b> .....	<b>33</b>

© 2007, Translated from English - Forrester Research, Inc. Alle Rechte vorbehalten. Forrester, Forrester Wave, RoleView, Technographics und Total Economic Impact sind Marken der Forrester Research, Inc. Alle anderen Marken sind das Eigentum ihrer jeweiligen Inhaber. Kunden von Forrester sind berechtigt, von jeder in diesem Dokument enthaltenen Abbildung eine persönliche Kopie bzw. ein Dia anzufertigen. Jede weitere Reproduktion ist strengstens untersagt. Informationen über zusätzliche Reproduktions- und Nutzungsrechte finden Sie auf der



Website [www.forrester.com](http://www.forrester.com). Die Informationen basieren auf den jeweils besten verfügbaren Quellen. Die ausgedrückten Meinungen entsprechen einer Bewertung zum gegebenen Zeitpunkt und können Änderungen unterliegen.



## Einführung

Im Juni 2007 beauftragte Lumension Security, zum damaligen Zeitpunkt noch SecureWave, die Firma Forrester Consulting mit der Untersuchung des „Total Economic Impact“ und des potenziellen „Return On Investment“, die sich für Unternehmen aus der Implementierung des Produkts Sanctuary Application and Device Control ergeben. Bei Sanctuary (ehemals SecureWave Sanctuary) Application and Device Control handelt es sich um eine integrierte Lösung zur Anwendungs- und Gerätekontrolle, die unternehmensweite Endpunktsicherheit bereitstellt. Diese Studie zeigt die finanziellen Vorteile der Migration von einer schwer durchzusetzenden, auf „freiwilliger“ Beteiligung basierenden Konformitätslösung hin zu einer IT-orientierten Lösung, die eine automatische und konsequente Durchsetzung von Richtlinien zur Endpunktsicherheit gewährleistet.

Im Rahmen fundierter Gespräche mit Verantwortlichen der John C. Lincoln Hospitals (JCL), Kunde und aktiver Benutzer von Sanctuary Application and Device Control, konnte Forrester bedeutende Vorteile für diese Einrichtung registrieren. Einige der erzielten Vorteile waren für diese ROI-Studie überaus einfach zu erfassen, andere hingegen konnten zwar nicht quantifiziert werden, sind aber zweifellos von weitaus größerem Wert. Die realisierten Vorteile lassen sich konkret in folgende Kategorien untergliedern: 1) Reduzierung des erforderlichen Aufwands durch die IT-Mitarbeiter für eine konsequente Umsetzung der Sicherheitsrichtlinien; 2) Reduzierung der Kosten und des Arbeitsaufwands für die Instandhaltung, Reparatur und Aufrüstung der Rechner; 3) Reduzierung des jährlichen Erwerbs neuer Rechner; 4) Reduzierung der Risiken/Kosten in Verbindung mit „Datenverlust“, d. h. der Entwendung sensibler Informationen auf USB-Laufwerken und anderen mobilen Speichergeräten; 5) Reduzierung der Risiken/Kosten in Verbindung mit der versehentlichen oder beabsichtigten Einführung von Malware; 6) Verbesserung der Lebensqualität für die IT-Mitarbeiter aufgrund der Reduzierung von Notfällen zu Nachtzeiten; 7) Verbesserung des Images der IT-Abteilung dank der Möglichkeit zur Bereitstellung einer größeren Zahl an Serviceleistungen und einer kürzeren Antwortzeit für das gesamte System der Gesundheitsversorgung und 8) Steigerung der Benutzerproduktivität aufgrund einer verbesserten Betriebsdauer und Leistung der Rechner dank der Verhinderung des Zugriffs auf Anwendungen ohne direkten Bezug zur Arbeit.

JCL stellte Messzahlen bereit, die eine Quantifizierung der ersten drei Vorteile ermöglichten. So konnte Forrester für JCL einen erwarteten ROI (Return On Investment) zwischen 365 % und 372 % durch den Einsatz von Sanctuary Application and Device Control festhalten.

## Ziel

Ziel dieser Studie ist es, den Leser mit einer Art Rahmenprogramm, einem Framework auszustatten, das ihm die Bewertung der potenziellen finanziellen Wirkung einer Verwendung



von Sanctuary Application and Device Control in seinem Unternehmen ermöglicht. Aus diesem Grund versucht Forrester, alle in der Analyse verwendeten Berechnungen und Annahmen klar herauszustellen. Mithilfe dieser Studie soll der Leser eine fundierte Kenntnis des Business Case einer Investition in Sanctuary Application and Device Control erhalten und in der Lage sein, den Business Case informationsbasiert weiterzuvermitteln.

## Methodologie

Für den Beschluss, die Firma Forrester mit der Durchführung dieses Projekts zu betrauen, gaben das umfassende Know-how der Firma in Sachen IT-Sicherheit sowie die von Forrester entwickelte Analysemethodologie „Total Economic Impact™“ (TEI) den Ausschlag. Bei der TEI-Methode werden nicht nur Kosten und Kostenreduzierungen gemessen (Aspekte, die im IT-Bereich standardmäßig berücksichtigt werden), sondern darüber hinaus wird auch der Wert einer Technologie als treibende Kraft für eine globale Effizienzsteigerung des gesamten Geschäftsbetriebs gewichtet.

Für diese Studie setzte Forrester vier grundlegende TEI-Komponenten zur Modellierung von Sanctuary Application and Device Control ein:

1. Kosten und Kostenreduzierung
2. Vorteile für das gesamte Unternehmen
3. Flexibilität
4. Risiken

Angesichts der zunehmenden Komplexität der Kostenanalysen, die von Unternehmen im Hinblick auf Investitionen im IT-Bereich eingesetzt werden, erweist sich die TEI-Methodologie von Forrester als überaus hilfreich, da sie ein komplettes Bild der gesamtwirtschaftlichen Wirkung von Kaufentscheidungen bereitstellt. Weitere Informationen zur TEI-Methodologie finden Sie in Anhang A.

## Konzept

Für die Studie griff Forrester auf ein 4-Stufen-Konzept zurück:

1. Forrester gruppierte alle Daten der bisherigen Forrester-Forschung zur Sanctuary-Lösung sowie zum Endpunktsicherheitsmarkt im Allgemeinen.



2. Forrester führte Gespräche mit Lumension Security-Mitarbeitern aus Marketing und Vertrieb, um sich umfassend mit dem potenziellen (oder angestrebten) Wertangebot der Sanctuary-Lösung vertraut zu machen.
3. Forrester führte fundierte, detaillierte Gespräche mit einem Unternehmen, bei dem derzeit die Sanctuary-Lösung von Lumension Security zum Einsatz kommt.
4. Forrester erstellte auf der Grundlage dieser Gespräche ein repräsentatives Finanzmodell. Dieses Modell wird im Abschnitt „TEI-Framework“ vorgestellt.

## Ergebnisse im Überblick

Die von Forrester geleitete Studie ergab folgende zentrale Ergebnisse:

- ROI.** Auf der Grundlage der Gespräche mit einem aktuellen Kunden erstellte Forrester ein TEI-Framework und eine entsprechende ROI-Analyse, aus der die Bereiche hervorgehen, in denen sich eine finanzielle Wirkung feststellen lässt. Aus Tabelle 1 lässt sich entnehmen, dass der risikogewichtete ROI für das Unternehmen bei 365 % liegt, mit einem Deckungspunkt (Amortisationszeit) von 19 Monaten ab Implementierung. Der Kostendeckungspunkt hätte früher erreicht werden können, wenn Application Control direkt im 1. Jahr zusammen mit Device Control und nicht erst im 2. Jahr implementiert worden wäre.
- Nutzen.** Wie bereits angesprochen, ließen sich zahlreiche Vorteile, die sich aus dem Einsatz des Sanctuary-Produkts ergaben, im Rahmen dieser Studie nur schwer quantifizieren. Für die ROI-Analyse wurde ausschließlich eine Quantifizierung des Nutzens in Verbindung mit folgenden Aspekten vorgenommen: Reduzierung des für die Durchsetzung der Endpunktsicherheit erforderlichen Headcount, Reduzierung von Arbeitsaufwand und Kosten für die Instandhaltung und Reparatur der Endbenutzer-Rechner und Reduzierung des Aufrüstungs- und Ersatzbedarfs für die Rechner. Der risikogewichtete gegenwärtige Nutzwert beläuft sich auf 632.966 US-\$ über einen Zeitraum von 4 Jahren.
- Kosten.** Die Implementierung von Sanctuary erfolgte in einem reibungslosen und schnellen Prozess. Insbesondere in Bezug auf Device Control war für den Kunden ein überaus geringer Implementierungsaufwand gegeben sowie nahezu kein Bedarf an professioneller Unterstützung. Darüber hinaus ging aus den Gesprächen hervor, dass für das Produkt nahezu kein laufender Support erforderlich ist. Damit beschränkt sich das Gros der Kosten auf die Lizenz- und Instandhaltungsgebühren. Die Kosten weisen derzeit einen risikogewichteten Gegenwartswert in Höhe von 136.040 US-\$ über einen Zeitraum von 4 Jahren auf.



Tabelle 1 zeigt den risikogewichteten Cashflow von JCL auf der Grundlage der im Rahmen der Gespräche gesammelten Daten und besonderen Gegebenheiten. Forrester hat diese Werte um das vorliegende Risiko berichtigt, sodass die potenzielle Unsicherheit bei der Schätzung der Kosten und des Nutzens einer Technologieinvestition berücksichtigt wird. Der risikogewichtete Wert soll eine konservative Schätzung ermöglichen, in die alle potenziellen Risikofaktoren einfließen, die sich zu einem späteren Zeitpunkt ggf. auf die ursprünglichen Kosten- und Nutzenschätzungen auswirken können. Eine detaillierte Erklärung zu den Risiken und Risikogewichtungen im Rahmen dieser Studie finden Sie im Abschnitt „Risiken“.

**Tabelle 1: ROI des Unternehmens, ursprünglich und risikogewichtet**

Übersicht über die Finanzergebnisse	Nicht gewichtet (Idealfall)	Risikogewichtet
ROI (vier Jahre)	372 %	365 %
Amortisationszeit*	16 Monate	19 Monate
Gesamtkosten für 4 Jahre (GW)	(140.384 US-\$)	(136.040 US-\$)
Gesamtnutzwert für 4 Jahre (GW)	662.092 US-\$	632.966 US-\$
Gesamtnettoeinsparungen für 4 Jahre (NGW)	521.709 US-\$	496.926 US-\$

\*Hinweis: Die Amortisationszeit wäre kürzer ausgefallen, wenn die Implementierung nicht über einen Zeitraum von zwei Jahren erfolgt wäre.

Quelle: Forrester Research, Inc.

## Wichtige Hinweise

Der Leser sollte stets folgende Grundvoraussetzungen im Auge behalten:

- Die Studie wurde von Lumension Security in Auftrag gegeben und von der Forrester Consulting-Gruppe realisiert.
- Lumension Security nahm eine Prüfung der Studie vor und übermittelte Forrester



zusätzliche Informationen und Kommentare, die Abfassung der Studie und deren Ergebnisse unterlagen jedoch der alleinigen Kontrolle von Forrester. Forrester untersagte und untersagt jegliche Änderungen an der Studie, die nicht mit den von Forrester gewonnenen Erkenntnissen übereinstimmen oder die Grundaussage und Bedeutung der Studie verschleiern.

- ▣ Der Name des Kunden für die Gespräche wurde von Lumension Security übermittelt.
- ▣ Forrester stellt keine Hypothesen in Bezug auf eine potenzielle Investitionsrendite (ROI) für andere Unternehmen auf. Forrester legt dem Leser nahe, für das mit dem Bericht bereitgestellte Framework eigene Schätzungen zu verwenden, um die Angemessenheit einer Investition in die Sanctuary-Lösung zu bestimmen.
- ▣ Diese Studie versteht sich keinesfalls als wettbewerbliche Produktanalyse.



## Sanctuary Application And Device Control:Einführung

Lumension Security zufolge ermöglicht Sanctuary ein einheitliches und umfassendes Policy Enforcement im Hinblick auf eine effiziente zentrale Verwaltung und Überwachung der Anwendungs- und Gerätenutzung, durch die ein Unternehmen proaktiv vor Datenbedrohungen wie Datenverlust, Malware und Spyware geschützt werden kann. In Sanctuary kommt der gesamte Funktionsumfang der bereits bewährten integrierten Module zur Anwendungs- und Gerätekontrolle zum Einsatz. Damit stattet Sanctuary Unternehmen mit einer Komplettlösung für das Endpunkt-Sicherheitsmanagement aus – und das über eine einzige Konsole. Daraus ergibt sich das Beste für beide Welten – IT-Administratoren erhalten erneut umfassende Kontrolle und Endbenutzer die benötigte Flexibilität.

- ▣ Sanctuary Application Control, die erste Sanctuary-Komponente, ermöglicht eine policybasierte Kontrolle der Anwendungsnutzung im Hinblick auf den Schutz der Endpunkte vor Malware, Spyware, Zero-Day-Bedrohungen und unerwünschter oder nicht lizenzierter Software. Durch den Rückgriff auf ein Whitelist-Konzept sorgt Sanctuary Application Control dafür, dass nur autorisierte Anwendungen in Netzwerken sowie auf Servern, Terminal Services-Servern, Thin-Clients, Laptops oder Desktops ausgeführt werden können. Die Ausführung nicht autorisierter Anwendungen wird kurzerhand verweigert.
- ▣ Sanctuary Device Control, die zweite Sanctuary-Komponente, ermöglicht eine policybasierte Kontrolle der Nutzung externer Geräte im Hinblick auf die Steuerung des ein- und abgehenden Datenflusses an den Endpunkten. Durch den Rückgriff auf ein Whitelist-Konzept sorgt Sanctuary Device Control dafür, dass nur autorisierte Geräte auf Netzwerke, Laptops, Thin-Clients oder Desktops zugreifen können. Der Zugriff auf nicht autorisierte Geräte wird kurzerhand verweigert.



## Analyse

Wie bereits in der kommentierten Zusammenfassung angesprochen, wandte Forrester für seine Studie ein mehrstufiges Konzept an, um die Wirkung der Implementierung von Sanctuary auf ein Unternehmen zu bewerten.

- ▣ Gespräche mit den Marketing- und Vertriebsmitarbeitern von Lumension Security
- ▣ Fundierte Gespräche mit einem Unternehmen, indem derzeit Sanctuary Application and Device Control zum Einsatz kommt
- ▣ Erarbeitung eines finanziellen Frameworks für die Implementierung von Sanctuary Application and Device Control

## Ergebnis der Gespräche: John C. Lincoln Hospitals

JCL ist eine gemeinschaftsbasierte, gemeinnützige Einrichtung zur Gesundheitspflege. Die Einrichtung umfasst zwei Krankenhäuser, mehrere Arztpraxen und zahlreiche öffentliche Sozialprogramme. Insgesamt beschäftigt die Einrichtung über 3.500 Mitarbeiter, darüber hinaus haben sich zusätzlich 1.400 Ärzte dem Netzwerk angeschlossen.

Als Sanctuary Device Control im Jahr 2005 implementiert wurde, standen den Mitarbeitern für ihre jeweilige Tätigkeit etwa 2.500 Rechner (Desktops und Laptops) zur Verfügung. Jeder Rechner stellte ein Endpunktsicherheitsrisiko dar, entweder hinsichtlich der Einschleusung von Malware (d. h. Viren, Key-Logger usw.) oder in Bezug auf Datenverlust. Die Verhinderung des Verlusts sensibler Informationen, wie Krankenblätter und ärztliche Aufzeichnungen, ist insbesondere angesichts der HIPAA-Vorgaben (Health Insurance Portability and Accountability Act von 1996) von grundlegender Bedeutung.

Hinzu kam die genehmigte Nutzung von ca. 750 Anwendungen. Die Gewährleistung der ordnungsgemäßen Installation dieser Anwendung und der Vermeidung möglicher Softwarekonflikte war für die IT-Mitarbeiter ein aufwändiges Unterfangen. Diese Aufgabe wurde durch die unzulässige Installation nicht genehmigter Anwendungen und Dateien zusätzlich erschwert, u. a. von Spielen, MP3-Dateien und Instant-Messaging-Programmen.

Aus den Gesprächen ergaben sich folgende Punkte, die entweder für die ROI-Analyse von Bedeutung waren oder für den Leser von Interesse sein könnten:

- ▣ Sanctuary wurde im Rahmen einer umfassenden Sicherheitsstrategie des Kunden implementiert, die ebenfalls einen Antivirus-Schutz umfasste. Das Unternehmen verwendet Gateway-Antivirus-Programme, Netzwerk-Firewalls und andere Technologien, die in der Regel unternehmensweit implementiert werden.
- ▣ Die Wahl des CIO von JCL, Rob Israel, fiel insbesondere deshalb auf Sanctuary, weil das Produkt eine Best-Practice-Lösung in einem bekannten Risikobereich darstellte, dem



Datenverlust. Der CIO hatte vom dramatischen Verlust sensibler Daten in anderen Unternehmen gelesen, u. a. der Veterans Administration, und wollte die bestmögliche Lösung bereitstellen, noch bevor auch JCL einen derartigen Verlust zu beklagen hätte. JCL war sich keiner Vorfälle in Verbindung mit Datenverlust innerhalb der Einrichtung bewusst, „wäre aber nicht unbedingt darüber informiert, wenn sich ein derartiger Vorfall ereignen würde“. Darüber hinaus war JCL davon überzeugt, dass durch die Implementierung von Sanctuary die Antwortzeiten beim Kundensupport um einiges verkürzt und grundlegende, periodische Supportaufgaben vollständig ausgegrenzt werden könnten.

- ▣ JCL hatte zwei Erfahrungen von geringfügiger Bedeutung gemacht, die dem Unternehmen den Bedarf an zusätzlichen Vorkehrungen zur Endpunktsicherheit verdeutlicht hatten:
  - 2004 wurde JCL Opfer des Slammer-Virus. Der Virus wurde höchstwahrscheinlich über eine Diskette eingeführt, die auf einem nicht gesicherten Rechner verwendet wurde. Das IT-Team reagierte prompt und effizient und konnte dadurch den Ausfall klinischer Systeme und missionskritischer Anwendungen verhindern. Der E-Mailaustausch wurde für etwa 8 Stunden unterbrochen und alle externen Internetverbindungen wurden deaktiviert. Die 25 IT-Experten arbeiteten die ganze Nacht, um den Betrieb der Systeme zu gewährleisten und zum Normalbetrieb zurückzukehren.
  - Kurze Zeit nach diesem Vorfall wurde in einem der Krankenhäuser ein Laptop gestohlen. Glücklicherweise war der Laptop brandneu, sodass keine sensiblen Informationen darauf gespeichert waren. Dennoch wurde dadurch erneut ersichtlich, wie wichtig eine umfassende Kontrolle über den jeweiligen Speicherort von Informationen und den Gerätezugriff der Benutzer war. Der Schutz kritischer Informationen erwies sich als wirklich ernst zu nehmende Angelegenheit.
  - Bei der Suche nach einer Lösung zur Kontrolle der Anwendungs- und Gerätenutzung zog der Kunde mehrere Anbieter in die nähere Auswahl. Er entschied sich letztendlich für Sanctuary, da ihn die Gesamtqualität der Lösung überzeugte und sich das Produkt durch eine „besonders einfache Implementierung und Administration“ auszeichnete.
- ▣ Die Implementierung von Sanctuary erwies sich als extrem einfacher Prozess, insbesondere in Bezug auf Device Control. Für die Implementierung von Device Control waren lediglich 3 Tage erforderlich, die nachfolgende Detailkonfiguration nahm etwa 1 Woche in Anspruch. Für Application Control wurden 2 Monate benötigt, in erster Linie für die Einrichtung von Anwendungskatalogen und die Beherrschung der detaillierten Parameter auf Patch- und Update-Ebene.
- ▣ Die Lernphase bis zur uneingeschränkten Nutzung sämtlicher Vorteile von Sanctuary war äußerst kurz. In Bezug auf Device Control wurden die angestrebten Vorteile fast unmittelbar realisiert. Die Vorteile von Application Control kamen nach etwa 3 Monaten umfassend zum Tragen.



- Die IT-Abteilung verfügte über detaillierte, schriftlich festgelegte Sicherheitsrichtlinien für die Gewährleistung der Endpunktsicherheit, insbesondere in Zusammenhang mit dem Anschluss nicht autorisierter Geräte, der Installation von Anwendungen und Dateien und der Ausführung von Informationen aus den Geschäftsräumen. Die Umsetzung dieser Richtlinien basierte jedoch in erster Linie auf dem Verantwortungsbewusstsein und der Arbeitsethik der Mitarbeiter sowie auf manuellen Prozessen für die Durchführung von Audits. Nach der Implementierung von Sanctuary kam ein automatisches Policy Enforcement zum Einsatz, durch das potenzielle Probleme noch vor ihrem Auftreten umgangen werden konnten.

## TEI-Framework

### EINFÜHRUNG

Ausgehend von den im Rahmen der fundierten Gespräche gesammelten Informationen hat Forrester für Unternehmen, die eine Implementierung von Sanctuary Application and Device Control in Betracht ziehen, ein TEI-Framework erstellt. Ziel dieses Frameworks ist die Identifizierung der Kosten, nutzbringenden Vorteile, Flexibilität und Risikofaktoren, die bei einem Investitionsbeschluss berücksichtigt werden müssen.

### ANNAHMEN FÜR DAS FRAMEWORK

In Tabelle 2 werden der für die Berechnungen der Gegenwarts- und Nettogegenwartswerte verwendete Diskontsatz und der Planungshorizont für die Finanzmodellierung aufgezeigt.

**Tabelle 2: Allgemeine Annahmen**

Ref	Allgemeine Annahmen	Wert
A1	Diskontsatz	10%
A2	Analysezeitraum	4 Jahre

Quelle: Forrester Research, Inc.

Unternehmen verwenden je nach ihrer aktuellen Umgebung in der Regel einen Diskontsatz zwischen 8 % und 16 %. Der Leser sollte auf jeden Fall Rücksprache mit der Finanzabteilung seines Unternehmens halten, um den auf sein Unternehmen am ehesten zutreffenden Diskontsatz zu bestimmen.

Als Analysedauer wurde ein Zeitraum von 4 Jahren gewählt, da Device Control im 1. Jahr und Application Control im 2. Jahr implementiert wurde. Innerhalb von 4 Jahren konnten sich alle



Vorteile in Verbindung mit beiden Implementierungen vollständig etablieren. In diesem Zusammenhang muss darauf hingewiesen werden, dass sich durch eine Implementierung beider Produkte Device und Application Control im 1. Jahr der Gesamtnutzen wesentlich früher bemerkbar gemacht hätte, woraus sich wiederum eine wesentlich kürzere Amortisationszeit ergeben hätte.

Zusätzlich zu den finanziellen Annahmen für die Cashflow-Analyse können Tabelle 3 die für die Analyse verwendeten gehaltsbezogenen Annahmen entnommen werden.

**Tabelle 3: Gehaltsspezifische Annahmen**

Ref	Messgröße	Berechnungswert	Wer
B1	Belastete Jahreskosten pro IT-Mitarbeiter (1. Jahr)	[Anstieg mit Inflation]	37.000 US-\$
B2	Arbeitstage pro Jahr		200
B3	Belastete Tageskosten pro IT-Mitarbeiter (1. Jahr)	(B1/B2)	185 US-\$

Quelle: Forrester Research, Inc.

## Kosten

Die Kosten für die Implementierung und Verwaltung von Sanctuary Application and Device Control umfassen die Planungs- und Implementierungskosten, die Lizenz- und die Instandhaltungsgebühren für die Software. Der größte Anteil der Kosten entfällt auf die ursprünglichen Lizenzgebühren. Für die Verwaltung von Sanctuary entstehen keine bedeutenden laufenden Kosten. Demgegenüber ergab sich aus der Implementierung von Sanctuary eine Reduzierung des Headcount für den Kunden, auf den im Abschnitt „Nutzen“ weiter unten noch genauer eingegangen werden.

### KOSTEN FÜR PLANUNG UND IMPLEMENTIERUNG: DEVICE CONTROL

Die IT-Abteilung brachte mehrere Monate damit zu, verschiedene Optionen in Übereinstimmung mit ihren Anforderungen in Sachen Endpunktsicherheit zu untersuchen. Diese Prüfung erfolgte auf Teilzeitbasis, sobald freie Arbeitszeit zur Verfügung stand. Im Anschluss an die Auswahl von Sanctuary wurde für die eigentliche Implementierung keine ganze Woche benötigt, etwa eine weitere Woche war für die Detailkonfiguration erforderlich.



Für das Hosting der Lösung wurde bereits vorhandene Hardware eingesetzt, sodass die Implementierungskosten einzig und allein aus den mit der Implementierung verbundenen Arbeitskosten bestehen. Die Gesamtarbeitskosten des Kunden für die Planung und Implementierung von Device Control entsprechen dem Erzeugnis aus der Anzahl von Mitarbeitern am Projekt, dem voll belasteten Gehalt pro Mitarbeiter pro Tag und der Anzahl der für das Projekt aufgewendeten Arbeitstage. Das voll belastete Gehalt pro Mitarbeiter der IT-Administration im 1. Jahr der Studie beläuft sich auf 37.000 US-\$. Ausgehend von 200 Arbeitstagen pro Jahr entspricht das belastete Tagesgehalt damit 185 US-\$. Daraus ergeben sich Gesamtkosten in Höhe von 3.700 US-\$.

**Tabelle 4: Gesamtkosten für die Planung und Implementierung von Device Control , nicht risikogewichtet**

REF	Messgröße	Berechnungswert	Wert
C1	Anzahl der Mitarbeiter*		2,0
C2	Voll belastete IT-Ressourcenkosten pro Tag		185 US-\$
C3	Arbeitstage pro Person		10,0
<b>Ct</b>	<b>Planungs- und Implementierungskosten: Device Control</b>	<b>(C1 * C2 * C3)</b>	<b>3.700 US-\$</b>

\*Nur ein Mitarbeiter war mit der eigentlichen Implementierung beschäftigt. Der zweite Mitarbeiter spiegelt den Aufwand für Forschung und Planung wider.

Quelle: Forrester Research, Inc.

#### **LIZENZGEBÜHREN: DEVICE CONTROL**

Die Sanctuary-Kosten basieren auf einer Lizenzierung pro Arbeitsplatz. Die in dieser Studie berücksichtigten Lizenzgebühren entsprechen dem um Mengenrabatte berichtigten Listenpreis. Device Control wurde im 1. Jahr dieser Studie implementiert.

Auf der Grundlage der Anzahl der erworbenen Device Control-Lizenzen und deren Bündelung mit Application Control entstanden für Device Control pro Arbeitsplatz Kosten in Höhe von 35 US-\$.



Der Kunde erwarb 1.000 Lizenzen für Device Control, wodurch sich ein Gesamtkostenbetrag von 35.000 US-\$ ergibt.

**Tabelle 5: Gesamtlizenzgebühren für Device Control, nicht risikogewichtet**

Ref	Messgröße	Berechnungswert	Wert
D1	Lizenzgebühren pro Arbeitsplatz – Device Control		35 US-\$
D2	Anzahl an Arbeitsplätzen		1.000
<b>Dt</b>	<b>Lizenzgebühren: Device Control</b>	<b>(D1 * D2)</b>	<b>35.000 US-\$</b>

Quelle: Forrester Research, Inc.

#### **KOSTEN FÜR PLANUNG UND IMPLEMENTIERUNG: APPLICATION CONTROL**

JCL unterzog Application Control bereits während der Implementierungsplanung von Device Control einer konkreten Prüfung. Da die IT-Abteilung jedoch mit verschiedenen anderen Projekten beschäftigt war, wurde die Implementierung von Application Control auf das folgende Jahr verschoben.

Die Implementierung von Application Control nahm in etwa 2 Monate in Anspruch. Die meiste Zeit wurde dabei auf die Einrichtung

von Anwendungskatalogen verwendet. Auf Patch- und Upgrade-Ebene des Katalogs wurden einige Schwierigkeiten angetroffen, diese konnten jedoch durch Rücksprachen mit Lumension Security und den betroffenen Anwendungsanbietern beseitigt werden. Der Kunde verfügte insgesamt über 750 genehmigte Anwendungen, die getestet und im Katalog hinzugefügt werden mussten.

Insgesamt wurden anderthalb Vollzeitäquivalente (VZÄ) über einen Zeitraum von 2 Monaten für die Forschung und Implementierung von Application Control aufgewendet. Das belastete Gesamtgehalt pro Tag im 2. Jahr der Studie entspricht einem Betrag von 192,40 US-\$. Anderthalb Mitarbeiter verbrachten jeweils 60 Tage mit der Implementierung, woraus sich Implementierungsgesamtkosten in Höhe von 17.316 US-\$ ergeben.

**Tabelle 6: Gesamtkosten für die Planung und Implementierung von Application Control , nicht risikogewichtet**

Red	Messgröße	Berechnungswert	Wert
E1	Anzahl der Mitarbeiter		1,5
E2	Voll belastete IT-Ressourcenkosten pro Tag		192,40 US-\$
E3	Tage		60,0
<b>Et</b>	<b>Planungs- und Implementierungskosten: Application Control</b>	<b>(E1 * E2 * E3)</b>	<b>17.316 US-\$</b>

Quelle: Forrester Research, Inc.

#### LIZENZGEBÜHREN: APPLICATION CONTROL

Die Lizenzgebühren pro Arbeitsplatz für Application Control belaufen sich unter Berücksichtigung des Lizenzvolumens und der Bündelung mit Device Control auf 23,33 US-\$ pro Arbeitsplatz. Der Kunde erwarb 3.000 Lizenzen, woraus sich Gesamtkosten in Höhe von 69.990 US-\$ ergeben.

Application Control wurde ein Jahr nach Device Control implementiert.

**Tabelle 7: Gesamtlizenzgebühren für Application Control, nicht risikogewichtet**



Ref	Messgröße	Berechnungswert	WERT
F1	Lizenzgebühren pro Arbeitsplatz: Application Control		23,33 US-\$
F2	Anzahl an Arbeitsplätzen		3.000
Ft	<b>Lizenzgebühren: Device Control</b>	<b>(F1 * F2 )</b>	<b>69.990 US-\$</b>

Quelle: Forrester Research, Inc.

#### **JÄHRLICHE KOSTEN FÜR DIE INSTANDHALTUNG: APPLICATION AND DEVICE CONTROL**

Auf der Grundlage des Gesamtwerts der Lizenzen fallen jährlich standardmäßig 15 % an Instandhaltungsgebühren an.

Die Instandhaltungsgebühren beginnen im auf den Erwerb folgenden Jahr, d. h. für Device Control im 2. Jahr und für Application Control im 3. Jahr.

#### **Tabelle 8: Gesamtinstandhaltungskosten, nicht risikogewichtet**



Ref	Messgröße	Berechnungswert	Anfänglich	Jahr 1	Jahr 2	Jahr 3	Jahr 4
G1	Vorjahr Lizenzgebühren	(= Dt + Ft)		0	35.000 US-\$	104.99 0 US-\$	104.99 0 US-\$
G2	Softwareinstandhaltung Prozentsatz		15%	15%	15%	15 %	15%
<b>Gt</b>	<b>Softwareinstandhaltungsggebühren</b>	<b>(G1 * G2)</b>			<b>5.250 US-\$</b>	<b>15.749 US-\$</b>	<b>15.749 US-\$</b>

Quelle: Forrester Research, Inc.

### GESAMTKOSTEN

Tabelle 9 vermittelt einen Überblick über die Gesamtkosten, die in Verbindung mit der Implementierung von Sanctuary Application and Device Control für den Kunden anfallen.

**Tabelle 9: Gesamtkosten für Sanctuary Application And Device Control, nicht risikogewichtet**

Ref	Kosten	Initial kosten	Jahr 1	Jahr 2	Jahr 3	Jahr 4	GW	INSG
Ct	Planungs- und Implementierungskosten: Device Control	3.700 US-\$					3.700 US-\$	3.700 US-\$
Dt	Lizenzgebühren: Device Control		35.000 US-\$				35.000 US-\$	31.818 US-\$
Et	Planungs- und Implementierungskosten: Application Control			17.316 US-\$			17.316 US-\$	14.311 US-\$
Ft	Lizenzgebühren: Application			69.99			69.990	63.627



	Control			0 US-\$			US-\$	US-\$
Gt	Softwareinstandhaltungsgebühren			5.250 US-\$	15.749 US-\$	15.749 US-\$	36.747 US-\$	26.927 US-\$
	<b>Insg</b>	<b>3.700 US-\$</b>	<b>35.000 US-\$</b>	<b>92.556 US-\$</b>	<b>15.749 US-\$</b>	<b>15.749 US-\$</b>	<b>162.753 US-\$</b>	<b>140.384 US-\$</b>

Quelle: Forrester Research, Inc.

## Nutzen

Der von Rob Israel, CIO von JCL, angestrebte und realisierte Nutzen übersteigt den in dieser ROI-Analyse quantifizierten Nutzen um einiges. Aus diesem Grund wird in diesem Abschnitt zunächst detailliert auf die Nutzenberechnungen im Rahmen der ROI-Analyse eingegangen, anschließend wird der qualitative Nutzen beschrieben, der in der ROI-Analyse nicht berücksichtigt wurde. Unter zahlreichen Gesichtspunkten ist der qualitative Nutzen von größerem Wert als der quantitative und sollte deshalb bei der Analyse der Investitionsrendite (ROI), die sich insgesamt in Verbindung mit der Sanctuary-Lösung ergibt, auf jeden Fall in Betracht gezogen werden.

### REDUZIERUNG DES IT-AUFWANDS FÜR DIE DURCHSETZUNG DER ENDPUNKTSICHERHEITSPOLICY

Vor der Implementierung von Sanctuary war für die Durchsetzung der Endpunktsicherheitsrichtlinien und die Behebung damit verbundener Probleme ein in hohem Grad manueller und höchst intensiver Arbeitsaufwand erforderlich. Durch die Implementierung von Sanctuary konnte der mit diesen Aufgaben betraute VZÄ-Headcount von 4,0 auf 1,5 reduziert werden. Darüber hinaus ließ sich ein weiteres Ansteigen des Headcount bei JCL umgehen.

Die Headcount-Reduzierung begann im 1. Jahr mit der Implementierung von Device Control. Im Folgenden wurde die Headcount-Reduzierung durch die Implementierung von Application Control weiter verstärkt, gleichzeitig konnte eine zukünftige Steigerung des Headcount vermieden werden. In diesem Zusammenhang sei darauf hingewiesen, dass die Arbeitskosten bei JCL unter denjenigen zahlreicher anderer Unternehmen liegen. Der Leser sollte deshalb die eigenen Arbeitskosten in das Modell aufnehmen, da der finanzielle Nutzen mit großer Wahrscheinlichkeit höher ausfällt als der in dieser Studie berechnete Wert.

**Tabelle 10: Gesamtreduzierung des IT-Headcount, nicht risikogewichtet**

Ref	Messgröße	Berechnungswert	Jahr 1	Jahr 2	Jahr 3	Jahr 4
H1	Anzahl an Mitarbeitern (gesichert)		0,5	1,0	2,5	3,5
H2	Belastete jährliche Gesamtkosten pro IT- Administrator		37.000 US-\$	38.480 US-\$	40.019 US-\$	41.620 US-\$
Ht	<b>Headcount-Reduzierung</b>	<b>(H1 * H2)</b>	<b>18.500 US-\$</b>	<b>38.480 US-\$</b>	<b>100.048 US-\$</b>	<b>145.670 US-\$</b>

Quelle: Forrester Research, Inc.

### REDUZIERUNG DER KOSTEN FÜR DAS RE-IMAGING DER RECHNER

Vor der Implementierung von Sanctuary verursachte die Instandhaltung der Rechner einen äußerst hohen manuellen Arbeitsaufwand. Nicht autorisierte Anwendungen und Dateien mussten entfernt, Anwendungskonflikte beseitigt, Malware entfernt werden usw. Mit Sanctuary wurde es kurzerhand unmöglich, derartige Anwendungen und Dateien auf einem Rechner zu installieren, wodurch sich die Anzahl der Rechner, für die jährliche Instandhaltungsarbeiten anfielen, grundlegend reduzieren ließ.

In Tabelle 11 wird die Reduzierung der pro Jahr instand zu haltenden Rechner berechnet. Dabei wird davon ausgegangen, dass für 15 % aller Rechner jedes Jahr Instandhaltungseingriffe erforderlich sind. Diese Grundannahme wird etwa proportional zur Reduzierung des für die Instandhaltung der Rechner benötigten Headcount reduziert.

### **Tabelle 11: Reduzierung der Anzahl an Rechnern mit Rückgriff auf Supportleistungen**



Ref	Messgröße	Berechnungswert	Jahr 1	Jahr 2	Jahr 3	Jahr 4
I1	Anzahl an Rechnern		2.500	3.000	3.700	3.885
I2	Prozentsatz der Rechner mit Supportbedarf		15 %	15 %	15 %	15 %
I3	Anzahl der Rechner mit Supportbedarf (Grundannahme)	(I1 * I2)	375	450	555	583
I4	Reduzierung des Prozentsatzes der Rechner mit Supportbedarf		5 %	15 %	40 %	50 %
It	<b>Reduzierte Anzahl an Rechnern mit Supportbedarf</b>	<b>(I3 * I4 [gerundet])</b>	<b>19</b>	<b>68</b>	<b>222</b>	<b>291</b>

Quelle: Forrester Research, Inc.

Von den in Anspruch genommenen Supportleistungen entfallen 30 % auf Re-Imaging. Die aktivitätsbasierten Gesamtkosten für das Re-Imaging eines Rechners belaufen sich auf 250 US-\$. Da in der obigen Analyse den Headcount-Einsparungen Rechnung getragen wird, wird dieser Wert reduziert, um eine Doppelzählung zu vermeiden. Forresters Schätzung zufolge sind 30 % der Gesamtkosten, bzw. 83,33 US-\$, auf den Arbeitsausfall der Benutzer aufgrund eines Instandhaltungseingriff an ihrem Rechner sowie auf andere nicht-IT-bezogene Arbeitskosten zurückzuführen.

**Tabelle 12: Reduzierung der Kosten für das Re-Imaging der Rechner, nicht risikogewichtet**



Ref	Messgröße	Berechnungswert	Jahr 1	Jahr 2	Jahr 3	Jahr 4
J1	Reduzierte Anzahl der Rechner mit Supportbedarf	( = It)	19	68	222	291
J2	Prozentualer Anteil des Re-Imaging an der Rechnerinstandhaltung		30 %	30 %	30 %	30 %
J3	Reduzierte Anzahl der Rechner mit Re-Imaging-Bedarf	(J1 * J2 [gerundet])	6,0	20,0	67,0	87,0
J4	Kosten für das Re-Imaging eines Rechners		83,33 US-\$	83,33 US-\$	83,33 US-\$	83,33 US-\$
Jt	<b>Reduzierte Kosten für das Rechner-Re-Imaging</b>	<b>(J3 * J4)</b>	<b>500 US-\$</b>	<b>1.667 US-\$</b>	<b>5.583 US-\$</b>	<b>7.250 US-\$</b>

Quelle: Forrester Research, Inc.

### REDUZIERUNG DER KOSTEN FÜR DIE AUFRÜSTUNG DER RECHNER

Zusätzlich zur Reduzierung der Kosten für das Re-Imaging der Rechner reduzierte sich die Anzahl an Rechnern, für die jährlich eine Aufrüstung vorgenommen werden musste. Eine Aufrüstung besteht in der Erweiterung des vorhandenen RAM. Da die Rechner nicht mit der Ausführung nicht autorisierter und speicherintensiver Anwendungen belastet wurden, boten sie ein Leistungsniveau, das den Arbeitsanforderungen durchaus gerecht wurde, und das ohne Installation zusätzlichen Speichers.

70 % der Supportanfragen von Rechnern, für die andernfalls ein Instandhaltungseingriff erforderlich wäre, betreffen eine Speichererweiterung. Die aktivitätsbezogenen Gesamtkosten für die Durchführung einer Aufrüstung beläuft sich auf 200 US-\$.

Auch dieser Wert wurde wieder reduziert, da die IT-Arbeitskomponente bereits im Nutzen der Headcount-Reduzierung weiter oben berücksichtigt wurde. Der Wert in Höhe von 100 US-\$



entspricht den Kosten des Zusatzspeichers, der Benutzerausfallzeiten und anderer anfallender Kosten.

**Tabelle 13: Reduzierung der Kosten für die Aufrüstung der Rechner, nicht risikogewichtet**

Ref	Messgröße	Berechnungswert	Jahr 1	Jahr 2	Jahr 3	Jahr 4
K1	Reduzierte Anzahl der Rechner mit Supportbedarf	(= It)	19	68	222	291
K2	Prozentualer Anteil der Aufrüstungen an der Rechnerinstandhaltung		70 %	70 %	70 %	70 %
K3	Reduzierte Anzahl an aufzurüstenden Rechnern	(L1 * L2 [gerundet])	13	48	155	204
K4	Kosten für die Aufrüstung eines Rechners		100 US-\$	100 US-\$	100 US-\$	100 US-\$
Kt	Reduzierte Kosten für die Aufrüstung der Rechner	(L3 * L4)	1.300 US-\$	4.800 US-\$	15.500 US-\$	20.400 US-\$

Quelle: Forrester Research, Inc.

### **REDUZIERUNG DER KOSTEN FÜR DEN AUSTAUSCH DER RECHNER**

Einer Schätzung des CIO zufolge konnte die Einrichtung des Gesundheitswesens nach der Realisierung sämtlicher Vorteile aus der Implementierung von Application and Device Control den Erwerb von jährlich 250 neuen Rechnern umgehen. Hierbei handelt es sich um den Austausch von Rechnern, die normalerweise ausrangiert werden müssen, da sie nicht zu reparieren sind oder für die die Reparaturkosten den Wiederbeschaffungspreis übersteigen. Da dies eine vollständige Abschreibung des Vermögenswerts und keine Erweiterung des Lebenszyklus bedeutet, wird in dieser ROI-Analyse der Gesamtwert des Rechners berücksichtigt.

**Tabelle 14: Reduzierung der Kosten für den Austausch der Rechner, nicht risikogewichtet**

Ref	Messgröße	Berechnungswert	Jahr 1	Jahr 2	Jahr 3	Jahr 4
L1	Reduzierte Anzahl der auszuwechselnden Rechner		0	100	250	250



L2	Kosten für den Austausch eines Rechners		900 US-\$	900 US-\$	900 US-\$	900 US-\$
Lt	<b>Reduzierte Kosten für den Rechneraustausch</b>	<b>(K1 * K2)</b>		<b>90.000 US-\$</b>	<b>225.000 US-\$</b>	<b>225.000 US-\$</b>

Quelle: Forrester Research, Inc.

### INSGESAMT QUANTIFIZIERTER NUTZEN

Tabelle 15 vermittelt einen Gesamtüberblick über sämtliche Vorteile, die bei JCL durch die Implementierung von Sanctuary Application and Device Control realisiert werden konnten.

**Tabelle 15: Gesamtnutzen von Sanctuary Application And Device Control, nicht risikogewichtet**

	Vorteile	Jahr 1	Jahr 2	Jahr 3	Jahr 4	INSG	Gesamtgegenwartswert
Ht	Headcount-Reduzierung	18.500 US-\$	38.480 US-\$	100.048 US-\$	145.670 US-\$	302.698 US-\$	223.282 US-\$
Jt	Reduzierte Kosten für das Re-Imaging der Rechner	500 US-\$	1.667 US-\$	5.583 US-\$	7.250 US-\$	15.000 US-\$	10.979 US-\$
Jt	Reduzierte Kosten für die Aufrüstung der Rechner	1.300 US-\$	4.800 US-\$	15.500 US-\$	20.400 US-\$	42.000 US-\$	30.728 US-\$
Lt	Reduzierte Kosten für den Austausch der Rechner	US-\$	90.000 US-\$	225.000 US-\$	225.000 US-\$	540.000 US-\$	397.104 US-\$
	<b>Insg</b>	<b>20.300 US-\$</b>	<b>134.947 US-\$</b>	<b>346.131 US-\$</b>	<b>398.320 US-\$</b>	<b>899.698 US-\$</b>	<b>662.092 US-\$</b>



Quelle: Forrester Research, Inc.

### **REDUZIERUNG DER SICHERHEITSRISIKEN: DATENVERLUST UND/ODER EINSCHLEUSUNG VON MALWARE**

Die Hauptmotivation des Kunden für die Implementierung von Sanctuary bestand in der Beseitigung der endpunktbezogenen Sicherheitsrisiken – Einführung von Malware und/oder Datenverlust. Dies entspricht den vorrangigen Beweggründen der meisten Sanctuary-Kunden. Die Quantifizierung der Sicherheitsrisiken und der damit verbundenen Kosten kann allerdings äußerst problematisch sein. Ein Unternehmen ist häufig nicht über die Entstehung eines Sicherheitslecks auf dem Laufenden, vor allem dann nicht, wenn es sich dabei um Datenverlust handelt. Wie bereits angesprochen, konnte sich der Kunde, der an dieser Studie teilgenommen hat, auf zwei Vorfälle in Verbindung mit der Endpunktsicherheit beziehen: 1) Infektion mit dem Slammer-Virus und 2) Diebstahl eines Laptops. In beiden Fällen waren die Auswirkungen nicht sonderlich dramatisch. Aber das bedeutet bei Weitem nicht, dass ein zukünftiger Vorfall nicht wesentlich schwerwiegendere Folgen mit sich bringen kann. Aus diesem Grund entschloss sich der Kunde zur Implementierung einer ganzen Reihe von Sicherheitslösungen mit Sanctuary als einer zentralen Komponente.

Für die Schätzung der Kosten eines Sicherheitseinbruchs wird häufig auf den Bericht der CSI/FBI-Studie zu Computerverbrechen und -sicherheit aus dem Jahr 2006 Bezug genommen<sup>1</sup>. Dieser Umfrage zufolge beliefen sich die durchschnittlichen Kosten pro Sicherheitsleck auf 167.713 US-\$. Das entspricht einem Rückgang von 18 % im Vergleich zum Vorjahr. Einer der wenigen Bereiche, in denen ein Anstieg der Kosten von 2005 bis 2006 zu verzeichnen war, betraf den Verlust in Verbindung mit mobiler Hardware, d. h. Laptops oder USB-Laufwerken. Diese Kosten erfuhren eine Steigerung von über 50 % auf 30.057 US-\$ pro Vorfall. Diese Entwicklung ist vorwiegend auf die mit einem derartigen Verlust einhergehenden Folgen zurückzuführen und nicht auf den Eigenwert der Hardware.

Eine im April 2007 veröffentlichte Studie von Forrester zur Berechnung der Kosten eines Sicherheitslecks<sup>2</sup> stellt Messzahlen und -größen für die Berechnung der potenziellen Kosten eines Sicherheitslecks für ein vorgegebenes Unternehmen bereit. In der Studie werden die „Kosten pro Datensatz“ für drei verschiedene Unternehmensprofile berechnet:

 Zweitrangiges Sicherheitsleck in einem Unternehmen ohne brancheninterne Regelungen

---

<sup>1</sup> „2006 CSI/FBI COMPUTER CRIME AND SECURITY SURVEY“. LAWRENCE A. GORDON, ET AL., COMPUTER SECURITY INSTITUTE, 2006

<sup>2</sup> „CALCULATING THE COST OF A SECURITY BREACH“. KHALID KARK, ET AL., FORRESTER RESEARCH, APRIL 2007



(90 US-\$)

- ▣ Zweitrangiges Sicherheitsleck in einem Unternehmen mit brancheninternen Regelungen (155 US-\$)
- ▣ Hochrangiges Sicherheitsleck in einem Unternehmen mit umfassender brancheninterner Regelung (305 US-\$)

Für einen bedeutenden Leistungsanbieter im Bereich Gesundheitspflege – einer hoch regulierten Branche – bringt ein Sicherheitseinbruch mit großer Wahrscheinlichkeit schwerwiegende Folgen mit sich. Angesichts der tausenden an gespeicherten Patientendaten würde sich aus einem Sicherheitsleck bei Kosten in Höhe von 305 US-\$ pro Datensatz für den Kunden ein beträchtlicher Kostenbetrag ergeben.

### **VERBESSERUNG DER IT-SERVICELEISTUNGEN FÜR DAS UNTERNEHMEN**

Dem Kunden gelang die Bereitstellung von 2,5 VZÄ aus der IT-Abteilung für Projekte mit größerem strategischen Wert und höherer Wertsteigerung. Daraus ergab sich eine Verbesserung des Serviceangebots für das gesamte Unternehmen sowie ein insgesamt besseres Image der IT-Abteilung, die mehr Serviceleistungen bei reduzierter Reaktionszeit erbringen konnte.

Darüber hinaus konnte gleichzeitig die Lebensqualität der IT-Teammitglieder verbessert werden. Sie werden heute wesentlich seltener zu Notfällen in späten Nachstunden gerufen, können sich mehr auf Aktivitäten mit höherem strategischen Wert konzentrieren und ihren Teil zum globalen Erfolg der Gesundheitsversorgung beitragen.

### **STEIGERUNG DER BENUTZERPRODUKTIVITÄT**

Die Produktivität der Benutzer konnte aus zwei Gründen verbessert werden. Zum einen wurde die Betriebszeit der Rechner der Endbenutzer erhöht. Zum anderen benutzten die Mitarbeiter bei JCL, wie in den meisten anderen Unternehmen auch, ihren Arbeitsrechner für Aktivitäten ohne jeden Bezug zu ihrer Arbeit. Dieser Missbrauch erstreckte sich von der Anzeige von Videoclips bis hin zu privaten Schreibarbeiten im Nachtdienst. Durch die Verhinderung der Nutzung nicht autorisierter Anwendungen und Dateien auf den Geschäftsrechnern sind die Mitarbeiter nicht mehr in der Lage, bei der Arbeit privaten Beschäftigungen nachzugehen. Die dadurch eingesparte Arbeitszeit wird natürlich nicht vollständig in zusätzliche produktive Arbeit umgesetzt, aber es hat sich daraus ein bedeutender, nicht quantifizierter Nutzen für den Kunden ergeben.

## **Risiken**

Der Risikofaktor bildet die dritte Komponente im TEI-Modell und fungiert als Filter für die Erfassung der Unsicherheit bei der Schätzung von Kosten und Nutzen. Wenn ein um das Risiko berichteter ROI nach wie vor auf einen beeindruckenden Business Case verweist, steigt das Vertrauen in einen wahrscheinlichen Erfolg der Investition, da die das Projekt bedrohenden



Risiken in Betracht gezogen und quantifiziert wurden. Die risikogewichteten Zahlen sollten als „realistische“ Erwartungen angesehen werden, da sie den erwarteten Wert unter Berücksichtigung der Risiken vermitteln. Risiken beeinflussen im Allgemeinen den Nutzen in Form einer Reduzierung und die Kosten in Form einer Erhöhung der ursprünglichen Schätzungen.

In dieser Studie wurden vorrangig folgende Risiken berücksichtigt:

- ▣ Das Risiko, dass die Implementierungskosten aufgrund höherer voll belasteter Kosten für einen IT-Mitarbeiter höher ausfallen könnten.
- ▣ Das Risiko, dass ein Unternehmen ggf. nicht in der Lage sein könnte, durch die Vermeidung von Kosten für den Erwerb neuer Rechner ausreichend Geld einzusparen.

Alle anderen Risiken wurden als „niedrig“ oder „nicht existent“ eingestuft.

Das TEI-Modell greift für die Berechnung der risikogewichteten Werte auf eine Verteilungsmethode mit dreieckiger Struktur zurück. Im Hinblick auf eine Verteilung müssen zunächst die niedrigen, die wahrscheinlichsten und die hohen Werte geschätzt werden, die in der aktuellen Umgebung auftreten könnten. Der „wahrscheinlichste“ Wert wird immer mit 100 % eingestuft. Der risikogewichtete Wert ist das Mittel der Verteilung dieser Punkte.

Den Kosten für die Planung und Implementierung von Application Control wird z. B. ein „hohes“ Risiko zugeordnet. Diese Risikostufe wurde gewählt, da der Kunde niedrigere belastete Gesamtkosten für eine IT-Ressource aufweist als zahlreiche andere Unternehmen. Damit ist es überaus wahrscheinlich, dass ein Leser mit höheren Implementierungskosten konfrontiert wird. Die ursprünglich geschätzten Kosten betragen 17.316 US-\$. Für die Berechnung der risikogewichteten Kosten wurde das „wahrscheinlichste“ Szenario auf 100 % der Kosten gesetzt, dem „hohen“ Szenario wurden 125 % der Kosten und dem „niedrigen“ Szenario 100 % der Kosten zugeordnet. Das gerundete Mittel dieser drei Werte beträgt 108 %. Daraus ergeben sich in den risikogewichteten Tabellen Kosten in Höhe von 18.701 US-\$ bzw. 108 % von 17.316 US-\$.

Die Lizenzgebühren wiederum weisen eine Risikostufe von „nicht existent“ auf. Da der Listenpreis mit zutreffenden Mengenrabatten verwendet wird, kann der Leser davon ausgehen, dass er einen ähnlichen Preis erhalten wird. Damit ist mit dieser Schätzung kein Risiko verbunden.

Die nachstehenden Tabellen zeigen die Werte, die bei einer Risikogewichtung angesichts der Unsicherheit bei den Kosten- und Nutzenschätzungen verwendet werden. Dem Leser wird nahe gelegt, die eigenen Risikobereiche auf der Grundlage seines Vertrauens in die Kosten- und Nutzenschätzungen anzuwenden.

#### **Tabelle 16: Risikogewichtung der Kosten**



Ref	Risikogewichtung der Kosten	Niedrig	Am wahrscheinlichsten	Hoch	Risikogewichtet
M1	Planungs- und Implementierungskosten: Device Control (Hoch)	100 %	100 %	125 %	108 %
M2	Lizenzgebühren: Device Control (Nicht existent)	100 %	100 %	100%	100%
M3	Planungs- und Implementierungskosten: Application Control (Hoch)	100 %	100 %	125 %	108 %
M4	Lizenzgebühren: Application Control (Nicht existent)	100 %	100 %	100%	100%
M5	Softwareinstandhaltungsgebühren (Nicht existent)	100 %	100 %	100 %	100 %

Quelle: Forrester Research, Inc.

**Tabelle 17: Risikogewichtung des Nutzens**

Ref	Risikogewichtung des Nutzens	Niedrig	Am wahrscheinlichsten	Hoch	Risikogewichtet
N1	Headcount-Reduzierung (Niedrig)	90 %	100 %	105 %	98 %
N2	Reduzierung der Kosten für das Re-Imaging der Rechner (Niedrig)	90 %	100 %	105 %	98 %



N3	Reduzierung der Kosten für die Aufrüstung der Rechner (Niedrig)	90 %	100 %	105 %	98 %
N4	Reduzierung der Kosten für den Austausch der Rechner (Mittel)	80%	100 %	103%	94%

Quelle: Forrester Research, Inc.

## Flexibilität

Der Definition von Forrester zufolge bedeutet Flexibilität eine Investition in zusätzliche Kapazität bzw. in die Fähigkeit, einen Geschäftsvorteil für weitere Investitionen in der Zukunft zu realisieren. Bei der Bewertung für ein spezifisches Projekt kann Flexibilität ebenfalls quantifiziert werden (detaillierte Beschreibung in Anhang A).

Im Rahmen dieser Studie greift der Kunde auf keine zusätzlichen Serviceleistungen außerhalb der ursprünglichen Lizenzen zurück, auch liegen keine Pläne für einen derartigen Rückgriff in nächster Zukunft vor. Aus diesem Grund ergibt sich die vom Kunden erzielte Flexibilität aus dem Sicherheitskonzept von Lumension Security.

Da die anwendungs- und gerätespezifischen Genehmigungen auf der Grundlage einer entsprechenden Whitelist erfolgen, verfügt der Kunde über ein zufrieden stellendes Sicherheitsniveau in Bezug auf zukünftige, unbekannte Bedrohungen der Endpunktsicherheit.

### TEI-FRAMEWORK: ZUSAMMENFASSUNG

Unter Rückgriff auf das zuvor aufgestellte finanzielle Framework können die Ergebnisse der Abschnitte über Kosten, Nutzen und Risiken zur Bestimmung der Investitionsrendite (ROI), des Nettogegenwartswerts und der Amortisationszeit herangezogen werden. Tabellen 18 und 19 zeigen die risikogewichteten Kosten und Nutzwerte, wobei die im Abschnitt „Risiken“ angeführte Methode der Risikogewichtung sowie die Werte der Tabellen 16 und 17 bis zu den Zahlen in den Tabellen 9 und 15 verwendet werden.

#### **Tabelle 18: Risikogewichtete Kosten**



Ref	Gesamtkosten, risikogewichtet	Anfänglich	Jahr 1	Jahr 2	Jahr 3	Jahr 4	Gesamt -	gegenwartswert
L1	Planungs- und Implementierungskosten: Device Control	3.996 US-\$					3.996 US-\$	3.996 US-\$
L2	Lizenzgebühren: Device Control		35.000 US-\$				35.000 US-\$	31.818 US-\$
L3	Planungs- und Implementierungskosten: Application Control			18.701 US-\$			18.701 US-\$	15.456 US-\$
L4	Lizenzgebühren: Application Control			69.990 US-\$			69.990 US-\$	57.843 US-\$
L5	Softwareinstandhaltunggebühren (Jährlich)			5.250 US-\$	15.749 US-\$	15.749 US-\$	36.747 US-\$	26.927 US-\$
Lt	Insg	3.996 US-\$	35.000 US-\$	93.941 US-\$	15.749 US-\$	15.749 US-\$	164.434 US-\$	136.040 US-\$

Quelle: Forrester Research, Inc.

**Tabelle 19: Risikogewichteter Nutzen**

Ref	Gesamtnutzen, risikogewichtet	Jahr 1	Jahr 2	Jahr 3	Jahr 4	Gesamt -	gegenwartswert
M1	Headcount-Reduzierung	18.130 US-\$	37.710 US-\$	98.047 US-\$	142.756 US-\$	296.644 US-\$	218.816 US-\$
M2	Reduzierte Kosten für das Re-Imaging der Rechner	490 US-\$	1.633 US-\$	5.472 US-\$	7.105 US-\$	14.700 US-\$	10.759 US-\$



M3	Reduzierte Kosten für die Aufrüstung der Rechner	1.274 US-\$	4.704 US-\$	15.190 US-\$	19.992 US-\$	41.160 US-\$	30.113 US-\$
M4	Reduzierte Kosten für den Austausch der Rechner	US-\$	84.600 US-\$	211.500 US-\$	211.500 US-\$	507.600 US-\$	373.278 US-\$
	Insg	19.894 US-\$	128.648 US-\$	330.209 US-\$	381.353 US-\$	860.104 US-\$	632.966 US-\$

Quelle: Forrester Research, Inc.

Es muss darauf hingewiesen werden, dass die im TEI-Framework verwendeten Werte ausnahmslos auf den fundierten Gesprächen mit einem bestimmten Unternehmen basieren. Forrester stellt keine Hypothesen in Bezug auf eine potenzielle Investitionsrendite für andere Unternehmen auf. Forrester legt dem Leser nahe, für das mit dem Bericht bereitgestellte Framework eigene Schätzungen zu verwenden, um die erwartete finanzielle Wirkung einer Implementierung von Sanctuary Application and Device Control zu bestimmen.



## Bilanz der Studie

Aus den fundierten Gesprächen zwischen Forrester und einem Kunden von Sanctuary Application and Device Control, den John C. Lincoln Hospitals, ergaben sich folgende Feststellungen:

- ☐ Unternehmen können in etlicher Hinsicht einen quantitativen Nutzen verbuchen: Reduzierung der Kosten für die Verwaltung der Endpunktsicherheit, Reduzierung der Kosten für die Instandhaltung und Aufrüstung der Rechner und Umgehung der Kosten für den Erwerb neuer Rechner.
- ☐ Durch den Einsatz von Sanctuary lässt sich darüber hinaus das Risiko einer Einführung von Malware und eines Datenverlusts eingrenzen. Zu weiteren Vorteilen gehört eine unternehmensweiten Verbesserung des Images der IT-Abteilung und eine gesteigerte Arbeitszufriedenheit unter den IT-Mitarbeitern.

Die in dieser Studie angeführte Finanzanalyse stellt eine mögliche Bewertung der potenziellen Wertsteigerung dar, die sich mit Sanctuary Application and Device Control in einem Unternehmen erzielen lässt. Auf der Grundlage der bei einem Kunden gesammelten Informationen hat Forrester einen risikogewichteten ROI über 4 Jahre von 365 % mit einer Amortisationszeit von 1,6 Jahren berechnet. Hierbei muss herausgestellt werden, dass die Amortisationszeit kürzer ausgefallen wäre, wenn der Kunde beide Produktkomponenten, Device and Application Control, bereits im 1. Jahr implementiert hätte. Alle definitiven Schätzungen sind um die gegebenen Risiken berichtigt und tragen damit der potenziellen Unsicherheit bei der Berechnung von Kosten und Nutzen Rechnung.

**Tabelle 20: ROI, ursprünglich und risikogewichtet**

Übersicht über die Finanzergebnisse	Ungewichtet (Idealfall)	Risikogewichtet
ROI (vier Jahre)	372 %	365 %
Amortisationszeit*	16 Monate	19 Monate
Gesamtkosten für 4 Jahre (GW)	(140.384 US-\$)	(136.040 US-\$)
Gesamtnutzwert für 4 Jahre (GW)	662.092 US-\$	632.966 US-\$
Gesamtnettoeinsparungen für 4 Jahre (NGW)	521.709 US-\$	496.926 US-\$



\*Hinweis: Die Amortisationszeit wäre kürzer ausgefallen, wenn die Implementierung nicht über einen Zeitraum von zwei Jahren erfolgt wäre.

Quelle: Forrester Research, Inc.

## Anhang A: Total Economic Impact™ im Überblick

Total Economic Impact ist eine von Forrester Research entwickelte Methodologie zur Unterstützung von Unternehmen bei der Entscheidungsfindung im Technologiebereich sowie von Anbietern bei der Präsentation des Wertangebots ihrer Produkte und Dienstleistungen. Die TEI-Methodologie ermöglicht die Illustration, den Nachweis und die Realisierung des erfassbaren Werts von IT-Initiativen gegenüber der Unternehmensleitung und anderen Teilhabern und Beteiligten eines Unternehmens.

Die TEI-Methodologie setzt sich aus vier Komponenten zusammen, die eine Bewertung des Investitionswerts ermöglichen: Nutzen, Kosten, Risiken und Flexibilität. Für diese Analyse wurde die Wirkung der Flexibilität nicht quantifiziert.

### Nutzen

Der Nutzen bezieht sich auf den dem Unternehmen bzw. der Abteilung des Benutzers — IT und/oder Geschäftseinheit — durch das betroffene Produkt oder Projekt bereitgestellten Mehrwert. Häufig wird bei der Begründung des Erwerbs eines Produkts oder der Durchführung eines Projekts der Schwerpunkt ausschließlich auf IT-Kosten und Kostenreduzierung gelegt. Dabei bleibt wenig Spielraum für die Analyse der Wirkung der Technologie auf das gesamte Unternehmen.

Bei der TEI-Methodologie und dem sich daraus ergebenden Finanzmodell wird der Messung des Nutzens und der Messung der Kosten ein gleichbedeutender Stellenwert eingeräumt, sodass die Auswirkungen der Technologie auf die gesamte Geschäftsaktivität umfassend geprüft werden können. Die Berechnung des geschätzten Nutzens setzt einen klaren Dialog mit dem Unternehmen des Benutzers voraus, damit der spezifische realisierte Wert erfasst werden kann. Darüber hinaus fordert Forrester eine übersichtliche Buchführung mit konkreter Integration der Messung und des Nachweises des geschätzten Nutzens nach Abschluss des Projekts. Dadurch kann sichergestellt werden, dass die Nutzenschätzung direkt mit der Saldozeile verknüpft wird.

### Kosten

Die Kosten beziehen sich auf die für eine Realisierung des Werts bzw. Nutzens des vorgelegten Projekts erforderliche Investition.

Die IT-Abteilungen bzw. betroffenen Geschäftseinheiten können Kosten in Bezug auf voll belastete Arbeitskräfte, Vertragsnehmer oder Material vorbringen. Die Kosten umfassen sämtliche



Investitionen und Ausgaben, die für die Umsetzung des vorgegebenen Mehrwerts erforderlich sind. In der TEI-Kostenkategorie werden darüber hinaus auch inkrementale Kosten in Bezug auf die vorhandene Umgebung für laufende Kosten in Zusammenhang mit der Lösung erfasst. Sämtliche Kosten müssen in Bezug zu dem erzielten Nutzen gesetzt werden.

## Risiken

Ein Risiko misst die Unsicherheit bei den Nutzen- und Kostenschätzungen in Verbindung mit der Investition. Für die Messung der Unsicherheit sind zwei Aspekte zu berücksichtigen: Die Wahrscheinlichkeit, dass die Kosten- und Nutzenschätzungen den ursprünglichen Prognosen gerecht werden, und die Wahrscheinlichkeit, dass die Schätzungen über einen längeren Zeitraum hinweg gemessen und verwaltet werden.

TEI wendet auf die eingegebenen Werte eine Wahrscheinlichkeitsdichtefunktion an, bekannt unter der Bezeichnung „Dreiecksverteilung“. Dabei werden jeweils mindestens drei Werte berechnet, um eine Schätzung des zu Grunde liegenden Wertebereichs für Kosten und Nutzen vornehmen zu können.

## Flexibilität

In der TEI-Methodologie bildet der direkte Nutzen einen Teil des Investitionswerts. Direkter Nutzen kann vorrangig zur Rechtfertigung eines Projekts herangezogen werden, allerdings sollten Unternehmen Forrester zufolge in der Lage sein, auch den strategischen Wert einer Investition zu messen. Flexibilität bedeutet den Wert, der für zukünftige, zusätzliche Investitionen auf der Grundlage der ursprünglich getätigten Investition erzielt werden kann. So kann durch eine Investition in eine unternehmensweite Aufrüstung einer Büroproduktivitätssuite eine potenzielle Steigerung der Standardisierungsniveaus (zur Effizienzsteigerung) sowie eine Reduzierung der Lizenzierungskosten erzielt werden.

Allerdings kann sich auch eine integrierte Kollaborationsfunktion in einer gesteigerten Mitarbeiterproduktivität ausdrücken, wenn sie aktiviert wird. Die Kollaboration kann jedoch nur in Verbindung mit einer zusätzlichen Investition in Schulungen zu einem späteren Zeitpunkt genutzt werden. Dennoch weist die Möglichkeit zur Erfassung dieses Nutzens einen Gegenwartswert auf, der geschätzt werden kann. Dieser Wert wird von der TEI-Flexibilitätskomponente erfasst.

## Anhang B: Glossar

**Diskontsatz:** Der in Cashflow-Analysen verwendete Zinssatz zur Berücksichtigung des Zeitwerts von Geld. Zwar gibt die Zentralbank einen Diskontsatz vor, Unternehmen legen jedoch häufig einen Diskontsatz in Abhängigkeit von ihrer Geschäfts- und Investitionsumgebung fest. Forrester geht für diese Analyse von einem jährlichem Diskontsatz in Höhe von 10 % aus. Unternehmen



verwenden je nach ihrer aktuellen Umgebung in der Regel einen Diskontsatz zwischen 8 % und 16 %. Der Leser sollte auf jeden Fall Rücksprache mit seinem Unternehmen halten, um den auf seine Umgebung am ehesten zutreffenden Diskontsatz zu bestimmen.

**Nettgegenwartswert (NGW):** Der aktuelle oder Gegenwartswert zukünftiger (diskontierter) Netto-Cashflows unter Berücksichtigung eines vorgegebenen Zinssatzes (Diskontsatz). Ein positiver Projekt-NGW verweist im Normalfall darauf, dass eine Investition getätigt werden sollte, sofern nicht andere Projekte mit höherem NGW vorhanden sind.

**Gegenwartswert (GW):** Der aktuelle oder Gegenwartswert geschätzter (diskontierter) Kosten und Nutzen unter Berücksichtigung eines vorgegebenen Zinssatzes (Diskontsatz). Der GW von Kosten und Nutzen fließt in den Nettogesamtgegenwartswert der Cashflows ein.

**Amortisationszeit:** Der Kostendeckungspunkt bzw. die Gewinnschwelle für eine Investition. Der Zeitpunkt, zu dem der Nettogewinn (Umsatz minus Kosten) die ursprüngliche Investition bzw. die ursprünglichen Kosten deckt.

**Investitionsrendite oder Return On Investment (ROI):** Eine Messung der erwarteten Rendite eines Projekts in Prozentangaben. Der ROI wird durch Teilung des Nettogewinns (Umsatz minus Kosten) durch die Kosten berechnet.

### **ANMERKUNG ZU DEN CASHFLOW-TABELLEN**

Nachstehend eine Anmerkung zu den in dieser Studie enthaltenen Cashflow-Tabellen (siehe Beispieltabelle unten).

Die Spalte mit der ursprünglichen Investition enthält die zum „Zeitpunkt 0“ oder zu Beginn des 1. Jahres aufgetretenen Kosten.

Diese Kosten werden nicht diskontiert. Alle anderen Cashflows in den Jahren 1 bis einschließlich 4 werden unter Rückgriff auf den in Tabelle 2 ausgewiesenen Diskontsatz am Jahresende diskontiert. Für jede Schätzung von Gesamtkosten und –nutzen wird ein Gegenwartswert (GW) berechnet. Die Berechnung des Nettgegenwartswerts (NGW) erfolgt erst in den Übersichtstabellen und verweist auf die Summe der ursprünglichen Investition und der diskontierten Cashflows in jedem Jahr.

Beispieltabelle



Ref.	Kategorie	Berechnung	Urspr. Kosten	Jahr 1	Jahr 2	Jahr 3	Insg.

Quelle: Forrester Research, Inc.



**Lumension Security**

15880 N. Greenway-Hayden Loop, Suite 100

Scottsdale, AZ 85260

[www.lumension.com](http://www.lumension.com)