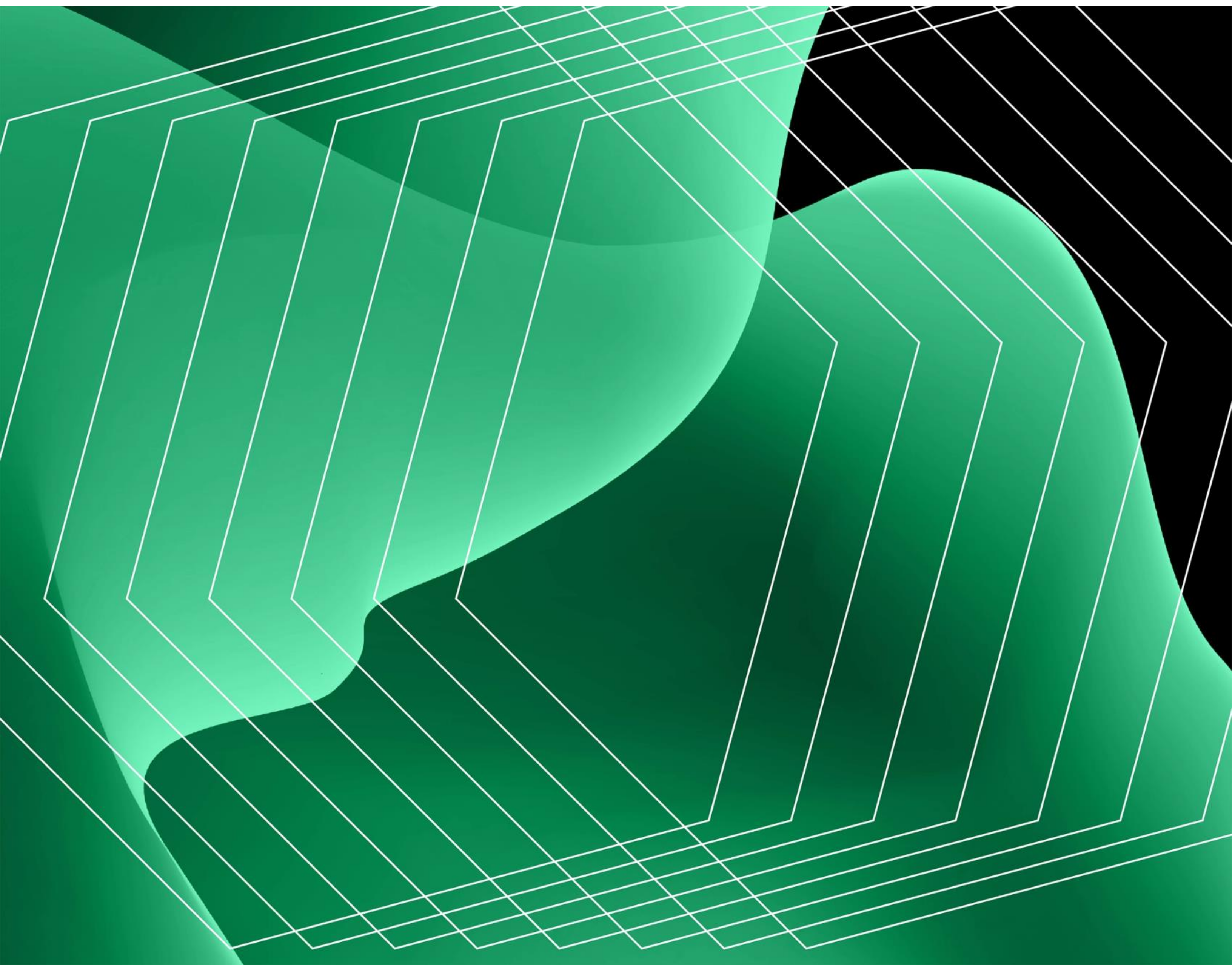
# The Total Economic Impact™ Of Carbon Black App Control

Cost Savings And Business Benefits Enabled By App Control

A Forrester Total Economic Impact™ Study
Commissioned By Carbon Black, February 2024



# Table Of Contents



**Consulting Team:**


Roger Nauth


**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

**As security threats and malware evolve, so has the need for technologies to combat these threats. Organizations can't afford the loss of productivity caused by unscheduled downtime or performance degradation associated with a security breach nor can they afford the loss of reputation and subsequent costs. Given this rapidly evolving threat landscape, organizations are searching for security that works.**

Carbon Black App Control leverages a positive security model allowing only trusted software to run. It can be deployed on-premises or on private and public clouds. It is effective in specialized use cases, such as end-of-life operating systems (EOL OS), protecting critical systems, and securing fixed function devices and air-gapped systems.

Carbon Black App Control continuously protects against cyberthreats that evade traditional security defenses by employing a positive security model, which enables a default/deny security posture. App Control does not rely on a library or list of files to maintain, which can easily become outdated. Instead, it employs multiple approval methods, including IT- and cloud-driven trust, trusted publishers, custom rules, and validated external sources

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 App Control.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of App Control on their organizations.

Return on investment (ROI)
**207%**

Net present value (NPV)
**$1.10M**

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four representatives with experience using App Control. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization that is a mission-critical financial services or government organization of 6,000 employees and a revenue of more than $500 million per year with high security risk.

Interviewees said that prior to using App Control, their organizations experienced malware and ransomware incidents, had a great deal of unknown and unauthorized software running in their environments, experienced version control issues, and did not have any solutions that could provide allow-listing and deny-listing.

After the investment in App Control, the interviewees had greater knowledge of the software running in their organizations' environments and were able to implement security controls to the file and kernel levels. Interviewees appreciated App Control's ease of use, positive security model that provided granular policies to guard against zero-day threats, and effective monitoring of their organizations' endpoints. Some interview participants expressed their organizations had not experienced any security incidents after deploying App Control in high enforcement.

## KEY FINDINGS

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

- **Increased productivity resulting from reduction in time spent on reimaging machines, worth a risk-adjusted $1.3 million over three years.** With App Control's functionality, the composite organization saves 1,500 hours annually from end-user support, diagnosis, and reimaging machines.
- **Increased productivity by reducing time addressing malware, worth a risk-adjusted $207,000 over three years.** App Control drives the savings of 2.25 hours for each of the approximately 500 average malware incidents for the composite organization.
- **Increased productivity resulting from effort saved in conducting extensive investigations to identify sources of security problems, worth a risk-adjusted $117,000 over three years.** The composite saves effort from

conducting deep-dive investigations and root-cause analyses identifying sources of security issues because of App Control, amounting to 140 hours in Year 1, 126 hours in Year 2, and 113 hours in Year 3.

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

- **Risk management guesswork reduction.** Interviewees touted that they saved time from taking guesswork out of risk management by two-thirds.
- **Meeting compliance mandates.** The interviewees noted their organizations increased their ability to meet compliance mandates.
- **Ease of use.** Forrester learned from interview participants that App Control is easy to use.

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

- **App Control server and desktop licenses.** The composite organization pays risk-adjusted license fees of $234,000 for Carbon Black App Control over three years.
- **Carbon Black professional services fees.** The composite organization incurs a risk-adjusted $298,000 for professional services over the initial two years to configure App Control, with most of these costs occurring in Year 1.

The representative interviews and financial analysis found that a composite organization experiences benefits of $1.63 million over three years versus costs of $532,000, adding up to a net present value (NPV) of $1.10 million and an ROI of 207%.

> "Think about the productivity being lost from that employee. We're having to wait for the machine to be reimaged, then having to wait to get any prior applications installed, reinstalled so they can get back to the state they were. And then also the possibility of any data that was work-related on the machines is now lost because we had to reimage. So I would estimate that it's probably saved us in the tens of thousands just over time, if we're putting a dollar sign on time."
>
> **CYBERSECURITY ANALYST, GOVERNMENT**

Return on investment (ROI)

**207%**

Benefits PV

**$1.63M**

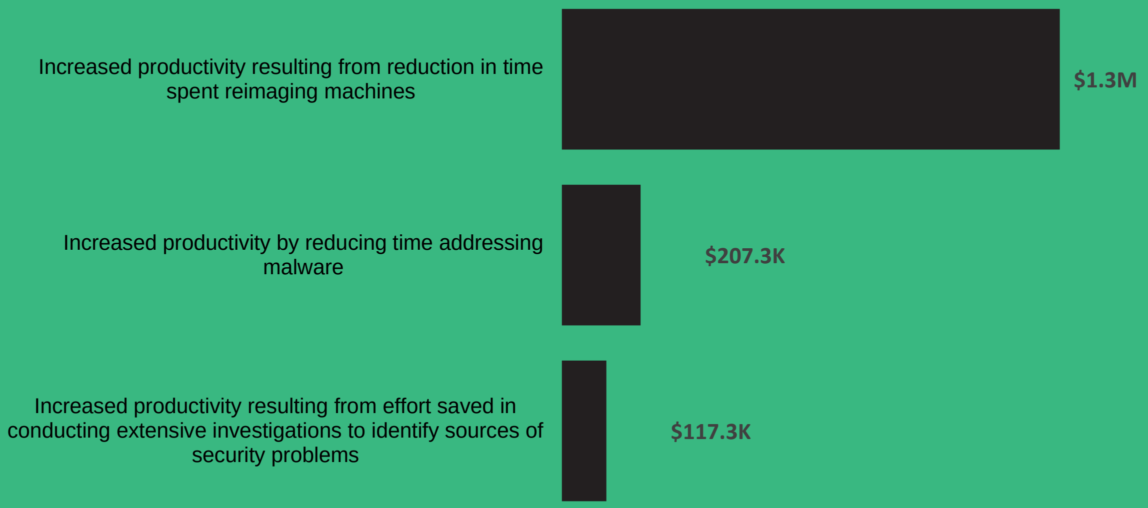
Net present value (NPV)

**$1.10M**

Payback

**7 months**

## Benefits (Three-Year)



## TEI FRAMEWORK AND METHODOLOGY

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

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 App Control can have on an organization.

**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 App Control.

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.

**Due Diligence**
Interviewed Carbon Black stakeholders and Forrester analysts to gather data relative to App Control.

**Interviews**
Interviewed four representatives at organizations using App Control to obtain data about costs, benefits, and risks.

**Composite Organization**
Designed a composite organization based on characteristics of the interviewees' organizations.

**Financial Model Framework**
Constructed a financial model representative of the interviews using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewees.

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

# The Carbon Black App Control Customer Journey

## Drivers leading to the App Control investment

**Interviews**

| Role | Industry | Region | Employees | Revenue |
|---|---|---|---|---|
| Cybersecurity manager | Financial services/banking | US | 9,000 | $1.8B |
| Senior systems administrator | Financial services/investment management | US | 7,900 | $6.2B |
| Cybersecurity analyst | Government | US | 5,000 | Not reported |
| Information security manager | Financial services/banking | US | 875 | $100M |

### KEY CHALLENGES

The interviewees noted how their organizations struggled with common challenges, prior to implementing Carbon Black App Control, including:

- **The need to evaluate additional security.** Two of the interviewees noted their organizations had experienced security incidents. Even though their organizations were insured, these interview participants expressed that ransomware incidents were highly influential pain points leading to their organizations' decision to evaluate solutions.
- **A lack of allow-listing and deny-listing capabilities.** Interviewees told Forrester that their organizations did not have any application to do allow-listing and deny-listing.
- **The realization of running unauthorized software.** Interviewees explained that their organizations were aware they were running a lot of unauthorized software.

- **Version-control issues.** Interview participants told Forrester that they had version control issues, which opened their organizations up to significant security risks.

> "You definitely could have a situation where all the endpoints become affected. And even worse, they can also spread to servers and that's extremely scary."
>
> CYBERSECURITY ANALYST, GOVERNMENT

## COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an ROI analysis that illustrates the areas financially affected. The composite organization is representative of the four interviewees, and it is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

**Description of composite.** The composite organization is a mission-critical financial services or government organization with 6,000 employees and a revenue of more than $500 million per year with high security risk.

**Deployment characteristics.** The composite organization deploys App Control across approximately 11,000 endpoints, including servers and desktops.

**Key Assumptions**

More than $500 million in revenue

6,000 employees

Mission-critical organization

High security risk

# 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 | Increased productivity resulting from reduction in time spent reimaging machines | $526,500 | $526,500 | $526,500 | $1,579,500 | $1,309,328 |
| Btr | Increased productivity by reducing time addressing malware | $83,363 | $83,363 | $83,363 | $250,088 | $207,310 |
| Ctr | Increased productivity resulting from effort saved in conducting extensive investigations to identify sources of security problems | $51,870 | $46,683 | $42,015 | $140,568 | $117,302 |
| | Total benefits (risk-adjusted) | $661,733 | $656,546 | $651,877 | $1,970,155 | $1,633,940 |

## INCREASED PRODUCTIVITY RESULTING FROM REDUCTION IN TIME SPENT REIMAGING MACHINES

**Evidence and data.** Interviewees noted that Carbon Black App Control was instrumental in preventing their organizations from having to reimage machines and provide end-user support and diagnosis of security issues as a result. When hit with malware, many environments will simply reimage the impacted endpoints to ensure the device returns to a known good state which is often a time-consuming process.

Interviewees told Forrester that their organizations reduced the time spent reimaging machines by 75%, saving an average of 1,500 hours each year due to App Control.

**Modeling and assumptions.** To calculate the value of this benefit for the composite organization, Forrester assumes the following:

- The average number of endpoints for the composite organization is 11,000. Carbon Black App Control is deployed at organizations with significantly more endpoints than this; however, this is the average number of endpoints purchased for the interviewees' organizations.

- The average number of hours spent for end-user support, diagnosis, and reimaging machines is 5.5 per incident.
- Prior to App Control, the composite organization spent an average of 2,000 hours reimaging machines on an annual basis.
- The fully burdened hourly salary of an IT analyst involved in these activities and tasks is $65.
- Six FTEs involved in these activities are reallocated to working on more value-added tasks.

**Risks.** The value of this benefit can vary across organizations due to the following:

- The number of devices requiring reimaging will depend on the size of the organization and the relative sophistication of its 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 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.3 million.

**75%**

Savings of time on reimaging machines

> “Obviously, App Control blocks a lot of these things that we don’t approve. Because of that, I would say there has been a lot of operational benefit because we built out a lot of efficiencies that we didn’t really have before by just starting to do application whitelisting in the way that App Control supports.”
>
> INFORMATION SECURITY MANAGER, FINANCIAL SERVICES/BANKING

> “We’re looking at the entire time we’ve had App Control in high enforcement from 2016 until now. It’s been in the thousands of hours. Thousands of hours have been saved because, since App Control can stop this different type of malware, we don’t have to reimage.”
>
> CYBERSECURITY ANALYST, GOVERNMENT

| Increased Productivity Resulting From Reduction In Time Spent Reimaging Machines | | | | | |
|---|---|---|---|---|---|
| **Ref.** | **Metric** | **Source** | **Year 1** | **Year 2** | **Year 3** |
| A1 | Average number of endpoints for composite | Composite | 11,000 | 11,000 | 11,000 |
| A2 | Average time spent reimaging machines per endpoint prior to App Control (hours) | Interviews | 5.5 | 5.5 | 5.5 |
| A3 | Subtotal: Total annual time spent reimaging machines prior to App Control (hours) | A1/A2 | 2,000 | 2,000 | 2,000 |
| A4 | Percentage of time saved reimaging machines with App Control (percent) | Interviews | 75% | 75% | 75% |
| A5 | Subtotal: Time saved reimaging machines by using App Control (hours) | A3*A4 | 1,500 | 1,500 | 1,500 |
| A6 | Fully burdened hourly salary of IT analyst | TEI standard | $65 | $65 | $65 |
| A7 | Number of FTEs involved reimaging machines reallocated to more value-added tasks | Interviews | 6 | 6 | 6 |
| At | Increased productivity resulting from reduction in time spent reimaging machines | A5*A6*A7 | $585,000 | $585,000 | $585,000 |
| | Risk adjustment | ↓10% | | | |
| Atr | Increased productivity resulting from reduction in time spent reimaging machines (risk-adjusted) | | $526,500 | $526,500 | $526,500 |
| | **Three-year total: $1,579,500** | | **Three-year present value: $1,309,328** | | |

## INCREASED PRODUCTIVITY BY REDUCING TIME ADDRESSING MALWARE

**Evidence and data.** Interviewees noted that App Control increased the efficiency and productivity of its security operations (SecOps) and IT operations (IT Ops) professionals' activities and workflow in addressing malware. Not all environments will reimage endpoints that have been compromised through malware or ransomware; they will instead use tools to clean the malicious software and ensure the endpoint is returned to a trusted state. By providing better tools for limiting application execution, App Control reduces the cleanup time used to deal with malicious software.

Interviewees told Forrester that they saved 2 hours and 15 minutes per incident from addressing malware, including file-based malware and ransomware, a total of 1,125 hours per year and 3,375 hours over three years.

**Modeling and assumptions.** To calculate the value of this benefit for the composite organization, Forrester assumes the following:

- The composite organization experiences an average of 500 malware incidents per year, which may include a range of incidents including file-based malware and ransomware.
- The composite organization spent 3 hours per incident prior to App Control working to address malware.
- The composite organization now spends 45 minutes per incident addressing malware after App Control, a 75% reduction from the prior state.
- The fully burdened hourly salary of a SecOps/IT Ops specialist is $78.

**Risks.** The value of this benefit can vary across organizations due to the following:

- The number of endpoints purchased by organizations in which App Control is deployed may vary significantly by size of organization.
- Malware incidents vary widely and include a variety of threats including ransomware, which may have significant financial implications for companies.
- The extent of savings will vary by the relative sophistication of the organization's security team and the organization's prior state.
- Average fully loaded salaries of SecOps and IT Ops would vary by industry and geography.

**Results.** To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $207,000.

**75%**

Reduction in time addressing malware

# 3,375 hours

Three-year time savings from addressing malware

“It’s not just the benefit of stopping malware and protecting users from themselves, but also policy enforcement and stopping users from installing things they shouldn’t be installing because you have to have proper authorization through your supervision to say, ‘Hey, I want to use this program or this application.’ So it’s actually stopped people or at least slowed them down. So it’s helped us from a policy enforcement standpoint as well.”

CYBERSECURITY ANALYST, GOVERNMENT

“As far as locking down workstations, locking down applications, and being able to have insight on what’s running, I think it’s a good value there. You’re really going to get a good detail of what is being blocked.”

SENIOR SYSTEMS ADMINISTRATOR, FINANCIAL SERVICES/INVESTMENT MANAGEMENT

> “I would say the biggest benefit is ransomware protection. That is, of the malware out there, that’s probably the scariest and maybe the most damaging given what it does. I think one of the biggest benefits is protection against that, since essentially the application functions as a file execution control. Since it controls file execution, it can stop malware.”
>
> CYBERSECURITY ANALYST, GOVERNMENT

**Increased Productivity By Reducing Time Addressing Malware**

| Ref. | Metric | Source | Year 1 | Year 2 | Year 3 |
|---|---|---|---|---|---|
| B1 | Annual number of malware incidents per year | Composite | 500 | 500 | 500 |
| B2 | Time to address malware before App Control (hours) | Interviews | 3.00 | 3.00 | 3.00 |
| B3 | Reduction in time addressing malware (percentage) | Interviews | 75% | 75% | 75% |
| B4 | Time to address malware after App Control (hours) | Interviews | 0.75 | 0.75 | 0.75 |
| B5 | Subtotal: Savings from addressing file-based malware (hours) | B2-B4 | 2.25 | 2.25 | 2.25 |
| B6 | Fully burdened hourly salary of SecOps/IT Ops specialist | TEI standard | $78 | $78 | $78 |
| Bt | Increased productivity by reducing time addressing malware | B2*B5*B6 | $87,750 | $87,750 | $87,750 |
| | Risk adjustment | ↓5% | | | |
| Btr | Increased productivity by reducing time addressing malware (risk-adjusted) | | $83,363 | $83,363 | $83,363 |
| | **Three-year total: $250,088** | | **Three-year present value: $207,310** | | |

## INCREASED PRODUCTIVITY RESULTING FROM EFFORT SAVED IN CONDUCTING EXTENSIVE INVESTIGATIONS TO IDENTIFY SOURCES OF SECURITY PROBLEMS

**Evidence and data.** Interviewees noted their organizations increased productivity from time saved investigating problems, particularly spending significant amounts of effort determining the root-causes of problems.

Interviewees also noted that their organizations saved 140 hours in Year 1, 126 in Year 2, and 113 hours in Year 3 from conducting extensive investigations to identify sources of security problems as a result of App Control.

**Modeling and assumptions.** To calculate the value of this benefit for the composite organization, Forrester assumes the following:

- The time spent conducting extensive investigations to identify sources of security problems prior to App Control is 200 hours in Year 1, reducing by 10% each year to 180 and 162 hours in Years 2 and 3.
- The composite organization experiences a time savings of 70% from investigating sources of security problems.
- The fully burdened hourly salary of SecOps/IT Ops specialists is $78.
- Five of these security and IT operations professionals were required to conduct these investigations prior to App Control.

**Risks.** The value of this benefit can vary across organizations due to:

- The extent of savings will vary by the relative sophistication of the organization’s security team and the organization’s prior state.
- Average fully loaded salaries of SecOps and IT Ops would vary by industry and geography.

**Results.** To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $117,000.

| Increased Productivity Resulting From Effort Saved In Conducting Extensive Investigations To Identify Sources Of Security Problems | | | | | |
|---|---|---|---|---|---|
| **Ref.** | **Metric** | **Source** | **Year 1** | **Year 2** | **Year 3** |
| C1 | Time spent conducting extensive investigations to identify sources of security problems prior to App Control (hours) | Interviews | 200 | 180 | 162 |
| C2 | Percentage of time saved from investigating sources of security problems | Interviews | 70% | 70% | 70% |
| C3 | Subtotal: Time saved from conducting extensive investigations to identify sources of security problems as a result of App Control (hours) | C1*C2 | 140 | 126 | 113 |
| C4 | Fully burdened hourly salary of SecOps/IT Ops specialist | TEI standard | $78 | $78 | $78 |
| C5 | Number of SecOps/IT Ops specialists | Composite | 5 | 5 | 5 |
| Ct | Increased productivity resulting from effort saved in conducting extensive investigations to identify sources of security problems | C3*C4*C5 | $54,600 | $49,140 | $44,226 |
| | Risk adjustment | ↓5% | | | |
| Ctr | Increased productivity resulting from effort saved in conducting extensive investigations to identify sources of security problems (risk-adjusted) | | $51,870 | $46,683 | $42,015 |
| | **Three-year total: $140,568** | | **Three-year present value: $117,302** | | |

# 380 hours

Three-year time savings conducting extensive investigation of security issues

## UNQUANTIFIED BENEFITS

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

- **Meeting compliance mandates.** Interviewees noted their organizations increased their ability to meet compliance mandates.

- **Risk management guesswork reduction.** Interviewees touted that they took the guesswork out of risk management, saving up to two-thirds of the time they would typically spend on this activity.
- **Ease of use.** Forrester learned from interviewees that App Control is easy to use. A cybersecurity analyst at a government organization said: “When I got my hands on [App Control], I have to say it wasn’t very hard to learn. It’s really just point and click. It’s very easy to use.”

> “App Control’s ability to do reputation-based approvals and publisher-based approvals are really helpful for managing the system. Obviously, it would be very difficult to try to go out and whitelist every individual hash that’s out there, but there are definitely some tools and features built into the product that help make it easy to manage for us. It wouldn’t be feasible without those features to actually get to high enforcement application whitelisting.”
>
> INFORMATION SECURITY MANAGER, FINANCIAL SERVICES/BANKING

> "Actually, when I got my hands on it, I have to say it wasn't very hard to learn. This is pretty easy to use because since it's a GUI, it's really just point and click. It's very easy to use. And that's one of the reasons why we want to fight to keep it. Someone wanted us to look at a competing product and comparing this to the competing product was like, 'Wait a minute, App Control is way easier to use,' because all we have to do is point and click. The competing product required using PowerShell, Scripts, and SCCM [and it] was like, 'No, App Control is way easier.'"
>
> **CYBERSECURITY ANALYST, GOVERNMENT**

# Analysis Of Costs

Quantified cost data as applied to the composite

| Total Costs | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Ref.** | **Cost** | **Initial** | **Year 1** | **Year 2** | **Year 3** | **Total** | **Present Value** |
| Dtr | App Control license fees | $0 | $94,248 | $94,248 | $94,248 | $282,744 | $234,381 |
| Etr | Carbon Black professional services fees | $273,000 | $27,300 | $0 | $0 | $300,300 | $297,818 |
| | Total costs (risk-adjusted) | $273,000 | $121,548 | $94,248 | $94,248 | $583,044 | $532,199 |

### APP CONTROL LICENSE FEES

**Modeling and assumptions.** The composite organization pays Carbon Black a risk-adjusted total of $234,381 over three years for service and desktop license fees.

**Risks.** The value of this cost can vary across organizations due to:

- Whether or not the organization receives preferred pricing if it is a desirable tier-one client.
- Changes in pricing as the organization grows and requires additional functionality.

**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 $234,000.

| App Control License Fees | | | | | | |
|---|---|---|---|---|---|---|
| **Ref.** | **Metric** | **Source** | **Initial** | **Year 1** | **Year 2** | **Year 3** |
| D1 | Average number of endpoints for composite | A1 | | 11,000 | 11,000 | 11,000 |
| D2 | Servers as percentage of endpoints (percent) | Interviews | | 0.5% | 0.5% | 0.5% |
| D3 | Number of servers | D1*D2 | | 55 | 55 | 55 |
| D4 | Total server license fees | Composite | | $2,200 | $2,200 | $2,200 |
| D5 | Desktops as percentage of endpoints (percent) | Interviews | | 99.5% | 99.5% | 99.5% |
| D6 | Number of desktops | D1*D5 | | 10,945 | 10,945 | 10,945 |
| D7 | Total desktop license fees | Composite | | $87,560 | $87,560 | $87,560 |
| Dt | App Control license fees | D4+D7 | | $89,760 | $89,760 | $89,760 |
| | Risk adjustment | ↑5% | | | | |
| Dtr | App Control license fees (risk-adjusted) | | $0 | $94,248 | $94,248 | $94,248 |
| | **Three-year total: $282,744** | | | **Three-year present value: $234,381** | | |

### CARBON BLACK PROFESSIONAL SERVICES FEES

**Modeling and assumptions.** The composite organization incurred initial professional services fees to deploy App Control amounting to $260,000 initially and $26,000 in Year 1. After the limited costs in Year 1, no configuration fees are required in Years 2 and 3 if the scope of deployment does not change.

**Risks**. The value of this cost can vary across organizations due to:

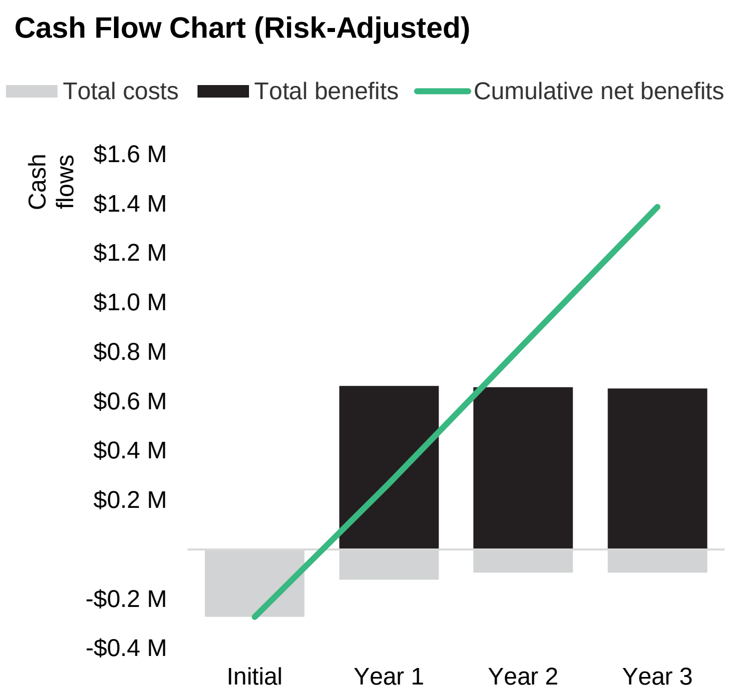
- The average fully burdened annual salaries and hourly rates of the FTEs who configure App Control at the organization.
- The availability of skilled FTEs required to configure App Control.

**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 $298,000.

| Carbon Black Professional Services Fees | | | | | | |
|---|---|---|---|---|---|---|
| **Ref.** | **Metric** | **Source** | **Initial** | **Year 1** | **Year 2** | **Year 3** |
| E1 | Carbon Black professional services fees | Composite | $260,000 | $26,000 | $0 | $0 |
| Et | Carbon Black professional services fees | E1 | $260,000 | $26,000 | $0 | $0 |
| | Risk adjustment | ↑5% | | | | |
| Etr | Carbon Black professional services fees (risk-adjusted) | | $273,000 | $27,300 | $0 | $0 |
| | **Three-year total: $300,300** | | | **Three-year present value: $297,818** | | |

# Financial Summary

## Consolidated Three-Year, Risk-Adjusted Metrics




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 | ($273,000) | ($121,548) | ($94,248) | ($94,248) | ($583,044) | ($532,199) |
| Total benefits | $0 | $661,733 | $656,546 | $651,877 | $1,970,155 | $1,633,940 |
| Net benefits | ($273,000) | $540,185 | $562,298 | $557,629 | $1,387,111 | $1,101,741 |
| ROI | | | | | | 207% |
| Payback | | | | | | 7.0 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."

### 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.

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

## APPENDIX B: ENDNOTES

[1] 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.