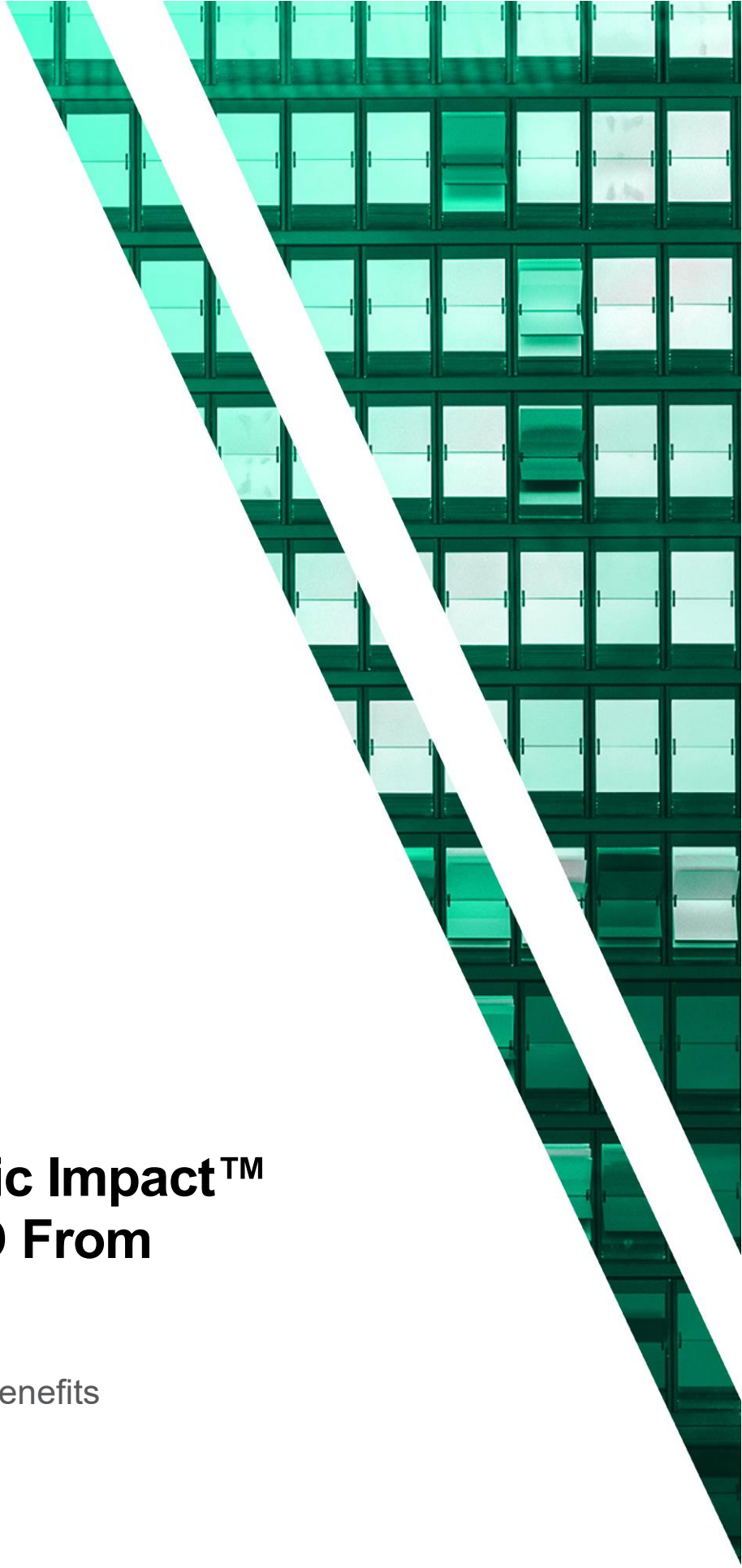
FORRESTER®



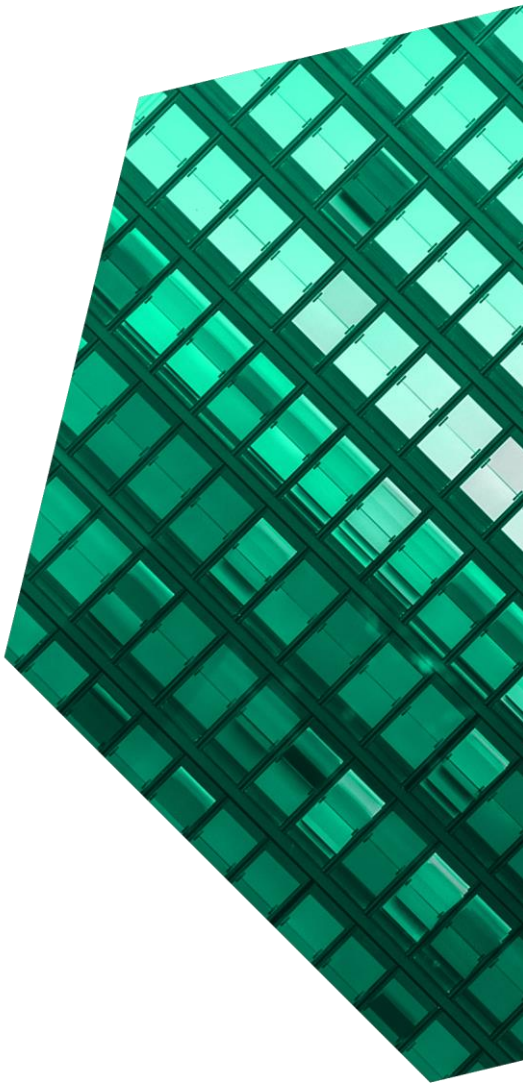
The Total Economic Impact™ Of CylanceGUARD From BlackBerry

Cost Savings And Business Benefits Enabled By CylanceGUARD

OCTOBER 2023

Table Of Contents

Consulting Team: Henry Huang
Kara Luk



ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key transformation outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute on their priorities using a unique engagement model that tailors to diverse needs and ensures lasting impact. For more information, visit forrester.com/consulting.

Executive Summary

Bad actors in the cyberworld are plentiful, but cyberprotectors are not. When companies need to scale, this issue is magnified further. As malicious activities emerge more frequently, the need to protect is increasingly difficult, requiring the need for managed detection and response (MDR) to take part in mitigating risk across the enterprise. Forrester's research indicates that a majority of organizations need a MDR partner to augment and complement internal security resources to be defensible.[1]

Organizations find that CylanceGUARD®, the BlackBerry MDR service, is the arm that enables the body of their security operations center (SOC) to combat malicious activity. CylanceGUARD adds to the operational capability of organizations with MDR services on a 24/7 level, complete with an endpoint protection platform (EPP) to cover activity that goes beyond signature-based detection for both known and zero-day threats.

BlackBerry commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying CylanceGUARD.[2] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of CylanceGUARD on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four representatives from SMB and mid-market organizations with experience using CylanceGUARD. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization that is a B2B organization with 3,000 employees and a revenue of over $100 million per year.

KEY STATISTICS

Return on investment (ROI)
293%

Net present value (NPV)
$2.16M

Incidents avoided with CylanceGUARD
98%

Prior to using CylanceGUARD, these interviewees noted that they had leaned heavily upon their internal resources, which were overburdened. This left their security teams with a continuous amount of security events to identify and remediate, leaving them with little time to stay ahead of perpetrators. It was a constant battle to combat bad actors with little room to address large-scale breaches.

After the investment in CylanceGUARD, the interviewees were able to address the majority of incidents so that their internal teams could concentrate on threat hunting and improving the security posture of the organization.

Key results from the investment include lower operational effort to manage security incidents,

protect assets faster and sooner when placed into production, and finally remove legacy security point solutions.

KEY FINDINGS

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

- **Reduction of 90% of internal security operations effort with the CylanceGUARD service.** Security incidents that the composite organization needs to handle are reduced both through the EPP and the monitored and managed services by BlackBerry. With the additive intelligence provided by BlackBerry, internal information security (infosec) operators and IT response teams also drastically reduce triage and investigation times. The benefit of shifting a large portion of security labor to BlackBerry, especially in the case of 24x7x365 protection, provides a benefit of $917,000 PV over three years.
- **Faster to protect new assets by 90% while using fewer people resources.** With CylanceGUARD, protecting assets is immediate for the composite organization and requires few internal resources to defend against malicious activity. The resources available from CylanceGUARD make it possible to defend incidents immediately, with a significantly lower mean time to remediate (MTTR). The composite organization reaps the benefit of $410,000 from standing up security faster.
- **Reallocation of personnel by sunsetting legacy solutions.** The composite organization reallocates two security and operations (SecOps) personnel and three IT personnel to alternative tasks, such as threat hunting and service-level agreement (SLA) improvement, upon retiring existing Endpoint protection platforms (EPP)/Endpoint detection and response (EDR) solutions. The analysts and engineers are able to move from operational activities to other high-value tasks, such as threat hunting and recovery of end-user systems, providing a benefit of $1.6 million PV over three years.

Unquantified benefits. Benefits that provide value for the interviewees' organizations but are not quantified in this study include:

- **Regulatory and institutional fines were prevalent and averted by CylanceGUARD but could vary greatly between different types of organizational verticals.** Some interviewees indicated that by using CylanceGUARD, they caught incidents involving payment data that would have fallen under payment card industry (PCI) regulations. The deflection of such fines was highly variable between the interviewees' organizations and thus not asserted as a quantified benefit.
- **The use of CylanceGUARD decreased the need to produce additional hires.** Due to the optionality available for managed services and in the interest of not duplicating the count of benefits, this benefit has not been quantified. However, this factor is a variable between different organizations due to existing security resources and could potentially be a greater benefit for many organizations.

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

- **Licensing and MDR costs.** The cost of CylanceGUARD is based on the licensing of the BlackBerry EPP solution, CylanceENDPOINT™, which also encapsulates the cost of managed detection and response at a 24x7x365 level. Over the course of three years, the PV costs amount to approximately $725,800.
- **Onboarding and training costs.** In switching to an MDR solution, the composite organization onboards IT operations (ITOps) employees as well as SecOps employees to work with

CylanceGUARD so that the solution becomes an extension of the in-house operational staff. The cost includes initial onboarding and the turnover of employees across a three-year period amounting to $12,000 PV.

The representative interviews and financial analysis found that a composite organization experiences benefits of $2.90M over three years versus costs of $738K, adding up to a net present value (NPV) of $2.16M and an ROI of 293%.

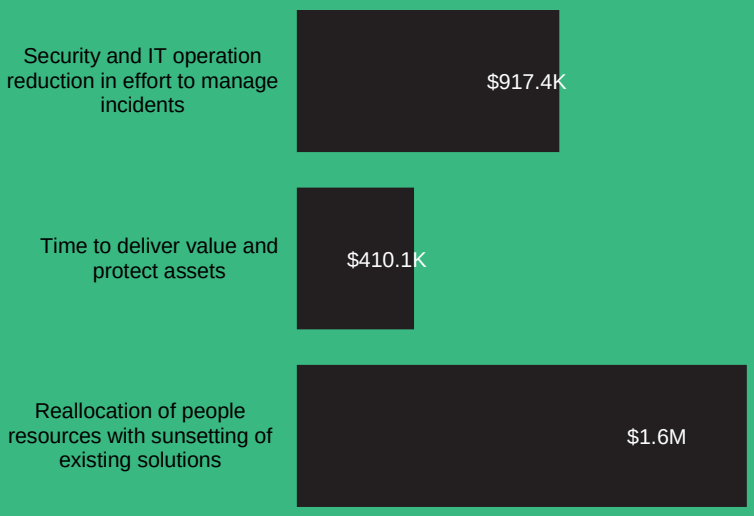
ROI
293%

BENEFITS PV
$2.90M

NPV
$2.16M

PAYBACK
<6 months

Benefits (Three-Year)



Security incidents are deflected by 90% with CylanceGUARD.

CylanceGUARD protects 24x7x365, filling a gap for traditional infosec teams.

“The biggest benefit is the coverage that it provides us, because we don’t have a 24/7 IT operations. The CylanceGUARD team will take care of it … even when we are sleeping”

— CIO, professional services

TEI FRAMEWORK AND METHODOLOGY

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

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 CylanceGUARD can have on an organization.

Forrester Consulting conducted an online survey of 351 cybersecurity leaders at global enterprises in the US, the UK, Canada, Germany, and Australia. Survey participants included managers, directors, VPs, and C-level executives who are responsible for cybersecurity decision-making, operations, and reporting. Questions provided to the participants sought to evaluate leaders' cybersecurity strategies and any breaches that have occurred within their organizations. Respondents opted into the survey via a third-party research panel, which fielded the survey on behalf of Forrester in March 2021.

DISCLOSURES
Readers should be aware of the following:
This study is commissioned by BlackBerry 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 study to determine the appropriateness of an investment in CylanceGUARD.
BlackBerry 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 provided the customer names for the interviews but did not participate in the interviews.

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

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

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

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

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

The CylanceGUARD Customer Journey

Drivers leading to the CylanceGUARD investment

Interviews			
Role	**Industry**	**Region**	**Revenue**
Head of security	Financial institution	EMEA	$1B+
Head of infosec	Transportation	APAC	$1B+
Chief information officer (CIO)	Professional services	North America	$100M+
Director of security	Hospitality	North America	$100M+

KEY CHALLENGES

Organization representatives reported that prior to their move to CylanceGUARD, they faced a number of challenges, but the highlight was simply that they were under-resourced and couldn't address endpoint-related threats. The issues were broken down further in the following:

- **The lack of people resources protracted SLAs and remediation times.** Interviewees noted that the scarcity of security operations resources available on the market and the difficulty in retaining those already on the team posed the issue of being able to investigate and identify the root cause of incidents. The trickle-down effect was that end users suffered from extenuating recovery time and an associated productivity loss. One interviewee expressed: "Where do we go from here? How much can we help our users without blowing the bank?"
- **Traditional signature-based antivirus solutions were no longer adequate.** Many interviewees identified that their organizations' signature-based solutions were not protecting their endpoints with an acceptable level of efficacy. The continual updating of signatures simply did not happen fast enough to defend against zero-day and new threats. The end game was to deflect as many of the threats as possible with some degree of artificial intelligence as a quicker initial layer of defense against bad actors.
- **Being SMBs and mid-market organizations, the interviewees' organizations did not have the capability to respond on a 24x7x365 level.** Hiring and retraining security operations FTEs on a nine-to-five schedule is one thing, but having people around the clock to manage the defense was a different matter. Interviewees recognized that their smaller teams and the difficulty they faced regarding hiring for an around-the-clock team left a significant gap for perpetrators to

> **"It was very manual with our old solution. When there was something happening, we didn't have all the details. With CylanceGUARD, they would pick it up immediately and be done with the issue within 15 minutes."**
>
> *Head of IT security, financial institution*

infiltrate and dwell in their networks. The answer for them was to augment their teams with something scalable and agile to keep up with the off-hours.

SOLUTION REQUIREMENTS/INVESTMENT OBJECTIVES

The interviewees' organizations searched for a solution that could:

- Identify malicious activity on the endpoints to reduce overall incidents.
- Provide 24x7x365 coverage, both on a detection and response level with the BlackBerry in-house teams and expert security staff.
- Be scalable and applicable across various regions.
- Provide full workflow assistance from detection through remediation.
- Leverage predictive AI.

After a request for proposal (RFP) and business case process evaluating multiple vendors, the interviewees' organizations chose CylanceGUARD and began deployment:

- After an initial POC to test efficacy of detection, the process continued to test speed of remediation, which proved to be effective.
- The interviewees' organizations went through a quick training session for both infosec and IT personnel.
- The implementation of the CylanceGUARD solution was brought in to be complementary to the existing infosec team.
- Time to be implemented, which included consultations of risk tolerance and associated policies, was performed within a month.
- Multiple interviewees stated that initiating the service was extremely quick with a director of security at a hospitality organization stating that, "It literally was up and protecting us within a week."

"We don't have a 24/7 IT center and we don't work weekends. We realized that we had a pretty big hole, especially with workers connecting remotely, and had a lot of vulnerable areas. It became a crystal-clear moment to us that we needed a service-based security solution and not just a product."

CIO, professional services

"Our security team is very lean. We needed a solution that is AI- and machine-learning-based. [Further,] we didn't want the team to be in 24/7 monitoring situations. The solution needed to be smart enough to quarantine attacks along with a competent team like Cylance to handle the escalation layer."

Head of infosec, transportation

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an ROI

analysis that illustrates the areas financially affected. The composite organization is representative of the four interviewees, and it is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. The organization is a B2B, smaller enterprise with approximately 3,000 employees. Endpoints include servers in addition to end-user devices. The infosec/SecOps team does most of the investigation work while IT is responsible for response, effectively optimizing the cost of people resources. There is an existing security stack and endpoint protection is the largest area of concern because it took the bulk of IT and infosec resources and was increasingly difficult to address.

Key Assumptions Of Composite

- **North American organization**
- **$100M+ revenues**
- **3,000 employees**
- **3,600 endpoints protected**
- **No existing MDR**
- **Lean SecOps and response team on-premises**

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits

Ref.	Benefit	Year 1	Year 2	Year 3	Total	Present Value
Atr	Security and IT operation reduction in effort to manage incidents	$313,571	$400,781	$400,781	$1,115,134	$917,402
Btr	Time to deliver value and protect assets	$451,069	$0	$0	$451,069	$410,063
Ctr	Reallocation of people resources with sunsetting of existing solutions	$632,655	$632,655	$632,655	$1,897,965	$1,573,319
	Total benefits (risk-adjusted)	$1,434,510	$1,070,651	$1,070,651	$3,575,813	$2,900,784

SECURITY AND IT OPERATION REDUCTION IN EFFORT TO MANAGE INCIDENTS

Evidence and data. Interviewees stated that their organizations benefited from deflected threats due to the Cylance EPP solution efficacy and the contextual information where threats became incidents. The vast majority of threats were automatically deflected and handled with the EPP but those that made it through could be handled and remediated more quickly due to the full field information that CylanceGUARD provided to infosec FTEs.

- Infosec/SecOps FTEs acted as the first line against threats, investigating and triaging. Interviewees noted that with the additive context from CylanceGUARD, half of the effort to ascertain the issues was saved.
- Interviewees' organizations often had more than the 1.5 FTE represented on table calculations, but 1.5 FTE is the representation of the FTE that were assigned to endpoint protection.
- Many interviewees noted their organizations parsed duties for IT to handle remediation once the causation was determined. The response and remediation of endpoints was largely assigned to this group, who saw a 90% reduction on time to fix.
- The MDR service also contained suspect threats to prevent lateral damage. The head of infosec from a transportation organization said: "Last night, I got a call from the MDR team, and they said there was a high possibility of malware in a few endpoints. They quarantined the devices and that was that. I'm very happy with that containment."

"We have the CylanceGUARD team do our detection because we simply can't have people doing 24/7 monitoring. GUARD will inform us via SMS or email, and it's handled within 15 minutes typically."

Head of security, financial institution

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

- The number of infosec/SecOps FTEs dedicated to endpoint investigations and triage grows to two FTEs in Years 2 and 3.
- Four IT FTEs work on remediation. As IT personnel have a variety of tasks, a percentile is calculated against their total work dedicated to the security tasks.
- Deflections of security incidents are represented, relating to efficacy of the EPP and efficiency of MDR over legacy AV solutions.

Risks. Forrester accounts for variability and potential risks that may impact financial models and are listed as follows:

- The maturity of existing security teams can vary between organizations and their prior state.
- The blend between IT and SecOps often are different. Forrester advises adjusting calculations dependent on the specific group that addresses incident response.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $917,000.

"If we saw something odd before, we didn't have context and spent a lot of time trying to figure out the real risk and if we needed to take action. Now, we have that in front to do what is necessary."

Director of IT Security, hospitality

Security And IT Operation Reduction In Effort To Manage Incidents

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	SecOps FTEs	Composite	1.5	2.0	2
A2	SecOps effort reduced on incident examination, triage, and remediation	% reduction of SecOps effort	50%	50%	50%
A3	SecOps annual salary, fully loaded	TEI standard	$148,500	$148,500	$148,500
A4	IT FTEs	Composite	4	5	5
A5	IT time spent on security-related incidents and response	Interviews	75%	75%	75%
A6	IT security-based incident deflected by MDR	Interviews	90%	90%	90%
A7	IT annual salary, fully loaded	TEI standard	$81,000	$81,000	$81,000
At	Security and IT operation reduction in effort to manage incidents	(A1*A2*A3)+(A4*A5 *A6*A7)	$330,075	$421,875	$421,875
	Risk adjustment	↓5%			
Atr	Security and IT operation reduction in effort to manage incidents (risk-adjusted)		$313,571	$400,781	$400,781
	Three-year total: $1,115,134			**Three-year present value: $917,402**	

TIME TO DELIVER VALUE AND PROTECT ASSETS

Evidence and data. New assets and a switch in security systems were often time-consuming for the interviewee organizations. Factors that interviewees presented included the following:

- The time it took the interviewees' organizations to create/adjust policies and rules to modern standards. CylanceGUARD is powered by Cylance AI and ML which helped the interviewees' organizations reduce the time to properly protect assets. The CIO from a professional service organization explained that the fine-tuning of existing policies took up to 10 months for larger assets with legacy endpoint protection, whereas CylanceGUARD was able to adjust policies and protect effectively in under a month. The effort expended by internal teams was saved and shifted to new activities.
- Deployment of CylanceGUARD on new assets took one month at maximum with most interviewees finishing within two weeks.
- With CylanceGUARD, interviewees noted their organizations no longer had to rotate additive SecOps to enable protection of assets.

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

- SecOps/infosec FTEs are compensated at $110,000 with a 1.35x multiplier to account for benefits.
- A total of three SecOps/infosec FTEs rotate for coverage.

Risks. Forrester accounts for variability and potential risks that may impact financial models and are listed as follows:

- The amount of policies and rules that might need forming varies between industries.
- Establishing baselines differ between organizations due to risk tolerance and security maturity.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $410,000.

Time reduction to protect new assets

90%

Time To Deliver Value To Protect Assets					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	SecOps involved in investigative work, triage, and resolution	Interviews	1.5		
B2	Additive SecOps FTE needed	Interviews	3		
B3	Deployment time of CylanceGUARD (months)	Interviews	1		
B4	Deployment time calculated in months with non-MDR solution on assets	Interviews	10		
B5	Cost of SecOps FTE annually, fully loaded	TEI standard	$148,500		
Bt	Time to deliver value and protect assets	(B1+B2)*(B4-B3)*B5/12	$501,188	$0	$0
	Risk adjustment	↓10%			
Btr	Time to deliver value and protect assets (risk-adjusted)		$451,069	$0	$0
	Three-year total: $451,069			**Three-year present value: $410,063**	

REALLOCATION OF PEOPLE RESOURCES WITH THE SUNSETTING OF EXISTING SOLUTIONS

Evidence and data. Interviewees indicated that their organizations had not only retired their existing AV/EDR solutions, but also removed the infrastructure the operations required to support those pieces.

- Costs for existing AV or EDR solution were paid annually and were sunsetted upon the switch to CylanceGUARD and EPP.
- Interviewees' organizations in general moved their people resources to higher-value activities, such as threat hunting. IT teams were able to improve on their SLAs.
- Interviewees also expressed that they were able to remove FTEs from operations of existing solutions that required piecing together of information from multiple sources.

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

- The composite is able to reallocate three SecOps/infosec personnel and two IT response FTEs.

"Knowing that we didn't have the coverage night or weekends, we had an eye-opening incident where there was a web shell in our on-premises exchange server. We realized then that things can happen anytime, day or night. We needed someone to watch our systems when we couldn't. That saves us from having to bring more people on to handle these tasks."

CIO, professional services

- Legacy tool costs are eliminated, which include rationalization of hardware.

Risks. Forrester accounts for variability and potential risks that may impact financial models and are listed as follows:

- The architecture of existing AV/EDR solutions.
- Highly variable costs of legacy tools, depending on pricing structures.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $1.6 million.

"Before CylanceGUARD, we didn't have time to focus on real cyber risk. With CylanceGUARD, we now have the time to do threat hunting and fine-tune our policies regularly."

Head of security, financial institution

Reallocation Of People Resources With Sunsetting Of Existing Solutions

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	EDR and infrastructure solution costs, prior state	Assumption	$136,800	$136,800	$136,800
C2	Incremental SecOps labor required to run non-MDR solution	3 FTE*$148,500/yr	$445,500	$445,500	$445,500
C3	Incremental IT labor required to run alternate non-MDR solution	2 FTE*$81,000/yr	$162,000	$162,000	$162,000
Ct	Reallocation of people resources with sunsetting of existing solutions	C1*C2*C3	$744,300	$744,300	$744,300
	Risk adjustment	↓15%			
Ctr	Reallocation of people resources with sunsetting of existing solutions (risk-adjusted)		$632,655	$632,655	$632,655
	Three-year total: $1,897,965			**Three-year present value: $1,573,319**	

UNQUANTIFIED BENEFITS

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

- **Mitigates regulatory fines that are prevalent in many industries.** Interviewees whose organizations were in the financial services, retail, and healthcare industries were particularly at risk of regulatory fines, which could be significant. Forrester's internal research suggests that with a simple PCI-DSS fine, it could result in fines well over $100,000. Erring on conservatism with our calculations, Forrester has not included these figures due to extreme variability of regulatory fines from industry to industry and in cost.

  In addition to PCI-DSS fines, GDPR and CCPA fines, among others, are a consideration of data that could be impacted.

- **Reduces hiring and onboarding fees for SecOps/infosec and IT FTEs accrue substantial costs.** Interviewees noted that when their organizations scaled, it was costly for new employees to be onboarded. It held extremely true when employee churn occurred in the very tight security personnel field.

FLEXIBILITY

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

- **Improved agility and scalability.** Interviewees noted that organizations grow geographically and in size. CylanceGUARD was adaptable with scaling, in that the managed response resources could shift with customer needs. Interviewees indicated that there were no better solutions, even contracting workers.

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

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Dtr	Cost of CylanceGUARD	$0	$291,849	$291,849	$291,849	$875,546	$725,785
Etr	Internal IT/InfoSec team effort	$4,840	$2,904	$2,904	$2,904	$13,552	$12,062
	Total costs (risk-adjusted)	$4,840	$294,753	$294,753	$294,753	$889,098	$737,847

COST OF CYLANCEGUARD

Evidence and data. Interviewees noted that the cost of CylanceGUARD was predicated on the endpoints protected and is inclusive of EPP software and MDR services.

- A director of IT security from a hospitality organization noted: “I don’t need to worry about trying to staff an SOC. I know that I can rely on the people that are trained by BlackBerry and can staff to the right levels — especially with people that know the solution in and out and help us tune it as we go.”
- Costs are shown at list levels but may be lower depending on negotiations with BlackBerry.

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

- The CylanceGUARD annual subscription is $170,208.
- The BlackBerry Endpoint Protection annual fee is $198,288.
- This cost is inclusive of EPP software and the MDR provided by CylanceGUARD.
- A small discount from list level pricing is assumed.

Results. Forrester finds a three-year, risk-adjusted total PV (discounted at 10%) of $726,000.

Cost Of CylanceGUARD						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
D1	CylanceGUARD subscription	BlackBerry		$122,550	$122,550	$122,550
D2	BlackBerry Endpoint Protection	BlackBerry		$142,767	$142,767	$142,767
Dt	Cost of CylanceGUARD	D1+D2	$0	$265,317	$265,317	$265,317
	Risk adjustment	↑10%				
Dtr	Cost of CylanceGUARD (risk-adjusted)		$0	$291,849	$291,849	$291,849
	Three-year total: $875,546			**Three-year present value: $725,785**		

INTERNAL IT/INFOSEC TEAM EFFORT

Evidence and data. Interviewees noted that it required very little effort to integrate the CylanceGUARD team with their own security team. Overall, the only required internal costs were onboard training. Baselining and policy-making tasks were minimal with CylanceGUARD.

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

- Calculations take into account for churn in workforce in years two and three.
- It takes 40 hours to onboard both ITOps and SecOps FTEs initially. This reduces to 24 hours annually after implementation.
- The hourly cost of an ITOps FTE is $39. For a SecOps FTE, it's $71. The hourly costs of infosec FTE and ITOps FTE are adjusted with a 1.35x multiplier to account for benefits.

> **"BlackBerry provides us the flexibility in terms of investment. It also helped us to reduce the cost of hiring by having MDR in place. With them, I can better understand situations that arise and thus can reduce risk."**
>
> *Head of infosec, transportation*

Risks. Forrester identified that there are variables that may affect this potential cost which are:

- Utilization of IT vs. infosec personnel.
- Churn rate of FTEs, which is contingent on IT vs. infosec FTE mix, affecting the overall cost of onboarding.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $12,100.

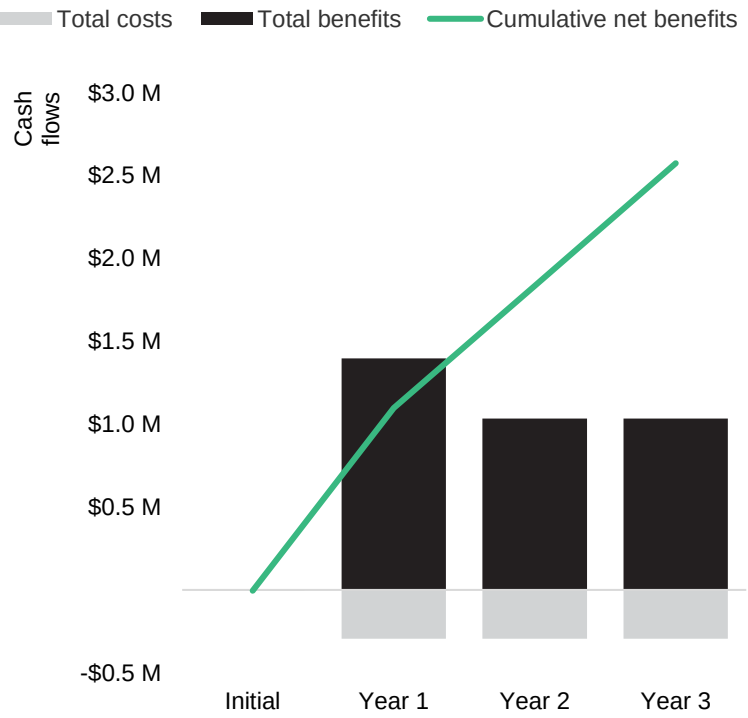
Internal IT/InfoSec Team Effort

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
E1	ITOps time to onboard (hours)	Interviews	40	24	24	24
E2	Cost of ITOps per hour	TEI standard	$39	$39	$39	$39
E3	SecOps time to onboard (hours)	Interviews	40	24	24	24
E4	Cost of SecOps FTE per hour	TEI standard	$71	$71	$71	$71
Et	Internal IT/infosec team effort	E1*E2+E3*E4	$4,400	$2,640	$2,640	$2,640
	Risk adjustment	↑10%				
Etr	Internal IT/InfoSec team effort (risk-adjusted)		$4,840	$2,904	$2,904	$2,904
	Three-year total: $13,552			**Three-year present value: $12,062**		

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



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

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

Cash Flow Analysis (Risk-Adjusted Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($4,840)	($294,753)	($294,753)	($294,753)	($889,098)	($737,847)
Total benefits	$0	$1,397,295	$1,033,436	$1,033,436	$3,464,168	$2,900,784
Net benefits	($4,840)	$1,102,542	$738,683	$738,683	$2,575,069	$2,162,937
ROI						293%
Payback						<6 months

Appendix A: Total Economic Impact

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

TOTAL ECONOMIC IMPACT APPROACH

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

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

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

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

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

PRESENT VALUE (PV)

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

NET PRESENT VALUE (NPV)

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

RETURN ON INVESTMENT (ROI)

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

DISCOUNT RATE

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

PAYBACK PERIOD

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

Appendix B: Supplemental Material

Related Forrester Research

"Forrester Infographic: The Managed Detection and Response (MDR) Market in 2021," Forrester Research, Inc., August 20, 2021

"The Managed Detection And Response Landscape, Q1, 2023," Forrester Research, Inc., January 30, 2023

Appendix C: Endnotes

[1] Source: Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q1 2021.

[2] 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.


FORRESTER®