The Total Economic Impact™ Of CylancePROTECT® And CylanceOPTICS™

Cost Savings And Business Benefits Enabled By CylancePROTECT® And CylanceOPTICS™
# Table Of Contents

## Executive Summary
- Key Findings 1
- TEI Framework And Methodology 4

## The CylancePROTECT and CylanceOPTICS Customer Journey
- Interviewed Organization 5
- Key Challenges 5
- Key Results 6

## Analysis Of Benefits
- Decommissioned Legacy On-Premises Endpoint Security Solution 7
- Improved Cybersecurity Team Productivity 8
- Reduced Cost Of A Major Security Breach 9
- Time Savings From Faster Investigation And Remediation 10
- Time Savings From Less Frequent Endpoint Reimaging 11
- Reduced Cost Of Software Audits 12
- Unquantified Benefits 13
- Flexibility 14

## Analysis Of Costs
- BlackBerry Cylance SaaS And Service Provider Fees 15
-Internal Labor Cost 16
- Implementation Internal Labor Cost 17

## Financial Summary
- CylancePROTECT® and CylanceOPTICS™: Overview 19

## Appendix A: Total Economic Impact 20

## Appendix B: Endnotes 21

---

**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.

© 2019, Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. For additional information, go to forrester.com.
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.
Reduction of 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%.
The Total Economic Impact™ Of CylancePROTECT® and CylanceOPTICS™

Financial Summary

Total benefits PV, $14.0M
Total costs PV, $7.0M

Initial Year 1 Year 2 Year 3

Benefits (Three-Year)

Decommissioned legacy software
Time savings, faster investigation and remediation
Reduced cost of security breach
Additional benefits

Benefits:

- Decommissioned legacy software: $8.4M
- Time savings, faster investigation and remediation: $3.3M
- Reduced cost of security breach: $1.9M
- Additional benefits: $453.0K

Initial benefits: $8.4M
Year 1 benefits: $3.3M
Year 2 benefits: $1.9M
Year 3 benefits: $453.0K

Decommissioned legacy software
Time savings, faster investigation and remediation
Reduced cost of security breach
Additional benefits

Benefits (Three-Year)
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 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:

**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*
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

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

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.
**The Total Economic Impact™ Of CylancePROTECT® and CylanceOPTICS™**

**Improve 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.

- 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.

---

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

## Reduced Cost Of A Major Security Breach: Calculation Table

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

### Reduced Cost of a Major Security Breach

<table>
<thead>
<tr>
<th>REF.</th>
<th>METRIC</th>
<th>CALC.</th>
<th>YEAR 1</th>
<th>YEAR 2</th>
<th>YEAR 3</th>
</tr>
</thead>
</table>

### 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*
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

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

### 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 reimagining 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 reimagining 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 reimagined 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 reimagining.

“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.

### Time Savings From Less Frequent Endpoint Reimaging: Calculation Table

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

> “As we have lowered the number of infected machines, we are able to investigate where it is 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*

---

**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.

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

<table>
<thead>
<tr>
<th>REF.</th>
<th>METRIC</th>
<th>CALC.</th>
<th>YEAR 1</th>
<th>YEAR 2</th>
<th>YEAR 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>F1</td>
<td>Software license audits per year</td>
<td></td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>F2</td>
<td>Time per audit (weeks)</td>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>F3</td>
<td>Security analyst FTEs required for software audit</td>
<td></td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>F4</td>
<td>Security operations staff fully loaded annual salary per FTE</td>
<td></td>
<td>$160,000</td>
<td>$160,000</td>
<td>$160,000</td>
</tr>
<tr>
<td>F1<em>F2</em>F3*F4/52</td>
<td>Reduced cost of software audits</td>
<td></td>
<td>$24,615</td>
<td>$24,615</td>
<td>$24,615</td>
</tr>
<tr>
<td></td>
<td>Risk adjustment</td>
<td></td>
<td>↓10%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F1<em>F2</em>F3<em>F4</em>F5/52</td>
<td>Reduced cost of software audits (risk-adjusted)</td>
<td></td>
<td>$22,154</td>
<td>$22,154</td>
<td>$22,154</td>
</tr>
</tbody>
</table>

### 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.
The Total Economic Impact™ Of CylancePROTECT® and CylanceOPTICS™

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 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 million.

<table>
<thead>
<tr>
<th>REF.</th>
<th>COST</th>
<th>INITIAL</th>
<th>YEAR 1</th>
<th>YEAR 2</th>
<th>YEAR 3</th>
<th>TOTAL</th>
<th>PRESENT VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gtr</td>
<td>BlackBerry Cylance SaaS and service provider fees</td>
<td>$349,832</td>
<td>$2,598,750</td>
<td>$2,598,750</td>
<td>$2,598,750</td>
<td>$8,146,082</td>
<td>$6,812,538</td>
</tr>
<tr>
<td>Htr</td>
<td>Internal labor cost</td>
<td>$0</td>
<td>$84,000</td>
<td>$84,000</td>
<td>$84,000</td>
<td>$252,000</td>
<td>$208,896</td>
</tr>
<tr>
<td>Itr</td>
<td>Implementation internal labor cost</td>
<td>$22,615</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$22,615</td>
<td>$22,615</td>
</tr>
</tbody>
</table>

Total costs (risk-adjusted) | $372,447 | $2,682,750 | $2,682,750 | $2,682,750 | $8,420,697 | $7,044,049 |

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.

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.
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.
  - 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.

## Cylance SaaS And Service Provider Fees: Calculation Table

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

## Internal Labor Cost: Calculation Table

<table>
<thead>
<tr>
<th>REF.</th>
<th>METRIC</th>
<th>CALC.</th>
<th>INITIAL</th>
<th>YEAR 1</th>
<th>YEAR 2</th>
<th>YEAR 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1</td>
<td>Security analyst for internal support</td>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>H2</td>
<td>% of time dedicated to managing CylancePROTECT and CylanceOPTICS</td>
<td>50%</td>
<td>50%</td>
<td>50%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H3</td>
<td>Security analyst fully loaded annual salary</td>
<td>$160,000</td>
<td>$160,000</td>
<td>$160,000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ht</td>
<td>Internal labor cost</td>
<td>H1<em>H2</em>H3</td>
<td>$80,000</td>
<td>$80,000</td>
<td>$80,000</td>
<td></td>
</tr>
<tr>
<td>Htr</td>
<td>Internal labor cost (risk-adjusted)</td>
<td></td>
<td>$0</td>
<td>$84,000</td>
<td>$84,000</td>
<td>$84,000</td>
</tr>
<tr>
<td></td>
<td>Risk adjustment</td>
<td>↑5%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

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

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

<table>
<thead>
<tr>
<th>CylancePROTECT®</th>
<th>CylanceOPTICS™</th>
</tr>
</thead>
<tbody>
<tr>
<td>› AI-driven malware prevention</td>
<td>› AI-driven root-cause analysis</td>
</tr>
<tr>
<td>› Real-time memory protection</td>
<td>› Enterprise-wide threat hunting</td>
</tr>
<tr>
<td>› Integrated script and application control</td>
<td>› Dynamic threat detection</td>
</tr>
<tr>
<td>› Device usage policy enforcement</td>
<td>› Automated incident response</td>
</tr>
</tbody>
</table>


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.
Appendix B: Endnotes

1 Source: Forrester Analytics’ Business Technographics® Security Survey, 2018