A Forrester Total Economic Impact™
Study Commissioned By VMware
May 2020

The Total Economic Impact™ Of VMware Carbon Black Cloud

Cost Savings And Business Benefits Enabled By Carbon Black Cloud

FORRESTER®

Table Of Contents

Project Director:
Sam Conway
Project Contributor:
Sam Sexton

Executive Summary

According to Forrester's research: "Network-based security has become insufficient due to the prevalence of transport layer encryption and the increasing amount of work done outside of the corporate network. As a result, endpoint security suites are the first line of defense for most organizations, and a critical one, as attackers today focus on the endpoint almost as much as they do the sensitive corporate servers."[1]

The VMware Carbon Black Cloud provides a cloud-native endpoint protection platform that comprises of next-generation antivirus (NGAV), audit and remediation, and enterprise detection and response (EDR) capabilities. The platform consists of: Endpoint Standard for NGAV and behavioral EDR; Audit and Remediation for remote audit and risk remediation for IT, compliance, and security; and Enterprise EDR for advanced threat hunting and incident response. These modules are delivered using a single lightweight agent and console, affording end users improved protection without degrading device performance or increasing IT support effort.

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

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed two customers with years of experience using Carbon Black Cloud. Additionally, Forrester surveyed 34 enterprise users of Carbon Black Cloud.

Prior to using Carbon Black Cloud, the customers used outdated or simple tools which lacked the capabilities to stop advanced attacks and conduct advanced investigations and root cause analysis. In fact, 44% of surveyed firms experienced a data breach or ransomware attack, which led them to invest in Carbon Black Cloud.

Key Findings

Quantified benefits. The following risk-adjusted present value (PV) quantified benefits are representative of those experienced by the interviewed companies and modeled after an organization with 6,000 endpoints:

- **Improved detection, investigation, and root cause analysis capabilities saved over 2,000 hours of FTE time.** Switching from legacy solutions provided interviewees with a more complete view of endpoint activity — allowing them to act more confidently and quickly. Furthermore, the legacy antivirus (AV) solutions used by interviewees did not provide attack visualizations or behavioral analysis, both of which are required to conduct effective root cause analysis.
- **Behavioral analytics, customizable policies, and continuous offline protection reduced risk profiles by 20%.** Moving to a next-generation platform improved organizations' proactive detection and prevention capabilities, reducing the threat of a successful attack.

Key Benefits

ROI
379%

Time savings from faster investigation and remediation:
60% of benefits

Avoided cost of a data breach:
14% of benefits

Cost savings from simplified operations:
12% of benefits

ROI
379%

Benefits PV
$3.78 million

NPV
$2.99 million

Payback
<3 months

- **Having a single, lightweight cloud platform reduced the time and effort required by IT teams to maintain security systems.** Consolidating to a single agent and shifting to a cloud deployment eliminated 4 hours of daily work for IT and security teams. Maintaining the legacy AV, antimalware, and EDR solutions, all deployed on-premises, required supporting infrastructure and consistently updating the policies and definitions. It also created duplicated efforts in managing alerts across multiple consoles. The platforms' cloud deployment and ability to offer multiple services through a single console eliminated these inefficiencies.

- **Organizations built consistency into operation reporting and auditing processes, accelerating time to complete audits.** With Audit and Remediation, organizations could quickly query and provide information required for audits. Furthermore, being able to provide a complete and accurate picture of organizational compliance reduced the likelihood that firms would incur regulatory penalties.

- **Real-time, remote investigation, fewer false positives, and improved visibility into endpoint activity helped reduce reimaging by 75%.** Being able to act immediately — and having full confidence in the information received — enabled interviewees to reduce the number of reimages performed by their organizations. Not only did this eliminate unnecessary IT work, but it also allowed end users to remain on task.

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

- **Avoided legal penalties for misuse of company devices.** Complete visibility into endpoint activity — including offline devices — allowed organizations to enforce device use policies and stop illegal activities such as downloading copyrighted material.

- **Endpoint performance improvements from a single agent.** The consolidation of security tools reduced the number of agents and improved end user device and application performance.

- **Reduced training time for new analysts.** The use of a single security platform both reduced the number of tools which analysts needed to learn and accelerated ramp time.

- **Extension of enterprise security to homeworkers' devices.** The new normal of increased remote working means organizations require visibility and security for worker devices that are outside the office. Carbon Black Cloud's enhanced visibility and control provides organizations with the confidence that homeworkers' environments are secure.

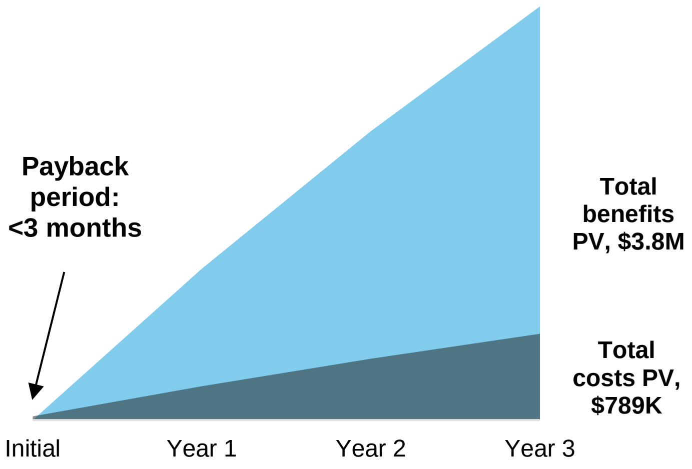
Costs. The interviewed organizations experienced the following risk-adjusted PV costs:

- **Carbon Black Cloud subscription.** Organizations paid a license fee to VMware for the use of Carbon Black Cloud.

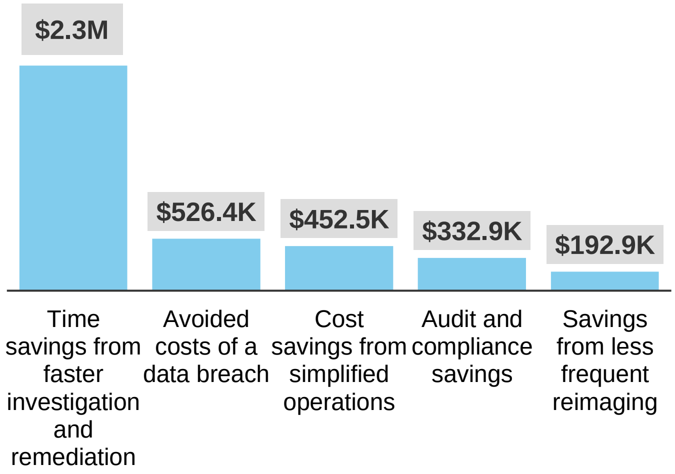
- **Training and deployment costs.** Organizations incurred nominal internal costs to deploy Carbon Black Cloud and train users.

Forrester's interviews with two existing customers, a survey with 34 firms, and subsequent financial analysis found that an organization based on these interviewed organizations experienced benefits of $3.78 million over three years versus costs of $788,999, adding up to a net present value (NPV) of $2.99 million and an ROI of 379%.

Financial Summary



Benefits (Three-Year)



TEI Framework And Methodology

From the information provided in the interviews, Forrester has constructed a Total Economic Impact™ (TEI) framework for those organizations considering implementing VMware Carbon Black Cloud.

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 VMware Carbon Black Cloud can have on an organization:

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

DUE DILIGENCE
Interviewed VMware stakeholders and Forrester analysts to gather data relative to Carbon Black Cloud.

CUSTOMER INTERVIEWS AND SURVEY
Interviewed two organizations and surveyed an additional 34 organizations using Carbon Black Cloud to obtain data with respect to costs, benefits, and risks.

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

CASE STUDY
Employed four fundamental elements of TEI in modeling VMware Carbon Black Cloud'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 VMware 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 VMware Carbon Black Cloud.

VMware 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.

VMware provided the customer names for the interviews but did not participate in the interviews.

The Carbon Black Cloud Customer Journey

BEFORE AND AFTER THE CARBON BLACK CLOUD INVESTMENT

Interviewed Organizations

For this study, Forrester conducted two interviews with VMware Carbon Black Cloud customers. Interviewed customers include the following:

INDUSTRY	REGION	INTERVIEWEE	NUMBER OF ENDPOINTS
Healthcare	United States	Senior system administrator	5,000
Real estate	United States	Director of infrastructure and cybersecurity	1,300

Surveyed Organizations

To help validate the information determined in interviews, Forrester conducted an additional survey of 34 Carbon Black Cloud users in the United States.

Average employees **4,500**

97% US-based

3% Canadian

$678.8M Average revenue

91% Of surveyed firms use multiple Carbon Black products

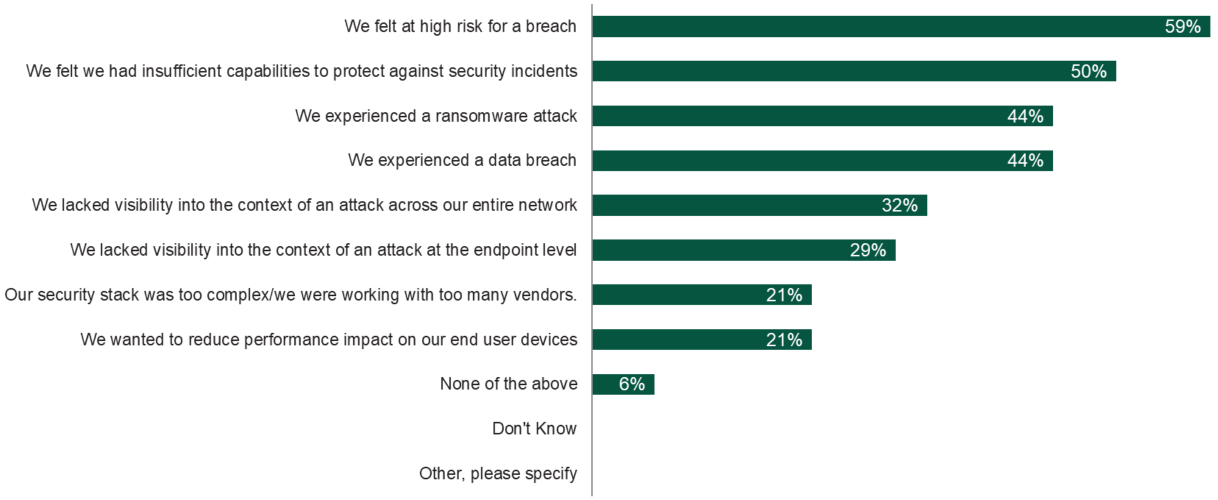
Key Challenges

Prior to investing in Carbon Black Cloud, both interviewees leveraged more generalized security products, with one organization using two different solutions. Both cited the following challenges that led them to invest in Carbon Black Cloud:

- **Insufficient threat prevention.** Both interviewees had a lack of confidence in their specific organization's ability to prevent threats, with one organization citing ransomware as a primary concern. Of the firms surveyed, 59% felt at high risk for a breach, and 50% had insufficient capabilities to protect against security incidents.
- **Lack of visibility into activity on endpoints.** The interviewees, as well as 62% of those surveyed, were concerned about a lack of visibility into their endpoints and the limited threat hunting capabilities with their prior solution(s).
- **Investigating and remediating threats required significant effort.** Limited tools and visibility made investigating potential threats costly and time-consuming. Reimaging, in particular, was a long and expensive process that impacted operations and required physically shipping hardware. Surveyed firms reported an average of 7 hours required to detect and remediate threats.
- **Redundant legacy security solutions drained resources**. One of the interviewed organizations layered two security systems together to cover endpoints, paying two licenses for outdated tools that required manual effort to use. Twenty-one percent of surveyed firms reported their security was too complex and impacted performance.

> "Our toolset was pretty slim. If a computer was compromised, we would go back to doing things the old-fashioned way: Take out this computer for a day while we wipe it, reimage, and bring it back to life. It was a very antiquated way of doing things, but we just didn't have the tools or staff needed to really do true threat hunting."
>
> *Director of infrastructure and cybersecurity, real estate*

“What drivers or pain points led you to invest in Carbon Black Cloud?”



Base: 34 VMware Carbon Black users

Source: A commissioned study conducted by Forrester Consulting on behalf of VMware Carbon Black, April 2020

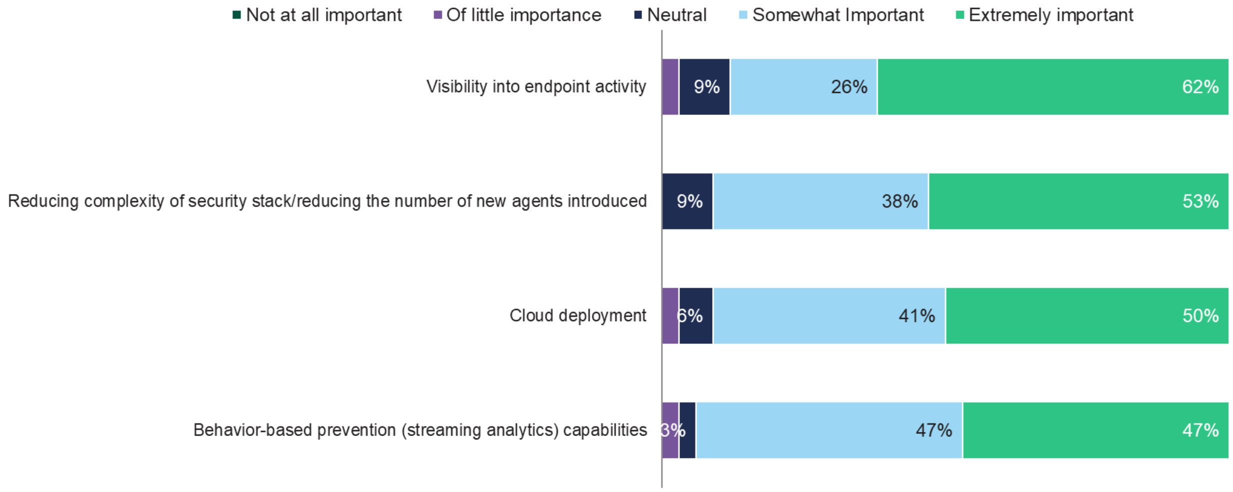
Solution Requirements

The interviewed organizations searched for a solution that would provide:

- A platform with multiple capabilities and tools to protect the firm from the increasing number and diversity of threats.
- The ability to protect the firm based on a set of actions, or AI, instead of malware definitions.
- The tools to conduct intelligent threat hunting.
- A reduction in the number of reimages.
- Scalable capabilities without increasing the number of vendors and related support costs.
- Retirement of legacy solutions and related support costs.

> “There were a bunch of configuration-type things that were kind of open. We were almost like sitting ducks [before Carbon Black].”
>
> *Senior system administrator, healthcare*

“How important were the following aspects of Carbon Black Cloud when you were making your investment decisions? Please rate each option on a scale of 1 to 5.”



Base: 34 VMware Carbon Black users

Source: A commissioned study conducted by Forrester Consulting on behalf of VMware Carbon Black, April 2020

Key Results

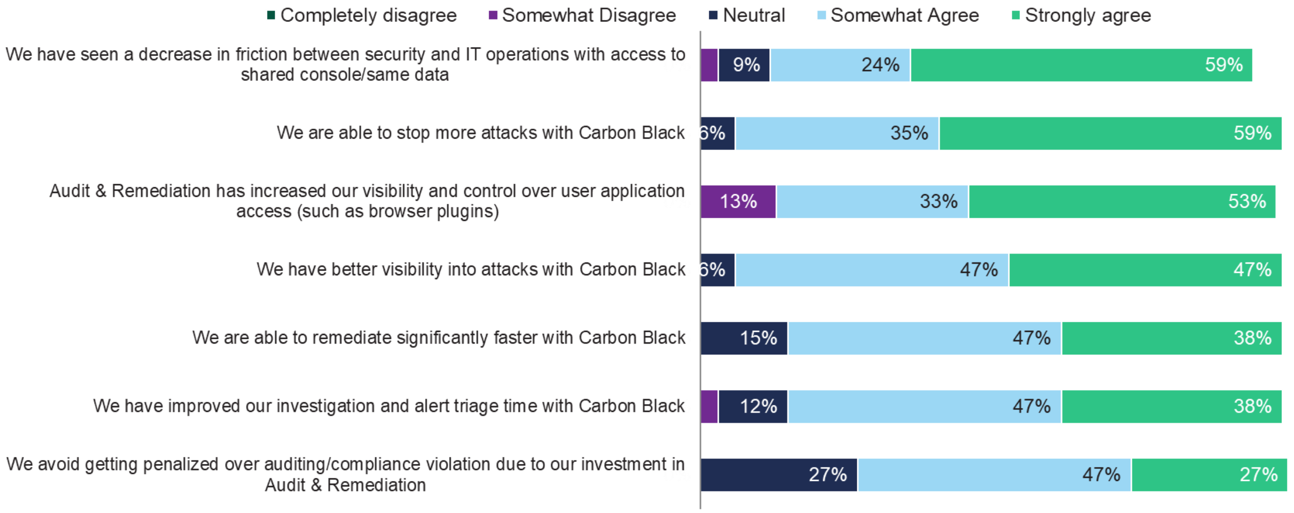
The interviews revealed that key results from the Carbon Black Cloud investment include:

- **Stronger endpoint security.** Both organizations, as well as 94% of those surveyed, expressed confidence that Carbon Black Cloud provided a significant improvement in their endpoint security efficacy.
- **Improved visibility and speed.** Both the two interviewees and 86% of surveyed firms were especially impressed with the improved visibility provided by Carbon Black Cloud. One of the interviewed organizations stated that its previous solution made threat hunting a time-consuming task, adding that it did not have the required staff to devote hours to manually hunting through logs: "Whereas Carbon Black has given us that visibility in a matter of moments. So, that's definitely been an outstanding change." This has significant implications for threat hunting, detection and remediation, and reimaging.
- **Consolidated, simplified operations.** Due to the fact that Carbon Black Cloud can cover the entire endpoint security landscape, organizations can safely retire legacy services and eliminate a significant source of expense and wasted time. Thirty-eight percent of surveyed firms stated that they have either already realized or expect to realize consolidation.

> "We usually know within the first 5 minutes whether it was a false positive or not. Whereas back in the day, it was not the case, right? Imaging a PC could take 24 hours. Usually we're doing that in 5 minutes now, which has greatly reduced the time and wasteful spend."
>
> *Director of infrastructure and cybersecurity, real estate*

> "Before Carbon Black we would probably have to ship the PC overnight. It's not cheap — it's like $100 a pop for a PC. But now, we're able to go in with Carbon Black, and as long as there's an internet connection we're able to check the admin account, modify, do stuff in the command prompt. It has saved us on multiple occasions."
>
> *Senior system administrator, healthcare*

"Thinking about your experience with Carbon Black Cloud compared to your previous environment, how much do you agree with each of the following statements?"



Base: 34 VMware Carbon Black users

Source: A commissioned study conducted by Forrester Consulting on behalf of VMware Carbon Black, April 2020

Composite Organization

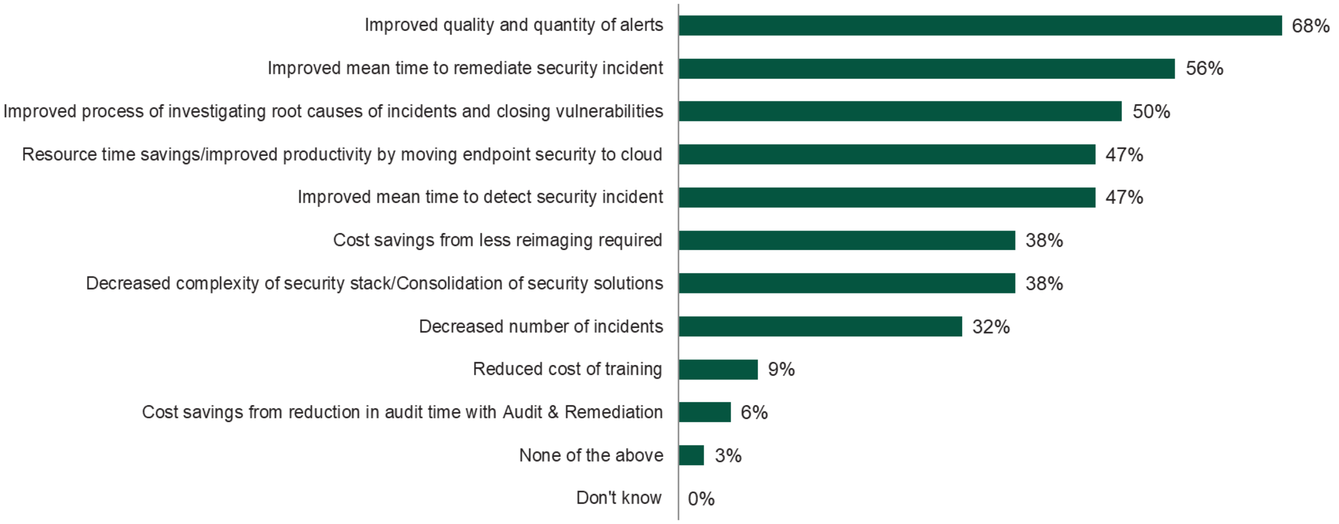
Based on the interviews, Forrester constructed a TEI framework, a composite company, and an associated ROI analysis that illustrates the areas financially affected. The composite organization is representative of both the two companies that Forrester interviewed and the 34 surveyed firms. This model is used to present the aggregate financial analysis in the next section. The composite organization that Forrester synthesized from the customer interviews has the following characteristics:

- The composite organization is a US-based global enterprise, which relies on its network to meet customer and internal user demand. The organization's 6,000 employees primarily work out of the company's main headquarters, with some working out of regional offices or at home.
- Prior to deploying Carbon Black Cloud, the composite organization relied on legacy on-premises AV and antimalware tools to protect its 6,000 endpoints. The firm implements VMware Carbon Black Cloud Endpoint Enterprise — comprised of Endpoint Standard, Audit and Remediation, and Enterprise EDR modules — to protect, remediate, and audit its endpoint landscape. After implementing Carbon Black Cloud, the composite organization retired its legacy software.

Key assumptions:

- 6,000 endpoints
- US-based global firm
- 8 reimages per week
- 6 incidents per day
- 6 audits per year

"Which of the following benefits has your organization realized/expect to realize as a result of your investment in Carbon Black Cloud?"



Base: 34 VMware Carbon Black users

Source: A commissioned study conducted by Forrester Consulting on behalf of VMware Carbon Black, April 2020

Analysis Of Benefits

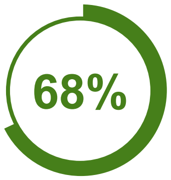
QUANTIFIED BENEFIT DATA AS APPLIED TO THE COMPOSITE

Total Benefits

REF.	BENEFIT	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Atr	Time savings from faster investigation and remediation	$916,207	$916,207	$916,207	$2,748,621	$2,278,471
Btr	Avoided costs of a data breach	$211,680	$211,680	$211,680	$635,040	$526,417
Ctr	Cost savings from simplified operations	$181,953	$181,953	$181,953	$545,859	$452,490
Dtr	Audit and compliance savings	$133,875	$133,875	$133,875	$401,625	$332,927
Etr	Savings from less frequent reimaging	$77,571	$77,571	$77,571	$232,713	$192,908
	Total benefits (risk-adjusted)	$1,521,286	$1,521,286	$1,521,286	$4,563,858	$3,783,213

The table above shows the total of all benefits across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total benefits to be a PV of more than $3.7 million.

Organizations save 7.5 hours per incident with Carbon Black Cloud.



Of survey respondents experienced improved quality and quantity of alerts

Time Savings From Faster Investigation And Remediation

Prioritized alerts, the ability to remotely triage endpoints, and robust visualizations are all Carbon Black Cloud capabilities which interviewees have found fundamental in reducing investigation and remediation times. Prior to having Carbon Black Cloud, interviewees went through a painstaking process of trying to determine the cause of alerts, assuming their legacy system alerted them at all. They often resorted to reimages due to a lack of information and an overabundance of caution.

With Carbon Black Cloud, organizations can stop threats before they execute, and security teams have the information they need to quickly decide how to respond. Endpoint events, both online and offline, are continuously analyzed, and all alerts are accompanied by easy to understand attack visualizations which allow users to make quick and intelligent decisions.

A senior system administrator in healthcare told Forrester: “You could see that there was malware on a box. I would get it after the fact. You would see there was malware, but it didn’t say where it came from. There was no process tree or anything like that. Basically, you would just get an alert saying there was some bad software on a machine with no context.”

The director of infrastructure and cybersecurity for a real estate firm explained its organization’s experience after switching to Carbon Black Cloud: “First, it’s the alert that we get via email. Once the alert hits, you click the investigate button, which immediately breaks us into threat hunting mode where we are able to break out 100% what this application did, what it was trying to execute, why it was trying to execute. And it categorizes the process from high to low with indicators of whether you’re at the top of what was running and what was blocked and why it was blocked. We can honestly click that email and by the time we get in the platform and we've read the two different pieces we know within 5 minutes whether something is truly wrong, and if it is, where we need to start working."

Based on the interviews and surveys conducted for the composite organization, Forrester assumes that:

- It detects six events each day that require triage or remediation.
- The security and IT professionals save 7.5 total hours per incident: 3 hours in investigation, 4 hours in remediation, and 0.5 hours in root cause analysis. Affected knowledge workers also experience 7.5 hours less downtime during these events.
- The security and IT resources and knowledge workers convert 50% of the hours saved into productive time.
- The average fully loaded salary is $169,000 for an IT operations resource and $104,000 for a knowledge worker.

This time savings benefit will vary with:

- The organization's original level of protection — specifically the functionality available through its previous security stack and its collective effectiveness.
- The skill set of the security and IT professionals.
- The organization's overall security maturity, including strength of other technologies and processes.
- Average fully loaded salaries.

To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $2,278,471.

56% **Of survey respondents improved mean time to remediate security incidents.**

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

Time Savings From Faster Investigation And Remediation: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
A1	Number of incidents requiring investigation (annually)	6 a day*365 days	2,190	2,190	2,190
A2	Reduced time to investigate (hours)		3	3	3
A3	Reduced time to remediate (hours)		4	4	4
A4	Reduced time for root cause analysis (hours)		0.5	0.5	0.5
A5	Average hourly rate for IT ops staff	$169,000/2,080	$81.25	$81.25	$81.25
A6	Average hourly rate for knowledge worker	$104,000/2,080	$50.00	$50.00	$50.00
A7	Productivity recapture		50%	50%	50%
At	Time savings from faster investigation and remediation (rounded)	A1*(A2+A3+A4)*(A5+A6)*A7	$1,077,891	$1,077,891	$1,077,891
	Risk adjustment	↓15%			
Atr	Time savings from faster investigation and remediation (risk-adjusted)		$916,207	$916,207	$916,207

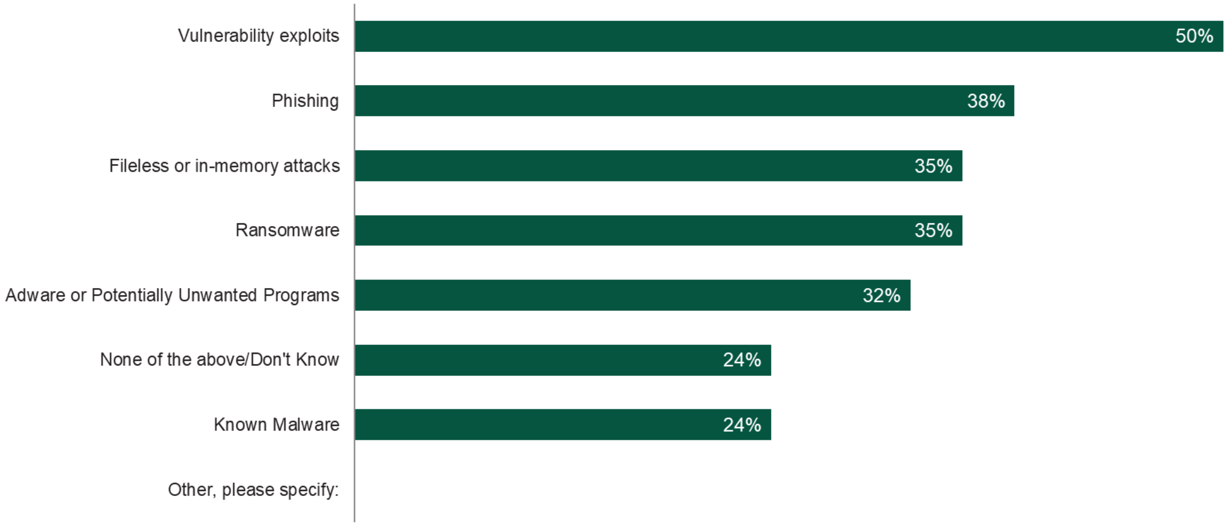
Avoided Costs Of A Data Breach

Endpoint Standard and Enterprise EDR detect and prevent threats by collecting unbiased data about endpoint activity. By applying ongoing behavioral analytics to this data, Carbon Black Cloud is able to uncover patterns and indicators to ascertain current threats and anticipate future ones. The comprehensive prevention afforded by Carbon Black Cloud protects organizations from known and unknown attacks, leading to fewer malware infections and minimizing risks of a breach. Furthermore, firms can utilize Carbon Black's customizable prevention policies for different user groups to further prevent risk of breach and adapt the solution to their specific business requirements.

Prior to deploying Carbon Black Cloud, organizations lacked the capability to protect against a number of serious threats. In fact, 44% of respondents experienced a ransomware attack and 44% experienced a data breach.

44% **Of survey respondents experienced a data breach with legacy solutions.**

"What types of threats were you unable to detect/prevent prior to Carbon Black Cloud?"



Base: 34 VMware Carbon Black users

Source: A commissioned study conducted by Forrester Consulting on behalf of VMware Carbon Black, April 2020

- The real estate firm rated its prior security stack a 2 out of 10 and had experienced a ransomware attack before investing in Carbon Black Cloud. With Carbon Black Cloud, the firm rated its security level as 8.5 out of 10.
- The healthcare organization rated the security level of its previous solution a 4 out of 10. And with Carbon Black Cloud, it rated its security level as 10 out of 10.

In modeling the benefit of a reduction in risk of a data breach, Forrester assumes:

- An average data breach cost of $4.41 million. This is based on the 2019 Ponemon estimate for enterprises sized between 5,001 and 10,000 employees.[2]
- The composite organization starts with a 30% risk of experiencing a breach and reduces the probability of occurrence by 20% with Carbon Black Cloud.

88% of survey respondents find Carbon Black Cloud to provide better levels of protection than their previous solution.

This benefit may vary based on:

- The level of protection for any organization’s previous security environment — specifically the functionality available through the previous security stack and collective effectiveness.
- Size, region, and vertical of organization.
- An organization’s diligence in updating policies and maturity of security practices.

To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $526,417.

!

Survey respondents who had previously been hit by ransomware paid an average of $90,053 for ransoms alone, prior to Carbon Black Cloud.

Avoided Costs Of A Data Breach: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
B1	Cost of a data breach		$4,410,000	$4,410,000	$4,410,000
B2	Risk of a data breach before Carbon Black investment		30%	30%	30%
B3	Reduction in risk profile with Carbon Black		20%	20%	20%
Bt	Avoided costs of a data breach	B1*B2*B3	$264,600	$264,600	$264,600
	Risk adjustment	↓20%			
Btr	Avoided costs of a data breach (risk-adjusted)		$211,680	$211,680	$211,680

Cost Savings From Simplified Operations

Carbon Black Cloud consolidates multiple capabilities — in the cloud — using a single endpoint agent, console, and data set. Prior to deploying Carbon Black Cloud, organizations engaged multiple vendors for different tools. This approach to endpoint security increased capex, degraded endpoint performance, and created a complex layer of vendor management that distracted from mission critical security tasks. Now, with Carbon Black Cloud, organizations can continue to scale security capabilities without adding new infrastructure or software deployments.

The director of infrastructure and cybersecurity for a real estate firm explained: “We like having everything in one basket. We don’t want to have one malware application and then one ransomware protector or traditional antivirus. It’s not beneficial from a systems standpoint, and it’s not beneficial from a management standpoint having three different portals. We had conflicting scans, conflicting runs along PCs. Three different agents potentially causing impact to the PC and general performance of the end user throughout the day.”

The composite organization used legacy antivirus and antimalware tools that were deployed on-premises to protect its 6,000 endpoints. The legacy deployment required resources to manage infrastructure and update software.

Based on interviews and surveys conducted for the composite organization, Forrester assumes that:

The average survey respondent replaced 2.67 vendors for security solutions by switching to Carbon Black Cloud.

47%

Of survey respondents experienced resource time savings by moving to the cloud

- IT resources save roughly 40 minutes per day, over 260 working days, managing or configuring support hardware.
- IT and security resources eliminate approximately 3.3 hours per day, over 260 working days, managing security solutions.
- A fully burdened salary of $130,000 for resources.
- Annual spend of $150,000 on prior software licenses, which is discontinued with the deployment of Carbon Black Cloud.

Cost savings from simplified operations will vary with:

- Size and type of previous solution.
- Average fully loaded salaries.

To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $452,490.

Cost Savings From Simplified Operations: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
C1	Time saved from managing hardware		178	178	178
C2	Time saved from managing security solutions		847	847	847
C3	Fully loaded salary	$130,000/2,080	$62.50	$62.50	$62.50
C4	Retired subscription costs		$150,000	$150,000	$150,000
Ct	Cost savings from simplified operations (rounded)	(C1+C2)*C3+C4	$214,063	$214,063	$214,063
	Risk adjustment	↓15%			
Ctr	Cost savings from simplified operations (risk-adjusted)		$181,953	$181,953	$181,953

Audit And Compliance Savings

With Audit and Remediation, organizations can take advantage of a number of prebuilt queries — or design their own — to establish proactive IT hygiene and establish consistent reporting and auditing processes. Not only does this allow organizations to track patch levels and enforce endpoint configuration and compliance policies, it affords visibility into software license inventory and any unwanted browser plug-ins. These capabilities are important, as organizations face stiff penalties from vendors if they either are under-licensed or violate government regulations such as the EU's General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA).

The director of infrastructure and cybersecurity explained: "We're using [Audit and Remediation] for multiple things and have found a way to tailor it to our needs outside security. We've used it to track OS licenses and understand what we need to phase out because things are going end of life, but also we can readily provide the information regarding what we have licenses for when they come in with one of their assessments."

Organizations reduce the time required to complete an audit by 20% with Carbon Black Cloud.

In modeling this benefit for the composite organization, Forrester assumes:

- The organization conducts six audits per year, and prior to investing in Carbon Black Cloud, the average audit required 5 hours to complete.
- The organization reduces the time to complete an audit by 20%, by maintaining consistent reporting processes and utilizing Carbon Black's query capabilities.
- The average hourly cost to conduct an audit is $1,250, consisting of internal labor and third-party auditors.
- The organization avoids $150,000 in potential fines for non-compliance.

Audit and compliance savings may vary based on:

- Industry and prevalent regulations.
- Prior-state capabilities and frequency of audits.

To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $332,927.

Audit And Compliance Savings: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
D1	Audits per year		6	6	6
D2	Time to conduct audit (hours) before Carbon Black		5	5	5
D3	Time savings with Carbon Black		20%	20%	20%
D4	Hourly cost incurred during audit		$1,250	$1,250	$1,250
D5	Avoided noncompliance savings		$150,000	$150,000	$150,000
Dt	Audit and compliance savings	D1*D2*D3*D4+D5	$157,500	$157,500	$157,500
	Risk adjustment	↓15%			
Dtr	Audit and compliance savings (risk-adjusted)		$133,875	$133,875	$133,875

Savings From Less Frequent Reimaging

Prior to investing in Carbon Black Cloud, interviewed organizations lacked the ability to conduct investigations, remotely access machines, and effectively prevent incidents. With rudimentary tools for investigation, interviewees often opted to simply reimage machines, rather than waste time trying to figure out what the issue was. While this was an effective way to ensure that issues were resolved, it was highly inefficient and organizations with remote workers incurred the costs of shipment and user downtime.

Being able to quickly filter out false alerts and visualize threats, remotely, ensures that organizations are comfortable with threat resolution and all but eliminates the need to perform reimages.

75% reduction in reimages with Carbon Black Cloud.

The director of infrastructure and cybersecurity detailed: "It could be a very small thing, but we just weren't confident that [our prior solution] had taken care of the problem. We were doing reimages to be better safe than sorry in the event there were any remnants left over. We just weren't confident in the platform. Today, we're just like, 'Oh this is malware. This is the correct file.' We are 100% confident that Carbon Black stopped it before it even asks us to do anything."

The senior system administrator in healthcare explained: "[Carbon Black] has definitely saved a few headaches. People would say there's a virus on their computer, but it's just a pop up or something minor we can fix remotely. We've also had some issues where a PC will lose connectivity to the domain, but we're able to go in through the live response and pull up command prompt and run commands. Before Carbon Black, we would probably have had the practice ship the PC to us — usually an overnight type deal, so it's not cheap. But with Carbon Black, as long as there is an internet connection, we're able to check the admin account, modify, and do stuff in the command prompt. It has saved us on multiple occasions."

Based on surveys and interviews for the composite organization, Forrester assumes that:

- Prior to Carbon Black Cloud, the organization was performing six reimages a week.
- It decreases the amount of reimages by 75%.
- The time required to perform a reimage is 8 hours.
- The average fully loaded salary of a service desk technician is $91,000.
- The average fully loaded salary of a service desk technician is $104,000.
- Fifty percent (50%) of hours saved, for service desk technicians and knowledge workers, are converted into productive time.
- Due to its semi-remote workforce, 15% of devices require shipping. The average cost incurred when shipping a device is $100.

Reimaging savings will vary with:

- Baseline level of protection and frequency of reimages.
- The composite organization's security maturity, including strength of other technologies and processes.
- Average fully loaded salaries.

To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $192,908.

Savings From Less Frequent Reimaging: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
E1	Frequency of reimaging required (annually) with legacy solutions		312	312	312
E2	Percent decrease in reimaging with Carbon Black		75%	75%	75%
E3	Time required for a service desk tech to reimage device		8	8	8
E4	Average hourly rate for service desk staff	$91,000/2,080	$43.75	$43.75	$43.75
E5	Average hourly rate for knowledge worker	$104,000/2,080	$50.00	$50.00	$50.00
E6	Productivity recapture		50%	50%	50%
E7	Percent of devices requiring shipping		15%	15%	15%
E8	Average cost of shipment		$100	$100	$100
Et	Savings from less frequent reimaging	(E1*E2*E3*(E4+E5)*E6)+ (E1*E2*E7*E8)	$91,260	$91,260	$91,260
	Risk adjustment	↓15%			
Etr	Savings from less frequent reimaging (risk-adjusted)		$77,571	$77,571	$77,571

Unquantified Benefits

In addition to the benefits above, the composite organization experienced four benefits which Forrester was unable to quantify.

- **Avoiding legal penalties for misuse of company resources.** Carbon Black Cloud's enhanced visibility and controls allow companies to ensure their hardware is not misused. The director of infrastructure and cybersecurity told Forrester an incident where an employee's child got ahold of their laptop and attempted to pirate games. The IT staff were able to see this happening and put a stop to it, before any consequences could take shape.

- **Endpoint performance improvements from a single agent.** Switching from multiple services to a single agent reduced processor demands for end users. One interviewee noted that its accounting department frequently complained about spreadsheets slowing them down, but since the transition to Carbon Black Cloud no complaints have been received. The director of infrastructure and cybersecurity explained: “We have a rather large accounting staff, managing 30,000 homes across the US and working with 11,000 vendors, so we carry an accounting staff of about 150 members. They’re in spreadsheets all day, crunching numbers and whatnot. With the previous solution, we actually had to go and ask them not to do such invasive scans, and we needed to hold off on longer ongoing scans at the end of the month because we were having to tell people to walk away from their systems during [the scans]. With Carbon Black, we’re seeing a lighter footprint and better response from end users.”

- **Reduced training time for new analysts**. Simplifying the security stack also simplifies training, making it easier to get new analysts up to speed.

- **Hardware savings.** Many companies refresh their hardware every three to five years, with an average server valued at $15,000. Moving endpoint security services to the cloud with Carbon Black Cloud removes or greatly reduces the need to refresh security hardware, which leads to organization wide savings in hardware purchasing.

Flexibility

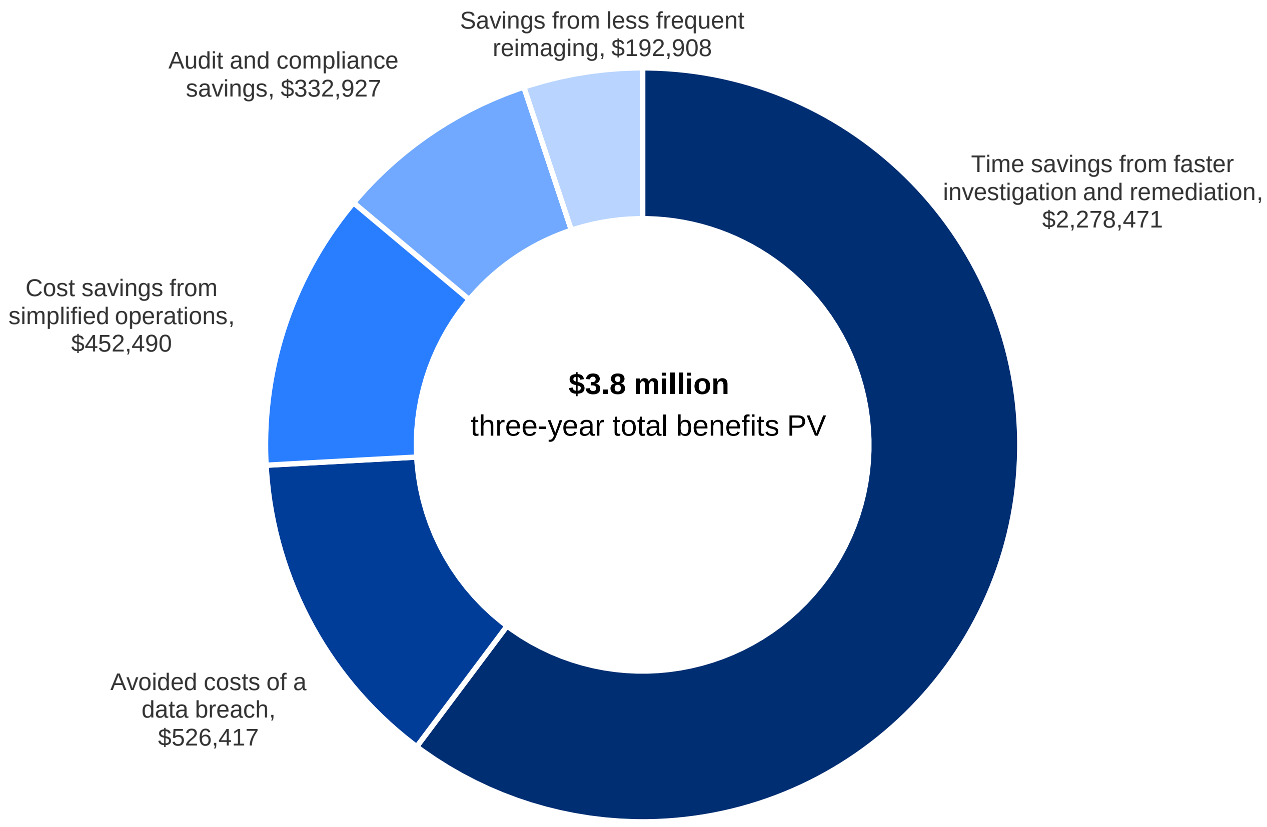
The value of flexibility is clearly unique to each customer, and the measure of its value varies from organization to organization. There are multiple scenarios in which a customer might choose to implement Carbon Black Cloud and later realize additional uses and business opportunities, including:

- **Extension of security to homeworker’s personal devices with the new normal of remote work.** The newfound necessity of working from home due to COVID-19 means organizations have a need for visibility and security on worker devices that are being used outside of the office. Carbon Black Cloud’s enhanced visibility and controls provide organizations with the confidence that workers’ devices are secure regardless of whether they are on or off the corporate network.

- **Reduced equipment and software costs.** With the agent’s lightweight footprint and cloud-processing, organizations could explore purchasing less expensive devices with less processing power. Furthermore, with the Audit and Remediation capabilities, organizations can identify and retire unused licenses or strategically target and migrate applications to the cloud facilitating further hardware savings.

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

Flexibility, as defined by TEI, represents an investment in additional capacity or capability that could be turned into business benefit for a future additional investment. This provides an organization with the “right” or the ability to engage in future initiatives but not the obligation to do so.


Savings from less frequent reimaging, $192,908
Audit and compliance savings, $332,927
Time savings from faster investigation and remediation, $2,278,471
Cost savings from simplified operations, $452,490
$3.8 million
three-year total benefits PV
Avoided costs of a data breach, $526,417

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
Ftr	Carbon Black Cloud subscription fees	$0	$290,160	$290,160	$290,160	$870,480	$721,585
Gtr	Training and deployment	$33,469	$13,650	$13,650	$13,650	$74,419	$67,414
	Total costs (risk-adjusted)	$33,469	$303,810	$303,810	$303,810	$944,899	$788,999

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 composite organization expects risk-adjusted total costs to be a PV of more than $789K.

VMware Carbon Black Cloud Subscription Fees

Fees to VMware for Carbon Black Cloud are based on the number of endpoints and the functionality deployed. For the full platform deployment on 6,000 endpoints, the composite organization pays $290,160 annually.

This cost will vary based on:

- The number of endpoints.
- The functionality deployed.

To account for these risks, Forrester adjusted this cost upward by 0%, yielding a three-year, risk-adjusted total PV of $721,585.

Carbon Black Cloud Subscription Fees: Calculation Table

REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
F1	Carbon Black Cloud subscription fees			$290,160	$290,160	$290,160
Ft	Carbon Black Cloud subscription fees	F1		$290,160	$290,160	$290,160
	Risk adjustment	0%				
Ftr	Carbon Black Cloud subscription fees (risk-adjusted)		$0	$290,160	$290,160	$290,160

Training And Deployment

Deploying Carbon Black Cloud involves installing agents, testing, deploying to machines, and monitoring and adjusting rules. Training involves one 8-hour session for each employee that needs to maintain and operate the platform.

Forrester assumes that the composite organization dedicates 30 person-hours to the implementation and deployment of Carbon Black Cloud. The composite organization trains 60 employees for 8 hours, for a total training time of 480 hours. Management requires 208 person-hours per year.

These costs will vary based on:

- The size of the deployment, including the number of endpoints, integration, and the use of open APIs.
- The skill set of the resources.
- The hourly rate of resources deploying, training, and maintaining the solution.

To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $67,414.

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.

30 hours
Total implementation and deployment time

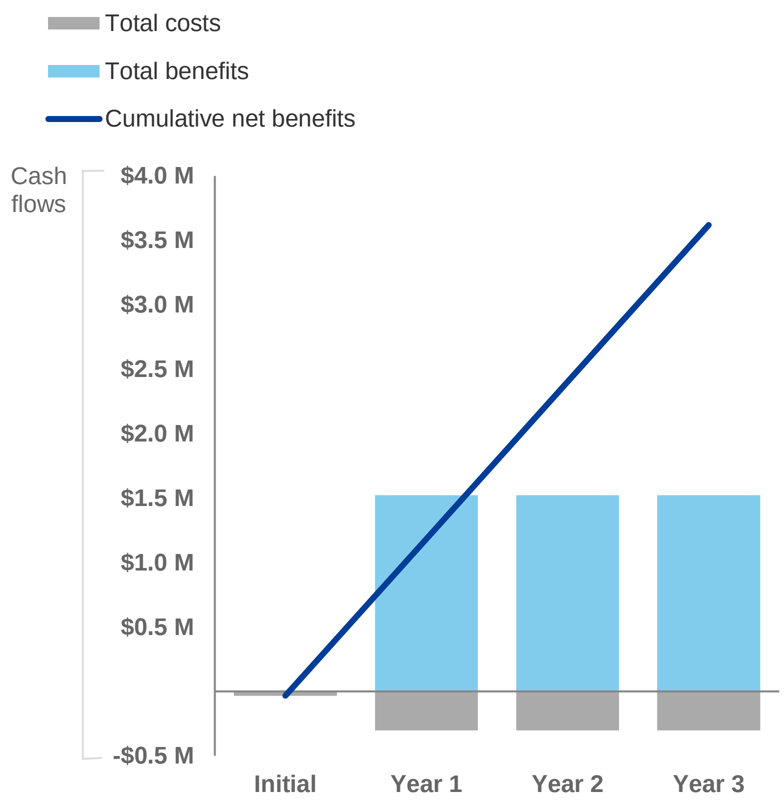
Training And Deployment: Calculation Table

REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
G1	Deployment time (hours)		30			
G2	Training time (hours)	8*60	480			
G3	Ongoing management (hours)	Previous study (4 per week)	0	208	208	208
G4	Effective hourly rate	$130K/2,080	$62.50	$62.50	$62.50	$62.50
Gt	Training and deployment	(G1+G2+G3)*G4	$31,875	$13,000	$13,000	$13,000
	Risk adjustment	↑5%				
Gtr	Training and deployment (risk-adjusted)		$33,469	$13,650	$13,650	$13,650

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 Table (Risk-Adjusted)

	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Total costs	($33,469)	($303,810)	($303,810)	($303,810)	($944,899)	($788,999)
Total benefits	$0	$1,521,286	$1,521,286	$1,521,286	$4,563,858	$3,783,213
Net benefits	($33,469)	$1,217,476	$1,217,476	$1,217,476	$3,618,960	$2,994,214
ROI						379%
Payback period						<3 months

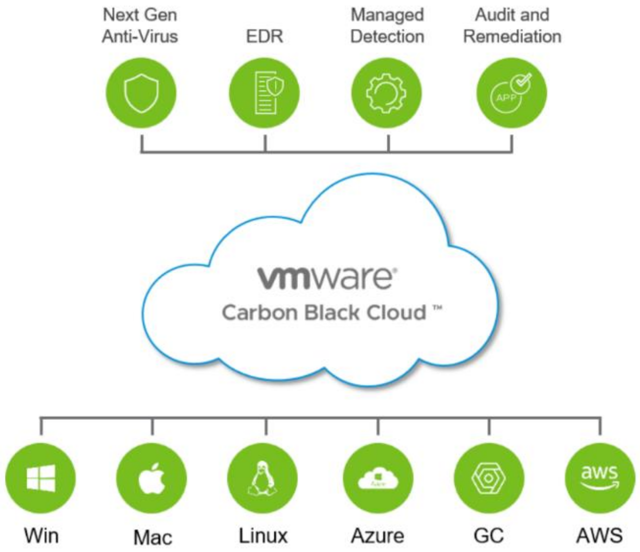
VMware Carbon Black Cloud: Overview

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

Endpoint Protection That Adapts to Your Business

The VMware Carbon Black Cloud is a cloud-native endpoint protection platform (EPP) that combines the intelligent system hardening and behavioral prevention needed to keep emerging threats at bay.

This platform consolidates multiple endpoint security capabilities using one agent and console, helping you operate faster and more effectively. As part of VMware's intrinsic security approach, VMware Carbon Black Cloud spans the system hardening and threat prevention workflow to accelerate responses and defend against a variety of threats.



Endpoint Standard – next-generation antivirus and behavioral EDR
Analyze attacker behavior patterns over time to detect and stop never-seen-before attacks, whether they are malware, fileless, or living-off-the-land attacks.

Audit and Remediation – real-time device assessment and remediation
Easily audit the current system state to track and harden the security posture of all your protected devices.

Enterprise EDR – threat hunting and incident response
Proactively hunt for abnormal activity using threat intelligence and customizable detections.

Managed Detection – managed alert monitoring and triage
Gain 24-hour visibility from our security operations center of expert analysts, who provide validation, context into root cause and automated monthly reporting.

Appendix A: Total Economic Impact

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

Total Economic Impact Approach

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

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

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

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

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

Present value (PV)

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

Net present value (NPV)

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

Return on investment (ROI)

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

Discount rate

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

Payback period

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

Appendix B: Endnotes

[1] Source: “The Top Trends Shaping Endpoint Security Suites In 2020,” Forrester Research, Inc., April 6, 2020.
[2] Source: “Cost of a Data Breach Report, 2019,” IBM Security (https://www.ibm.com/security/data-breach).