The Total Economic Impact™ Of CylancePROTECT From BlackBerry

Cost Savings And Business Benefits Enabled By CylancePROTECT

OCTOBER 2022

Table Of Contents

Consultant: *Jonathan Whaling*

Executive Summary

Endpoint protection solutions are a critical component of any size organization's security portfolio. CylancePROTECT from BlackBerry enables organizations to manage their endpoint protection in a more efficient way by using artificial intelligence instead of signatures to detect threats across a variety of devices. The solution helps organizations manage threat detection with fewer resources and reduces impact on end users, in addition to reducing overall risks.

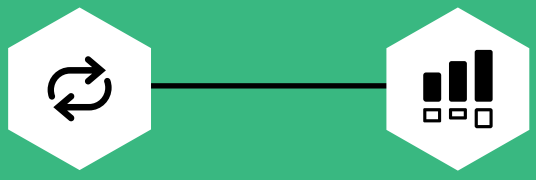
CylancePROTECT® from BlackBerry[1] provides an AI-driven threat prevention security solution that protects endpoints and servers. CylancePROTECT offers predictive threat prevention and visibility into the endpoint environment, allowing security teams to discover and stop potential threats with minimal oversight.

BlackBerry commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying CylancePROTECT. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of CylancePROTECT on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four representatives with experience using CylancePROTECT. Forrester then aggregated their experiences and combined the results into a single composite organization that is a manufacturing organization with $3 billion in revenues per year.

Prior to using CylancePROTECT, these interviewees noted how their organizations suffered from multiple employee phishing attacks that existing endpoint solutions failed to detect. These solutions also required significant management time to monitor threats and end-user time to update virus signatures. Inconsistent solutions also hampered the sharing of threat information among security analysts across the organizations.

KEY STATISTICS



Return on investment (ROI)
100%

Net present value (NPV)
$1.24M

After the investment in CylancePROTECT, the interviewees reported zero endpoint security breaches. Staff time for administration and incident remediation was greatly reduced, freeing up IT resources and improving end-user productivity.

KEY FINDINGS

Quantified benefits. Three-year, risk-adjusted present value (PV) quantified benefits for the composite organization include:

- **A reduction of the cost of security breaches by nearly $1.3 million.** Organizations that suffer security breaches from phishing attacks incur costs in the tens and hundreds of thousands of dollars to investigate and recover from them. Since implementing CylancePROTECT, the composite organization has had zero breaches. By modeling data from Forrester's annual security survey, the composite organization saves nearly $1.3 million (present value) over three years.

- **A reduction in subscription costs from decommissioned software.** The composite organization saves just under $806,000 over three years by removing its legacy endpoint protection software.
- **A reduction in annual time investigating and recovering from security incidents of over 30%.** CylancePROTECT enables the composite organization to greatly reduce time spent investigating incidents and remediating devices. This benefit saves it nearly $227,000 over three years.
- **A savings of over 8,000 hours from elimination of antivirus updates.** Through its use of artificial intelligence, CylancePROTECT eliminates the need for updating signatures on endpoints. This translates to labor savings of just under $167,000 over three years for the composite organization.

Unquantified benefits. Benefits that provide value for the composite organization but are not quantified in this study include:

- **Enabling incident response support with CylanceOPTICS®.** Though not expressly covered in this study, organizations can use the CylancePROTECT companion product CylanceOPTICS to support incident response with automated scripts.
- **Increasing employee satisfaction and awareness of cybersecurity.** After implementing CylancePROTECT alongside an accompanying training program, an organization increased cybersecurity ratings on employee surveys by 25 points. Employees felt more assured that their devices were protected.
- **Providing support for multiple device types and operating systems.** CylancePROTECT can support many device types and operating systems, including legacy systems, enabling organizations to simplify their security environments by eliminating overlapping tools.
- **Delivering peace of mind for security professionals.** Security professionals give CylancePROTECT high compliments for the peace of mind it provides that their endpoints are secure and there is minimal risk to reputational damage from loss of customer and organizational data.

Costs. Three-year, risk-adjusted PV costs for the composite organization include:

- **Software license fees of $1.0 million.** BlackBerry charges an annual per-device license fee of $41.25 for its software-as-a-service (SaaS) solution. For the composite organization with 10,000 devices, this cost totals $1.0 million (present value) over three years.
- **Implementation costs of just more than $141,000.** This cost consists of fully burdened salaries for two FTEs over six months.
- **Administrative costs of just less than $71,000 over three years.** These costs include fully burdened salaries for .25 FTEs per year.

The representative interviews and financial analysis found that a composite organization experiences benefits of $2.48 million over three years versus costs of $1.24 million, adding up to a net present value (NPV) of $1.24 million and an ROI of 100%.

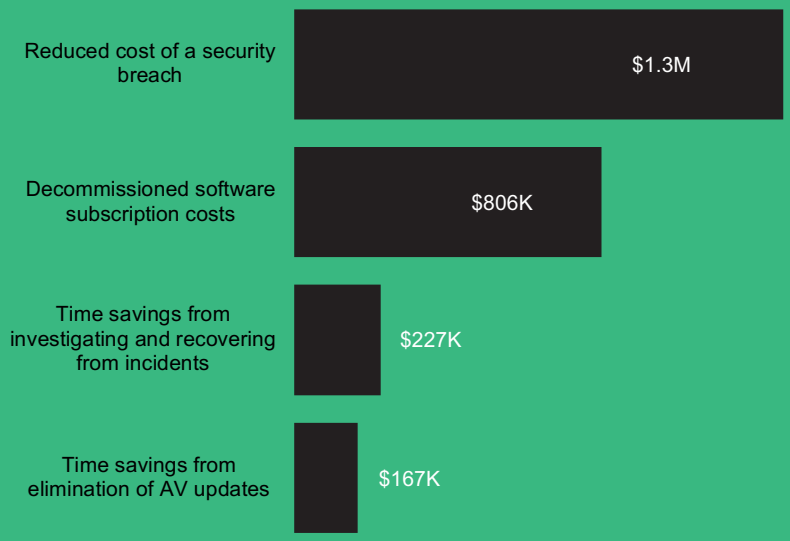
ROI
100%

BENEFITS PV
$2.48M

NPV
$1.24M

PAYBACK
<6 months

Benefits (Three-Year)



"Since we purchased and implemented CylancePROTECT, we haven't had a single incident relating to antivirus or endpoint protection. I think that is extremely significant, given we used to re-image a computer every few days."

— IT Director, education

TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in CylancePROTECT.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that CylancePROTECT can have on an organization.

Forrester Consulting conducted an online survey of 351 cybersecurity leaders at global enterprises in the US, the UK, Canada, Germany, and Australia. Survey participants included managers, directors, VPs, and C-level executives who are responsible for cybersecurity decision-making, operations, and reporting. Questions provided to the participants sought to evaluate leaders' cybersecurity strategies and any breaches that have occurred within their organizations. Respondents opted into the survey via a third-party research panel, which fielded the survey on behalf of Forrester in November 2020.

DUE DILIGENCE
Interviewed BlackBerry stakeholders and Forrester analysts to gather data relative to CylancePROTECT.

INTERVIEWS
Interviewed four representatives at organizations using CylancePROTECT to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION
Designed a composite organization based on characteristics of the interviewees' organizations.

FINANCIAL MODEL FRAMEWORK
Constructed a financial model representative of the interviews using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewees.

CASE STUDY
Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

The CylancePROTECT Customer Journey

Drivers leading to the CylancePROTECT investment

Interviews			
Role	**Industry**	**Region**	**Protected Devices**
Technical consultant	Manufacturing	Europe	300
Business development manager	Energy	Europe	2,000
IT director	Education	North America	22,000
Director, IT operations	Manufacturing	North America	30,000

KEY CHALLENGES

The interviewees' organizations had a variety of endpoint protection solutions in place from legacy solutions to built-in operating system protection. Some devices in certain divisions or offline applications had no protection at all. This resulted in several challenges in endpoint security monitoring, including:

- **Preventing breaches.** Interviewees' organizations incurred breaches from phishing and ransomware. In all cases, existing endpoint protection solutions failed to stop these attacks, but damage was minimal because they were detected shortly after occurrence. Nonetheless, each breach resulted in unplanned internal costs associated with its investigation, recovery, and the prevention of future incidents. In cases where employee or customer data was exposed outside the organization, external costs for regulatory agencies and other third parties were also incurred.
- **Maintaining signature-based solutions.** Traditional, signature-based antivirus solutions required IT staff at the interviewees' organizations to execute manual processes for reviewing identified threats and frequently update virus signatures. In some cases, these teams could not devote adequate time to manage existing solutions. Additionally, these solutions required periodic endpoint updates, which translated into short downtimes for end users.
- **Inconsistent solutions across diversified operating units.** One large, diversified organization in the study had dozens of endpoint monitoring solutions in place, each managed by a different IT team. This prevented corporate oversight and limited sharing of incident data across the enterprise. As its Director of IT operations stated, "There were constant events, and because there was no consistent solution, dealing with those incidents was a one-off every time one happened." Other divisions in this same organization had no endpoint monitoring in place.
- **Inability to protect all installed IT assets with a single solution.** Interviewees' organizations had installed a variety of devices and equipment. Most of them were connected to the Internet, but some were in a standalone or closed network environment. These included mobile devices for employees, network transmission equipment, and manufacturing control computers. Many of these endpoints were not protected by a single solution or protected at all. In addition, organizations were faced with the task of enabling all employees to work from home during the pandemic, sometimes on personal devices. These unprotected systems

presented additional exposure and risks as well as increased security burdens for IT staff.

SOLUTION REQUIREMENTS

The interviewees' organizations searched for a solution that could:

- **Replace traditional signature-based methods with AI capabilities**. Interviewees' organizations that had encountered breaches were looking for a more advanced method of detection beyond virus signatures. Two of the organizations performed comparison tests against competitive products using existing and zero-day viruses, and CylancePROTECT outperformed the chosen competitors.
- **Offer easy implementation and ongoing management**. Organizations wanted to move away from manual maintenance tasks of antivirus (AV) solutions, such as distributing signature files, to implement a more fully automated solution that would require minimal oversight as well as provide lightweight resource requirements for disk and memory utilization.
- **Offer compatibility with multiple devices and operating systems**. This search for compatibility was for both older or outdated operating systems and newer handheld and mobile devices. The technical consultant shared, "We were looking for an XP-capable system. And there's very little choice, in fact I think that there were no [other options] at all."
- **Monitor and protect personal devices and USB drives**. This was particularly important to support work-from-home arrangements during the pandemic.
- **Obtain support from the vendor for incident response.** Organizations with limited IT staff and little cybersecurity knowledge wanted a partner that provided vendor and community support in analyzing incidents.

"What was important for us was that we don't install pattern-based antivirus software, but one that relies on machine learning. We wanted to go in the direction of an algorithm and not a pattern so that machines would not be connected to the Internet and have to pull any updates. Years of experience with [antivirus] products have shown that whenever there are updates, you can run into errors."

Technical consultant, manufacturing

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an ROI analysis that illustrates the areas financially affected. The composite organization is representative of the four interviewees, and it is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. The multibillion-dollar manufacturing organization produces supplies for businesses across several consumer-facing industries. The composite organization has multiple operations across Europe, where most of its customers are located. The organization generates annual revenue of $3 billion and has 10,000 employees.

Deployment characteristics. Prior to implementing CylancePROTECT, the composite organization relied on a legacy endpoint protection solution. Its fleet of devices is primarily laptops and desktops, with several hundred tablets for field service employees. The organization has been rolling out CylancePROTECT across its divisions and operating units in phases over a period of several months.

Key Assumptions

- **$3 billion revenue**
- **10,000 employees**
- **10,000 devices**
- **Legacy endpoint protection solution**

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits						
Ref.	**Benefit**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Atr	Reduced cost of a security breach	$451,696	$520,934	$587,082	$1,559,712	$1,282,240
Btr	Decommissioned software subscription costs	$324,000	$324,000	$324,000	$972,000	$805,740
Ctr	Time savings from investigating and recovering from incidents	$88,200	$91,440	$94,680	$274,320	$226,887
Dtr	Time savings from elimination of AV updates	$65,304	$67,162	$69,019	$201,485	$166,728
	Total benefits (risk-adjusted)	$929,200	$1,003,536	$1,074,781	$3,007,517	$2,481,595

REDUCED COST OF A SECURITY BREACH

Evidence and data. Two of the interviewees' organizations suffered security breaches from one or more phishing incidents prior to implementing CylancePROTECT. The endpoint protection solutions in place did not prevent the attacks in either case, and these incidents motivated the affected organizations to evaluate and obtain improved endpoint protection solutions. While neither incident resulted in negative publicity or brand impact, they resulted in costs associated with:

- IT/security and finance staff time investigating the incidents.
- Internal compliance staff time to reevaluate and amend internal security control procedures.
- Legal staff time to support and respond to regulatory agency inquiries.
- Hiring outside consultants to search for data potentially exposed from the incident.
- Reentering lost data that was not backed up prior to the incident.

After implementing CylancePROTECT, none of the organizations in the study experienced a breach.

> **"The internal probe into our phishing attack lasted over two months and involved dozens of internal staff, including legal, finance, internal controls, as well as administrative support. The total cost was several hundred thousand dollars."**
>
> *Business development manager, energy*

Modeling and assumptions. For the composite organization, Forrester assumes:

- Before CylancePROTECT, there are an average number of 2.8 material breaches each year.[2]
- The average cost of each breach is $605,000 before the solution.[3]

- Each breach impacts two-thirds (65%) of employees, resulting in 3.9 hours of lost productivity before CylancePROTECT.[4]
- The incremental improvement in security risk efficacy for CylancePROTECT is 5% compared to the previous legacy endpoint protection solution. This translates to five fewer incidents for every 100 threats when compared to its legacy endpoint protection solution.

Risks. With new security threats emerging all the time, it is difficult to predict with absolute certainty the occurrence and costs of a security breach:

- The efficacy of most existing solutions will vary within a narrow window of 90-99%.
- The estimated cost of a security breach will depend upon its scope, depth of data exposed, and extent of employees involved in recovery.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $1.3 million.

Reduced Cost Of A Security Breach

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Average number of material breaches per year	Forrester research	2.8	2.8	2.8
A2	Average cost of data breach, excluding user downtime	Forrester research	$605,000	$605,000	$605,000
A3	Percent reduction in security risk with new solution	Findings	5%	5%	5%
A4	Subtotal: Avoided data security business risk costs	A1*A2*A3	$84,700	$84,700	$84,700
A5	Number of employees	Composite	10,000	10,000	10,000
A6	Average hourly salary: business user	TEI standard	$35	$36	$37
A7	Reduced user productivity per breach (hours)	Forrester research	3.9	3.9	3.9
A8	Percentage of employees affected per breach	Forrester research	65%	65%	65%
A9	Productivity recapture	TEI standard	25%	25%	25%
A10	Subtotal: Cost of reduced productivity	A1*A5*A6*A7 *A8*A9	$621,075	$638,820	$656,565
A11	Improvement in detection over time	Composite	80%	90%	99%
At	Reduced cost of a security breach	(A4+A10)*A11	$564,620	$651,168	$733,852
	Risk adjustment	↓20%			
Atr	Reduced cost of a security breach (risk-adjusted)		$451,696	$520,934	$587,082
	Three-year total: $1,559,712			**Three-year present value: $1,282,240**	

DECOMMISSIONED SOFTWARE SUBSCRIPTION COSTS

Evidence and data. Organizations removed existing antivirus software across the user base prior to installing CylancePROTECT. These previous solutions ranged from built-in operating system products to more extensive legacy platform solutions. These costs were typically not a driving factor in the decision to switch to CylancePROTECT but need to be factored in to offset its license costs. Examples included:

- The savings among organizations in the study ranged from $165,000 to $355,000 annually, adjusted for composite size.
- The Director of IT operations noted that his organization consolidated all endpoint protection license spending at the corporate level, providing a volume discount. He stated, “When you look at it from the perspective of the individual business, they viewed it as a total savings because corporate picked up the tab.”

Modeling and assumptions. To estimate savings, Forrester used a published license fee of $36 per device per year for a widely used legacy antivirus solution.

Risks. The savings from decommissioning a legacy antivirus solution will vary based upon the solution’s age, its deployment model, and the size of installation.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $806,000.

Decommissioned Software Subscription Costs

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Annual software subscription	Findings	$360,000	$360,000	$360,000
B2	Percent captured	Findings	100%	100%	100%
Bt	Decommissioned software subscription costs	B1*B2	$360,000	$360,000	$360,000
	Risk adjustment	↓10%			
Btr	Decommissioned software subscription costs (risk-adjusted)		$324,000	$324,000	$324,000
	Three-year total: $972,000			**Three-year present value: $805,740**	

TIME SAVINGS FROM INVESTIGATING AND RECOVERING FROM INCIDENTS

Evidence and data. Previous endpoint protection solutions presented frequent events that required investigation on the part of security analysts at the interviewees' organizations. In some cases, IT had to take endpoints offline for cleaning and reimaging. Organizations with few resources struggled to keep up with these tasks, often falling behind on incident investigations. Specific examples from interviewees included:

- One organization could not dedicate sufficient time to reviewing false positives flagged by the legacy endpoint solution. These tasks went away with CylancePROTECT.
- One organization reduced its security staff by three FTEs due to time saved from analyzing signatures after installing CylancePROTECT.
- Reimaging of infected devices occurred one to two times per week at another organization, resulting in several hours of user downtime plus a half day of IT staff time. These events have been eliminated almost entirely.

Modeling and assumptions. For the composite organization, Forrester assumes:

- Security teams spend 30 hours per week investigating potential threats before CylancePROTECT, which total 1,500 hours per year.
- Before CylancePROTECT, IT teams need to quarantine and reimage two endpoints per week, which consumes 4 hours of time, including transportation logistics. This totals 400 hours per year.
- End users lose 8 hours per incident, including time for shipping infected PCs and setting up loaner devices, before CylancePROTECT. This totals 800 hours per year.
- After implementing CylancePROTECT, the composite reclaims the previously lost time and effort. Forrester assumes a 25% productivity recapture rate for the regained time.

Risks. The following factors can affect this benefit:

- The frequency of threats requiring investigation and remediation before CylancePROTECT can vary with the efficacy of the previous legacy endpoint solution.
- IT staff time can vary for the effort required to clean or reimage infected devices and recover data.
- Salaries and burden rates may vary.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $227,000.

> **"CylancePROTECT presents us with relevant data, not just a bunch of false positives. And the community score saves us a bunch of time in terms of managing the system. So, within five minutes, you're done with your daily operational tasks."**
>
> *Director IT, education*

Time Savings From Investigating And Recovering From Incidents					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Annual hours saved from investigating incidents	Findings	1,500	1,500	1,500
C2	Hourly salary - security analyst	TEI standard	$50	$52	$54
C3	Annual hours saved from removing malware and reimaging devices	Findings	400	400	400
C4	Hourly salary - information technology support	TEI standard	$40	$41	$42
C5	End-user downtime recaptured	Findings	800	800	800
C6	End-user average annual salary	TEI standard	$35	$36	$37
C7	Productivity recapture for end users	25%	25%	25%	25%
Ct	Time savings from investigating and recovering from incidents	C1*C2 + C3*C4 + C5*C6*C7	$98,000	$101,600	$105,200
	Risk adjustment	↓10%			
Ctr	Time savings from investigating and recovering from incidents (risk-adjusted)		$88,200	$91,440	$94,680
	Three-year total: $274,320			**Three-year present value: $226,887**	

TIME SAVINGS FROM ELIMINATION OF ANTIVIRUS UPDATES

Evidence and data. A requirement for interviewees' organizations' prior endpoint protection solutions was updating virus signatures for end-user devices on a regular basis. Depending upon the solution in place, these updates could sometimes run in the background, but they often required interaction on the part of end users and coordination from IT staff. With CylancePROTECT, these updates are eliminated. Organizations reported that:

- Antivirus updates consumed up to 15 minutes of end-user time per occurrence.
- One organization had to hire outside resources to help with updates, which required dedicated manual effort on certain devices.
- In cases of automated updates, organizations reported an increase in help desk calls for support.

Modeling and assumptions. For the composite organization, Forrester assumes:

- Each legacy antivirus update consumes 12 minutes of time per end user and updates occur four times per year.
- End-user productivity recapture rate is 25%.
- Each legacy antivirus update consumes 8 hours of IT staff time, again four times per year.

Risks. The following factors can affect this benefit:

- The time and effort required on behalf of end users varies based on the frequency and timing of AV updates and availability of devices.
- Time requirements for IT support of AV updates can also vary based on procedures and scripts in place.
- Salaries and burden rates can vary.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $167,000.

Time Savings From Elimination Of AV Updates					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
D1	Number of workers w devices	Composite	10,000	10,000	10,000
D2	Annual salary - average FTE	TEI standard	$35	$36	$37
D3	Average annual time for AV update (hours)	Findings	0.8	0.8	0.8
D4	Elimination of hours for updates	D1*D2*D3	$280,000	$288,000	$296,000
D5	Productivity recapture	25%	25%	25%	25%
D6	Number of IT staff	Composite	2	2	2
D7	Hourly salary - information technology support	C4	$40	$41	$42
D8	Average annual time for AV update (hours)	Findings	32	32	32
D9	Elimination of hours for updates	D6*D7*D8	$2,560	$2,624	$2,688
Dt	Time savings from elimination of AV updates	D4*D5 + D9	$72,560	$74,624	$76,688
	Risk adjustment	↓10%			
Dtr	Time savings from elimination of AV updates (risk-adjusted)		$65,304	$67,162	$69,019
	Three-year total: $201,485			**Three-year present value: $166,728**	

UNQUANTIFIED BENEFITS

Interviewees mentioned the following additional benefits that their organizations experienced but were not able to quantify:

Enabling incident response support with CylanceOPTICS. Though not a focus of this TEI study, one customer leveraged the CylancePROTECT companion product, CylanceOPTICS, to provide a more comprehensive endpoint detection and response solution. Using CylanceOPTICS, security analysts can create scripts to execute forensic data collection and endpoint remediation steps when an incident occurs. These scripts can execute automatically, giving analysts a head start on incident response.

- **Increasing employee satisfaction and awareness of cybersecurity.** One organization realized significant improvements in employee satisfaction surveys on questions regarding cybersecurity. Scores improved by 25 points compared to surveys conducted prior to implementation of CylancePROTECT. Part of this could be attributed to internal training videos around how users should respond to phishing emails.

"I have peace of mind [knowing that], even if a machine were to become infected, CylancePROTECT would accordingly activate its protection and the machines are safe."

Technical consultant, manufacturing

"I think of [CylanceOPTICS] as part of our overall [endpoint detection and response] solution. It has helped us significantly in incident response situations."

Director IT operations, manufacturing

- **Providing support for multiple device types and operating systems.** Interviewees noted that CylancePROTECT's support of many device types and operating systems was an important selection criterion. This benefit enabled interviewees' organizations to eliminate more endpoint security tools, thereby simplifying the environment. One organization wanted to protect several dozen Windows XP machines that were not connected to the Internet and remarked that CylancePROTECT was the only product on the market that offered this compatibility. This benefit enabled organizations to eliminate more endpoint security tools, thereby simplifying the environment.
- **Delivering peace of mind for security professionals.** All interviewees in the study commented that CylancePROTECT has brought them peace of mind regarding cybersecurity. This reflects their experiences with the solution eliminating all their breaches and the reduced impact on staff and end users relative to traditional antivirus tools. One organization noted it wanted to minimize personal contact between IT support staff and end users during the COVID pandemic, which CylancePROTECT helped enable.

FLEXIBILITY

The value of flexibility is unique to each customer. There are scenarios in which a customer might implement CylancePROTECT and later realize additional uses and business opportunities, including:

- **Support for multiple devices and operating systems.** In addition to being a solution requirement as noted earlier in this report, CylancePROTECT's capability to support multiple device types offers organizations flexibility to expand its protection to additional devices and platforms in the future.

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

"It is great to know that BlackBerry is adding on platforms that it can support. I know that it is looking into different types of security, such as CylancePERSONA™, which learns the behavior of users and mouse clicks. So, I feel as though the company is continuing to develop. I don't think it's stagnated, it's still a leader. I can see it being part of our security strategy for the foreseeable future."

— IT Director, education

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Etr	Subscription license fees	$0	$412,500	$412,500	$412,500	$1,237,500	$1,025,826
Ftr	Implementation costs	$141,350	$0	$0	$0	$141,350	$141,350
Gtr	Administrative costs	$0	$27,665	$28,490	$29,343	$85,498	$70,741
	Total costs (risk-adjusted)	$141,350	$440,165	$440,990	$441,843	$1,464,348	$1,237,917

SUBSCRIPTION LICENSE FEES

Evidence and data. BlackBerry charges an annual per-device license fee for its SaaS solution. This fee is $41.25 (list price) per device for the composite, as provided by the vendor. BlackBerry offers volume discounts for different device points.

Modeling and assumptions. For the composite organization, Forrester assumes that the organization has 10,000 devices using CylancePROTECT. At $41.25 per device, total license costs are $412,500 per year.

Risks. Licensing fees may vary by deal size.

Results. As BlackBerry priced the composite organization directly with Forrester, licensing costs have not been adjusted for risk. This yields a three-year, risk-adjusted total PV (discounted at 0%) of $1.0 million.

Subscription License Fees						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	License fees	Findings	$0	$412,500	$412,500	$412,500
Et	Subscription license fees	E1	$0	$412,500	$412,500	$412,500
	Risk adjustment	0%				
Etr	Subscription license fees (risk-adjusted)		$0	$412,500	$412,500	$412,500
Three-year total: $1,237,500			**Three-year present value: $1,025,826**			

IMPLEMENTATION COSTS

Evidence and data. The approach and timing of implementing CylancePROTECT varied among the interviewees' organizations. Most assigned one or two individuals to do the implementation. This consisted of downloading and installing agents on all devices, setting up the administrative console, and training the IT team. The length of time ranged widely, from less than two weeks to nearly two years. This variability was due to the types of devices protected and the operating systems it was installed on, as well as the number of operating units within the interviewees' organizations. Additional experiences included:

- The interviewees reported that tuning the algorithms was required, which consisted of having CylancePROTECT running in the organizations' environments for a few weeks in an alert-only mode while it reviewed each alert to mark false positives and identify valid alerts. This ensured that CylancePROTECT was optimally blocking legitimate security threats while having no disruption to legitimate day-to-day business operations.
- BlackBerry provided advisory services where needed to interviewees' organizations, usually for one to two weeks. There were no additional fees for these services. The vendor noted that it can provide a consulting services package called ThreatZERO® for the full implementation period. Cost of this service is $54,000, which could reduce internal costs.
- The shortest implementation among organizations in the study was two weeks, with another two to three weeks for tuning.
- Longer implementations were over one year, due in part to updating and configuring older operating systems. Organizations consisting of multiple business units with different environments also took longer periods.

> **"We negotiated implementation services as part of the initial contract. Those implementation services included a dedicated success manager."**
>
> *Director IT operations, manufacturing*

Modeling and assumptions. For the composite organization, Forrester assumes:

- The organization assigns two full-time cybersecurity engineers to manage the implementation for a period of six months.
- All salary expenses include a 30% overhead burden rate to cover benefits and payroll taxes. Additionally, 3% annual increases are factored into each salary.

Risks. The following factors can affect these costs:

- Salaries and burden rates may vary.
- Implementation time will vary based on complexity of the environments, types of endpoints, and operating systems.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $141,000.

Implementation Costs						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
F1	Number of people	Findings	2	0	0	0
F2	Annual salary - cybersecurity engineer	TEI standard	$128,500	$0	$0	$0
F3	Months to install	Findings	6	0	0	0
Ft	Implementation costs	F1*F2*F3/12	$128,500	$0	$0	$0
	Risk adjustment	↑10%				
Ftr	Implementation costs (risk-adjusted)		$141,350	$0	$0	$0
	Three-year total: $141,350			**Three-year present value: $141,350**		

ADMINISTRATIVE COSTS

Evidence and data. Interviewees' organizations typically allocated less than one full-time resource to managing CylancePROTECT. Their responsibilities included:

- Auditing devices and monitoring threats.
- Reviewing memory protection and script control events.
- Auditing user accounts, removing stale devices, updating agents and auditing agent health.
- Reviewing the Cylance community score for unknown files caught by the software. Also, subscribing to the latest alerts and technical resources.

ThreatZERO services were also available to interviewees' organizations as a maintenance service. The fee for this would be $21,000 per year for the composite organization (10,000 endpoints).

Modeling and assumptions. For the composite organization, Forrester assumes:

- The organization assigns one cybersecurity analyst at 25% time to manage and support CylancePROTECT on an ongoing basis.

> **"CylancePROTECT has given us quite a level of confidence that it knows what is bad and quarantines it automatically. We have the rules set up that way. For the ones we have to review, there's just a handful of them where it's unsure or hasn't seen enough samples out there."**
>
> *IT Director, education*

- All salary expenses include a 30% overhead burden rate to cover benefits and payroll taxes. Additionally, 3% annual increases are factored into each salary.

Risks. The following factors can affect these costs:

- The number and time allotment of resources assigned to review CylancePROTECT data. This may decrease over time.
- Salaries and burden rates may vary.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of less than $71,000.

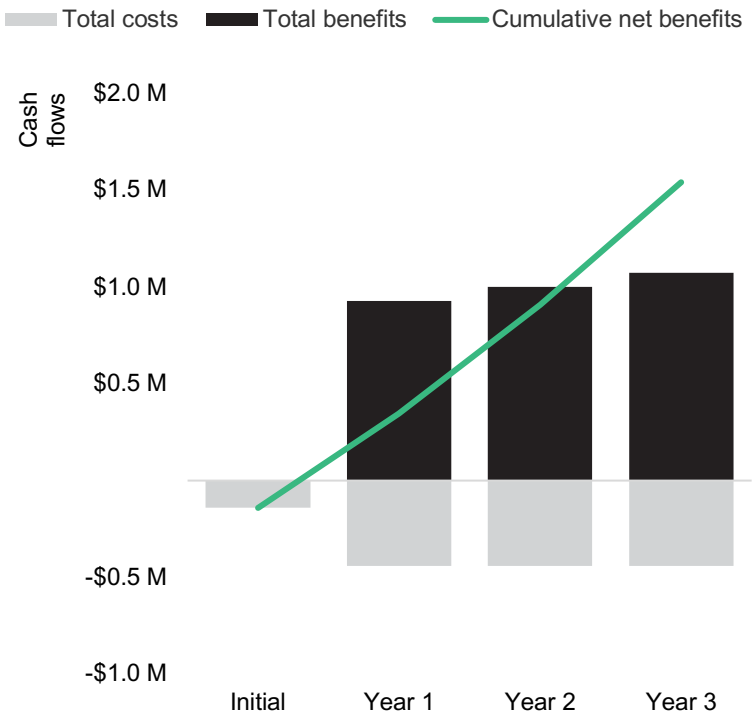
Administrative Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
G1	Number of people	Findings	0	0.25	0.25	0.25
G2	Annual salary - cybersecurity analyst	TEI standard	$0	$100,600	$103,600	$106,700
Gt	Administrative costs	G1*G2	$0	$25,150	$25,900	$26,675
	Risk adjustment	↑10%				
Gtr	Administrative costs (risk-adjusted)		$0	$27,665	$28,490	$29,343
	Three-year total: $85,498			**Three-year present value: $70,741**		

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI, NPV, and payback period values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

Cash Flow Analysis (Risk-Adjusted Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($141,350)	($440,165)	($440,990)	($441,843)	($1,464,348)	($1,237,917)
Total benefits	$0	$929,200	$1,003,536	$1,074,781	$3,007,517	$2,481,595
Net benefits	($141,350)	$489,035	$562,546	$632,939	$1,543,170	$1,243,678
ROI						100%
Payback						<6 months

Appendix A: Total Economic Impact

Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

TOTAL ECONOMIC IMPACT APPROACH

Benefits represent the value delivered to the business by the product. The TEI methodology places equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization.

Costs consider all expenses necessary to deliver the proposed value, or benefits, of the product. The cost category within TEI captures incremental costs over the existing environment for ongoing costs associated with the solution.

Flexibility represents the strategic value that can be obtained for some future additional investment building on top of the initial investment already made. Having the ability to capture that benefit has a PV that can be estimated.

Risks measure the uncertainty of benefit and cost estimates given: 1) the likelihood that estimates will meet original projections and 2) the likelihood that estimates will be tracked over time. TEI risk factors are based on "triangular distribution."

The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations in the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value calculations of the Total Benefits, Total Costs, and Cash Flow tables may not exactly add up, as some rounding may occur.

PRESENT VALUE (PV)

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

NET PRESENT VALUE (NPV)

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

RETURN ON INVESTMENT (ROI)

A project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits less costs) by costs.

DISCOUNT RATE

The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

PAYBACK PERIOD

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

Appendix B: Supplemental Material

Related Forrester Research

"The State Of Endpoint Security, 2022," Forrester Research, Inc., July 21, 2022.

"Now Tech: Endpoint Detection And Response, Q4 2021," Forrester Research, Inc., November 16, 2021.

Appendix C: Endnotes

[1] Trademarks, including but not limited to BLACKBERRY, EMBLEM Design and CYLANCE, are the trademarks or registered trademarks of BlackBerry Limited, used under license, and the exclusive rights to such trademarks are expressly reserved.
[2] Source: Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q1 2021.
[3] Source: Ibid
[4] Source: Ibid

FORRESTER®