A Forrester Total Economic Impact™ Study

Commissioned By

Cylance

Project Director:
Anish Shah

October 2016

The Total Economic Impact™ Of Cylance

Cost Savings And Business Benefits Enabled By CylancePROTECT® + ThreatZero™

FORRESTER®

Table Of Contents

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®

Executive Summary

> **"The State County Government and I as the Chief Information Security Officer are extremely proud of our zero downtime record from any cyber-related attack. Cylance provides us with the right endpoint solution that offers the great detection and block rate of malware attacks that our citizens expect from us."**
>
> **— Chief Information Security Officer, Large State County in the U.S.**

Cylance commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying its advanced threat protection solution, CylancePROTECT®, and its deployment and configuration services, ThreatZero™. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of CylancePROTECT® + ThreatZero™ on their organizations, to leverage advanced cybersecurity and antivirus protection solutions to win, serve, and retain customers.

To better understand the benefits, costs, and risks associated with an investment in Cylance, Forrester interviewed the Chief Information Security Officer for a Large State County Government who has over a year of experience using CylancePROTECT® + ThreatZero™. Cylance's solution is a new-generation, predictive, cybersecurity, and malware prevention solution that leverages artificial intelligence to prevent malware from executing on endpoints in real time. This is usually implemented with ThreatZero™. ThreatZero™ is a continuous professional service program rendered by Cylance to users of CylancePROTECT® that holds their hands through the planning, implementation, integration, and ongoing optimization of the solution. This often includes end user education, training, and support to totally eliminate endpoint threats and incidents.

Prior to investing in Cylance, the State County had used other cybersecurity and endpoint security solutions. However, the process to mitigate threats was highly manual, which put a lot of burden on its internal IT and security resources. Additionally, previous solutions failed to prevent attacks on the system in a predictive and repeatable manner, which led to reimaging of endpoints. With CylancePROTECT® + ThreatZero™, the organization was able to reduce security breaches to almost zero, catching malware before it gained access to public records. This significantly reduced costs of remediation/reimaging and incidence response and boosted IT and security employees' productivity.

CYLANCE SIGNIFICANTLY REDUCES THE RISK OF SECURITY BREACHES AND IMPROVES IT AND SECURITY FTE PRODUCTIVITY FOR A LARGE STATE COUNTY IN THE U.S.

Our interview with a Large State County and subsequent financial analysis found that the organization experienced the risk-adjusted ROI, benefits, and costs shown in Figure 1.[1] See Appendix A for a description of the interviewed organization.

The analysis points to benefits of $7,699,716 versus costs of $2,195,721 over three years. This adds up to a net present value (NPV) of $5,503,996 over the three-year period covered in the study. The quantified benefits include cost avoidance due to preventive and real-time detection of incidents before they can cause harm, reduced endpoint reimaging and remediation costs, and IT and security full-time equivalent (FTE) productivity.

FIGURE 1
Financial Summary Showing Three-Year Risk-Adjusted Results

Source: Forrester Research, Inc.

Benefits. Large State County experienced the following risk-adjusted benefits:

- **Yearly cost savings of $2.3 million due to reduced incidence of zero-day threats and data breaches.** The State County reported almost perfect malware detection and catch rates since its investment in CylancePROTECT®. The solution reduced the possibility of having a data breach by almost 99%, for the State County's confidential, high-value information across all of its 20,000 customer records.
- **Over $260,000 in cost savings related to remediating/reimaging systems.** Prior to the implementation of Cylance, the State County incurred significant costs in terms of employee and end user time reimaging machines that had been compromised due to malicious software. This was reduced by 98% following the introduction of Cylance, saving the organization over $260,000 across three years.
- **Improved productivity for IT, network, and security FTEs of 3 –year present value of $1.8 million.** With its legacy antivirus protection solution, the State County dedicated a number of IT and security employees (security engineers, network engineers, and security analysts) to carry out a continuous process of chasing down malicious software and resolving issues in a semi manual process. Cylance reduced the time needed to manage the cybersecurity process significantly, helping the IT and security employees to be 40% more productive, focusing on other tasks that brought incremental value to the State County's security infrastructure.
- **Avoidance of hardware and memory costs.** Although this benefit was not quantified in the study or by the county, the organization noted that Cylance only required a fraction of the memory capacity that was needed to run its legacy solution. Furthermore, Cylance had such minimal memory space requirements that the Large State County could run the solution optimally on all its endpoints without additional hardware purchases. In addition, The County realized that it could remove excess servers when it deleted its legacy antivirus solution. As a result, it enjoyed significant cost savings related to hardware purchases to run the new solution.

> *"Cylance provides us with a holistic security solution. Its technology uses mathematical algorithms to identify good traffic and proactively finds advanced threats, viruses, worms, Trojans, and malware."*
>
> — Chief Information Security Officer, Large State County in the U.S.

Costs. Large State County experienced the following risk-adjusted costs:

- **Cylance license and support cost of $846,900, or $48 per user per year.** These are the yearly license costs paid for CylancePROTECT® licenses for 17,500 endpoints and ThreatZero™ support fees. These costs are estimated at about $43 per endpoint for license costs and about $5 per endpoint for support costs. This support involves 24x7 help desk availability, performance optimization, ongoing updates, and incidence response as it relates to Cylance's platform.
- **Internal labor costs, including implementation and ongoing support, of about $90,000.** This includes the internal labor costs incurred by the State County to implement and set up Cylance in its environment, along with ongoing yearly labor costs.

Disclosures

The reader should be aware of the following:

- The study is commissioned by Cylance and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.
- Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the report to determine the appropriateness of an investment in CylancePROTECT® + ThreatZero™.
- Cylance 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.
- Cylance provided the customer name for the interviews but did not participate in the interviews.

TEI Framework And Methodology

INTRODUCTION

From the information provided in the interviews, Forrester has constructed a Total Economic Impact (TEI) framework for those organizations considering implementing CylancePROTECT® + ThreatZero™. The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision, to help organizations understand how to take advantage of specific benefits, reduce costs, and improve the overall business goals of winning, serving, and retaining customers.

APPROACH AND METHODOLOGY

Forrester took a multistep approach to evaluate the impact that CylancePROTECT® + ThreatZero™ can have on an organization (see Figure 2). Specifically, we:

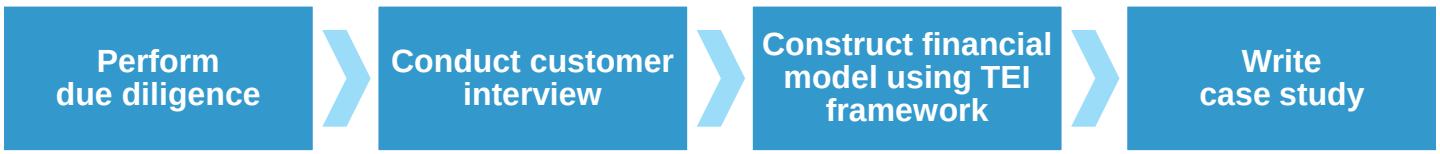
- Interviewed Cylance marketing, sales, and consulting personnel, along with Forrester analysts, to gather data relative to CylancePROTECT® + ThreatZero™ and the marketplace for CylancePROTECT® + ThreatZero™ support services.
- Interviewed A Large State County in the U.S., a government organization currently using CylancePROTECT® + ThreatZero™ to obtain data with respect to costs, benefits, and risks.
- Constructed a financial model representative of the interview using the TEI methodology. The financial model is populated with the cost and benefit data obtained from the interview.
- Risk-adjusted the financial model based on issues and concerns that the Large State County highlighted in the interview. Risk adjustment is a key part of the TEI methodology. While the interviewed organization provided cost and benefit estimates, some categories included a broad range of responses or had a number of outside forces that might have affected the results. For that reason, some cost and benefit totals have been risk-adjusted and are detailed in each relevant section.

Forrester employed four fundamental elements of TEI in modeling CylancePROTECT® + ThreatZero™ service: benefits, costs, flexibility, and risks.

Given the increasing sophistication that enterprises have regarding ROI analyses related to IT investments, Forrester's TEI methodology serves to provide a complete picture of the total economic impact of purchase decisions. Please see Appendix B for additional information on the TEI methodology.

FIGURE 2

TEI Approach



Source: Forrester Research, Inc.

Analysis

THE INTERVIEWED ORGANIZATION

For this study, Forrester conducted interviews with the Chief Information Security Officer of A Large State County, which is a Cylance customer based in the US:

- The State County is the most populous jurisdiction in the U.S. state that it operates, with 13.6% of the state's population.
- The State County provides critical services to a population of over 1.3 million citizens, including: law enforcement, fire and rescue, public transportation, health clinics, recreation centers, libraries, and disposal facilities for trash, etc. with highly sensitive and confidential public records.
- The State County employs 13,000 personnel and has 19,000 user accounts.
- It has total revenue and collections of around $3.5 billion annually.

"The price of a data breach, data loss, and image damage was too high for us to gamble on a solution that repeatedly showed it did not work. Cylance's solution is proactive, frees up our resources, and provides us with a peace of mind as it comes to security threats in our environment."

— Chief Information Security Officer, Large State County in the U.S.

After an extensive proof of concept and business case process evaluating multiple vendors, the organization chose Cylance as its only endpoint vendor and replaced its legacy solution entirely.

- Implementation started with gathering requirements around enterprise security architecture. The Large State County identified the system, time, and staffing needs of migrating to CylancePROTECT® from its legacy solution.
- The first phase involved decommissioning the old legacy antivirus system that was incapable of providing the State County the kind of cybersecurity that it needed to be kept safe from malicious attacks and security threats.
- CylancePROTECT® was deployed to 17,500 user endpoints.
- ThreatZero™ services were engaged to ensure smooth implementation, training, optimization, and continuous support for all endpoints.

Situation

The State County had a great track record with no major public breaches, but its systems were regularly infested with malware and other security attacks. The State County wanted to maintain this track record with a solution that provided a better proactive way of detecting threats and a better block rate on zero-day malware. Additionally, internal security and network staff were spending a considerable amount of time chasing malware-infected devices. This left the county more exposed to additional risks.

Prior to the investment in Cylance, the State County had another security vendor that provided data regarding endpoints that was detected with security threats. The county also had an in-depth internal network architecture to detect malware, viruses, and other security threats. The process to mitigate threats was highly manual for zero-day or more serious malware that could be caught but was not mitigated in advance. This led to high costs of reimaging machines and hurt end user productivity. It also put additional stress on internal resources, who were constantly chasing down issues.

Over the past 15 years, the State County had experienced a pretty stable horizon in terms of the prevention of malware resulting in public information and data breaches. However, there were several counties across the region that had not been

so fortunate. Many had suffered from data breaches related to public records and social security information. This prompted the county to look for a stronger and more proactive security solution. The State County also experienced an increase in the number of threats exposing its endpoints to unnecessary risks and reimaging costs. With this, the county started looking for and evaluating new solutions.

Some of the major motivations of the Large State County to migrate to Cylance were:

- The county needed to add a better endpoint solution that offers great detection and block rates on zero-day malware and different types of cyber-attacks.
- Security and network staff were spending way too much time remediating the malware-infected devices. Follow-up from agencies was arduous and intermittent at best, leaving the county exposed to unnecessary risks.
- The county wanted to maintain or increase its already successful business continuity track record and decrease the number of security threats and incidents.
- The county wanted to increase zero-day threat detection and decrease high false positive rates, operational overhead, and security management complexity.
- The other legacy antiviruses the county had used in the past took a lot of hard disk space and failed to detect zero-day malware. It needed a solution that would proactively defend public records against malware that were not already known.

> *"I hate to say it, but the agony of my peers has allowed me to justify the means. With the numbers of breaches that have occurred over the past several years, the cost of recovery from a breach, the loss of public trust were huge drivers for us to invest with Cylance."*
>
> — Chief Information Security Officer, Large State County in the U.S.

Solution

The county selected CylancePROTECT® + ThreatZero™ for its ability to conveniently and repeatedly predict and stop malware before they execute on the environment.

Results

The interview with a Large State County revealed the following:

- **Improved catch rate for zero-day malware.** Following the implementation of CylancePROTECT®, the State Country recorded a 99% block rate for all types of unwanted programs, including zero-day malware.
- **Reduction in time spent remediating/reimaging compromised devices.** The State County was able to reduce time spent by IT and security employees diagnosing and resolving issues after malware had executed on a user device. Additionally, it was able to increase the productivity of end users, as they did not have to wait to have access to their machines. This resulted in cost savings on IT labor and a boost in user productivity.
- **Improved cybersecurity confidence and reduced possibility of a data breach incidence.** The State County's already successful business continuity track record of avoidance of financial or reputational loss due to a data breach was further boosted by nearly 100%.
- **Reduction in hardware and memory requirements.** Because CylancePROTECT® required a significantly lower amount of disk space compared with the State County's legacy solution, the county was able to enjoy cost savings due to the avoidance of new hardware costs to run CylancePROTECT®.

"Prior to Cylance, we had spent a lot of manual time chasing down issues and reimaging machines. This cost not only reduced our end user productivity, but it also tied up our internal IT and security staff with chasing down issues."

— Chief Information Security Officer, Large State County in the U.S.

BENEFITS

"Well before an exploit has a chance to write to disk, we are in memory protection mode. It also protects us from execution of scripts, malicious and unwanted programs in real time."

~ Chief Information Security Officer, Large State County in the U.S.

The interviewed organization experienced a number of quantified benefits in this case study:

- Cost savings due to reduced incidence of zero-day threats and data breaches.
- Reduced cost of system remediation/reimaging.
- Improvement in IT and security employee productivity.

The Large State County also mentioned another important benefit: the psychological feeling of safety that it experienced following the implementation of CylancePROTECT® + ThreatZero™. The Large State County noted that this feeling helped to boost employee morale in the IT security department and alleviated employees from "living on the edge" because of the possibility of a serious malware attack or data breach. In the words of the county's Chief Information and Security Officer: "I hate to say it, but the agony of my peers has allowed me to justify the means. With the numbers of breaches that have occurred over the past several years, the cost of recovery from a breach, the loss of public trust are huge drivers for us."

Cost Savings Due To Reduced Incidence Of Zero-Day Threats And Risk Of Data Breach

The State County noted that the biggest quantified benefit of implementing CylancePROTECT® into its environment was its ability to reduce the risk of zero-day attacks. Prior to CylancePROTECT®, the county was "100%" vulnerable to cyber-attacks and security data breaches.

The State County has 20,000 customer records and estimates a $400 cost per record of a data breach. Prior to Cylance, the risk of a possible data breach of one of its customer records was estimated at 30%. The State County can confidently claim it has reduced its known and zero-day vulnerability risk by 99%, which equates to about $2.37 million in yearly cost savings (see Table 1).

TABLE 1
Cost Savings Due To Reduced Incidence Of Zero-Day Threats And Risk Of Data Breach

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
A1	Number of customer records	Large State County		20,000	20,000	20,000
A2	Estimated cost of data breach per compromised customer record	Large State County		$400	$400	$400
A3	Possibility of data breach	Forrester assumption		30%	30%	30%
A4	Reduction in zero-day threats and data breaches	Large State County		99%	99%	99%
At	Cost savings due to reduced incidence of zero-day threats and risk of data breach	A1*A2*A3*A4		$2,376,000	$2,376,000	$2,376,000
	Risk adjustment	↓5%				
Atr	**Cost savings due to reduced incidence of zero-day threats and risk of data breach (risk-adjusted)**		**$0**	**$2,257,200**	**$2,257,200**	**$2,257,200**

Source: Forrester Research, Inc.

Reduced Cost Of System Remediation/Reimaging

Prior to its investment in Cylance, The State County had security issues that resulted in an average of six endpoint remediations and reimages a month. On average, each of these issues resulted in internal IT and security FTEs spending 12 hours trying to identify and implement a solution. These issues also resulted in 12 hours of downtime and unproductive time for the business user.

Since implementing CylancePROTECT®, the State County has reported virtually no issues with reimaging endpoints. This equates to about $110,000 of yearly cost savings (see Table 2).

TABLE 2
Reduced Cost Of System Remediation/Reimaging

Ref.		Calculation	Initial	Year 1	Year 2	Year 3
B1	Number of endpoints reimaged per month	Large State County		6	6	6
B2	Number of months	Calculation		12	12	12
B3	Time requirement to reimage device, including assessment, ticket creation, desktop reimaging, and getting user back up and running (hours)	Large State County		12	12	12
B4	Reduction in remediation and reimaging costs	Large State County		98%	98%	98%
B5	Loss of end user productivity (hours)	Large State County		12	12	12
B6	Average hourly cost of IT and business user	Large State County		$65	$65	$65
Bt	Reduced cost of system remediation/reimaging	B1*B2*(B3+B5)*B4*B6		$110,074	$110,074	$110,074
	Risk adjustment	↓5%				
Btr	**Reduced cost of system remediation/reimaging (risk-adjusted)**		**$0**	**$104,570**	**$104,570**	**$104,570**

Source: Forrester Research, Inc.

IT And Security FTE Productivity Gains

The State County cited its ability to dramatically increase the productivity of its in-house IT and security teams. With CylancePROTECT® + ThreatZero™, the county was able to proactively get in front of memory-based attacks, malicious documents, and zero-day malware, and it also had fewer escalations. This all resulted in a boost of efficiency for its IT and security staff. With Cylance's ThreatZero™ support services, the county was able to learn best practices in network architecture, patch management, and internal- and external-facing services that could be vulnerable for malicious attacks.

The State County estimates that with its investment in Cylance, it was able to gain productivity worth the time of two full IT FTEs as it relates to investigating endpoints. Additionally, across its staff of 12 IT and security FTEs, it saw a productivity improvement of 40%. At a $120,000 average annual salary, this results in a yearly risk-adjusted benefit of $734,000 (see Table 3).

TABLE 3
IT And Security FTE Productivity Gains

Ref.		Calculation	Initial	Year 1	Year 2	Year 3
C1	Number of IT FTE requirements reduced to investigate endpoints from investment in Cylance	Large State County		2	2	2
C2	Average annual salary of security FTE	Large State County		$120,000	$120,000	$120,000
C3	IT and security FTEs	Large State County		12	12	12
C4	Improvement in security employee productivity	Large State County		40%	40%	40%
Ct	Improvement in security employee productivity	(C1*C2)+(C2*C3*C4)		$816,000	$816,000	$816,000
	Risk adjustment	↓10%				
Ctr	**IT and security FTE productivity gains**		**$0**	**$734,400**	**$734,400**	**$734,400**

Source: Forrester Research, Inc.

Total Benefits

Table 4 shows the total of all benefits across the three areas listed above, as well as present values (PVs) discounted at 10%. Over three years, the interviewed organization expects risk-adjusted total benefits to be a PV of about $7.7 million.

TABLE 4
Total Benefits (Risk-Adjusted)

Ref.	Benefit Category	Initial	Year 1	Year 2	Year 3	Total	Present Value
Atr	Cost savings due to reduced incidence of zero-day threats and risk of data breach	$0	$2,257,200	$2,257,200	$2,257,200	$6,771,600	$5,613,322
Btr	Reduced cost of system remediation/reimaging	$0	$104,570	$104,570	$104,570	$313,710	$260,050
Ctr	IT and security FTE (security engineers, network engineers, security analysts) productivity gains	$0	$734,400	$734,400	$734,400	$2,203,200	$1,826,344
	Total benefits (risk-adjusted)	**$0**	**$3,096,170**	**$3,096,170**	**$3,096,170**	**$9,288,510**	**$7,699,716**

Source: Forrester Research, Inc.

COSTS

The Large State County experienced a number of costs associated with the CylancePROTECT® + ThreatZero™ solution:

- CylancePROTECT® + ThreatZero™ license cost.
- Implementation and ongoing internal labor cost.

These represent the mix of internal and external costs experienced by the interviewed organization for initial planning, implementation, and ongoing maintenance associated with the solution.

CylancePROTECT® + ThreatZero™ License Cost

Software licensing fees for CylancePROTECT® + ThreatZero™ were incurred during the initial implementation period; in subsequent years, an annual license fee calculated based on the number of endpoints was applied. In years 1 through 3, the State County incurred software licensing fees for CylancePROTECT® of $764,900, or $43 per endpoint. Additionally, the State County paid $100,000 per year for Cylance's ThreatZero™ services (see Table 5).

It is important to note that software license costs vary from organization to organization, considering different licensing agreements, what other products may be licensed from the same vendor, and other discounts.

TABLE 5
CylancePROTECT® + ThreatZero™ Cost

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
D1	Number of endpoints to protect	Large State County		17,500	17,500	17,500
D2	CylancePROTECT® license cost per endpoint	Large State County ($42.68)		$43	$43	$43
D3	Yearly license cost	D1*D2		$746,900	$746,900	$746,900
D4	ThreatZero™ advance support cost	Large State County		$100,000	$100,000	$100,000
Dt	CylancePROTECT® cost + ThreatZero™ cost	D3+D4	$0	$846,900	$846,900	$846,900
	Risk adjustment	0%				
Dtr	**CylancePROTECT® cost + ThreatZero™ cost (risk-adjusted)**		**$0**	**$846,900**	**$846,900**	**$846,900**

Source: Forrester Research, Inc.

Internal Implementation And Ongoing Labor Cost

Once it made the investment, the State County took about a month to fully implement CylancePROTECT® across all of its endpoints. The county dedicated one full-time IT resource to integrate the solution with Cylance's support staff. This resulted in a one-time salary cost of $15,000.

The State County estimates that there is an ongoing minimal requirement of 25% of one FTE's time dedicated to managing Cylance's platform. This results in about $30,000 per year in salary costs for the State County (see Table 6).

TABLE 6
Implementation And Ongoing Internal Labor Cost

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
E1	Number of IT employees required for implementation	Large State County	1			
E2	Percentage of time dedicated time to deployment	Large State County	100%			
E3	Implementation time (months)	Large State County	1			
E4	Implementation labor cost (1.5 months' salary)	Large State County	$15,000			
E5	Security analyst for ongoing internal support	Large State County		1	1	1
E6	Percentage of time dedicated to managing Cylance	Large State County		25%	25%	25%
E7	Security operations staff annual salary	Large State County	$120,000	$120,000	$120,000	$120,000
Et	Internal implementation and ongoing labor cost	E4+(E5*E6*E7)	$15,000	$30,000	$30,000	$30,000
	Risk adjustment	0%				
Etr	**Internal implementation and ongoing labor cost (risk-adjusted)**		**$15,000**	**$30,000**	**$30,000**	**$30,000**

Source: Forrester Research, Inc.

Total Costs

Table 7 shows the total of all costs as well as associated present values (PVs), discounted at 10%. Over three years, the Large State County expects total costs to be a PV of about $2.2 million.

TABLE 7
Total Costs (Risk-Adjusted)

Ref.	Cost Category	Initial	Year 1	Year 2	Year 3	Total	Present Value
Dtr	CylancePROTECT® cost + ThreatZero™ cost	$0	$846,900	$846,900	$846,900	$2,540,700	$2,106,115
Etr	Internal implementation and ongoing labor cost	$15,000	$30,000	$30,000	$30,000	$103,846	$88,452
	Total costs (risk-adjusted)	**$15,000**	**$876,900**	**$876,900**	**$876,900**	**$2,644,546**	**$2,194,567**

Source: Forrester Research, Inc.

FLEXIBILITY

Flexibility, as defined by TEI, represents an investment in additional capacity or capability that could be turned into business benefit for some future additional investment. This provides an organization with the “right” or the ability to engage in future initiatives but not the obligation to do so. There are multiple scenarios in which a customer might choose to implement CylancePROTECT® + ThreatZero™ and later realize additional uses and business opportunities. Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix B).

The zero footprint nature and low CPU usage characteristics of the Cylance solution position present or future CylancePROTECT® + ThreatZero™ with huge flexibility in terms of scalability and marginal cost of provisioning for new users or endpoints. This is unlike many antivirus solutions that take a substantial amount of CPU space, which may lead to difficulties in installation and upgrades. Cylance provides the needed flexibility for increasing or cutting back on the number of active endpoints with the convenience of a single phone call. This may be highly valuable for organizations in times of mergers, acquisitions, or even a restructuring of the organization or certain departments.

RISKS

Forrester defines two types of risk associated with this analysis: “implementation risk” and “impact risk.” Implementation risk is the risk that a proposed investment in CylancePROTECT® + ThreatZero™ may deviate from the original or expected requirements, resulting in higher costs than anticipated. Impact risk refers to the risk that the business or technology needs of the organization may not be met by the investment in CylancePROTECT® + ThreatZero™, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for cost and benefit estimates.

TABLE 8
Benefit And Cost Risk Adjustments

Benefits	Adjustment
Cost savings due to reduced incidence of zero-day threats and risk of data breach	↓ 5%
Reduced cost of system remediation/reimaging	↓ 5%
Improvement in IT and security employee productivity	↓ 10%

Costs	Adjustment
CylancePROTECT® + ThreatZero™ cost	↑ 0%
Internal implementation and ongoing labor cost	↑ 0%

Source: Forrester Research, Inc.

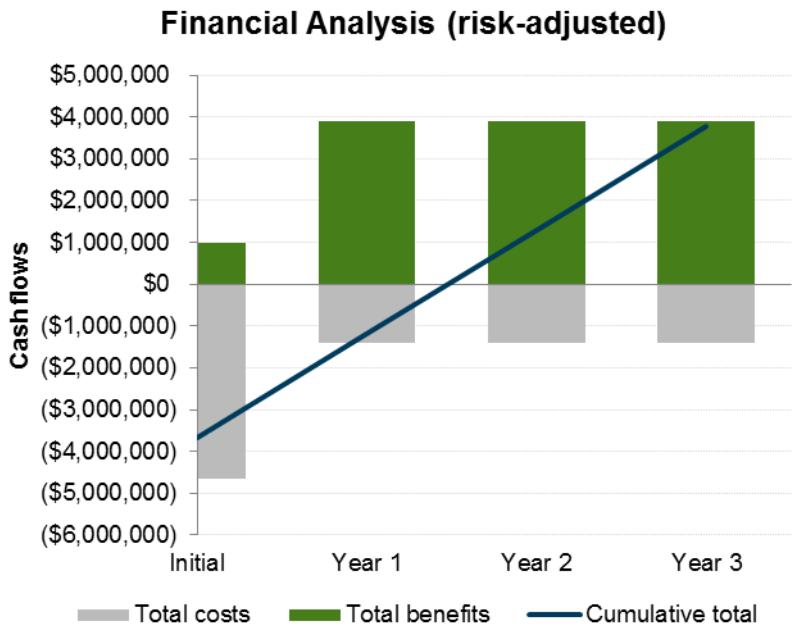
Quantitatively capturing implementation risk and impact risk by directly adjusting the financial estimates results provides more meaningful and accurate estimates and a more accurate projection of the ROI. In general, risks affect costs by raising the original estimates, and they affect benefits by reducing the original estimates. The risk-adjusted numbers should be taken as “realistic” expectations since they represent the expected values considering risk.

Financial Summary

The financial results calculated in the Benefits and Costs sections can be used to determine the ROI and NPV for The Large State County's investment in CylancePROTECT® + ThreatZero™.

Table 9 below shows the risk-adjusted ROI and NPV values. These values are determined by applying the risk-adjustment values from Table 8 in the Risks section to the unadjusted results in each relevant cost and benefit section.

FIGURE 3
Cash Flow Chart (Risk-Adjusted)



Source: Forrester Research, Inc.

TABLE 9
Cash Flow (Risk-Adjusted)

Summary	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($15,000)	($876,900)	($876,900)	($876,900)	($2,645,700)	($2,195,721)
Total benefits	$0	$3,096,170	$3,096,170	$3,096,170	$9,288,510	$7,699,716
Total	**($15,000)**	**$2,219,270**	**$2,219,270**	**$2,219,270**	**$6,642,810**	**$5,503,996**
ROI						**251%**

Source: Forrester Research, Inc.

Cylance CylancePROTECT® + ThreatZero™: Overview

The following information is provided by Cylance. Forrester has not validated any claims and does not endorse Cylance or its offerings. The sections below describe the standard offerings provided by Cylance to the customer. This includes an endpoint security prevention product and professional consulting services.

CYLANCEPROTECT®

CylancePROTECT® is an advanced threat prevention product that sits on each endpoint within an organization. It applies artificial intelligence and machine learning to instantly identify and prevent malware and cyberattacks from ever executing on the host machine.

CylancePROTECT® is a small, lightweight software agent that is deployed to every endpoint in an organization to prevent cyberattacks on the operating system and in memory. Prior to any binary being executed on the host, CylancePROTECT® uses static analysis and predictive modeling to determine if the binary contains malicious features. If deemed a threat, local host policy takes action to alert, notify, and/or quarantine the object.

Cylance takes a no signature, no heuristic approach to malware detection. All detections are predictive and preventive in nature.

CylancePROTECT® is PCI-DSS section 5.0 compliant, HIPAA antivirus compliant, a member of the Microsoft Virus Initiative, and recognized by Microsoft as an antivirus product. CylancePROTECT® can entirely replace an existing legacy AV solution or work together with any existing solution.

CylancePROTECT® uses less than 1% of a typical desktop CPU and less than 60 MB of memory.

CylancePROTECT® was also designed with sensitive and air-gapped environments in mind. The CylancePROTECT® agent runs entirely on the host endpoint and requires no outside internet connection to predict and prevent malware from executing.

CylancePROTECT® has an easy-to-use web console to handle alerts, zone and policy management, and reporting. Endpoint agents report into the console only for policy and occasional updates. The CylancePROTECT® agent does not require an internet connection to provide protection to the endpoint itself. CylancePROTECT® can be easily integrated into any of the top SIEM solutions via REST API, including native integration with Splunk. CylancePROTECT® is delivered as a standard MSI.

Artificial intelligence and machine learning allow Cylance to build mathematically sound relationships between features and correlate seemingly disparate features far beyond human ability. Both disciplines are proven to be more powerful, efficient, and accurate than any human or semiautomatic approach to cybersecurity. This approach allows Cylance to quickly build highly accurate predictive models that enable the endpoint agent to make autonomous, intelligent decisions on file binaries before the files are able to execute.

CylancePROTECT® is compatible with all current versions of Microsoft Windows and Mac operating systems.

CYLANCE THREATZERO™

ThreatZero™ Services

When enterprises initially deploy CylancePROTECT®, it is common to find active threats or evidence of previously unknown compromises.

Seamlessly integrated with Cylance's always-on, always-vigilant CylancePROTECT® product, ThreatZero™ services optimize its operationalization. Cylance experts expedite product implementation, mitigate risk immediately, and facilitate immediate ROI.

ThreatZero™ Addresses Unique Challenges

Integrating new software can be challenging for any organization. Common challenges include partial installation, lack of training, internal resource constraints, improper initial configuration, and an inability to maintain security optimization.

What Customers Get With ThreatZero™ Services

With ThreatZero™ services, enterprises get CylancePROTECT® basic, self-service health check functionality, and the following:

- **Legacy AV migration planning.** If required, assist in the planning/removal of existing traditional antivirus while ensuring all endpoints remain protected.
- **Deployment and best practices configuration.** Operationalize CylancePROTECT® with all project milestones met through a quick and low-impact implementation.
- **PUPZERO.** Research all potentially unwanted programs, determine quarantine recommendations, develop consensus with client team on strategy, and then achieve PUPZERO status.
- **Memory protection.** Implement memory protection in Alert-Only Mode, test, move to Block Mode, and then determine exclusion paths.
- **Script and application control.** Implement application control on appropriate systems if required and implement script control best practices.
- **Best practices training.** Specifically configure CylancePROTECT® agents with policies tailored to each customer environment and network configuration.

THE CYLANCE DIFFERENCE

- **Analyze threats.** The Cylance team classifies, analyzes, and waives trusted files.
- **Implement quickly.** CylancePROTECT® can be easily rolled out to most environments with little IT effort.
- **Access services.** Cylance's highly skilled deployment team will work with customers on security best practices, current malware trends, and deployment strategies, speeding and improving the efficacy of the CylancePROTECT® deployment.
- **Configure securely.** Cylance's consulting implementation team will work with end users to specifically configure the deployed CylancePROTECT® agents, with policies tailored to each customer environment and network configuration.
- **Get to zero threats.** After configuration and implementation, Cylance's team will ensure the environment contains zero threats.

Through a combination of technology, education, and expertise, the Cylance team allows customers to go forward knowing that all current threats to their endpoints have been eliminated.

Appendix A: Large State County& Framework Assumptions

For this study, Forrester conducted interviews with the Chief Information Security Officer of The Large State County, which is a Cylance customer based in the US:

- The Large State County is the most populous jurisdiction in one of the U.S. States.
- The Large State County provides critical services to a population of over 1.3 million citizens, including: law enforcement, fire and rescue, public transportation, health clinics, recreation centers, libraries, and disposal facilities for trash, etc. with highly sensitive and confidential public records.
- Large State County employs 13,000 personnel and has 19,000 user accounts.
- It has total revenue and collections of around $3.5 billion annually.

After an extensive proof of concept and business case process evaluating multiple vendors, the organization chose Cylance and began deployment:

- Implementation started with gathering requirements around enterprise security architecture. The Large State County identified the system, time, and staffing needs of migrating to CylancePROTECT® from its legacy solution.
- The first phase involved decommissioning the old legacy antivirus system that was incapable of providing Large State County the kind of cybersecurity that it needed to be kept safe from malicious attacks and security threats.
- CylancePROTECT® was deployed to 17,500 user endpoints.
- ThreatZero™ services were engaged to ensure smooth implementation, training, optimization, and continuous support for all endpoints.

FRAMEWORK ASSUMPTIONS

Table 10 provides the model assumptions that Forrester used in this analysis.

The discount rate used in the PV and NPV calculations is 10%, and the time horizon used for the financial modeling is three years. Organizations typically use discount rates between 8% and 16% based on their current environment. Readers are urged to consult with their respective company's finance department to determine the most appropriate discount rate to use within their own organizations.

TABLE 10
Model Assumptions

Ref.	Metric	Calculation	Value
X1	Hours per week		40
X2	Weeks per year		52
X3	Hours per year (M-F, 9-5)		2,080
X4	IT and security annual FTE salary		$120,000
X5	Possibility of data breach with regular antivirus		30%

Source: Forrester Research, Inc.

Appendix B: 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. TEI assists technology vendors in winning, serving, and retaining customers.

The TEI methodology consists of four components to evaluate investment value: benefits, costs, flexibility, and risks.

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 form 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.

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 enterprise wide 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. However, having the ability to capture that benefit has a PV that can be estimated. The flexibility component of TEI captures that value.

RISKS

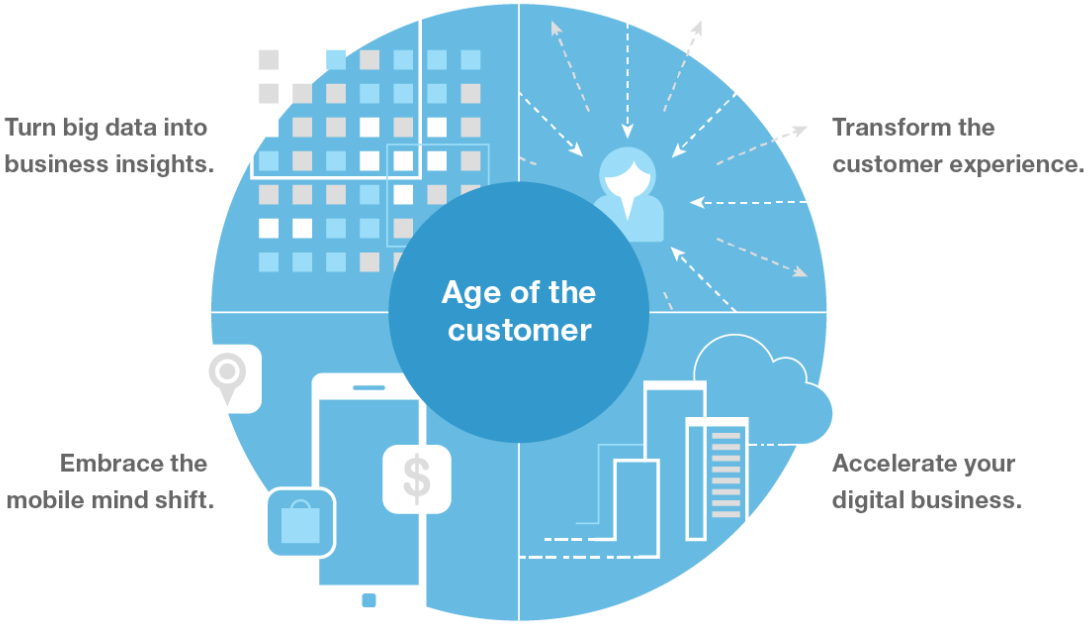
Risks measure the uncertainty of benefit and cost estimates contained within the investment. Uncertainty is measured in two ways: 1) the likelihood that the cost and benefit estimates will meet the original projections, and 2) the likelihood that the estimates will be measured and tracked over time. TEI risk factors are based on a probability density function known as "triangular distribution" to the values entered. At a minimum, three values are calculated to estimate the risk factor around each cost and benefit.

Appendix C: Forrester And The Age Of The Customer

Your technology-empowered customers now know more than you do about your products and services, pricing, and reputation. Your competitors can copy or undermine the moves you take to compete. The only way to win, serve, and retain customers is to become customer-obsessed.

A customer-obsessed enterprise focuses its strategy, energy, and budget on processes that enhance knowledge of and engagement with customers and prioritizes these over maintaining traditional competitive barriers.

CMOs and CIOs must work together to create this companywide transformation.



Forrester has a four-part blueprint for strategy in the age of the customer, including the following imperatives to help establish new competitive advantages:

Transform the customer experience to gain sustainable competitive advantage.

Accelerate your digital business with new technology strategies that fuel business growth.

Embrace the mobile mind shift by giving customers what they want, when they want it.

Turn (big) data into business insights through innovative analytics.

Appendix D: Glossary

Discount rate: The interest rate used in cash flow analysis to take into account the time value of money. Companies set their own 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 respective organizations to determine the most appropriate discount rate to use in their own environment.

Net present value (NPV): The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made, unless other projects have higher NPVs.

Present value (PV): The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total NPV of cash flows.

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

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

A NOTE ON CASH FLOW TABLES

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

Sums and present value calculations of the Total Benefits, Total Costs, and Cash Flow tables may not exactly add up, as some rounding may occur.

TABLE [EXAMPLE]
Example Table

Ref.	Metric	Calculation	Year 1	Year 2	Year 3

Source: Forrester Research, Inc.