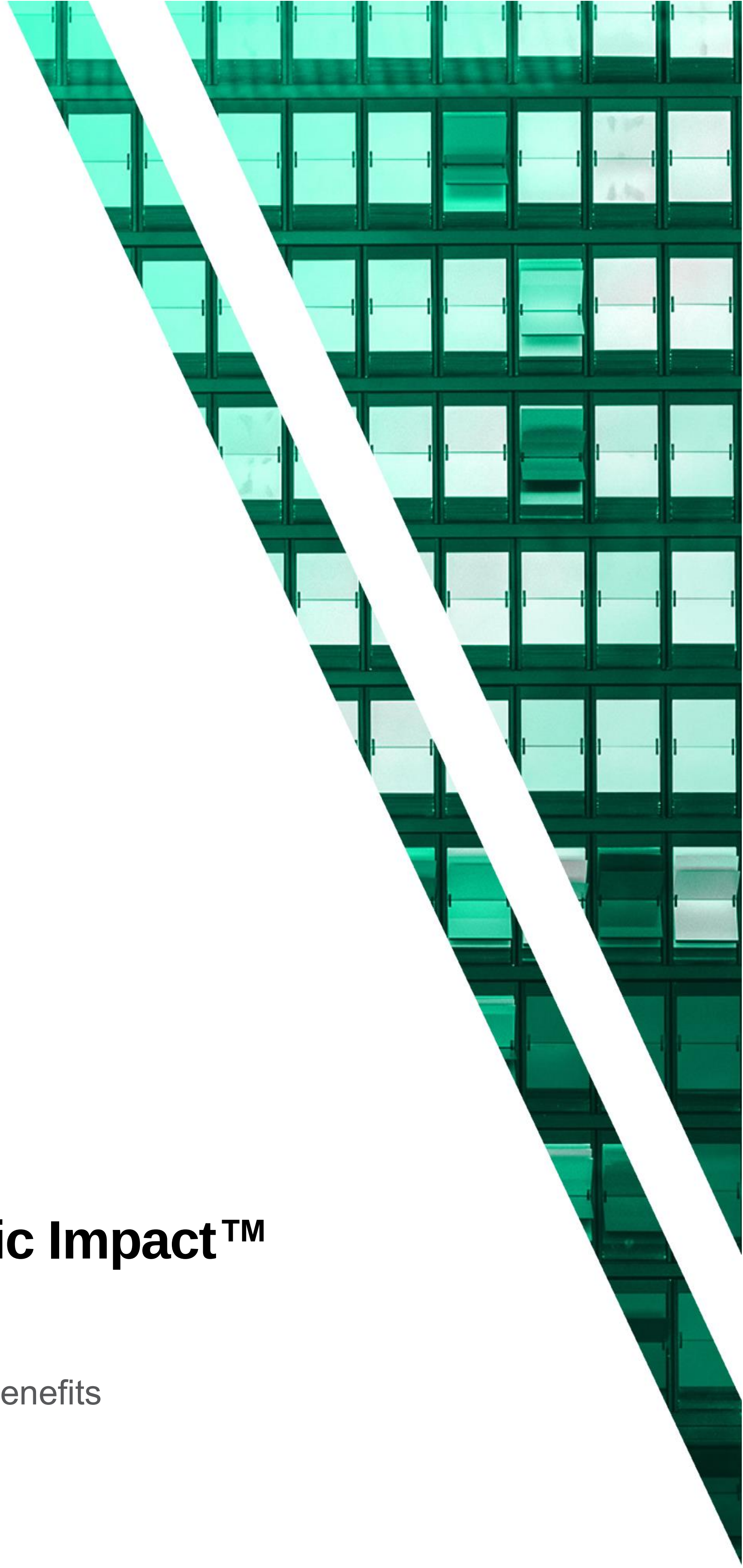
FORRESTER®



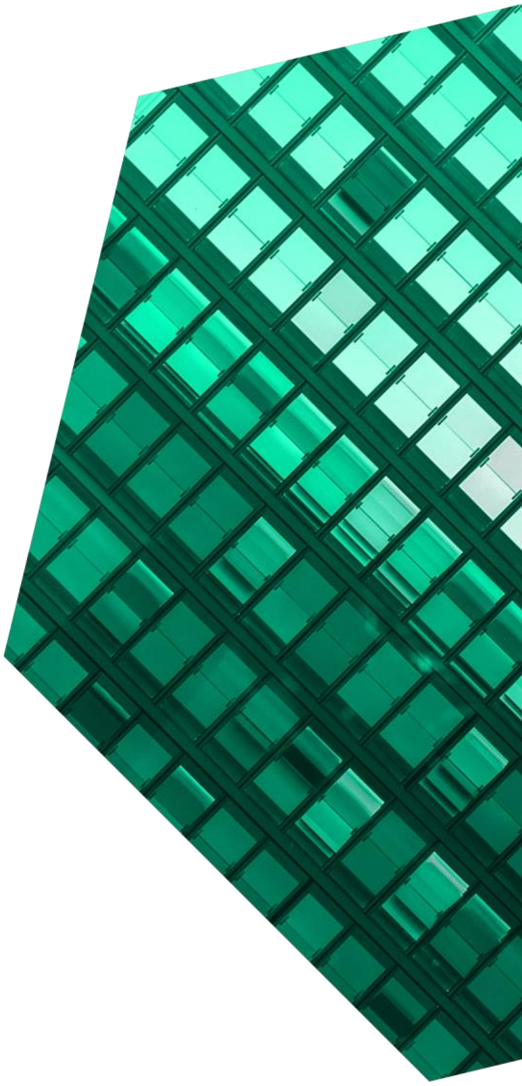
The Total Economic Impact™ Of Carbon Black

Cost Savings And Business Benefits Enabled By Carbon Black

DECEMBER 2023

Table Of Contents

Consulting Team: Erach Desai



ABOUT FORRESTER CONSULTING

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

Executive Summary

Successful cyberattacks, such as ransomware, can have a crippling impact on an organization and its customers. Extended detection and response is the evolution of endpoint detection and response, optimizing threat detection and expediting response times for security incidents. Carbon Black empowers security professionals to conduct faster investigation and remediation of incidents, avoid downtime from debilitating breaches, streamline security operations, and drive compliance and audit efficiencies.

KEY STATISTICS

Return on investment (ROI)
427%

Net present value (NPV)
$4.45M

Cyberattackers (e.g., criminal syndicates, nation-state actors, or solo hackers) deploy a variety of techniques to breach the technology ecosystems of organizations, ranging from malware to phishing to watering holes, with ransomware being one of the more debilitating breaches.

Right now, statistics pertaining to organizational security resilience are not encouraging. Data from a 2023 Forrester security survey identified two relevant trends. First, 77% of surveyed security decision-makers reported that their firm suffered at least one breach in the prior 12 months (compared to 74% in the 2022 survey and 48% to 58% who said the same in prior years). Second, survey respondents reported that the most common type of breach in the prior 12 months was an external attack specifically targeting their organization.[1]

The complexity of today's IT environments coupled with the rapidly changing nature of cyberthreats require security teams to evolve their security strategy. Because of this, security professionals want proactive, adaptive monitoring that enables them to employ more targeted and efficient threat response.[2]

Extended detection and response (XDR) is a comprehensive, effective approach to address today's expanding cybersecurity breach challenges. Forrester defines XDR as the evolution of endpoint detection and response (EDR), which optimizes threat detection, investigation, response, and hunting in real time. XDR unifies security-relevant endpoint detections with telemetry from security and business tools, such as network analysis and visibility (NAV), email security, identity and access management (IAM), cloud security, and more on a cloud-native platform.[3]

Carbon Black is a cloud-native endpoint protection platform that empowers security teams to close the risk gap they face today with deeper visibility and the ability to tailor response to their unique environments. Carbon Black XDR builds on enterprise detection and response (EDR) capabilities to provide extended

Reduction in risk of a large-scale data breach with Carbon Black

40%

visibility, depth of telemetry, automated root cause analysis, and cross-tool threat hunting.

Carbon Black also delivers core endpoint and workload protection with next-generation antivirus (NGAV), host-based firewall, device control, vulnerability management, and remote audit and risk remediation for IT, compliance, and security.

Carbon Black 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.[4] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Carbon Black on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed six representatives with experience in deploying and using Carbon Black for four organizations. In addition, Forrester surveyed 52 decision-makers with experience using Carbon Black products at their organizations (28 of whom use Carbon Black XDR with Managed Detection and Response [MDR]). For the purposes of this study, Forrester aggregated the experiences of the interviewees and survey respondents and combined the results into a single composite organization that is a US-based, global organization that generates $1.2 billion in annual revenue, serves customers globally, and employs 6,000 full-time workers.

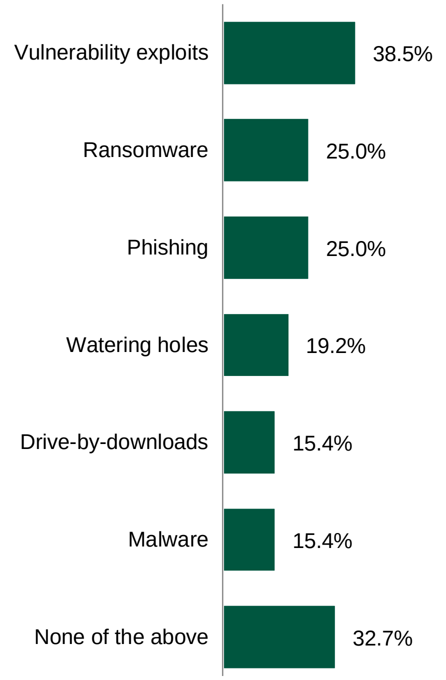
Prior to using Carbon Black, interviewees noted their organizations struggled with the growth and complexity of cybersecurity attacks, insufficient visibility for endpoint security vulnerabilities, and a general sense of insufficient threat protection. Most interviewees also noted that investigating and remediating threats required significant effort with several of them experiencing a high number of false-positive alerts from their legacy tools.

MTTR **reduction** for investigation of security incidents by Year 3

Gross: **75%**

Net: **75%**

What types of threats were you UNABLE TO detect/prevent?



Base: 52 decision-makers working as IT, IT operations, security, or executive management professionals across industries from organizations that have a least 100 employees and currently use multiple Carbon Black products

Source: A commissioned study conducted by Forrester Consulting on behalf of Carbon Black, September 2023

After the investment in Carbon Black, interviewees noted their interviewees' organizations orchestrated real-time responses to cyberattacks and executed on intelligent threat hunting. Leveraging behavior-based analytics, the interviewees' organizations were able to conduct high-quality threat detection with speed and accuracy, while reducing the complexity of security operations.

KEY FINDINGS

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

- **Faster investigation and remediation of cybersecurity incidents enabled by a 75% reduction in mean time to resolution (MTTR).** With Carbon Black, the composite organization stops threats before they become an issue. The composite's security teams also have the information they need to quickly decide how to respond. The composite reduces its MTTR for security incidents that require further investigation by 75% at gross and net levels by Year 3 (adjusted for the effectiveness ramp of the solution). The composite organization's productivity for incident management improves by 72.0% in Year 1, 77.3% in Year 2, and 82.5% in Year 3. Based on more efficient incident management, this benefit is valued at more than $2.2 million for the composite over three years.

- **Reduced downtime from a large-scale data breach driven by a 40% reduction in risk.** Carbon Black detects and prevents threats by collecting deep context on the data that matters in a singular view and dynamically applying behavioral analytics to this data, uncovering patterns and indicators of potential threats. This gives the composite organization granular control and flexibility to customize policies, watch lists, remediations and other actions to close their organization's risk gap. Due to a 40% reduction in risk of a large-scale breach, the composite organization retains $5.5 million of its revenues each year. On an operating basis, the composite organization benefits by just under $1.5 million over three years.

- **Streamlined security operations driving nearly $1.2 million in cost savings.** Carbon Black enables the composite organization to streamline security operations by consolidating multiple, overlapping toolsets to a single, cloud-based platform and reducing the requisite support and training. The composite saves 6,433 FTE hours in Year 1, 5,789 FTE hours in Year 2, and 5,354 FTE hours in Year 3 by mostly redeploying FTEs to higher-value-added work. Over three years, this benefit is valued at nearly $1.2 million.

- **Twenty percent time savings per audit by building in consistency into operational reporting and auditing processes.** With Carbon Black Audit and Remediation, the composite organization quickly queries its endpoints to provide information required for audits. Being able to provide a realistic picture of organizational compliance reduces the likelihood that the

"The very fact that we're not in the news can give you an idea of how well it's [Carbon Black] working. The investment in this product has definitely borne out in keeping us out of the news, first, and also making sure that we are constantly at the forefront of cutting-edge security at all times."

Director of cyberdefense, financial services

"I believe it [Carbon Black] is an awesome product and very worth it. It gives us very good insights into what's happening. I'm a big advocate of it at our organization."

Cybersecurity specialist, healthcare services

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

Base: 52 decision-makers working as IT, IT operations, security, or executive management professionals across industries from organizations that have a least 100 employees and currently use multiple Carbon Black products

Source: A commissioned study conducted by Forrester Consulting on behalf of Carbon Black, September 2023

composite incurs regulatory penalties. This benefit results in cost savings of nearly $464,000 over three years.

- **Remote remediation reduced reimaging by 55%.** Carbon Black enables the composite organization to remotely diagnose and resolve threats via its Live Response capabilities. Live Response provides administrators with a secure remote shell in any protected endpoint, allowing them to instantly remediate issues with confidence without requiring wasteful and inefficient reimaging**.** Not only does this eliminate unnecessary IT work, but it also allows end users to remain productive. The composite organization saves nearly $116,000 over three years from reduced reimaging of devices.

> **"The question should be, how much is the business worth to you? We have been able to stay on top of everything with what Carbon Black gives us. So, it's absolutely worth it."**
>
> *Information security administrator, call center services*

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

- **Peace of mind from improved security posture.** Interviewees noted that the goal for their security operations (SecOps) teams was to ensure that their organizations were not impacted by a crippling cyberattack — ever. Interviewees emphasized how Carbon Black has helped their organizations avoid cyberattacks, thus allowing the security teams to sleep well at night.

- **Proactive capabilities.** Most interviewees emphasized how the proactive features of Carbon Black — especially the behavioral analytics capabilities — enabled their organizations to potentially thwart newer and more dangerous attacks.

- **Solid postsales support.** Several interviewees noted the high level of postsales support provided for the Carbon Black solution that goes above and beyond that expected for day-to-day operations.

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

- **Carbon Black licensing costs.** The composite organization deploys Carbon Black XDR, Core Endpoint Protection, and Managed Detection and Response (MDR). Annual subscription pricing for the composite's 6,000 devices is $260,000, which translates into a three-year present value cost of just about $679,000.

- **Deployment and ongoing support expenses.** The composite incurs two internal costs. The first is related to deploying and training for Carbon Black into Year 1. The second is for ongoing in-production usage of the platform. Based on 2.5 FTEs spending 30% of their time maintaining and upgrading the platform, the composite spends just under $130,000 annually. The combined three-year cost is just over $362,000.

The financial analysis which is based on the interviews and survey found that a composite organization experiences benefits of $5.49 million over three years versus costs of $1.04 million, adding up to a net present value (NPV) of $4.45 million and an ROI of 427%.

"Carbon Black, with the counterpart of having the 24/7 SOC [security operation center], allows us to feel very confident that things that are coming into our environment are carefully identified and that we've always got a safety blanket on our network. It allows us to sleep at night and has been worth every dollar that we have spent. I don't think you can put a price on something like that."

— Network support services manager, educational system

ROI
427%

BENEFITS PV
$5.49M

NPV
$4.45M

PAYBACK
<6 months

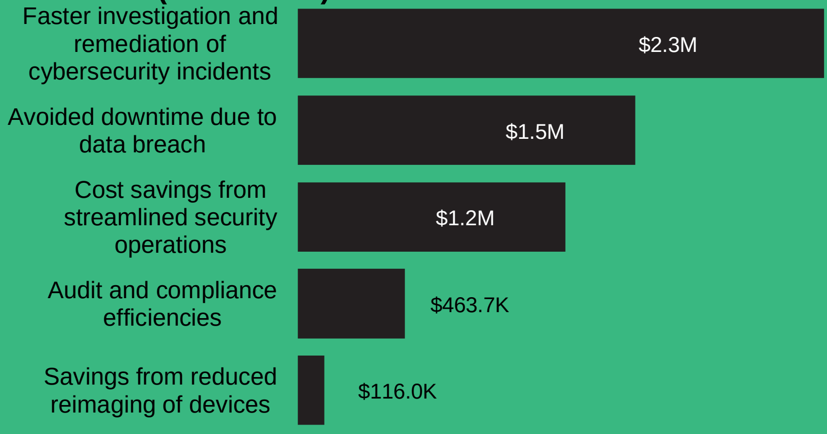
Net MTTR reduction for investigating security incidents by Y3
75%

Reduction in risk of large-scale security breach
40%

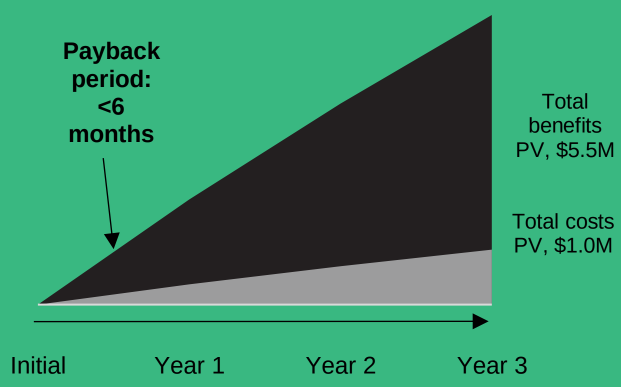
Reduction in FTE hours for security incidents by Y3
83%

Time savings per audit for cybersecurity compliance
20%

Benefits (Three-Year)



Financial Summary



TEI FRAMEWORK AND METHODOLOGY

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

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 Carbon Black 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 November 2020.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by Carbon Black 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 Carbon Black.

Carbon Black 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.

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

Forrester fielded the double-blind survey using a third-party survey partner.

DUE DILIGENCE

Interviewed Carbon Black stakeholders and Forrester analysts to gather data relative to Carbon Black.

INTERVIEWS AND SURVEY

Interviewed six representatives and surveyed 52 respondents at organizations using Carbon Black to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

Designed a composite organization based on characteristics of the interviewees and survey respondents.

FINANCIAL MODEL FRAMEWORK

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

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 Carbon Black Customer Journey

Drivers leading to the Carbon Black investment

KEY CHALLENGES

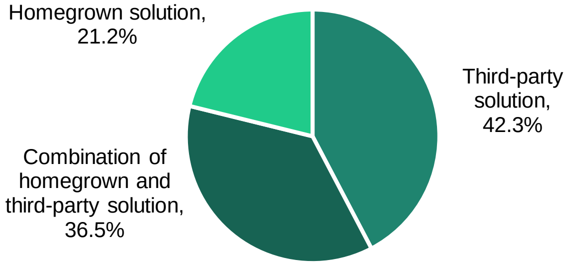
Forrester interviewed six decision-makers who oversee the monitoring and incident management of cybersecurity and network services for four organizations. All of the interviewees were experienced with deploying and overseeing the usage of Carbon Black across their organizations. In addition, Forrester surveyed 52 decision-makers with experience using Carbon Black products at their organizations (28 of whom use Carbon Black XDR with MDR). For more details on the survey respondents, see Appendix B.

Prior to the deployment of Carbon Black, interviewees' organizations struggled with the growth and complexity of cybersecurity attacks, insufficient visibility for endpoint security vulnerabilities, and a general sense of insufficient threat protection. Most interviewees also noted that investigating and remediating threats required significant effort with several of them experiencing a high number of false-positive alerts from their legacy tools.

Most of the interviewees also noted that their organizations experienced a significant cyberattack (primarily a ransomware attack) that prompted them to seek out and evaluate a cloud-based detection and response solution. Both interviewees and survey respondents noted how their organizations struggled with common challenges, including:

- **Limited cybersecurity protection with legacy tools.** Prior to deploying Carbon Black, most interviewees used a combination of traditional antivirus (AV) tools, some NGAV tools, and some homegrown solutions. In their prior state, interviewees cited a lack of confidence in their organizations' ability to prevent threats, with ransomware being their primary concern. Of the respondents surveyed, 39% felt their organization was unable to detect vulnerability exploits, while 25% felt that ransomware and phishing were the threats that were going the most undetected before the introduction of Carbon Black.

Prior to your investment in Carbon Black, how were you protecting your devices?



Base: 52 decision-makers working as IT, IT operations, security, or executive management professionals across industries from organizations that have a least 100 employees and currently use multiple Carbon Black products

Source: A commissioned study conducted by Forrester Consulting on behalf of Carbon Black, September 2023

- **Time-consuming efforts for investigating and remediating security incidents.** In addition to feeling vulnerable about emerging and more sophisticated cybersecurity attacks, interviewees said their legacy tools were limited in terms of visibility, automatic quarantining, and identifying vulnerable users. Interviewees felt that their existing tools made the investigation and remediation of security incidents time-consuming and required precious SecOps resources. Consequently, the default go-to solution was reimaging endpoint devices, a long and expensive process that impacted operations and required the physical shipment of hardware.

- **Operational inefficiencies chasing false-positive alerts.** In the prior state, several of the interviewees noted their organizations used some form of security information and event management (SIEM) tools. Interviewees stated that implementing SIEM technologies required a lot of work and fine-tuning. Coupled with the sheer volume of alerts generated, SIEM solutions sometimes overwhelmed security professionals.

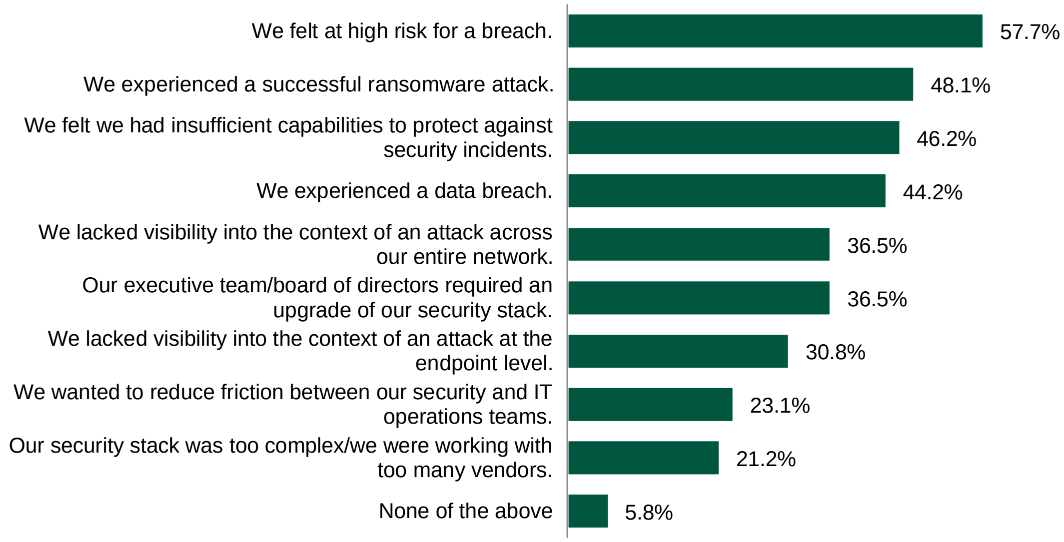
Interviewees cited how chasing false-positive alerts also diverted limited security resources.

- **The need for better visibility and detection with behavior-based tools.** Interviewees felt limited about their threat-hunting capabilities with their assortment of prior solutions. Thirty-seven percent of survey respondents felt that they lacked visibility into the context of an attack across their organization's entire network, and 31% were concerned about a lack of visibility into their organization's endpoints with their prior solution. There was a general assessment that newer solutions would close the coverage gaps by leveraging AI and behavioral analytics to stop malware and ransomware infections across the network including endpoints.

"We were looking to refresh our technology stack including cybersecurity. [Our legacy solution] was primarily an antivirus scanner with some SIEM capabilities. We wanted to add some more expansive capabilities and decided to have conversations with some of the leaders, such as Carbon Black."

Director of cyberdefense, financial services

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



Base: 52 decision-makers working as IT, IT operations, security, or executive management professionals across industries from organizations that have a least 100 employees and currently use multiple Carbon Black products

Source: A commissioned study conducted by Forrester Consulting on behalf of Carbon Black, September 2023

SOLUTION REQUIREMENTS

The interviewees and survey respondents searched for a solution that could:

- Automatically execute real-time responses to cyberthreats.
- Enable intelligent threat hunting.
- Drive behavior-based analytics enabled with AI to mitigate attacks.
- Execute high-quality threat detection and response with speed and accuracy across the network plus visibility into endpoint activity.
- Reduce the complexity of the security stack.
- Identify vulnerable users with increased visibility and automatic quarantining.
- Minimize the need for reactionary and wasteful reimaging of endpoints.

COMPOSITE ORGANIZATION

Based on the interviews and survey, 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 six interviewees from four organizations and the 52 survey respondents, 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 composite is a US-based, global organization that heavily relies on its network to meet customer and internal user needs. It generates $1.2 billion in annual revenue, serves customers globally, and employs 6,000 full-time workers. Employees work under a hybrid work policy; most are affiliated with headquarters or regional offices, though there is also a healthy mix of remote workers.

Deployment characteristics. Prior to deploying Carbon Black, the composite organization relied on a combination of on-premises AV and antimalware tools with some SIEM capabilities to protect its 6,000 endpoints. The firm implements Carbon Black to protect against threats, detect and respond to them, and audit its extended network landscape. Forrester opted to model endpoints only for this composite, though most organizations will also install Carbon Black agents on servers and virtual machines. The composite configures its Carbon Black deployment with MDR to supplement its internal security team.

In terms of the effective impact of the Carbon Black solution, the composite derives 80% of the effective value in Year 1, 90% in Year 2, and 100% in Year 3.

"Carbon Black is a next generation behavioral-based endpoint protection platform. It's not like your traditional [antivirus] tool that I worked with before. Completely different."

Cybersecurity specialist, healthcare services

"We did two POCs [proof of concepts]: one on [a competitive tool] and one on Carbon Black. We collectively agreed that Carbon Black was more user-friendly — something that we could evolve with — and had the key XDR functionality we wanted.'"

Information security administrator, call center services

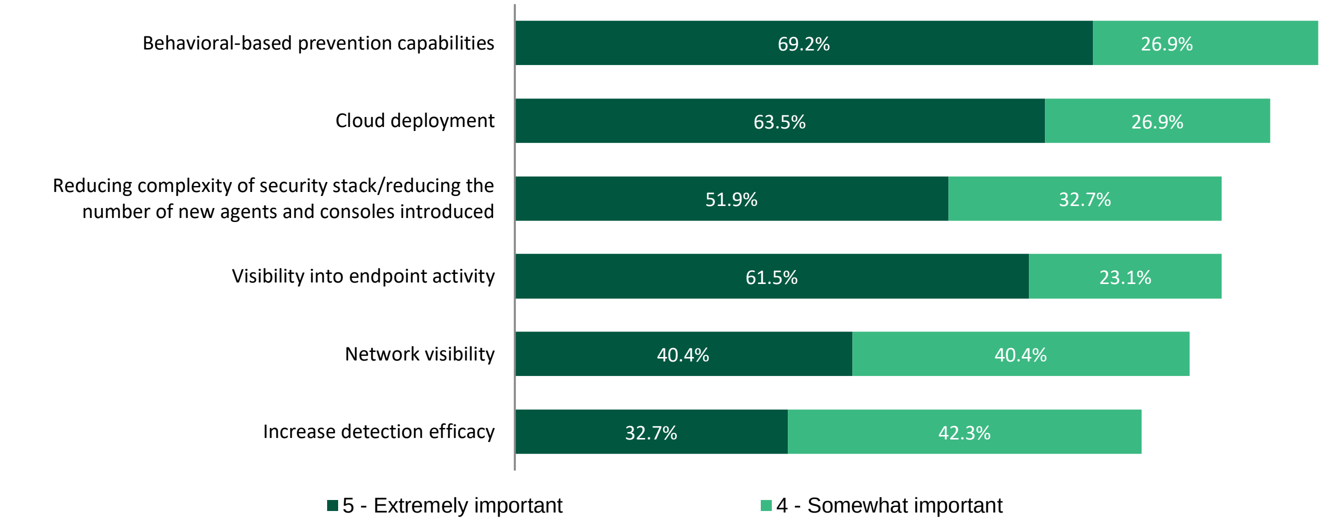
This is due to ongoing learnings from the usage of a newer technological solution.

Key Assumptions

- **Global organization based in the US**
- **$1.2 billion in revenue**
- **6,000 full-time employees with 6,000 endpoints deployed**
- **Effective impact of Carbon Black deployment: 80% in Y1, 90% in Y2, 100% in Y3**

After implementing Carbon Black, the composite organization retires its legacy software.

How important were the following aspects of Carbon Black Cloud when you were making your investment decisions?



Base: 52 decision-makers working as IT, IT operations, security, or executive management professionals across industries from organizations that have a least 100 employees and currently use multiple Carbon Black products

Source: A commissioned study conducted by Forrester Consulting on behalf of Carbon Black, September 2023

Analysis Of Benefits

Quantified benefit data as applied to the composite

Ref.	Benefit	Year 1	Year 2	Year 3	Total	Present Value
Total Benefits						
Atr	Faster investigation and remediation of cybersecurity incidents	$859,248	$921,902	$984,555	$2,765,705	$2,282,747
Btr	Avoided downtime due to data breach	$588,461	$588,461	$588,461	$1,765,383	$1,463,415
Ctr	Cost savings from streamlined security operations	$502,416	$459,780	$430,981	$1,393,177	$1,160,528
Dtr	Audit and compliance efficiencies	$186,480	$186,480	$186,480	$559,440	$463,748
Etr	Savings from reduced reimaging of devices	$46,628	$46,628	$46,628	$139,884	$115,957
	Total benefits (risk-adjusted)	$2,183,233	$2,203,251	$2,237,105	$6,623,589	$5,486,395

FASTER INVESTIGATION AND REMEDIATION OF CYBERSECURITY INCIDENTS

Evidence and data. Interviewees noted that prior to having Carbon Black, their organizations went through painstaking processes to prioritize and investigate alerts — assuming that their legacy on-premises NGAV and antimalware tools even alerted them or that their security teams weren't overwhelmed with the number of false-positive alerts with a SIEM tool. Without the ability to efficiently detect, investigate, and remediate security incidents that required further scrutiny, the interviewees' organizations' only option was to resort to reimaging devices out of an overabundance of caution.

"With Carbon Black, I can confidently say within a couple of hours maximum, we are able to find, identify a threat, and remediate it. And we're able to quarantine devices on which we find suspicious activity."

Head of information security, educational system

MTTR **reduction** for investigation of security incidents by Year 3

Gross: **75%**

Net: **75%**

Interviewees noted that Carbon Black capabilities like prioritized alerts, deep visibility and tracking capabilities, and the ability to remotely triage endpoints were critical in reducing investigation and remediation times. With Carbon Black, the interviewees' organizations stopped threats before they could become issues and security teams received the information they needed to quickly decide how to respond to threats. Additionally, extended detection and response capabilities enabled interviewees' organizations to skip some of the tedious, common, or repetitive detection engineering work, allowing them to focus SecOps resources on more targeted and specific incidents. Survey respondents, in general, echoed and reinforced these overall strengths.

- The cyberdefense team leader for a financial services firm explained: "With our legacy tools, we used to get a bunch of potentially unwarranted alerts. They were very benign, like known bad things or things that could very easily be taken care of. But distractions, nonetheless. Now when we do get alerts, they are predominantly higher fidelity alerts especially coming out of Carbon Black. When we see something, we genuinely know that we have to take action and it's not a waste of time to do so." The director of cyberdefense for the same company added: "I think 45 to 65 security events per week is what we are now seeing with [Carbon Black]. Previously we were more in the 75 to 100 event range. With Carbon Black, we're able to thwart the suspicious activity in a matter of minutes."
- The head of information security for a metropolitan educational system stated: "We have definitely gone from days to minutes for time to remediation. The systems that we had were separated, and we didn't have the SOC as we do now." They went on to add that they were now seeing about 50 potential incidents per week.

Reduction in number of FTE hours for security incidents by Year 3

82.5%

"It's the difference between operating in the dark in a house that you kind of were familiar with. Whereas with Carbon Black, the lights are on all day and all night. We can go to exactly what we want to see and wherever we want to see it."

Cyberdefense team leader, financial services

- The information security administrator for a call center services provider explained: "As far as improvement on detection time with Carbon Black, I'd say it's almost 75% to 80%. If hunting down an event took me an hour in [legacy tool], I can have it resolved in 15 minutes." They added, "When I log into Carbon Black first thing in the morning I might have 10 alerts, of which five are ones that I need to investigate further each day."
- In the survey, 85% of respondents noted that the median number of security incidents at their organization was 45 per day in their prior state. After deploying Carbon Black, the median number of security incidents dropped 44% to 25 per day.
- The survey also found that 42% of respondents noted that the median time to detect a security incident went from 52.5 minutes to 36 minutes with Carbon Black. For remediation time, this same percentage of respondents noted that median time was reduced from 45 minutes prior to 32.5 minutes with Carbon Black. Combining these for an overall mean time to respond (MTTR including detection), the survey respondents reported a 29.7% MTTR reduction.

Modeling and assumptions. This benefit is focused on how the composite improves SecOps and IT Ops productivity due to reduced security incidents and a reduction in MTTR for incidents that require investigation to avoid breaches. For the composite organization, Forrester assumes the following:

- In the prior state, the composite organization encounters 1,800 security incidents per year (or about 35 per week) based on interview and survey data adjusted for the number of employees (or endpoints).
- With proactive, behavior-based evaluation, the deployment of Carbon Black reduces the number of security incidents requiring further investigation by 30% for the composite.
- As cited, datapoints from interviewees for the time required to detect and remediate each credible security incident before deploying Carbon Black were meaningfully higher than the 1.6 hours median from the survey respondents. The composite assumes an average of 12 hours for detection and remediation of a credible security incident.
- The gross reduction in MTTR for detection and remediation of security incidents is assumed to be 75%. The net MTTR reduction, reflected in row A5, is based on the effectiveness ramp of the Carbon Black solution.
- Each security incident in the prior state and with Carbon Black deployed impacts the knowledge worker whose endpoint requires investigation (taken offline) and requires the effort of a full-time SecOps or IT Ops professional.
- The fully burdened annual salary of an experienced SecOps FTE or IT Ops FTE who is focused on security is $162,000. This equals an hourly rate of $78. The fully burdened annual salary of the average knowledge worker for the composite is assumed to be $108,000, which translates to $52 per hour.
- For benefits with productivity gains, Forrester applies a productivity adjustment factor that represents the percentage of productivity savings actually realized (i.e., 1 hour of time savings does not necessarily translate into 1 hour of productive work). For the duration of these security incidents requiring investigation, the composite's affected FTEs are assumed to lose 50% of their productivity during this time.
- Comparing the total number of FTE hours for SecOps and IT operations (IT Ops) professionals in the prior state to after Carbon Black implementation, the interviewees' productivity for incident management improves by 72.0% in Year 1, by 77.3% in Year 2, and by 82.5% in Year 3.

Risks. Forrester recognizes that these results may not be representative of all experiences and that the benefit will vary between organizations depending on the following:

- The number of security incidents per year in the prior state, which will vary by the number of devices and the complexity of the organization's network.
- The time required to investigate and remediate security incidents in the prior state, which will be dependent on the relative sophistication of the legacy cybersecurity toolset and the expertise of the SecOps team.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of over $2.2 million.

Faster Investigation And Remediation Of Cybersecurity Incidents

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Number of security incidents before Carbon Black	Composite	1,800	1,800	1,800
A2	Number of security incidents after Carbon Black	A1-(A1*30%)	1,260	1,260	1,260
A3	Time to investigate and remediate each security incident before Carbon Black (hours)	Composite	12	12	12
A4	Subtotal: Reduction in time due to fewer security incidents requiring remediation (hours)	(A1-A2)*A3	6,480	6,480	6,480
A5	Net reduction in MTTR with Carbon Black (adjusted for deployment ramp)	Interviews	60.0%	67.5%	75.0%
A6	Time to investigate and remediate after Carbon Black (hours)	A3*(1-A5)	4.8	3.9	3.0
A7	Subtotal: Reduction in time due to faster remediation of current security incidents (hours)	A2*(A3-A6)	9,072	10,206	11,340
A8	Total time savings for impacted employee and SecOps/IT Ops FTE (hours)	A4+A7	15,552	16,686	17,820
A9	Fully burdened hourly salary of SecOps/IT Ops specialist	TEI standard	$78	$78	$78
A10	Fully burdened hourly salary of average knowledge worker	TEI standard	$52	$52	$52
A11	Productivity adjustment factor	TEI standard	50%	50%	50%
At	Faster investigation and remediation of cybersecurity incidents	A8*(A9+A10)*A11	$1,010,880	$1,084,590	$1,158,300
	Risk adjustment	↓15%			
Atr	Faster investigation and remediation of cybersecurity incidents (risk-adjusted)		$859,248	$921,902	$984,555
	Three-year total: $2,765,705			**Three-year present value: $2,282,747**	

AVOIDED DOWNTIME DUE TO DATA BREACH

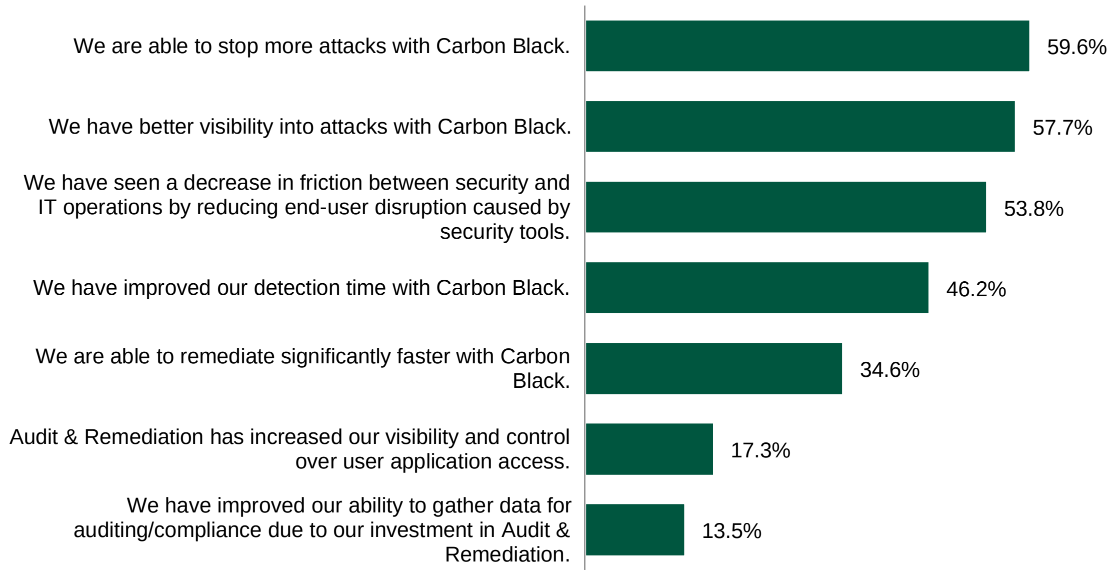
Evidence and data. Prior to the deployment of Carbon Black, interviewees' organizations did not have the tools or capabilities to confidently withstand a range of cybersecurity attacks. Most interviewees noted their organizations experienced a significant cyberattack — specifically ransomware attacks — that prompted them to seek out and evaluate a next-generation cybersecurity solution. More than 55% of survey respondents indicated that Carbon Black either enabled them to stop more attacks or have better visibility into attacks.

Interviewees who were present at the time of their organizations' ransomware attacks recalled how the incident essentially brought their organizations to their knees. They recalled how external specialist firms were brought on to navigate the incident. These firms introduced them to Carbon Black. The comprehensive protection afforded by Carbon Black helped the interviewees' organizations prevent known and emerging threats. All of the interviewees said their organizations had not experienced a successful cyberattack since deploying Carbon Black.

> **"We had a ransomware attack two weeks after I joined the team. It was all hands on deck (15 of us working together) for 16 hours a day for a month to remediate and fully resume operations. We have not had another incident like that since starting to use Carbon Black."**
>
> *Information security administrator, call center services*

- The cyberdefense team leader for a financial services firm explained: "Within Carbon Black, we can upgrade and update our policies in real time. In 15 minutes, every system on our network can now be protected from what we just found 20 minutes ago. That's huge! That's the difference between being protected and unprotected. It's the

Thinking about your experience with Carbon Black Cloud compared to your previous environment, which of the following are true?



Base: 52 decision-makers working as IT, IT operations, security, or executive management professionals across industries from organizations that have a least 100 employees and currently use multiple Carbon Black products

Source: A commissioned study conducted by Forrester Consulting on behalf of Carbon Black, September 2023

difference between stopping and attacking and being subjected to an attack."

- The head of information security for a metropolitan educational system stated: "We can proactively add categorized or published malware to the [Carbon Black] platform. Or we can reactively look and see if we missed something. But we haven't had any significant incidents like ransomware in the last year."
- The information security administrator for a call center services provider shared, "With Carbon Black and all of the other things that we've put in place, I would be surprised if we couldn't have people answering the phones within an hour after a breach."
- The cybersecurity specialist for a healthcare services provider explained: "But overall, I'm not seeing ransomware things happen. They're just not getting here because we have a layered approach. Carbon Black does a very good job of sending out alerts on their dashboard. It says here's some of the threats that we're seeing right now, some of the nasties that are out there."
- In the survey, 21.2% of respondents indicated that their organization's level of protection against cybersecurity events was "Significantly better" with Carbon Black, while another 67.3% stated that it was "Better."

Modeling and assumptions. This benefit is focused on the revenue the composite retains by reducing the downtime when being targeted by debilitating cybersecurity events. For the composite organization, Forrester assumes the following:

Reduction in risk of a large-scale data breach

40%

- Any technology-enabled organization is likely to have one large-scale data breach per year.[5]
- In its prior state, the composite organization has a 30% likelihood to have a large-scale data breach in any given year.
- The deployment and proactive usage of Carbon Black reduces the risk of a significant data breach by 40%, based on anecdotal assessments from interviews and interpreting results from the survey.
- Any successful large-scale data breach leads to 120 hours of downtime for the composite, based on two weeks of downtime for five business days per week at 12 working hours per day globally.
- Based on 3,120 hours of annual operations (52 weeks times five business days times 12 hours per day), the composite organization generates $384,615 in revenues per hour.
- The composite retains $5.5 million of its revenues annually by avoiding downtime due to a large-scale data breach.
- To determine the net business impact for the composite, the revenue benefit is converted into operating profits. The operating margin for the composite's industry is assumed to be 12.5%.

Risks. Forrester recognizes that these results may not be representative of all experiences and that the benefit will vary between organizations depending on the following:

- The reduced likelihood of a large-scale data breach with Carbon Black will depend on the extent of the deployment and the relative sophistication of the organization's SecOps team.
- The cost of downtime will depend on the revenue, product, and customer profile of the

organization, including hours of business operations.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of just under $1.5 million.

Avoided Downtime Due To Data Breach					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	Number of large-scale data breaches per year	Forrester research	1	1	1
B2	Average length of a large-scale data breach (hours)	2 weeks * 5 days/week * 12 hours/day	120	120	120
B3	Risk of a data breach before Carbon Black	Interviews and survey	30%	30%	30%
B4	Reduction in risk of a breach with Carbon Black deployed	Interviews and survey	40%	40%	40%
B5	Revenue per hour	Composite	$384,615	$384,615	$384,615
B6	Avoided revenue loss with Carbon Black	B1*B2*B3*B4* B5	$5,538,456	$5,538,456	$5,538,456
B7	Operating margin	Composite	12.5%	12.5%	12.5%
Bt	Avoided downtime due to data breach	B6*B7	$692,307	$692,307	$692,307
	Risk adjustment	↓15%			
Btr	Avoided downtime due to data breach (risk-adjusted)		$588,461	$588,461	$588,461
	Three-year total: $1,765,383			**Three-year present value: $1,463,415**	

COST SAVINGS FROM STREAMLINED SECURITY OPERATIONS

Evidence and data. Prior to having Carbon Black, interviewees noted their organizations utilized multiple solutions for detection and remediation, most of which were on-premises or installed on endpoint devices. Supporting multiple toolsets, which included the inefficiency of working with on-premises only solutions, required a larger staff of SecOps and IT Ops professionals in addition to annual training, etc. This approach to cybersecurity increased capital expenses, degraded endpoint performance, and created a complex layer of vendor management that distracted from mission-critical security tasks.

With the deployment of Carbon Black, interviewees benefited from using a single cloud-native agent, dashboard, and data set. With Carbon Black, the interviewees' organizations were able to streamline security operations, allowing SecOps and IT Ops professionals to focus on higher-value-added work.

- The cyberdefense team leader for a financial services firm explained: "Carbon Black's protection scheme gives us the ability to protect our users, servers, workstations from executions that we don't actually want to be successful and put policies in place where exceptions need to be allowed. Deploying new software is now simply a ticketed process that gets executed within a few minutes, rather than a few weeks when [our legacy vendor] needed to get involved. We're much more efficient and better protected with Carbon Black." They added: "So we use that time to threat hunt and to do cyberthreat-intel-based investigation. We can leverage some of our other capabilities now that we actually have more time to dedicate to them rather than chasing our tail in the endless sea of alerts."

- The network support services manager for a metropolitan educational system explained their leverage: "We are now able to do more with just three employees. They're able to accomplish significantly more work and get more done and able to take care of more events. I would say that it is noticeable compared to before, and that it has been something that has been a big impact to the way they're able to handle security events."

- The information security administrator for a call center services provider explained: "I used to spend a good deal of my day looking into issues I saw in [our legacy tool] prior to deploying Carbon Black. Now, I may spend 1 hour a day on the console. I would estimate that Carbon Black has given me back about 15 to 20 hours a week, that I would have spent working on [our legacy tool]."

- The cybersecurity specialist for a healthcare services provider stated: "Carbon Black is behavioral. I might make exceptions on your machine and your machine gets clobbered. But Carbon Black can [automatically] shut down your machine. It can also quarantine it, which keeps an event from spreading. It does a very good job of that."

> **"Because the fidelity of what we're doing [with Carbon Black] is higher, it allows the team to work on other areas that are also of high impact."**
>
> *Cyberdefense team leader, financial services*

Reduction in FTE hours per year from streamlined operations

Year 1 → Year 3

6,400 → 5,300

- Our survey found that 31% of respondents noted their organization replaced an average of 3.5 vendors for security solutions by switching to Carbon Black, saving an average of $198,000 in licensing costs per year.

Modeling and assumptions. This benefit captures the combined cost savings from support and training efficiencies by consolidating vendors into one cloud-based Carbon Black solution. For the composite organization, Forrester assumes the following with the savings reduced by 5% in Year 2 and Year 3:

- The key metrics and data points that informed the modeling of the composite for this overall benefit were derived from the survey. All such metrics were scaled for the size of the composite (6,000 devices) vs. the average from the survey (15,000 devices).
- The composite saves 41 hours in Year 1 from ongoing support of legacy security solutions (a base of 27 survey respondents saved an average of 8.6 hours per month).
- The composite saves 360 hours of training in Year 1 by consolidating on Carbon Black (a base of 10 survey respondents saved an average of $70,000 a year, which was converted to nearly 900 annual FTE hours).
- The composite redeploys 1.6 SecOps or IT Ops FTEs in Year 1 by moving to a cloud-based solution (a base of 27 survey respondents “Did not need to hire” an average of 4.0 FTEs per year).
- The composite redeploys 1.3 SecOps or IT Ops FTEs in Year 1 by moving to Carbon Black with MDR (a base of 13 survey respondents “Did not need to hire” an average of 3.3 FTEs per year).
- The fully burdened annual salary of an experienced SecOps FTE or IT Ops FTE focused on security is $162,000.

“This tool has enabled the team to become much more productive. They can monitor a lot more things. We’re not reactive anymore. We are proactive.”

Network support services manager, educational system

- The composite saves $90,000 per year in subscription costs by decommissioning legacy tools on an adjusted basis.
- The composite saves 6,433 FTE hours in Year 1, 5,789 FTE hours in Year 2, and 5,354 FTE hours in Year 3 by mostly redeploying FTEs to higher-value-added work.

Risks. Forrester recognizes that these results may not be representative of all experiences and that the benefit will vary between organizations depending on the following:

- The extent of savings across all metrics will vary by the relative sophistication of the organization’s security team, and the prior state.
- Average full-loaded salaries of SecOps, IT Ops and knowledge workers would vary by industry and geography.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of just under $1.2 million.

Cost Savings From Streamlined Security Operations

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Time saved from supporting legacy security solutions (hours)	Survey	41	39	37
C2	Training time savings by consolidating on Carbon Black (hours)	Survey	360	342	325
C3	Fully burdened hourly salary of SecOps/IT Ops specialist	TEI standard	$78	$78	$78
C4	Subtotal: Cost savings from support and training of legacy solutions	(C1+C2)*C3	$31,278	$29,718	$28,236
C5	Number of SecOps/IT Ops FTEs not required due to Carbon Black being on the cloud	Survey	1.6	1.4	1.3
C6	Number of SecOps/IT Ops FTEs not required due to MDR with Carbon Black	Survey	1.3	1.2	1.1
C7	Fully burdened annual salary of SecOps/IT Ops specialist	TEI standard	$162,000	$162,000	$162,000
C8	Subtotal: Cost savings enabled by Carbon Black and MDR	(C5+C6)*C7	$469,800	$421,200	$388,800
C9	**Retired subscription costs**	**Survey**	**$90,000**	**$90,000**	**$90,000**
Ct	Cost savings from streamlined security operations	C4+C8+C9	$591,078	$540,918	$507,036
	Risk adjustment	↓15%			
Ctr	Cost savings from streamlined security operations (risk-adjusted)		$502,416	$459,780	$430,981
	Three-year total: $1,393,177			**Three-year present value: $1,160,528**	

AUDIT AND COMPLIANCE EFFICIENCIES

Evidence and data. The interviewees noted that cost of maintaining compliance was far easier to bear than the expense of dealing with noncompliance issues. Additionally, organizations with a highly complex security infrastructure faced an average breach cost that was $2.15 million higher than those with lower complexity environments.[6]

Time savings per audit related to cybersecurity compliance

20%

With the audit and remediation capabilities included with Carbon Black, interviewees noted their organizations could take advantage of a number of prebuilt queries or design their own to establish proactive IT hygiene and establish consistent reporting and auditing processes. This allowed the interviewees' organizations to enforce endpoint configuration and compliance policies, as well as provided visibility into software license inventory and any unwanted browser plug-ins. These capabilities were important, as the interviewees' organizations faced stiff penalties from vendors if they either were underlicensed or violated government regulations, such as the EU's General Data Protection Regulation

(GDPR) or the U S's Health Insurance Portability and Accountability Act (HIPAA).

- The cybersecurity specialist for the healthcare services provider stated: "One of the capabilities Carbon Black has is that I can establish policies that now have to use a hardware-encrypted, managed USB drive. So I can make sure that you have a need. But now I know that when you lose it, I don't have to worry about a data breach because you just copy a spreadsheet that has 1,000 dummy records on it. I can prove to the compliance officer, 'No, he copied that onto a hardware-encrypted one instead of [another] one.' I can do that in Carbon Black."

Modeling and assumptions. This benefit combines the efficiencies achieved for audit and compliance processes relative to an organization's cybersecurity infrastructure by using Carbon Black audit and remediation capabilities. All of the key modeling assumptions for this benefit were derived from the survey. For the composite organization, Forrester assumes the following (Note: Given the nature of these metrics, they are not linearly scaled by organization size):

- The composite has six audits per year (a base of five survey respondents averaged 5.7 audits per year).
- In the prior state, each audit takes five hours (a base of five survey respondents averaged 4.9 hours per audit)
- The composite achieves 20% of time savings per audit (based on four respondents averaging savings of 20.8%).
- The cost of each audit is based on three internal FTEs (at $100 per hour), and three external professionals (billing at the rate of $300 per hour).
- Only two survey respondents estimated the annual cost savings or avoided penalties for noncompliance related to cybersecurity averaging $100,000 per year. Forrester believes that noncompliance penalties can run much higher than that. The mode assumes avoided noncompliance fines of $200,000 per year.[7]

Risks. Forrester recognizes that these results may not be representative of all experiences and that the benefit will vary between organizations depending on the following:

- The number of audits and time per audit will vary for organizations that are substantially larger or smaller compared to the composite organization.
- The fully loaded hourly audit cost will vary by geography and sizably larger or smaller organization.
- Avoided noncompliance fines will vary by industry.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of nearly $464,000.

Audit And Compliance Efficiencies					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
D1	Number of audits	Survey	6	6	6
D2	Time per audit (hours) before Carbon Black	Survey	5	5	5
D3	Audit time savings with Carbon Black	Survey	20%	20%	20%
D4	Fully loaded hourly cost of an audit	Assumption	$1,200	$1,200	$1,200
D5	Avoided noncompliance fines	Forrester research	$200,000	$200,000	$200,000
Dt	Audit and compliance efficiencies	(D1*D2*D3*D4) + D5	$207,200	$207,200	$207,200
	Risk adjustment	↓10%			
Dtr	Audit and compliance efficiencies (risk-adjusted)		$186,480	$186,480	$186,480
	Three-year total: $559,440		**Three-year present value: $463,748**		

SAVINGS FROM REDUCED REIMAGING OF DEVICES

Evidence and data. Prior to having Carbon Black, interviewees noted their organizations' IT professionals had the limited ability to remotely access devices to diagnose and remediate incidents. With rudimentary tools for detection and remediation, the only option of the interviewees' organizations was to resort to reimaging devices out of an overabundance of caution. While this was an effective way to resolve these incidents, it was highly inefficient and organizations with hybrid workers incurred the costs of downtime, plus shipment expenses.

Interviewees noted that Carbon Black enabled their organizations to remotely diagnose and resolve most threats with confidence without requiring wasteful and inefficient reimaging.

- The information security administrator for a call center services provider said: "Let's say a new threat report came out today on TrueBot. I put the hashes in, and I get three alerts, for an example. So within maybe a couple of hours of this even being discovered, I know if we have it, if we don't, and if we do, where it is. I know what I need to do to block it. Then I take these systems, isolate

> **"When it comes to malware itself, with a large number of users that we have, they go everywhere, and they click on everything. We're able to see what the malware is. Most of the time we're able to completely remediate without having to refresh or reimage the device."**
>
> *Head of information security, educational system*

them immediately, and they get reimaged. With Carbon Black, it's like amazingly quick." They added, "Currently, we are averaging less than one reimaging of devices per week."

- The network support services manager for a metropolitan educational system stated: "In the past, the handling of security events was reaching out to the help desk, requisitioning a technician to get the device, investigating the device, finding out what's wrong with it, and then remediation. So there were a lot of hands in that process. Now, we've been able to confidently remediate remotely without even touching the device."

- In our survey, 33% of respondents cited an average of 42.8 devices were required to be reimaged per month in their prior state, which was reduced to an average of 19.4 reimages after Carbon Black implementation. This computes to a reduction of 54.7%.

Modeling and assumptions. This benefit quantifies the savings derived from reduced reimaging of devices due to the Carbon Black solution. For the composite organization, Forrester assumes the following:

- The key metrics and data points that informed the modeling for this benefit were derived from the survey. All such metrics were scaled for the size of the composite (6,000 devices) vs. the average from the survey (15,000 devices).

- In the prior state, the composite organization requires 230 devices to be reimaged each year (a base of 17 survey respondents averaging 42.8 device reimages per month).

- The reduction in reimaging required per month and per year is 55%.

- The average time needed for an IT technician to reimage each device is 8 hours (a base of 18 survey respondents cited an average time of 8.0 hours per device for reimaging).

- The fully burdened annual salary of an experienced IT technician is $94,500. This equals an hourly rate of $45. The fully burdened annual salary of the average knowledge worker for the composite is assumed to be $108,000, which translates to $52 per hour.

- For the duration of reimaging a device, the composite's affected FTEs are assumed to be 50% productive during this time.

Risks. Forrester recognizes that these results may not be representative of all experiences and that the benefit will vary between organizations depending on the following:

- The number of devices requiring reimaging with legacy solutions will depend on the size of the organization and the relative sophistication of those legacy tools.

- The time required by an IT technician to reimage a given device will vary by the types of endpoint devices and relative expertise of the technician.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of nearly $116,000.

Reduction in need for reimaging of endpoint devices

55%

Savings From Reduced Reimaging Of Devices					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
E1	Number of devices requiring reimaging with legacy solutions	Survey	230	230	230
E2	Reduction in reimaging with Carbon Black	Survey	55%	55%	55%
E3	Time required for IT technician to reimage each device (hours)	Survey	8	8	8
E4	Fully burdened hourly salary of service desk IT technician	TEI standard	$45	$45	$45
E5	Fully burdened hourly salary of average knowledge worker	TEI standard	$52	$52	$52
E6	Productivity adjustment factor	TEI standard	50%	50%	50%
Et	Savings from reduced reimaging of devices	E1*E2*E3*(E4+E5)*E6	$49,082	$49,082	$49,082
	Risk adjustment	↓5%			
Etr	Savings from reduced reimaging of devices (risk-adjusted)		$46,628	$46,628	$46,628
	Three-year total: $139,884		**Three-year present value: $115,957**		

UNQUANTIFIED BENEFITS

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

- **Peace of mind from improved security posture.** Interviewees noted that the goal for their security teams was to ensure that their organizations were not impacted by a crippling cyberattack — ever. In addition to the disruption to the business, most interviewees noted their organizations would have to deal with the reputational impact of a cyberattack on top of dealing with any customer data that might get compromised (and subject the organizations to legal actions). Most interviewees emphasized how Carbon Black has helped their organizations avoid cyberattacks, thus allowing their security teams to sleep well at night.

  The head of information security for a metropolitan educational system stated: "With Carbon Black, we can query all our devices to see if we were impacted and didn't know about it. If Carbon Black hasn't flagged it, we're able to add that to the platform. I especially feel a lot of confidence when it comes to our endpoint management. I will say that lets me sleep better at night."

- **Proactive capabilities.** Most interviewees also emphasized how the proactive features of Carbon Black have enabled their organizations to potentially thwart newer and more dangerous attacks.

  The cyberdefense team leader for a financial services firm framed it as: "Based on a comparative analysis, we concluded that Carbon Black uses a more proactive model than most other EDR or XDR solutions. If it knows that something's bad, then it will try to block the bad thing. They are really good at detecting all the things that people already know are bad. But threat actors are a lot more cunning these days and you might fool some of the people some of the time. But Carbon Black looks for patterns and identifies emerging threats better than others."

- **Solid postsales support.** Several interviewees noted the high level of postsales support for the Carbon Black solution that went above and beyond what was expected for day-to-day operations.

  The network support services manager for a metropolitan educational system stated: "We do engage with [Carbon Black's support team],

"We really like the proactive measures. Even if Carbon Black hasn't caught it, we're able to add, train, supplement to the information that's on the platform. And we know that if anything that has been declared or flagged publicly, we can either be alerted or proactively block it."

Head of information security, educational system

"With Carbon Black, we're doing a very good job at a layered defense based on behavioral analysis. Overall, I feel very confident. I sleep well at night."

Cybersecurity specialist, healthcare services

> **"It's really derived from Carbon Black's ability to give us complete control of the systems that we have and making sure that they're always in a known good state. And when they're not, then we have the ability to isolate those systems and to take action on that and also deny that attempt to subvert our policy."**
>
> *Cyberdefense team leader, financial services*

usually on a quarterly basis. We have conversations and discussions about how the product is going overall. And, as you've already heard from us, we're very happy with the level of support."

FLEXIBILITY

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

- **Ability to customize.** Interviewees discussed the granular control of Carbon Black and the ability to customize rules for their unique environments. Examples ran the range of creating prevention policies, customized watchlists, and program automated remediation actions — all while being fully integrated with the rest of the organizations' security stack. The head of information security for a metropolitan educational system discussed the potential for Carbon Black being set up as a host intrusion prevention system with the ability to create firewall-like rules as one example of this flexibility.

- **Scalability.** Interviewees discussed possible future opportunities for expansion or expanding use cases of Carbon Black, including the potential for scaling with their organizations' future needs.

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**
Ftr	External: Carbon Black configuration fees	$0	$273,000	$273,000	$273,000	$819,000	$678,911
Gtr	Internal: Deployment and ongoing support expenses	$4,118	$146,678	$142,560	$142,560	$435,916	$362,388
	Total costs (risk-adjusted)	$4,118	$419,678	$415,560	$415,560	$1,254,916	$1,041,299

EXTERNAL: CARBON BLACK CONFIGURATION FEES

Evidence and data. Interviewees stated that their companies paid annual subscription fees based on the products or product packages utilized.

- Subscription pricing for Carbon Black products was based on the number of devices instrumented (laptops, desktops, workstations, servers, virtual machines, etc.) and the functionality deployed.
- Relative to adding on the MDR capability, the head of information security for a metropolitan educational system explained: "We are also paying for the 24x7 SOC monitoring through Carbon Black because we're not equipped for the 24/7 staffing. So they are monitoring and contact us, if and when needed."

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

- The composite deploys Carbon Black prior to Year 1 with 6,000 devices instrumented (matching the organizations' number of employees).
- For this configuration, pricing for an organization of the composite's size is $237,400 per year. Forrester used a higher price estimate, of $260,00 per year, to be conservative.
- Pricing may vary. Contact Carbon Black for additional details.

Risks. Forrester recognizes that these results may not be representative of all experiences, and that the costs will vary between organizations depending on the following factors:

- The size of the organization and the number of devices deployed with Carbon Black.
- The specific products or product packages utilized.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of just about $679,000.

External: Carbon Black Configuration Fees						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
F1	Carbon Black with MDR subscription fees	Composite		$260,000	$260,000	$260,000
Ft	External: Carbon Black configuration fees	F1	$0	$260,000	$260,000	$260,000
	Risk adjustment	↑5%				
Ftr	External: Carbon Black configuration fees (risk-adjusted)		$0	$273,000	$273,000	$273,000
	Three-year total: $819,000			**Three-year present value: $678,911**		

INTERNAL: DEPLOYMENT AND ONGOING SUPPORT EXPENSES

Evidence and data. Interviewees stated that using Carbon Black in a production mode was quite straightforward. Initial deployment involved installing agents, testing, deploying to machines, and monitoring and adjusting rules.

- The cyberdefense team leader for the financial services firm succinctly stated, “The level of effort during implementation was actually relatively minimal.” They went on to elaborate that for ongoing maintenance of the platform, their organization needed two to three FTEs for 25% to 30% of their time initially and a lower percentage in the following years.

- The network support services manager for a metropolitan educational system said: “During the deployment phase, I don’t think we ever ran into any issues with deployment. Both teams understood the goal. We had resources from Carbon Black and, along with our team, we were able to get that on board.” They went on to explain that maintenance of the platform only requires one FTE for 25% of their time given that their organization paid for 24x7 support from Carbon Black.

- The information security administrator for a call center services provider explained: “Carbon Black was extremely easy to install, and you can configure it very granularly. They have threat reports that come out just about every day with a new threat. I can incorporate that into Carbon Black with a simple text file import. It’s instantly configured.” For their organization that is much smaller relative to the composite, ongoing maintenance requires one FTE with “very occasional” usage.

- In terms of installation, survey respondents indicated an average of 41.0 FTE hours for installation of Carbon Black, requiring an average of 7.6 FTEs.

> **“[Carbon Black] keeps going on its own. It’s like omnipresent. As long as the end points are installed, they talk to the cloud. As far as actually maintaining it, I don’t maintain it. I work with the information it provides. In practice, [Carbon Black] actually maintains it in the cloud.”**
>
> *Information security administrator, call center services*

- For ongoing support, an average of 6.3 FTEs were needed requiring an average of 42.6% of their time.

Modeling and assumptions. For the composite organization, Forrester assumes the following, with all key survey metrics adjusted for the size of the composite:

- For initial deployment, including training, the composite organization utilizes three full-time SecOps and/or IT Ops professionals for 16 hours initially and in Year 1.
- For ongoing in-production usage, the composite utilizes the equivalent of 2.5 such FTEs who spend 30% of their time dedicated to maintaining and upgrading the Carbon Black platform.
- The fully burdened annual salary of an experienced SecOps FTE or IT Ops FTE is $162,000. This equals an hourly rate of $78.

Risks. Forrester recognizes that these results may not be representative of all experiences and that the benefit will vary between organizations depending on:

- The size of the organization and its specific configuration Carbon Black.
- The relative expertise of the organization's SecOps and IT Ops professionals.
- Average salaries will vary by industry and geography.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of just over $362,000.

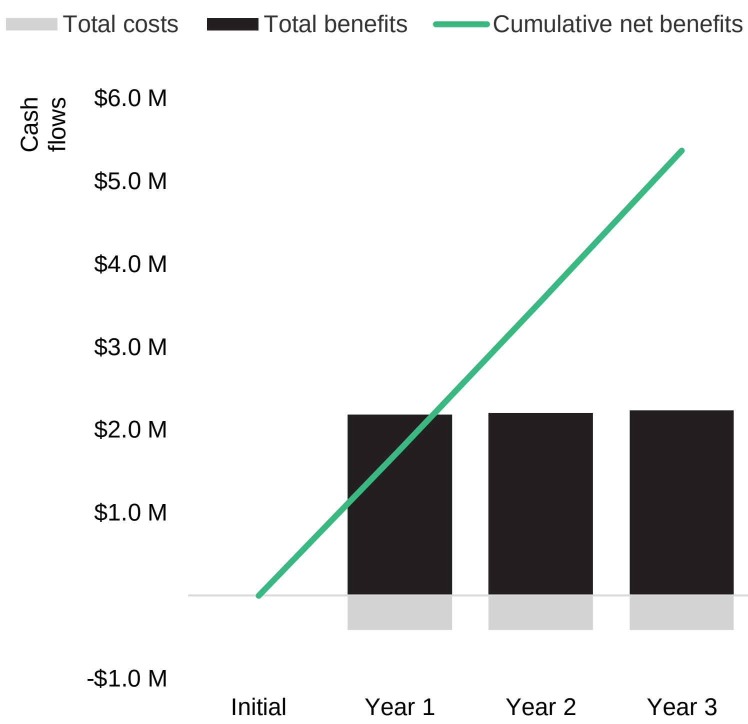
Internal: Deployment And Ongoing Support Expenses

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
G1	Carbon Black deployment and training time (hours per FTE)	Survey	16	16		
G2	Effective number of FTEs for deployment and training	Survey	3	3		
G3	Fully burdened hourly salary of SecOps/IT Ops specialist	TEI standard	$78	$78	$78	$78
G4	FTE hours required for ongoing maintenance of the Carbon Black platform	Interviews and survey		0.8	0.8	0.8
G5	Fully burdened annual salary of SecOps/IT Ops specialist	TEI standard	$162,000	$162,000	$162,000	$162,000
Gt	Internal: Deployment and ongoing support expenses	(G1*G2*G3)+(G4*G5)	$3,744	$133,344	$129,600	$129,600
	Risk adjustment	↑10%				
Gtr	Internal: Deployment and ongoing support expenses (risk-adjusted)		$4,118	$146,678	$142,560	$142,560
	Three-year total: $435,917			**Three-year present value: $362,388**		

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	($4,118)	($419,678)	($415,560)	($415,560)	($1,254,916)	($1,041,299)
Total benefits	$0	$2,183,233	$2,203,251	$2,237,105	$6,623,589	$5,486,395
Net benefits	($4,118)	$1,763,555	$1,787,691	$1,821,545	$5,368,673	$4,445,096
ROI						427%
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.

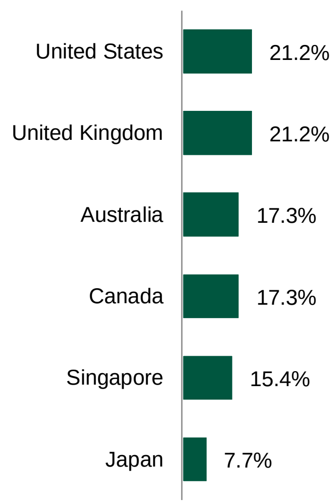
Appendix B: Interviews And Survey Demographics

Interviews

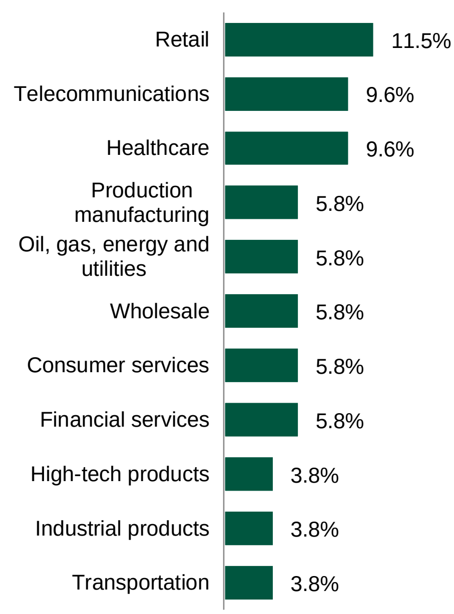
Role	Industry	Region	Revenue And Employees	Carbon Black Solution Configuration
• Head of information security • Network support services manager	Educational system	US metropolitan district	• No revenue • 130,000 employees and students	• Carbon Black NGAV, Audit & Remediation, and Vulnerability Management for endpoints and workloads • 200 sites • 50,000 to 100,000 devices deployed
• Director of cyberdefense • Cyberdefense team leader	Financial services	Global	• $800 million • 2,000 employees	• Carbon Black Endpoint Enterprise • 20 sites; laptops, servers, VMs • 50,000 to 100,000 devices deployed
Information security administrator	Call center services	North American regional	• $65 million • 500 employees (not including contractors)	• Carbon Black Endpoint Enterprise with MDR • 2 data centers • 3,000 devices deployed
Cybersecurity specialist	Healthcare services	Urban US	• $160 million • 1,200 employees	• Carbon Black Endpoint Standard and MDR • 1,200 endpoints (350 servers)

Survey Demographics

In which country are you located?



Which of the following best describes the industry to which your company belongs?

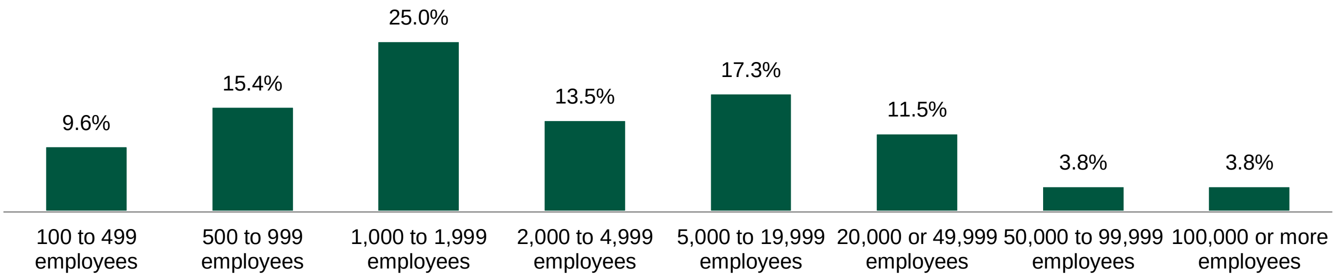


Base: 52 decision-makers working as IT, IT operations, security, or executive management professionals across industries from organizations that have a least 100 employees and currently use multiple Carbon Black products

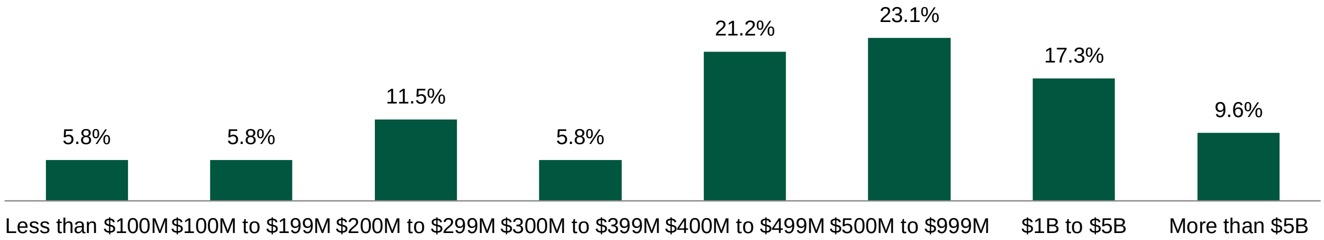
Source: A commissioned study conducted by Forrester Consulting on behalf of Carbon Black, September 2023

Survey Demographics

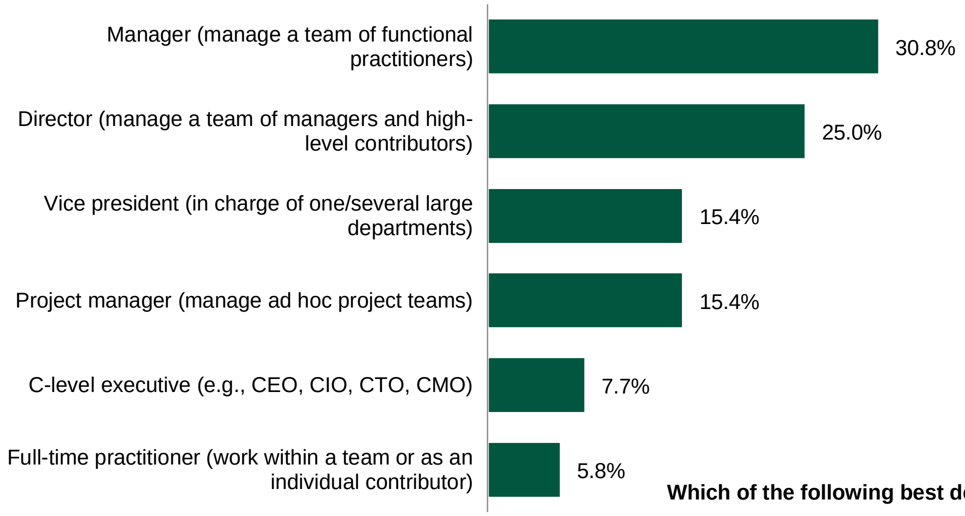
Using your best estimate, how many employees work for your organization worldwide?



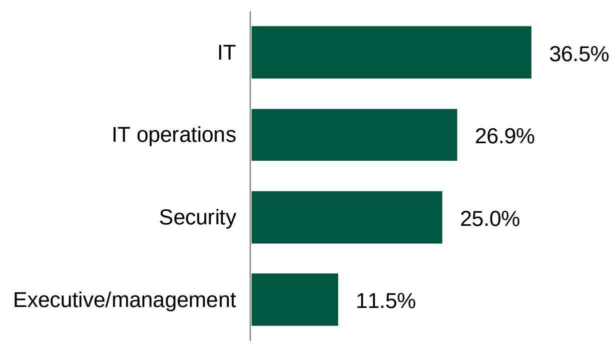
What is your organization's annual revenue?



Which title best describes your position at your organization?



Which of the following best describes the department you work in?



Base: 52 decision-makers working as IT, IT operations, security, or executive management professionals across industries from organizations that have a least 100 employees and currently use multiple Carbon Black products

Source: A commissioned study conducted by Forrester Consulting on behalf of Carbon Black, September 2023

Appendix C: Supplemental Information

Related Forrester Research

"New Tech: Extended Detection And Response (XDR) Providers, Q3 2021," Forrester Research, Inc., August 2, 2021.

Appendix D: Endnotes

---

[1] Source: Forrester Analytics Business Technographics® Security Survey, 2023.

[2] Source: "Evolving Security Operations Capabilities – Insights Into The XDR Paradigm Shift" a commissioned study conducted by Forrester Consulting on behalf of VMware, December 2022.

[3] Source: "Adapt Or Die: XDR Is On A Collision Course With SIEM And SOAR," Forrester Research, Inc., April 28, 2021.

[4] 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.

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

[6] Source: Jeff Purrington, "The True Cost of Non-Compliance," Saviynt, May 10, 2022.

[7] Ibid.


FORRESTER®