A Forrester Total Economic Impact™ Study
Commissioned By Cylance
February 2018

FORRESTER®

Cylance Proactively Prevents Security Threats, Increases Productivity, and Provides a Holistic Endpoint Security Solution

Market Overview: Endpoint Security

According to Forrester's research, as cyberthreats are increasing, both in number and in complexity, traditional approaches to endpoint security have become outdated and less effective. To battle the ever-increasing threats, security professionals now turn to endpoint security technologies to either augment or replace their failing antimalware solutions. Below are the key trends in endpoint security and the strategies that companies are undertaking to address them.

Key Trends in Endpoint Security

- **Cyberthreats are increasingly sophisticated.** Cybercriminals are no longer lone hackers, but rather sophisticated criminal organizations and endpoint security represents the frontline in the fight against cyberattacks. Hackers change their signatures faster than traditional antimalware software can be updated. New forms of malware can lay dormant for weeks or months before activating and morphing, making it more difficult to identify them.
- **Security teams are buried under massive amount of threat alerts.** Large quantities of security threats create an overload on security teams and in turn prevent them from focusing on critical security issues and alerts. This reactive firefighting creates inefficiencies within the security staff and doesn't solve the critical problem of threat prevention.
- **Lack of experienced security personnel.** With the increasing sophistication and volume of cyber-attacks, organizations are having a hard time finding skilled resources to help address their security needs. There is an increased movement to hire outsourcing companies, however, even these companies are experiencing a shortage of highly skilled security resources to hire.
- **Prevention, detection and response.** Companies often have multiple security solutions that perform prevention, detection and response in isolation. This multi-solution approach is difficult to manage and allows threats to get through. A consolidated single agent, single layer tool that can address all three security requirements is key in successful security management.

Strategies Organizations Are Undertaking

- **AI and machine learning emerges as a leading technology in security.** Endpoint security technologies use machine learning to proactively ensure that applications are running securely by monitoring deviations from "known good" code activity. Vendors often incorporate artificial intelligence and machine learning to identity patterns of behavior that are normal, as opposed to threatening.
- **Technical integration is yielding more effective suites.** Some of the competing technologies in the market are consolidating, which will ultimately lead to more breadth and depth of protection from single products. For instance, prevention-

SUMMARY

Based on a commissioned study, "The Total Economic Impact Of Cylance"

METHODOLOGY

The objective of the TEI 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 of Cylance, including interviews with Forrester analysts, Cylance stakeholders, and one current Cylance customer. Forrester constructed a financial model representative of the interview using the TEI methodology.

COMPOSITE ORGANIZATION

This analysis uses a composite organization, based on the interviewees, to present the aggregate financial analysis.

RISK ADJUSTMENT

Forrester risk-adjusted the financial model based on issues and concerns of the interviewed organizations to account for uncertainties in benefit and cost estimates.

focused tools such as antimalware and application integrity protection are beginning to pull in detection-focused capabilities (endpoint visibility and control and user behavior monitoring and analytics) and vice versa.

- **Merging existing and new technologies to leverage effects of modernization**. Antimalware, patch management, and secure configuration management enjoy continued adoption due to compliance mandates such as PCI and HIPAA and best practices. Security buyers complain that these technologies are ineffective against advanced attacks but are required nonetheless. Merging old technologies with modern technology such as machine learning and artificial intelligence could provide the benefits of security automation and prevention of new unknown threats.
- **Endpoint solutions focusing on future flexibility.** Inspections of user and application behavior have usually been performed in isolation by separate technologies, but the two are beginning to integrate in ways that will offer more advanced insight in future solutions. With these integrations, and the continuous use of intelligent automation via AI, future suites will be able to automatically identify malicious user and application behavior and contain it without the involvement of skilled security analysts.

Forrester Total Economic Impact of Cylance

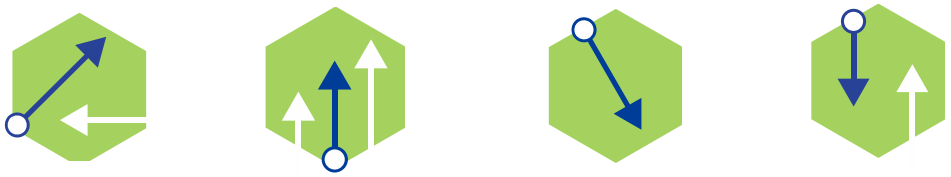
Forrester Consulting conducted a Total Economic Impact™ (TEI) study to provide readers with a framework to evaluate the potential financial impact of Cylance on their organizations. To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed one customer with experience using Cylance. Through this customer interview and data aggregation, Forrester concluded that companies who invested in Cylance's threat protection solution had the following three-year financial impact: $7.7 million in benefits versus costs of $2.2 million, resulting in a net present value (NPV) of $5.5 million and an ROI of 251%.

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

Quantified benefits

The following risk-adjusted quantified benefits are representative of those experienced by the State County interviewed:

- **A yearly cost savings of $2.3 million due to reduced incidence of zero-day threats and data breaches.** Cylance's solution reduced the possibility of having a data breach by almost 99%, for the State County's confidential, high-value information across all of its 20,000 customer records.
- **A $260,000 in cost savings related to remediating/reimaging systems.** The State County's significant costs in employee and end user time reimaging machines that had been compromised due to malicious software was reduced by 98% following the introduction of Cylance, saving the country over $260,000 across three years.
- **Improved productivity for IT, network, and security FTEs of three–year present value of $1.8 million.** Cylance reduced the time needed to manage the cybersecurity process, helping the IT and security employees to be 40% more productive, focusing on tasks that brought incremental value for the State County.



ROI
251%

Benefits
$7.7 million

Costs
$2.2 million

Payback
<1 year

Key Investment Drivers

The interviewed State County shared the following investment drivers:

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

> "Prior to Cylance, we had spent a lot of manual time chasing down issues and reimaging machines. This cost not only reduced our end user productivity, but it also tied up our internal IT and security staff with chasing down issues."
>
> *-- Chief Information Security Officer, large state county in the U.S.*

Key Results

Cylance met the solution requirements for the State County. Key quantified results from the Cylance investment for the State County include:

- Improved catch rate for zero-day malware.
- Reduction in time spent remediating/reimaging compromised devices.
- Improved cybersecurity confidence and reduced possibility of a data breach incidence.
- Reduction in hardware and memory requirements.

Cylance Saves Costs and Provides Total Endpoint Security

Cylance's solution is a new-generation, predictive, cybersecurity, and threat prevention solution that leverages artificial intelligence to prevent threats from executing on endpoints in real time. Benefits come in the form of cost savings due to reduced incidence of threats and data breaches, reduced cost of system remediation/reimagining, improved IT and security productivity. In addition, the minimal amount of disk space required by Cylance reduces costs in hardware and memory requirements.

The benefit impact experienced by a State County is based on the past and current experiences of the interviewee. Over three years, the organization expects risk-adjusted benefits to total a present value (PV) of $7.7 million.

Total Benefits

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

- **Cost savings due to reduced incidence of zero-day and risk of data breach.** The State County's 20,000 customer records, at an estimated $400 cost per record of a data breach, were at an estimated 30% risk of a possible data breach. With Cylance the State County can confidently claim that it has reduced its known and zero-day vulnerability by 99%, resulting in $2.37 million in yearly cost savings.
- **Reduced cost of system remediation/reimaging.** Prior to Cylance, the State County experienced an average of six endpoint remediations and reimages a month, which required in internal IT and security FTEs spending 12 hours to identify and implement a solution. Since implementing Cylance, the State Country ceased to experience remediation/reimaging issues, equating to about $110,000 of yearly cost savings.
- **IT and security FTE productivity gains.** The State County estimates that with its investment in Cylance, it was able to gain productivity worth the time of two full IT FTEs as it relates to investigating endpoints. Additionally, across its staff of 12 IT and security FTEs, it saw a productivity improvement of 40%. At a $120,000 average annual salary, this results in a yearly risk-adjusted benefit of $734,000.

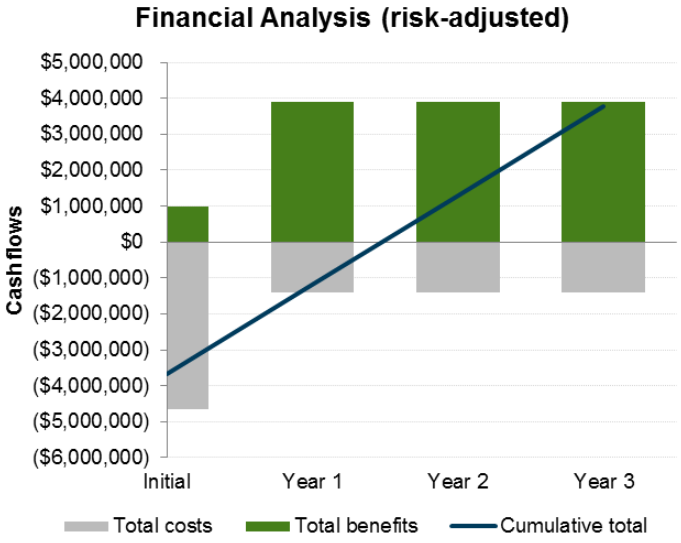
A Cylance Investment Today Can Create Future Opportunities

The value of flexibility is clearly unique to each client, and the measure of its value varies across organizations. There are many scenarios in which a client might choose to implement Cylance's solution and later realize additional uses and business opportunities, including:

- Scalability and marginal cost of provisioning for new users or endpoints.
- Increasing or cutting back on the number of active endpoints with the convenience of a single phone call; valuable for organizations in times of mergers, acquisitions, or even a restructuring of the organization or certain departments.

Financial Summary

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 in Cylance. Forrester assumes a yearly discount rate of 10% for this analysis. For more information, you can download the full Cylance TEI analysis here.



ROI
251%

NPV
$5.5 million

Payback
< 1 year

Disclosures

The reader should be aware of the following:

- The study is commissioned by Cylance and delivered by Forrester Consulting. It is not meant to be 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 Cylance.
- Cylance reviewed and provided feedback to Forrester. 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.
- Cylance provided the customer names for the interviews but did not participate in the interviews.

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. https://go.forrester.com/consulting/

ABOUT TEI

Total Economic Impact™ (TEI) 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. The TEI methodology consists of four components to evaluate investment value: benefits, costs, risks, and flexibility. https://go.forrester.com/consulting/content-marketing-consulting/

FORRESTER®