A Forrester Total Economic Impact™
Study Commissioned By BlackBerry
Cylance
May 2019

The Total Economic Impact™ Of CylancePROTECT® And CylanceOPTICS™

Cost Savings And Business Benefits Enabled By CylancePROTECT® And CylanceOPTICS™

FORRESTER®

Table Of Contents

Project Director:
Julia Fadzeyeva

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®

Benefits And Costs

Decommissioned on-premises legacy endpoint security software:
$8.4 million PV

Time savings from faster remediation:
$3.3 million PV

Total cost:
$7.0 million PV

Executive Summary

Employee endpoints are the interfaces between employees and the corporate data and applications they need to do their jobs. Attackers understand this — and actively target employee endpoints as well as the server endpoints hosting corporate data. More than 50% of companies experience a significant data breach each year, and endpoints, as a critical conduit for valuable corporate data, are the top targets for attack.[1] Endpoint security solutions provide a critical line of defense, protecting PCs, laptops, and servers from malicious threats.

CylancePROTECT® and CylanceOPTICS™ provide an AI-driven threat prevention, detection, and response security solution that protects endpoints, servers, and cloud workloads. CylancePROTECT offers real-time predictive threat prevention and visibility into the endpoint environment, allowing cybersecurity teams to discover and stop potential threats before they propagate. CylanceOPTICS enables faster enterprisewide threat hunting; security teams can interrogate endpoints in seconds and store critical data for future investigations.

BlackBerry 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 CylancePROTECT and CylanceOPTICS. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of the CylancePROTECT and CylanceOPTICS on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed one representative customer currently using CylancePROTECT and CylanceOPTICS. The customer looked to BlackBerry Cylance for more robust threat protection and wanted an endpoint security solution that was lightweight, easy to deploy, and easy to manage. The customer added endpoint detection and response (EDR) capabilities to quickly alert the cybersecurity team to potential threats.

Prior to using CylancePROTECT and CylanceOPTICS, the customer relied on a legacy on-premises endpoint security solution that did not have EDR capability. This solution required extensive manual workarounds and lacked real-time visibility into threats.

Key Findings

Quantified benefits. The interviewed organization experienced the following risk-adjusted present value (PV) quantified benefits:

- **Decommissioned legacy on-premises endpoint security solution, saving $8.4 million PV**. The organization fully decommissioned its legacy on-premises endpoint security solution after deploying the BlackBerry Cylance software-as-a-service (SaaS) solution.
- **Improved cybersecurity team productivity by 10%.** With BlackBerry Cylance, the cybersecurity team now proactively focuses on threat hunting and investigating more serious threats. Previously, the cybersecurity team spent time reactively troubleshooting and maintaining the legacy endpoint security solution.

FORRESTER®

ROI
99%

Benefits PV
$14.0 million

NPV
$7.0 million

- **Reduced the expected cost of a major security breach by 25 percentage points with more effective malware detection and protection.** BlackBerry Cylance uses AI to block potentially malicious applications and to stop attacks. The interviewee found BlackBerry Cylance to be more effective at threat blocking and protection versus the legacy endpoint security solution, minimizing the likelihood and potential cost of a major security breach.
- **Reduced lost time via faster investigation and remediation by 95%.** With BlackBerry Cylance, fewer end users are compromised. Faster threat investigation and remediation allow end users to quickly resume productive work.
- **Cut machine reimaging by 97%.** With BlackBerry Cylance, the interviewed organization takes fewer machines offline for reimaging. Less reimaging means less lost end user time and less IT time needed to reimage.
- **Eliminated manual software audits.** With BlackBerry Cylance, the cybersecurity team has more control over employee software downloads. If an employee downloads software that could be malicious, BlackBerry Cylance sends an alert to the security team. The software is blocked, and the employee must ask for approval before running the software. This eliminates the need for manual software audits.

Unquantified benefits. The interviewed organization experienced the following benefits, which are not quantified for this study:

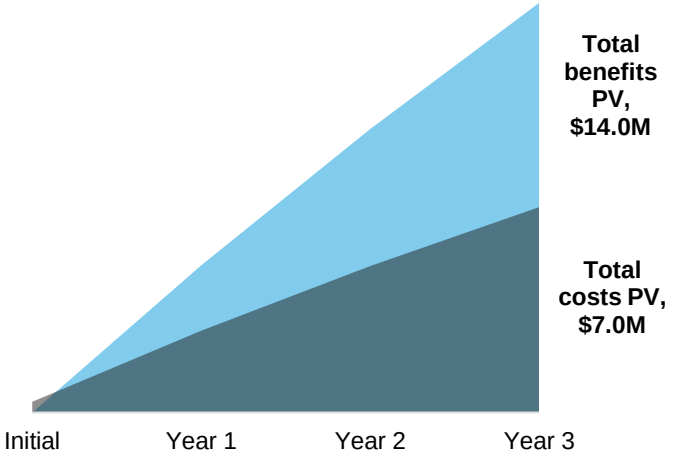
- **Withstanding threats without cloud connection.** The interviewee required endpoint security protection for multiple locations with varying levels of connectivity. Because the BlackBerry Cylance solution runs locally on the endpoint, security does not stop if the machine is not connected.
- **Decommissioning additional endpoint security tools**. Forrester has quantified the benefit of decommissioning the legacy endpoint security system, but the customer also decommissioned several other endpoint protection tools deployed on an ad hoc basis by individual teams. This simplified the endpoint security stack.
- **Limiting the burden on system resources**. Before BlackBerry Cylance, unauthorized software created machine performance issues.

Costs. The interviewed organization experienced the following risk-adjusted PV costs:

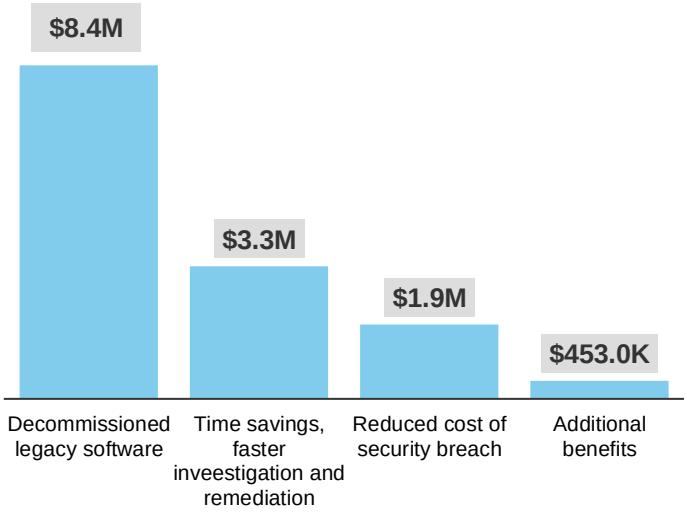
- **BlackBerry Cylance SaaS and service provider fees.** The organization pays an annual fee to its service provider for a bundled solution, including the service provider fee and the CylancePROTECT and CylanceOPTICS SaaS fee.
- **Internal labor cost.** While the service provider takes the lead in investigations and responding to alerts, the internal cybersecurity team devotes resources to manage and steer the service provider.
- **Internal labor installation cost.** The cybersecurity team worked with the service provider to install and test CylancePROTECT and CylanceOPTICS.

Forrester's interview with an existing customer and subsequent financial analysis found that the interviewed organization experienced benefits of $14,047,030 over three years versus costs of $7,044,049, adding up to a net present value (NPV) of $7,002,981 and an ROI of 99%.

Financial Summary



Benefits (Three-Year)



FORRESTER®

TEI Framework And Methodology

From the information provided in the interview, Forrester has constructed a Total Economic Impact™ (TEI) framework for those organizations considering implementing CylancePROTECT and CylanceOPTICS.

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 and CylanceOPTICS can have on an organization:

The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

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

CUSTOMER INTERVIEW
Interviewed one organization using CylancePROTECT and CylanceOPTICS to obtain data with respect to costs, benefits, and risks.

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

CASE STUDY
Employed four fundamental elements of TEI in modeling CylancePROTECT's and CylanceOPTICS's impact: 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 A for additional information on the TEI methodology.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by BlackBerry 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 and CylanceOPTICS.

BlackBerry 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.

BlackBerry Cylance provided the customer name for the interview but did not participate in the interview.

The CylancePROTECT and CylanceOPTICS Customer Journey

BEFORE AND AFTER THE CYLANCEPROTECT AND CYLANCEOPTICS INVESTMENT

Interviewed Organization

For this study, Forrester interviewed the head of cybersecurity at a multinational manufacturing company that is a CylancePROTECT and CylanceOPTICS customer:

- The multinational enterprise is headquartered in Europe and operates 500 locations in 150 countries with 45,000 employees.
- It manufactures tools and tooling systems for industrial metal cutting and provides services and technical solutions for the mining and construction industries, advanced stainless steels and special alloys, and products for industrial heating.
- It has a total revenue of $14 billion annually.
- It runs CylancePROTECT and CylanceOPTICS on 45,000 endpoints.

Key Challenges

The customer had been using an on-premises legacy endpoint security solution in partnership with a service provider. The legacy solution only offered signature-based antivirus (AV) without any EDR capabilities. Multiple challenges prompted the manufacturer to explore new endpoint security tools:

- **Insufficient protection against ransomware, malware, and other threats.** The company experienced multiple ransomware attacks in 2017, including a WannaCry attack that was reported in the media with a potential negative impact on brand reputation.
- **Operational problems with the legacy endpoint security solutions.** The company struggled to update the legacy endpoint security solution. The cybersecurity team was spending considerable time fixing problems with the legacy software, in addition to remediating compromised users and reimaging machines.
- **Lack of visibility into software downloads.** There was no way to effectively manage unauthorized employee software downloads. The unauthorized downloads created hardware performance issues and increased the risk that illegal software or malware could be downloaded and installed.

> "We wanted to move to a solution that was relatively lightweight, easy to deploy, and that we could work with."
>
> *Head of cybersecurity, manufacturing*

FORRESTER®

Key Results

The interview revealed that key results from the CylancePROTECT and CylanceOPTICS investment include:

- **Improved threat protection.** The customer has not experienced any major malware or ransomware attacks since deploying BlackBerry Cylance.
- **Simplicity — a single vision for cyberdefense.** The organization deployed BlackBerry Cylance companywide for endpoint protection. Previously, individual departments often deployed their own endpoint security solutions. Now BlackBerry Cylance provides a single endpoint security tool, and all other endpoint solutions have been decommissioned.
- **Faster threat response and mediation.** With BlackBerry Cylance, better threat protection has reduced the number of compromised users, and any necessary mitigation can be provided within minutes. BlackBerry Cylance has nearly eliminated the need to reimage machines. The cybersecurity team can now spend its time proactively, finding the root cause of problems rather than just providing fixes.
- **Improved visibility and control over employee software downloads.** With BlackBerry Cylance, the cybersecurity team has more control over illegal software or unwanted software within the network. BlackBerry Cylance, in effect, does software audits on a daily basis. If an employee downloads software that could be malicious, BlackBerry Cylance sends an alert to the security team. The software is blocked, and the employee must ask for approval before running the software.

> "I think the key is simplicity. You are rapidly able to deploy Cylance. It doesn't interfere with other solutions you have on the machines."
>
> *Head of cybersecurity, manufacturing*

Analysis Of Benefits

QUANTIFIED BENEFIT DATA

Total Benefits

REF.	BENEFIT	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Atr	Decommissioned legacy on-premises endpoint security solution	$3,375,000	$3,375,000	$3,375,000	$10,125,000	$8,393,125
Btr	Improved cybersecurity team productivity	$64,800	$64,800	$64,800	$194,400	$161,148
Ctr	Reduced cost of a major security breach	$652,500	$749,250	$868,725	$2,270,475	$1,865,083
Dtr	Time savings from faster investigation and remediation	$1,341,375	$1,341,375	$1,341,375	$4,024,125	$3,335,801
Etr	Time savings from less frequent endpoint reimaging	$95,213	$95,213	$95,213	$285,638	$236,780
Ftr	Reduced cost of software audits	$22,154	$22,154	$22,154	$66,462	$55,093
	Total benefits (risk-adjusted)	$5,551,042	$5,647,792	$5,767,267	$16,966,100	$14,047,030

The table above shows the total of all benefits across the areas listed below, 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 more than $14.0 million.

Decommissioned Legacy On-Premises Endpoint Security Solution

The customer completely decommissioned its legacy on-premises endpoint security solution after adopting BlackBerry Cylance.

- The customer paid its former service provider $4.5 million annually to protect 45,000 endpoints. This fee included the cost of on-premises legacy endpoint security software, service provider fees, and underlying infrastructure cost (e.g., servers).

The benefits and cost savings associated with decommissioning a legacy system will vary widely depending on the service provider agreement, legacy software vendor, deployment model, and age of the legacy system.

- The customer decommissioned an on-premises legacy endpoint solution and moved to a SaaS BlackBerry Cylance solution. A shift from a legacy SaaS solution to the BlackBerry Cylance SaaS solution is likely to have different cost savings benefits.

To account for these risks, Forrester adjusted this benefit downward by 25%, yielding a three-year risk-adjusted total PV of $8,393,125.

Impact risk is the risk that the business or technology needs of the organization may not be met by the investment, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for benefit estimates.

Decommissioned Legacy On-premises Endpoint Security Solution: Calculation Table					
REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
A1	Annual on-premises software cost (incl. service provider fee and infrastructure)		$4,500,000	$4,500,000	$4,500,000
A2	Years		1	1	1
At	Decommissioned legacy on-premises endpoint security solution	A1*A2	$4,500,000	$4,500,000	$4,500,000
	Risk adjustment	↓25%			
Atr	Decommissioned legacy on-premises endpoint security solution (risk-adjusted)		$3,375,000	$3,375,000	$3,375,000

Improved Cybersecurity Team Productivity

The manufacturer significantly improved the productivity of its cybersecurity team after implementing CylancePROTECT and CylanceOPTICS. Previously, the cybersecurity team spent time reactively troubleshooting and maintaining the legacy endpoint security solution. The cybersecurity team had to push out daily software for the legacy endpoint security system, but as a SaaS solution, BlackBerry Cylance is always up to date. The cybersecurity team can now proactively focus on threat hunting and investigating more serious threats. CylanceOPTICS gathers and stores data on threats to identify the root cause of attacks and to ensure any vulnerabilities or gaps are addressed before an attack.

> "We were spending most of our resources on fixing things, rather than finding things or working proactively. So the focus was on getting the [legacy] solution to work instead of actually using it."
>
> *Head of cybersecurity, manufacturing*

- The customer had difficulties updating its legacy on-premises endpoint security solution, so the version in use was not the most current. This increased the time the internal security team spent responding to issues.
- The cybersecurity team consists of 16 FTEs. Four to five cybersecurity team FTEs (4.5 FTEs average) were spending time troubleshooting the legacy endpoint security solution and ensuring it was deployed on every client.
- The average fully loaded cybersecurity salary is $160,000.
- While there was no reduction in cybersecurity team staffing, the 4.5 FTEs focusing on endpoint security can now focus on more productive, proactivity activities. Forrester assumes the productivity improvement to be 20%.
- The cybersecurity team converts 50% of the hours saved into productive time.

The improvement in cyberteam productivity will vary with:

- The original level of endpoint security protection.
- The size of the cybersecurity team and number of team members focusing on endpoint security.
- The skill set of the cybersecurity team.

To account for these risks, Forrester adjusted this benefit downward by 25%, yielding a three-year risk-adjusted total PV of $161,148.

Improved Cybersecurity Team Productivity: Calculation Table					
REF.	**METRIC**	**CALC.**	**YEAR 1**	**YEAR 2**	**YEAR 3**
B1	Cybersecurity FTEs focusing on endpoint security		4.5	4.5	4.5
B2	Cybersecurity team annual salary per FTE		$160,000	$160,000	$160,000
B3	Productivity improvement with BlackBerry Cylance		20%	20%	20%
B4	Productivity recapture		50%	50%	50%
Bt	Improved cybersecurity team productivity	B1*B2*B3*B4	$72,000	$72,000	$72,000
	Risk adjustment	↓10%			
Btr	Improved cybersecurity team productivity (risk-adjusted)		$64,800	$64,800	$64,800

Reduced Cost Of A Major Security Breach

The customer experienced multiple malware attacks in 2017, including a WannaCry ransomware attack. The press reported on the WannaCry attack, and the company was concerned the attack had a potential negative impact on its brand reputation. The ransomware attack was a key turning point in the company's decision to implement a new endpoint security solution.

- The customer has not experienced any major malware attacks since installing BlackBerry Cylance. During the rollout process, BlackBerry Cylance alerted the customer to a ransomware outbreak, while the legacy endpoint solution did not.

Reducing the number of breaches, and even the risk of a breach, saves organizations from costly cleanup and recovery efforts. Forrester looked to the Ponemon 2017 Cost of Cybercrime study for the average cost of malware and ransomware attacks.[2] Forrester assumes that:

- The customer started with a 30% risk of a major ransomware or malware attack while using the legacy endpoint security solution. The risk of a major attack has dropped to 5% with BlackBerry Cylance.
- The average annual cost of a malware attack is $2.4 million, growing at 20% per year.
- The average annual cost of a ransomware attack is $0.5 million, decreasing at 10% per year.
- The average cost of a ransomware and malware attack is stable over the next three years.

The reduction in the expected cost of a security breach will vary:

- New malware and security threats are constantly emerging. For example, cyberjacking has recently gained prominence as a new and growing security risk. The expected costs of new security threats could vary widely.
- The expected cost of a security breach will depend on the specifics of the organization, including size, industry, and geography.

To account for these risks, Forrester adjusted this benefit downward by

BlackBerry Cylance alerted the customer to a ransomware outbreak that the legacy system missed, during the rollout when both systems were running in parallel.

10%, yielding a three-year risk-adjusted total PV of $1,865,083.

Reduced Cost Of A Major Security Breach: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
C1	Average annual cost of a malware attack	Increasing at 20% per year	$2,400,000	$2,880,000	$3,456,000
C2	Average annual cost of a ransomware attack	Decreasing at 10% per year	$500,000	$450,000	$405,000
C3	Average annual cost of a major malware and ransomware breach before implementing Cylance	C1+C2	$2,900,000	$3,330,000	$3,861,000
C4	Risk of a major breach before implementing Cylance		30%	30%	30%
C5	Risk of a major breach after implementing Cylance		5%	5%	5%
C6	Reduction in risk of major breach	(C4-C5)	25%	25%	25%
Ct	Reduced cost of a major security breach	C3*C6	$725,000	$832,500	$965,250
	Risk adjustment	↓10%			
Ctr	Reduced expected cost of a major security breach (risk-adjusted)		$652,500	$749,250	$868,725

Time Savings From Faster Investigation And Remediation

The customer now has fewer compromised users and can remediate issues more quickly with BlackBerry Cylance. CylancePROTECT stops attacks before they happen by using AI to inspect applications that are attempting to execute on an endpoint, so the overall number of attacks is reduced. In the rare cases that there is a compromised user, CylanceOPTICS allows the cybersecurity team to quickly review files and activities that have been tagged as suspicious to determine if an endpoint has been compromised. This speeds the investigation process, and the appropriate mitigation can be dispatched within minutes.

- The manufacturer was seeing 50 compromised users per day with the legacy endpoint security solution. With BlackBerry Cylance, there are usually zero or somedays one compromised user.
- BlackBerry Cylance allows the customer to quickly mitigate issues. Because it's a SaaS solution, mitigation protection can be implemented within just minutes.

Forrester assumes that:

- When a user machine is compromised, the average knowledge worker loses 4 hours of time.
- The average annual, fully loaded knowledge worker salary is $104,000.
- The knowledge worker converts 50% of the hours saved by faster remediation into productive time.

The time savings benefit will vary with:

- An organization's original level of protection.

> "Now with Cylance, if we detect something, we are able to look into the clients, preempt, and deploy the mitigation protection just within minutes."
>
> *Head of cybersecurity, manufacturing*

> "We have gone from around 50 compromised users each day to around zero or one somedays. The situation has totally changed for us."
>
> *Head of cybersecurity, manufacturing*

FORRESTER®

- Time to remediate a compromised user.
- Average salaries.

To account for these risks, Forrester adjusted this benefit downward by 25%, yielding a three-year risk-adjusted total PV of $3,335,801.

Time Savings From Faster Investigation And Remediation: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
D1	Compromised users per day with prior solution		50	50	50
D2	Compromised users per day with Cylance		1	1	1
D3	Reduction in compromised users per day with Cylance	D1-D2	49	49	49
D4	End user productivity loss due to compromise (hours per incident)		4	4	4
D5	End user productivity loss due to compromise (hours per year)	D3*D4*365	71,540	71,540	71,540
D6	Average hourly rate for knowledge worker	$104,000/2,080	$50	$50	$50
D7	End user annual time savings	D5*D6	$3,577,000	$3,577,000	$3,577,000
D8	Productivity recapture		50%	50%	50%
Dt	Time savings from faster investigation and remediation	D7*D8	$1,788,500	$1,788,500	$1,788,500
	Risk adjustment	↓25%			
Dtr	Time savings from faster investigation and remediation (risk-adjusted)		$1,341,375	$1,341,375	$1,341,375

Time Savings From Less Frequent Endpoint Reimaging

BlackBerry Cylance has nearly eliminated the need to reimage machines. BlackBerry Cylance allows remote mitigation of most problems rather than taking a machine offline to reimage. Less reimaging means the BlackBerry Cylance solution saves both IT time and end user time. With fewer machines to reimage, the cybersecurity team can now focus on getting to the root cause of the problem.

- The manufacturer reimaged five to 10 machines per week with the legacy endpoint security solution.
- The reimaging process often meant waiting 24 hours to receive updated files from the legacy software vendor.
- With BlackBerry Cylance, there have been zero machines reimaged to date.

Forrester assumes that:

- Under the legacy solution, 30 machines were reimaged each month. With BlackBerry Cylance, only one machine is reimaged per month.
- It takes 8 hours to reimage a machine, but during that time, the IT service desk technician can also work on other tasks. Only 20% of the IT service desk technician's time is spent actively on the reimaging.

> "We haven't reimaged the machines with Cylance yet. As soon as we see something, we are able to mitigate most of the problems remotely instead."
>
> *Head of cybersecurity, manufacturing*

- The average annual, fully loaded IT service desk technician salary is $135,200.
- When a user machine needs to be reimaged, the average knowledge worker loses 4 hours of time.
- The average annual, fully loaded knowledge worker salary is $104,000.
- The IT service desk technician and knowledge worker convert 50% of the hours saved by faster remediation into productive time.

The time savings benefit will vary with:

- An organization's original level of endpoint protection.
- Average time spent by an IT service desk technician to reimage a compromised machine.
- Average salaries.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $236,780.

> "As we have lowered the number of infected machines, we are able to investigate where its coming from and what harm it is doing to the machine instead of just remediating. Now we are able to find a root cause."
>
> *Head of cybersecurity, manufacturing*

Time Savings From Less Frequent Endpoint Reimaging: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
E1	Endpoints reimaged (per month) with on-premises solution		30	30	30
E2	Endpoints reimaged (per month) with Cylance		1	1	1
E3	Reduction in endpoints reimaged (per month) with Cylance	E1-E2	29	29	29
E4	Time to reimage per machine (hours)		8	8	8
E5	IT active time during reimaging %		20%	20%	20%
E6	Average hourly rate for IT	$135,200/2,080	$65	$65	$65
E7	IT productivity saved with Cylance	E3*E4*E5*E6*12 months	$36,192	$36,192	$36,192
E8	End user time lost to reimaging (hours per incident)		4	4	4
E9	Average hourly rate for knowledge worker	$104,000/2,080	$50	$50	$50
E10	End user productivity saved with Cylance	E3*E8*E9* 12 months	$69,600	$69,600	$69,600
Et	Time savings from less frequent endpoint reimaging	E7+E10	$105,792	$105,792	$105,792
	Risk adjustment	↓10%			
Etr	Time savings from less frequent endpoint reimaging (risk-adjusted)		$95,213	$95,213	$95,213

Reduced Cost Of Software Audits

With BlackBerry Cylance, the cybersecurity team has much more control over illegal software or unwanted software within the network.

Previously, the cybersecurity team had limited visibility into employee software downloads and had to conduct regular software audits to identify unauthorized software.

- Before BlackBerry Cylance, the manufacturer did three or four software audits per year. The software audit was manual and therefore required significant effort. Each audit took about a week with two cybersecurity analysts devoted to the project.
- With BlackBerry Cylance, the customer, in effect, does software audits on a daily basis. If an employee downloads software that could be malicious, BlackBerry Cylance sends an alert to the security team. The software is blocked, and the employee must ask for approval before running the software.

> "There is much more control over illegal software or legacy software within the network."
>
> *Head of cybersecurity, manufacturing*

Forrester assumes that:

- Software audits previously took place quarterly, and each audit took one week.
- Two FTE security analysts were previously required for the software audits.
- The average annual, fully loaded cybersecurity salary is $160,000.

The time savings benefit will vary with:

- Frequency and time to conduct a software audit.
- Average salaries.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $55,093.

Reduced Cost Of Software Audits: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
F1	Software license audits per year		4	4	4
F2	Time per audit (weeks)		1	1	1
F3	Security analyst FTEs required for software audit		2	2	2
F4	Security operations staff fully loaded annual salary per FTE		$160,000	$160,000	$160,000
Ft	Reduced cost of software audits	F1*F2*F3*F4/52	$24,615	$24,615	$24,615
	Risk adjustment	↓10%			
Ftr	Reduced cost of software audits (risk-adjusted)		$22,154	$22,154	$22,154

Unquantified Benefits

CylancePROTECT and CylanceOPTICS provides additional unquantified benefits to the interviewed organization.

- **The client can withstand threats without cloud connection.** The customer required endpoint security protection for multiple locations with varying levels of connectivity. In the interview, the customer commented that for a company with many remote sites it was important for "the client to be able to withstand threats without constantly needing to connect to the cloud."

› **The organization could decommission additional endpoint security tools**. Forrester has quantified the benefit of the decommissioned legacy endpoint security system, but the customer also decommissioned other endpoint protection tools deployed on an ad hoc basis by individual teams. This simplified the endpoint security stack.

Flexibility

The value of flexibility is clearly unique to each customer, and the measure of its value varies from organization to organization. There are multiple scenarios in which a customer might choose to implement CylancePROTECT and CylanceOPTICS and later realize additional uses and business opportunities, including:

› **Enabling more flexibility for the cybersecurity team**. Before implementing BlackBerry Cylance, the cybersecurity team was caught up in the daily noise of managing the solution. Now, the team has more flexibility to spend time on investigations and threat hunting.

Flexibility would also be quantified when evaluated as part of a specific project.

BlackBerry Cylance protects clients in remote locations without constantly connecting to the cloud, since the threat protection runs locally on the endpoint.

Flexibility, as defined by TEI, represents an investment in additional capacity or capability that could be turned into business benefit for a 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.

Analysis Of Costs

QUANTIFIED COST DATA

Total Costs

REF.	COST	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Gtr	BlackBerry Cylance SaaS and service provider fees	$349,832	$2,598,750	$2,598,750	$2,598,750	$8,146,082	$6,812,538
Htr	Internal labor cost	$0	$84,000	$84,000	$84,000	$252,000	$208,896
Itr	Implementation internal labor cost	$22,615	$0	$0	$0	$22,615	$22,615
	Total costs (risk-adjusted)	$372,447	$2,682,750	$2,682,750	$2,682,750	$8,420,697	$7,044,049

The table above shows the total of all costs across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the interviewed organization expects risk-adjusted total costs to be a PV of more than $7.0 million.

BlackBerry Cylance SaaS And Service Provider Fees

The manufacturer deployed the CylancePROTECT and CylanceOPTICS SaaS solution in partnership with a service provider.

- For a 45,000-endpoint deployment, a customer typically pays its service provider a bundled fee of $2.6 million annually.
- The fee to the service provider includes the cost of both the service provider's services and the cost of the BlackBerry Cylance SaaS solution subscription.
- The customer ran a pilot on 500 machines, testing BlackBerry Cylance for three months. Then the customer rolled the product out to the entire organization of 45,000 endpoints.
- The customer incurred CylancePROTECT and CylanceOPTICS SaaS subscription and service provider fees during the initial implementation period. The enterprisewide, full-scale implementation took four weeks. The customer subsequently ran both BlackBerry Cylance and the legacy solution in parallel for three weeks, resulting in a total implementation time of seven weeks.

Implementation risk is the risk that a proposed investment may deviate from the original or expected requirements, resulting in higher costs than anticipated. The greater the uncertainty, the wider the potential range of outcomes for cost estimates.

The cost will vary based on:

- The number of endpoints.
- Customer-specific pricing including any discounts.
- The time to implement the BlackBerry Cylance solution.
- The type and breadth of services provided by the service provider.

Software subscription costs and service provider fees will vary by organization. Costs will vary based on the service provider service offering, different software licensing agreements, what other products may be licensed from BlackBerry Cylance, and potential discounts.

To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year risk-adjusted total PV of $6,812,538.

Cylance SaaS And Service Provider Fees: Calculation Table						
	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
G1	Annual Cylance SaaS and service provider fees		$2,475,000	$2,475,000	$2,475,000	$2,475,000
G2	Time to implement, test, and run parallel with legacy system (weeks)		7			
G3	Cylance SaaS and service provider fees during implementation	G1*G2/52	$333,173			
G4	Cylance SaaS and service provider fee, annual fee post installation			$2,475,000	$2,475,000	$2,475,000
Gt	Cylance SaaS and service provider fees	G3+G4	$333,173	$2,475,000	$2,475,000	$2,475,000
	Risk adjustment	↑5%				
Gtr	Cylance SaaS and service provider fees (risk-adjusted)		$349,832	$2,598,750	$2,598,750	$2,598,750

Internal Labor Cost

The manufacturer estimates that managing the BlackBerry Cylance platform requires 50% of one security team resource.

- The service provider takes the lead in investigations and responding to alerts.
- The internal cybersecurity team primarily manages and steers the service provider.
- The average fully loaded internal security analyst salary is $160,000.

These costs will vary based on:

- The skill set of the internal security team.

Internal labor costs may also vary depending the agreement with the service provider and service provider's expertise and capability.

To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year risk-adjusted total PV of $208,896.

One FTE spends 50% of their time on ongoing management of CylancePROTECT and CylanceOPTICS.

Internal Labor Cost: Calculation Table						
REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
H1	Security analyst for internal support			1	1	1
H2	% of time dedicated to managing CylancePROTECT and CylanceOPTICS			50%	50%	50%
H3	Security analyst fully loaded annual salary			$160,000	$160,000	$160,000
Ht	Internal labor cost	H1*H2*H3		$80,000	$80,000	$80,000
	Risk adjustment	↑5%				
Htr	Internal labor cost (risk-adjusted)		$0	$84,000	$84,000	$84,000

Implementation Internal Labor Cost

The manufacturer dedicated one internal security resource to initial implementation of BlackBerry Cylance.

- The average fully loaded security salary is $160,000.
- The customer ran a trial on 500 machines and then began a full companywide BlackBerry Cylance deployment. The implementation period was seven weeks, including four weeks for the enterprisewide installation and three weeks to test and run the BlackBerry Cylance system and the legacy system in parallel.
- The customer took steps during the installation process to manage false positives. The company ran BlackBerry Cylance for one week and then analyzed and classified the false positives to minimize the false positives during deployment.

These costs will vary based on:

- The size of the deployment, including the number of endpoints.
- The skill set of the internal security team.

To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year risk-adjusted total PV of $22,615.

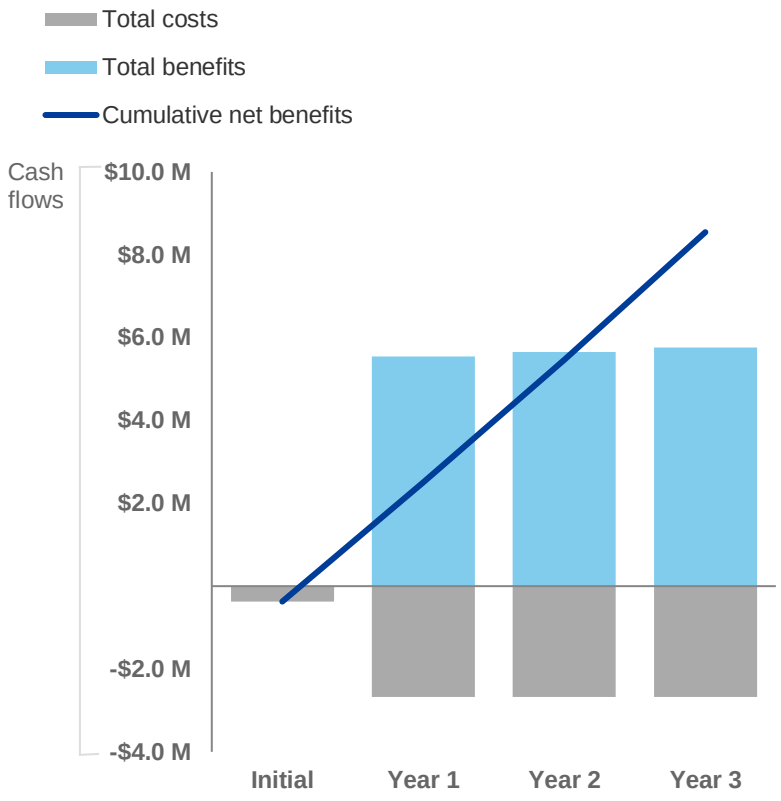
Implementation Internal Labor Cost: Calculation Table

REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
I1	Time to implement and test (weeks)		7			
I2	Security resources dedicated to implementation		1			
I3	Security analyst fully loaded annual salary		$160,000			
It	Implementation internal labor cost	I1/52*I2*I3	$21,538	$0	$0	$0
	Risk adjustment	↑5%				
Itr	Implementation internal labor cost (risk-adjusted)		$22,615	$0	$0	$0

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 and NPV for the interviewed organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

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

Cash Flow Table (Risk-Adjusted)

	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Total costs	($372,447)	($2,682,750)	($2,682,750)	($2,682,750)	($8,420,697)	($7,044,049)
Total benefits	$0	$5,551,042	$5,647,792	$5,767,267	$16,966,100	$14,047,030
Net benefits	($372,447)	$2,868,292	$2,965,042	$3,084,517	$8,545,403	$7,002,981
ROI						99%

FORRESTER®

CylancePROTECT® and CylanceOPTICS™: Overview

The following information is provided by BlackBerry Cylance. Forrester has not validated any claims and does not endorse BlackBerry Cylance or its offerings.

CylancePROTECT and CylanceOPTICS: Your AI-Driven Threat Prevention, Detection, and Response Solution

Simplifying your endpoint security stack while maintaining a secure environment can make your security team's work easier and their efforts far more efficient. The BlackBerry Cylance security platform, comprised of CylancePROTECT and CylanceOPTICS, can help you consolidate and distill the security tools your team uses down to a manageable set, in turn reducing redundancies, eliminating high infrastructure expenses, and improving your team's ability to more proactively secure your endpoints.

With CylancePROTECT and CylanceOPTICS, you get *real-time predictive threat prevention* combined with *prevention-based detection and incident response*. Built from the ground up to easily scale with your business, the solution delivers the following security functionality:

CylancePROTECT®	CylanceOPTICS™
› AI-driven malware prevention	› AI-driven root-cause analysis
› Real-time memory protection	› Enterprisewide threat hunting
› Integrated script and application control	› Dynamic threat detection
› Device usage policy enforcement	› Automated incident response

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: Endnotes

[1] Source: Forrester Analytics' Business Technographics® Security Survey, 2018
[2] Source: "2017 Cost of Cyber Crime Study," Ponemon Institute, October 1, 2017 (https://www.ponemon.org/blog/2017-cost-of-cyber-crime-study).