A Forrester Total Economic Impact™
Study Commissioned By Kaspersky
January 2020

The Total Economic Impact™ Of Kaspersky Security Solutions

Business Benefits And Cost Savings Enabled By Kaspersky Endpoint And Hybrid Cloud Security Solutions

FORRESTER®

Table Of Contents

Project Directors:
Richard Cavallaro
Julia Fadzeyeva

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®

Benefits And Cost Savings

Increased business uptime from reduction of endpoint breaches:
Nearly $1 million

FTE productivity savings from centralized management:
Over $800,000

Reduced likelihood of a major security breach:
Over $800,000

Executive Summary

Forrester's 2019 Global Business Technographics® Infrastructure survey indicates that security leaders are turning their attention to and adopting endpoint security suites, which consolidate multiple capabilities of endpoint threat prevention with detection and remediation capabilities. Fifty-six percent of those surveyed technology decision makers are either implementing or planning to implement one of these suites within their organization in the next 12 months.[1] Whether mandated by industry regulation or best practice, nearly all firms have some sort of antimalware solution. Antimalware, when used alone, has proven itself ineffective at stopping more sophisticated attacks, which are quickly becoming the norm for many organizations that don't invest in malicious behavior protection. Increasing security and IT complexity has caused most buyers to only consider new solutions that integrate threat prevention and detection. This is all in an effort to combat increasingly advanced security risks while dealing with internal tool friction.[2]

Kaspersky provides an integrated solution that increases the effectiveness of its customers' physical, virtual, and public cloud workload protection, improving overall security posture, visibility, and control, while providing a flexible management console which reduces the management burden on staff by consolidating multiple security capabilities within a single pane of glass. Kaspersky commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential ROI enterprises may realize by deploying Kaspersky's Endpoint Security solution, which in 2019 includes:

- Kaspersky Endpoint Security for Business
- Kaspersky Hybrid Cloud Security
- Kaspersky Endpoint Detection and Response

The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of the Kaspersky Endpoint Security solution on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed customers with years of experience using Kaspersky Endpoint Security.

Prior to using Kaspersky Endpoint Security, customers experienced frequent security breaches and vulnerabilities at the endpoint, which resulted in downtime for users and revenue-generating operations. Centralized solution management and effective threat hunting was difficult for IT and security teams as a result of their organizations' disparate collection of endpoint security solutions.

After deploying Kaspersky's Endpoint Security solution, organizations experienced fewer security breaches at their endpoints, resulting in more uptime for their users and business operations. Kaspersky's centralized management console simplified management of the organizations' endpoint security tools, freeing up valuable personnel hours for other IT or security tasks. Overall, interviewees described a much more robust security posture as a result of their Kaspersky investment, which they felt prepared them for the threats of today and tomorrow.

FORRESTER®

ROI
441%

Benefits PV
$2.8 million

NPV
$2.3 million

Payback
<12 months

Key Findings

Quantified benefits. The following risk-adjusted present value (PV) quantified benefits are representative of those experienced by the companies interviewed:

- **Reduced downtime and business disruption from improved endpoint protection of nearly $1.0 million.** Interviewees described and quantified the revenue impact of improved uptime at the endpoint from fewer instances of disruption.
- **Avoided cost to reimage endpoints of over $40,000.** By improving security at each endpoint, interviewees also noted that fewer security-related incidents saved IT productivity by reducing the need to reimage these endpoints.
- **Improved IT and security productivity from centralized management of over $800,000.** The centralized management console, which allows IT and security teams to manage all Kaspersky Endpoint Security solutions through a single pane of glass, was cited as a significant benefit by interviewees. IT personnel could more rapidly manage updates and endpoints, while the security operations center (SOC) could more efficiently hunt for and remediate threats. Facilitated management of multiple security solutions through the centralized management console drove productivity savings for these organizations.
- **Reduced chance of a major security breach of over $800,000.** By moving to the Kaspersky Endpoint Security solution, most notably Kaspersky Endpoint Detection and Response, each of the interviewed organizations described a major uplift to their overall security posture, reducing the chance of a "major" security breach which can do damage in the form of brand reputation, stock price, and cost of remediation efforts.
- **Consolidation and elimination of previous solution(s) of over $200,000.** Interviewees described to Forrester the cost savings associated with moving to Kaspersky for each of their endpoint security solution requirements (endpoint, virtualization, endpoint detection and response). By moving to Kaspersky, organizations saved on the license fees and inefficiencies associated with sourcing their solutions from multiple vendors.

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

- **Reduced performance burden on endpoint machines and virtualized servers.** Interviewees collectively described Kaspersky's agent for endpoints, virtual machines (VMs), and cloud-hosted servers as lightweight, with minimal performance impact compared with the previous solutions.
- **Superior support.** Support from the Kaspersky team was repeatedly cited by interviewees as a major benefit over the previous solution. An interviewee told Forrester, "Any time we've had to engage support, it's been a couple of quick emails back and forth and resolution the same day, it's been really simple to do."
- **End user productivity improvements.** End users are less likely to experience productivity impediments from malware, ransomware, phishing attacks, or other cyberthreats.

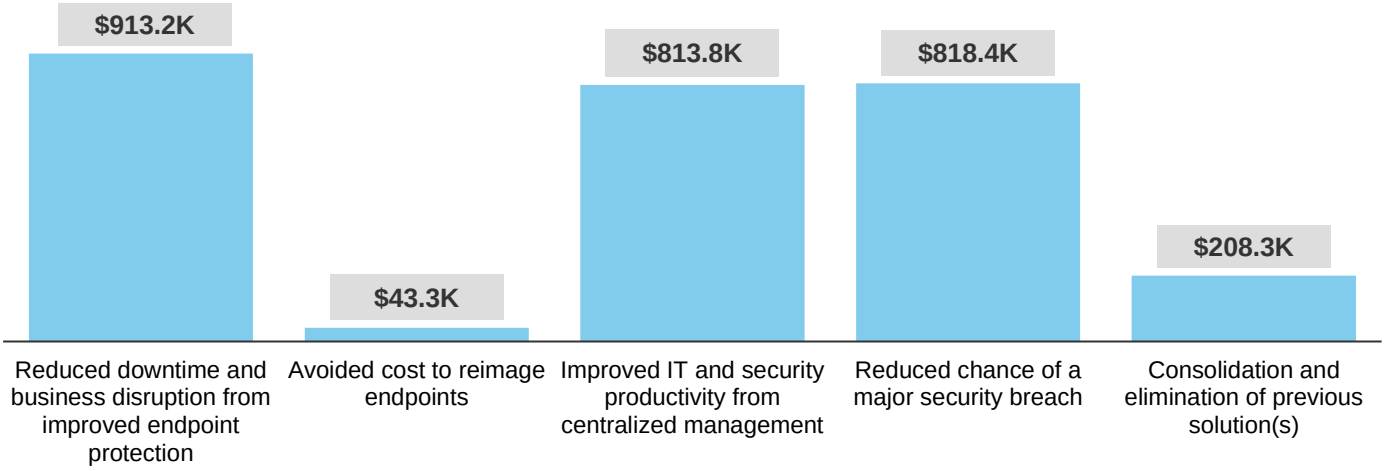
- **Improved user relationship with IT and security.** One interviewed customer told Forrester: “Our team’s [IT] relationship has improved with our users since we brought Kaspersky on board, since the time we’ve freed up from managing multiple obtrusive security solutions allows us more facetime with our users. We’ve also become more efficient with reimages when necessary.”

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

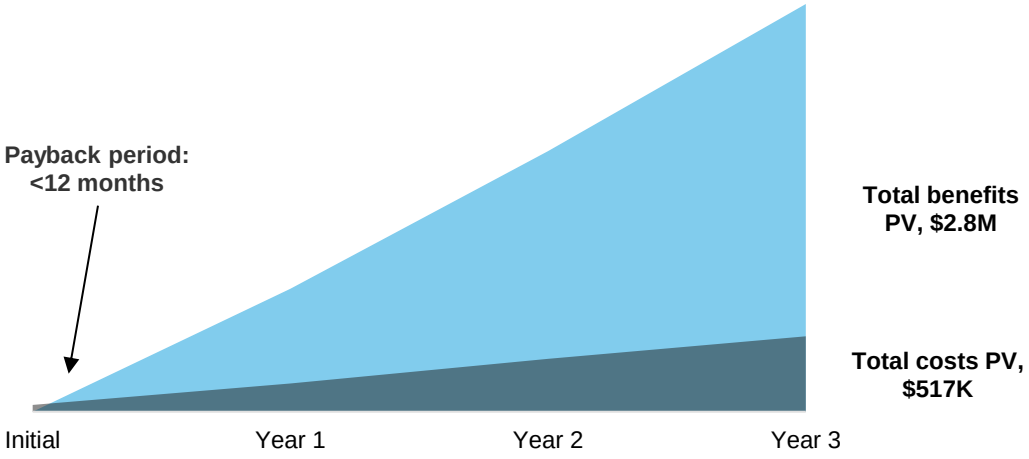
- **License fees paid to Kaspersky.** Interviewees paid license fees to Kaspersky based on the specific endpoint security solutions deployed.
- **Implementation and ongoing management.** Each organization dedicated FTE labor hours to the implementation effort around Kaspersky Endpoint Security solution and continues to dedicate personnel to management. These labor hours include training for the IT and security team(s).

Forrester’s interviews with existing customers and subsequent financial analysis found that an organization based on these interviewed organizations experienced benefits of $2.8 million over three years versus costs of over $500,000, adding up to a net present value (NPV) of $2.3 million and an ROI of 441%.

Benefits (Three-Year)



Financial Summary



FORRESTER®

TEI Framework And Methodology

From the information provided in the interviews, Forrester has constructed a Total Economic Impact™ (TEI) framework for those organizations considering implementing Kaspersky Endpoint Security.

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 Kaspersky's Endpoint Security solution can have on an organization:

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

DUE DILIGENCE
Interviewed Kaspersky stakeholders and Forrester analysts to gather data relative to Endpoint Security.

CUSTOMER INTERVIEWS
Interviewed six organizations using Endpoint Security to obtain data with respect to costs, benefits, and risks.

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

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

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

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by Kaspersky and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the report to determine the appropriateness of an investment in Kaspersky's Endpoint Security solution.

Kaspersky 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.

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

The Kaspersky Endpoint Security Customer Journey

BEFORE AND AFTER THE KASPERSKY ENDPOINT SECURITY INVESTMENT

Interviewed Organizations

For this study, Forrester conducted six interviews with Kaspersky Endpoint Security customers. Interviewed customers include the following:

INDUSTRY	REGION	INTERVIEWEE	KASPERSKY ENDPOINT SOLUTIONS DEPLOYED
Financial services	Global	Head of IT	One Kaspersky Endpoint solution
Banking	Russia	Head of AV solutions group	Two Kaspersky Endpoint solutions
Retail	New Zealand	Infrastructure network operations manager	One Kaspersky Endpoint solution
Financial services	United States	System administrator	Two Kaspersky Endpoint solutions
Telecommunication	Middle East	Director IT security	Three Kaspersky Endpoint solutions
Food processing	Global	IT security manager	Two Kaspersky Endpoint solutions

Key Challenges

- **Threats of increasing sophistication were more difficult to detect for current endpoint solutions.** Most all interviewees discussed the increasing sophistication in attack detection threatening their organizations. One interviewee summarized the challenge to Forrester, "For a number of years, our previous solution was not updating fast enough to protect against the latest threats." This left interviewed organizations exposed.
- **Security incidents were increasing in frequency.** Interviewees noted a steady increase in security events at the endpoint, which led to downtime. These events which were not detected or prevented by the previous endpoint security solutions included ransomware attacks, phishing scams, and malware. Downtime affected the organizations in multiple ways, including lost user productivity, lost revenue from operational disruption, and lost IT productivity for supporting and remediating these security incidents.
- **Technical issues were abundant in endpoint security software.** Poor security solution performance at the endpoint was cited as a key driver toward another endpoint security solution. One organization noted that its end users would experience frequent system or application crashes as a result of cumbersome endpoint security clients: "The email client would crash for our users at least once a week. Performance was poor across the board, despite our requests for support. This was very unsatisfactory."

> "Performance [on the legacy endpoint security solution] was poor across the board, despite our requests for support. This was very unsatisfactory."
>
> *Director IT security, telecommunication*

FORRESTER®

- **Virtualized desktops and servers often went unprotected.** Due to the technical and capacity limitations of the interviewed organizations, virtualized servers and endpoints frequently had very rudimentary endpoint protection, if any, which posed additional risk to the organizations.
- **Support was subpar.** Limited support from the previous endpoint security vendors was a recurring trend in Forrester's interviews. The Middle East-based interviewee noted: "Our previous vendor's support was quite unsatisfactory, since they didn't have a presence in our region. On the other hand, Kaspersky extends support to our region tremendously." Another interview told Forrester: "Our previous solution was not very intuitive, so we needed quite a bit of support. Unfortunately, the support was poor."

Solution Requirements

The interviewed organizations searched for a solution that:

- **Could be deployed with little to no disruption to users.** Interviewed customers were sensitive to the disruption end users would experience that deploying a new endpoint security solution could bring. The new solution needed to be deployed with little to know end user action or knowledge.
- **Provided responsive customer support.** Poor support was frequently cited as a driver to investigate new endpoint security vendors. Interviewees noted an emphasis on moving to a vendor that can provide timely support in multiple geographies.

> "Our Kaspersky solution is catching threats that our previous endpoint security solution was missing. I have no doubt that if we stayed on that solution we would have been hit by another form of an attack in the near future."
>
> *Infrastructure network operations manager, retail*

Key Results

The interviews revealed that key results from the Kaspersky's Endpoint Security solution investment include:

- **Significantly fewer security-related incidents.** Interviewees collectively cited a great reduction in security events such as malware, ransomware, and phishing scams after moving to Kaspersky's Endpoint Security. The retail customer noted: "Our Kaspersky solution is catching threats that our previous endpoint security solution was missing. I have no doubt that if we stayed on that solution we would have been hit by another form of an attack in the near future."
- **Less lost revenue from extended downtime.** Multiple interviewees noted that the Kaspersky solutions prevented security incidents at their critical, revenue-generating endpoints. Before moving to Kaspersky, interviewees described and quantified to Forrester the serious revenue impact of this downtime.
- **Facilitated solution management.** The centralized console which allows IT and security teams to manage their Kaspersky security agents across the entire infrastructure from one application allowed IT and security operations teams to improve productivity for their respective tasks.
- **Better security posture from improved visibility into threats.** Organizations felt better about their overall security posture on the Kaspersky Endpoint Security solution, as compared with their previous products. The retail interviewee summarized, "For us, some of the best value we get is the peace of mind that we're better protected against some of the current and future threats."

> "For us, some of the best value we get is the peace of mind that we're better protected against some of the current and future threats."
>
> *Infrastructure network operations manager, retail*

› **Improved support.** All of the organizations interviewed by Forrester noted an improvement in their endpoint security support after moving to Kaspersky. One organization noted, "Kaspersky won our RFP process on its support structure." Another added: "In addition to our 24x7 phone and email support, Kaspersky is coming out for policy configuration checks and additional support for us. And the operation of the solution is so stable, we don't need to invest in additional support."

"In addition to our 24x7 phone and email support, Kaspersky is coming out for policy configuration checks and additional support for us."

Director IT security, telecommunication

Composite Organization

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

Description of composite. The composite organization is a global, 5,000 employee, $1 billion organization which operates 200 locations that depend on the uptime of its endpoints for continued operations. Before deploying Kaspersky's Endpoint Security solution, the organization relied on separate endpoint security solutions for its business users and its virtualized resources. The SOC relied on endpoint detection and response capabilities from another vendor. Across all geographies of operation, the organization receives inconsistent performance from and support for its endpoint security solutions. The business is growing in both revenue and employee count and plans to scale its Kaspersky deployment accordingly.

Deployment characteristics. The organization has 5,000 endpoints (machines and VMs), 500 servers, and multiple public cloud instances which require protection. At the location-level, uptime of its main endpoints are critical for continued operations, as a security incident resulting in downtime translates to a loss of revenue which the organization can calculate by the location. The organization also has 500 servers. In Year 1 of the analysis, the organization deploys two components: Kaspersky Endpoint Security for Business (KESB) for its users' devices and physical servers and Kaspersky Hybrid Cloud Security (KHCS) for its virtualized resources and public cloud instances. In Year 2 of the analysis, the organization adds Kaspersky Endpoint Detection and Response (KEDR) to assist its SOC with advanced threats detection and automated response.

Key assumptions

- 5,000 total endpoints (machines and VMs)
- 500 servers
- 200 physical locations
- All components of the solution deployed

FORRESTER®

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	Reduced downtime and business disruption from improved endpoint protection	$367,200	$367,200	$367,200	$1,101,600	$913,172
Btr	Avoided cost to reimage endpoints	$17,401	$17,401	$17,401	$52,203	$43,274
Ctr	Improved IT and security productivity from centralized management	$327,250	$327,250	$327,250	$981,750	$813,822
Dtr	Reduced chance of a major security breach	$156,800	$333,670	$532,538	$1,023,008	$818,410
Etr	Consolidation and elimination of previous solution(s)	$59,500	$97,750	$97,750	$255,000	$208,317
	Total benefits (risk-adjusted)	$928,151	$1,143,271	$1,342,139	$3,413,561	$2,796,995

The table above shows the total of all benefits across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total benefits to be a PV of nearly $2.8 million.

Reduced Downtime And Business Disruption From Improved Endpoint Protection

Before moving to the Kaspersky Security solution, the interviewed organizations experienced extended downtime at their endpoints which affected not only user productivity, but also revenue-generating operations as well. The downtime was mainly a result of attacks and infections, which were not detected by the previously deployed endpoint security solutions, forcing the endpoint to be taken offline for remediation or reimaging. However, AV misbehavior or configuration problems were also cited by interviewees as reasons for downtime.

- A financial services interviewee noted that on its previous endpoint security solution, downtime from several ransomware attacks completely halted operations at its customer-facing locations. Until resolved, the organization was not able to conduct business with customers and therefore generate revenue: “At the time we didn’t have an online presence, so we couldn’t work with any customers during these events. So, this is devastating to our revenue stream.”
- Another organization described the impact that cyberattacks had on downtime of its network of payment machines, which allow customers to make credit card payments and order services: “Our kiosks were frequently infected with the old endpoint solution. When this happened, our only option was to take them offline and reimage them since we would expose our customers to these kiosks. The revenue impact was big though, since those kiosks bring us over $30 million per year.”

By moving to Kaspersky’s Security solution, interviewees estimated that security breach-related downtime was significantly reduced and nearly eliminated from improved protection at the endpoint.

For the financial model, Forrester assumes that:

- The composite organization operates 200 physical locations, which bring in an average revenue of $240 per hour.

The composite organization realizes a **50% reduction** of revenue impacting downtime on Kaspersky.

FORRESTER®

- Each of these locations is offline for 90 minutes per month due to security breaches, endpoint security solution misbehavior, or solution reconfiguration.
- By moving to Kaspersky, Forrester conservatively estimates based on interviewee responses that 50% of this downtime is avoided. Note that some interviewees cited a higher reduction.

This benefit will vary based on:

- An organization's industry, structure, and means of revenue generation.
- The scope and complexity of an organization's current endpoint security solution deployment.
- The skill and capacity of an organization's IT and/or security operations team(s).

To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $913,172.

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

Reduced Downtime And Business Disruption From Improved Endpoint Protection: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
A1	Location revenue per hour		$240	$240	$240
A2	Hours of downtime per location per year	1.5 hours per month *12 months	18	18	18
A3	Hours of downtime after implementing Kaspersky	(45 minutes per month *12 months)/60 minutes	9	9	9
A4	Downtime hours avoided per location per year	A2-A3	9	9	9
A5	Number of locations		200	200	200
At	Reduced downtime and business disruption from improved endpoint protection	A1*A4*A5	$432,000	$432,000	$432,000
	Risk adjustment	↓15%			

Avoided Cost To Reimage Endpoints

For serious security breaches at the endpoint, organizations told Forrester that their IT team would need to take the impacted machine offline for reimaging. This required a time commitment from the IT team, reducing its productivity on other value-adding tasks for the organization. Interviewees told Forrester that KESB improved overall endpoint protection, reducing serious security breaches and therefore the need to reimage machines.

For the composite organization, Forrester assumes that:

- Twenty (20) endpoints are reimaged per month with the previous endpoint security solution deployed.
- Nineteen (19) of these monthly reimaging instances are avoided once Kaspersky is deployed. Some interviewees cited a complete elimination, but Forrester assumes a 95% reduction for the model.
- It takes 8 hours to reimage a machine, IT personnel are active for 20% of that time.
- The hourly rate for an IT FTE is $53.

This benefit will vary based on:

- The scope and complexity of an organization's current endpoint security solution deployment.
- The skill and capacity of an organization's IT and/or security operations team(s).

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $43,274.

Avoided Cost To Reimage Endpoints: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
B1	Endpoints reimaged per month with prior endpoint security solution		20	20	20
B2	Endpoints reimaged per month with Kaspersky		1	1	1
B3	Reduction in endpoints reimaged per month with Kaspersky	B1-B2	19	19	19
B4	Time to reimage per machine (hours)		8	8	8
B5	IT time active during reimage		20%	20%	20%
B6	Average hourly rate for IT (rounded)	$110,000/2,080	$53	$53	$53
Bt	Avoided cost to reimage endpoints	B3*B4*B5*B6* 12 months	$19,334	$19,334	$19,334
	Risk adjustment	↓10%			
Btr	Avoided cost to reimage endpoints (risk-adjusted)		$17,401	$17,401	$17,401

Improved IT And Security Productivity Due To Centralized Management

Both IT and security personnel cited efficient management of endpoint security solutions as a major challenge for its previous endpoint security deployments. Management activities include updates, scans, and remediation efforts, which did not require reimaging. For security operations personnel, poorly filtered threat intelligence information lengthened mean investigation time, leaving less time for limited security staff to investigate threats.

- The laborious back and forth between IT and end users to manage scans, updates, and remediation for the previous endpoint security solutions was discussed by multiple interviewees, "It would take quite a bit of time and effort because we would need to be in constant communication with our users at potentially compromised locations to do simple scans."
- Another interviewee told Forrester that with its previous endpoint security solution, they needed to dedicate multiple IT FTEs to full-time management of the solution.

After moving to Kaspersky, the interviewed organizations' IT and security teams were able to improve their productivity significantly:

Over 80% reduction in FTE hours required to manage endpoint security solutions

FORRESTER®

- One interviewee estimated that they reduced the burden on its IT team by over three FTEs, compared to the previous solution, freeing up personnel to focus on other tasks within IT. They added: "This was when we only had around 7,000 endpoints. Now we have 20,000 endpoints, and we only need one FTE managing Kaspersky part-time because of the centralized management console."
- Another organization noted that the centralized management console combined with KEDR increased the productivity of its security operations personnel tasked with threat investigation, as well.

For the financial model, Forrester assumes that:

- Four (4) FTEs had previously been assigned to manage the organization's endpoint security deployment.
- After deploying Kaspersky, one FTE manages endpoint security part time.
- The average annual salary for an IT or security FTE is $110,000.

This benefit will vary based on:

- The scope and complexity of an organization's current endpoint security solution deployment.
- The scope of an IT or security team's responsibilities for endpoint security solution management.
- The skill and capacity of an organization's IT and/or security operations team(s).

To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $813,822.

Improved IT And Security Productivity From Centralized Management: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
C1	FTEs assigned to manage previous security solutions		4	4	4
C2	FTEs assigned to manage Kaspersky endpoint security solutions	1 FTE, 50% time on task	0.5	0.5	0.5
C3	FTE time saved	C1-C2	3.5	3.5	3.5
C4	Average annual salary		$110,000	$110,000	$110,000
Ct	Improved IT and security productivity from centralized management	C3*C4	$385,000	$385,000	$385,000
	Risk adjustment	↓15%			
Ctr	Improved IT and security productivity from centralized management (risk-adjusted)		$327,250	$327,250	$327,250

Reduced Chance Of A Major Security Breach

Major security breaches, which can negatively impact an organization in the form of bad publicity, stock price losses, and brand damage, were a significant concern for each of the organizations that Forrester interviewed.

Before deploying KEDR, some interviewees experienced poor visibility into threats that may represent a significant threat:

- The food processing interviewee cited a poor endpoint detection and response (EDR) capability in addition to limited SOC personnel as a great risk to its organization: "With all of the other security-related management our team needs time for on a daily basis, we didn't have the capacity we needed to go through our AV logs to identify threats that might affect our organization."

By deploying KEDR, interviewees gained a greater visibility, into threats which were previously undetected, and therefore a more robust security posture. Some interviewees were able to analyze the threat detection feeds with their SOC personnel, while some organizations could easily pass the output from KEDR to their managed security service provider (MSSP). Each interviewed organization estimated a reduced chance of a major security breach as described above as a result of more effective visibility into threats enabled by KEDR.

- The food processing interviewee noted after deploying KEDR: "We have more visibility and are more protected against zero-day threats and emerging threats. We are confident in the visibility we have."
- The telecommunication company described the new threat visibility enabled by its vendor: "Kaspersky Endpoint Detection and Response (KEDR) is giving us new visibility into real incidents which allows our SOC staff to better prioritize their time. It allows them to easily take a deep dive on any potentially malicious activity at our endpoints, all while delivering great reporting through the centralized dashboard."

For the financial model, Forrester assumes that:

- The composite organization achieves a 5% reduction in Year 1 resulting from the automated EDR capabilities within KESB. After KEDR is deployed starting in Year 2, the organization achieves a 10% reduction.
- By Year 3, the improved visibility into previously unknown threats improves the organization's overall security posture by 15%, a conservative estimate based on the interviews.
- The average cost of a data breach is $3,920,000 per year according to the Ponemon institute.[3] This number increases at 6.4% per year for each subsequent year of the analysis.

This benefit will vary based on:

- The visibility into threats and EDR capabilities currently deployed by an organization.
- The skill and capacity of an organization's IT and/or security operations team(s).

To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $818,410.

15% reduction in the chance of a major security breach by Year 3

"Kaspersky Endpoint Detection and Response (KEDR) is giving us new visibility into real incidents which allows our SOC staff to better prioritize their time. It allows them to easily take a deep dive on any potentially malicious activity at our endpoints, all while delivering great reporting through the centralized dashboard.

Director IT security, telecommunication

FORRESTER®

Reduced Chance Of A Major Security Breach: Calculation Table					
REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
D1	Average cost of a data breach	Increasing at 6.4% per year	$3,920,000	$4,170,880	$4,437,816
D2	Reduced chance of a major breach with Kaspersky EDR		5%	10%	15%
Dt	Reduced chance of a major security breach	D1*D2	$196,000	$417,088	$665,672
	Risk adjustment	↓20%			
Dtr	Reduced chance of a major security breach (risk-adjusted)		$156,800	$333,670	$532,538

Consolidation And Elimination Of Previous Solution(s)

By moving to Kaspersky, interviewees retired their previous endpoint security solutions and saved on the license fees they were paying while taking advantage of the efficiency and cost savings by bundling with a single vendor.

- One interviewee described its experience working with Kaspersky to replace its previous endpoint security solutions: "It was easy to bring everything in. Pricing was very straightforward and simple. There were no incremental fees, and everything was built in. It was great dealing with one bundled contract."

For the financial model, Forrester assumes that:

- The composite organization was paying $70,000 per year for protection across all its endpoints and virtualized resources.
- They were paying $45,000 to a separate vendor for endpoint detection and response capabilities, which are avoided starting in Year 2 of the model once KEDR is deployed.
- The price assumptions for the composite organization are based on interviewee responses and may include discounting from the previous vendor's list price.

This benefit will vary based on:

- The current vendor(s) and specific pricing an organization is currently paying for its endpoint security solutions.
- Factors such as contract duration, which may not allow an organization to retire its previous vendors immediately.

To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $208,317.

> "It was easy to bring everything in. Pricing was very straightforward and simple. There were no incremental fees, and everything was built in. It was great dealing with one bundled contract."
>
> *System administrator, financial services*

FORRESTER®

Consolidation And Elimination Of Previous Solution(s): Calculation Table					
REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
E1	Endpoint security solution		$70,000	$70,000	$70,000
E2	EDR solution			$45,000	$45,000
Et	Consolidation and elimination of previous solution(s)	E1+E2	$70,000	$115,000	$115,000
	Risk adjustment	↓15%			
Etr	Consolidation and elimination of previous solution(s) (risk-adjusted)		$59,500	$97,750	$97,750

Unquantified Benefits

Reduced performance burden on endpoint machines and virtualized servers. Interviewees collectively described Kaspersky's agent for endpoint, VMs, and cloud-hosted servers as lightweight, with minimal performance impact compared with the previous solutions.

- One interviewee told Forrester about the minimal impact the Kaspersky Endpoint Security solution has on the end user: "Scans and any detections all run much faster on the Kaspersky solution than they did on our old software, which would consume a noticeable amount of each machine's resources. Now it's virtually undetectable for the end user."
- The financial services organization noted that its previous solutions used to secure its virtual desktops and servers would use up nearly 20% to 30% of their CPU and memory utilization. They described their improvements with KHCS: "Now we have a small, lightweight application that the system barely notices, and a back-end VM brunt the load of it. It's been a savior for us from a resource perspective."

Superior support. Support from the Kaspersky team was repeatedly cited by interviewees as a major benefit over the previous solution.

- An interviewee told Forrester: "Any time we've had to engage support, it's been a couple of quick emails back and forth and resolution on the same day, it's been really simple to do."
- Another organization noted: "In addition to our 24x7 phone and email support, Kaspersky is coming out for policy configuration checks and additional support for us. Yet the solution is so stable, we don't need to invest in additional support."

End user productivity improvements. End users are less likely to experience productivity impediments from malware, ransomware, phishing attacks, or other cyberthreats. This may yield benefits to organizations in the form of improved user productivity and reclaimed working hours which were historically lost to security breach-related downtime.

Improved user relationship with IT and security. One interviewed customer told Forrester: "Our team's [IT] relationship has improved with our users since we brought Kaspersky on board, since the time we've freed up from managing multiple obtrusive security solutions allows us more facetime with our users. We've also become more efficient with reimages when necessary."

"Any time we've had to engage support, it's been a couple of quick emails back and forth and resolution on the same day, it's been really simple to do."

System administrator, financial services

FORRESTER®

Flexibility

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

- **Reduced costs for virtualization resources.** Interviewees noted that the lightweight KHCS required significantly fewer virtual resources (CPU, memory, etc.) to operate than their previous solution on virtualized desktops and servers. One executive told Forrester, "The virtual resource cost to protect our VMs was negligible for the Kaspersky solution, when compared with some of the other solutions we evaluated." Over time, this may yield savings on cloud resources for organizations protecting their virtualized environment with KHCS.
- **Expansion to additional Kaspersky Endpoint Security solution.** Organizations that have not yet expanded to the full suite of Kaspersky Endpoint Security solution beyond core components, can realize the benefits and efficiencies, which the interviewed organizations and composite organization from this study have experienced.

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

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

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	License fees paid to Kaspersky	$0	$95,334	$139,334	$139,334	$374,001	$306,502
Gtr	Implementation and ongoing management	$46,750	$66,000	$66,000	$66,000	$244,750	$210,882
	Total costs (risk-adjusted)	$46,750	$161,334	$205,334	$205,334	$618,751	$517,384

License Fees Paid To Kaspersky

Each interviewee, depending on the Kaspersky Endpoint Security solution deployed, paid a bundled license fee to Kaspersky for its endpoint security deployment. This license fee includes support costs comprising of 24x7 email and phone support and quarterly health checks.

For the financial model, Forrester assumes that:

- The composite organization deploys both of the following solutions in Year 1 of the analysis: 1) KESB to protect its physical endpoints and 2) KHCS to protect its virtualized resources.
- The organization adds the KEDR add-on in Year 2 of the model.
- The below pricing has been provided as an estimate by Kaspersky based on the characteristics of the composite organization.

This cost will vary based on:

- The specific Kaspersky Endpoint Security solution deployed.
- The scope of the deployment (number of endpoints, virtualized resources).

To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $306,502.

The table above shows the total of all costs across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total costs to be a PV of nearly $520,000.

Implementation risk is the risk that a proposed investment may deviate from the original or expected requirements, resulting in higher costs than anticipated. The greater the uncertainty, the wider the potential range of outcomes for cost estimates.

License Fees Paid To Kaspersky: Calculation Table

REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
F3	Bundled fee for KEDR, KESB, and KHCS			$86,667	$126,667	$126,667
Ft	License fees paid to Kaspersky			$86,667	$126,667	$126,667
	Risk adjustment	↑10%				
Ftr	License fees paid to Kaspersky (risk-adjusted)		$0	$95,334	$139,334	$139,334

Implementation And Ongoing Management

The organizations interviewed for the study described their experience implementing and managing their Kaspersky Endpoint Security solution to Forrester.

- All interviewees characterized the deployment process for their Kaspersky Endpoint Security solution deployment as straightforward, without any additional effort from IT.
- The interviewed organizations all noted a very minimal impact to end users during deployment.
- The interviewee from the retail organization noted: “As far as deployment was concerned, getting our Kaspersky solution up and running was the easy part. Getting rid of our old endpoint security solutions was the hardest part.”

For the financial model, Forrester assumes that:

- One FTE in IT manages the deployment for the composite organization with 100% of its working hours during the deployment period.
- The implementation takes a total of three months, which includes deploying KESB and KHCS across all endpoints and servers. This period also includes removal of the previous endpoint security solution(s).
- Once deployed, one FTE manages all of Kaspersky solutions part-time, as threat investigation overflow is outsourced to a MSSP.
- Training requirements are minimal, as the organization arranges a number of training sessions for security staff and some IT help desk personnel at the cost of $15,000 in personnel hours at initial deployment.
- Additional training at the cost of $5,000 in personnel hours is held in each of the subsequent years of the analysis to account for additional training and regular personnel attrition.

This cost will vary based on:

- The specific Kaspersky’s Endpoint Security solution deployed.
- The scope of the deployment (number of endpoints, virtualized resources).
- The skill and capacity of an organization’s IT and/or security operations team(s).

To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $210,882.

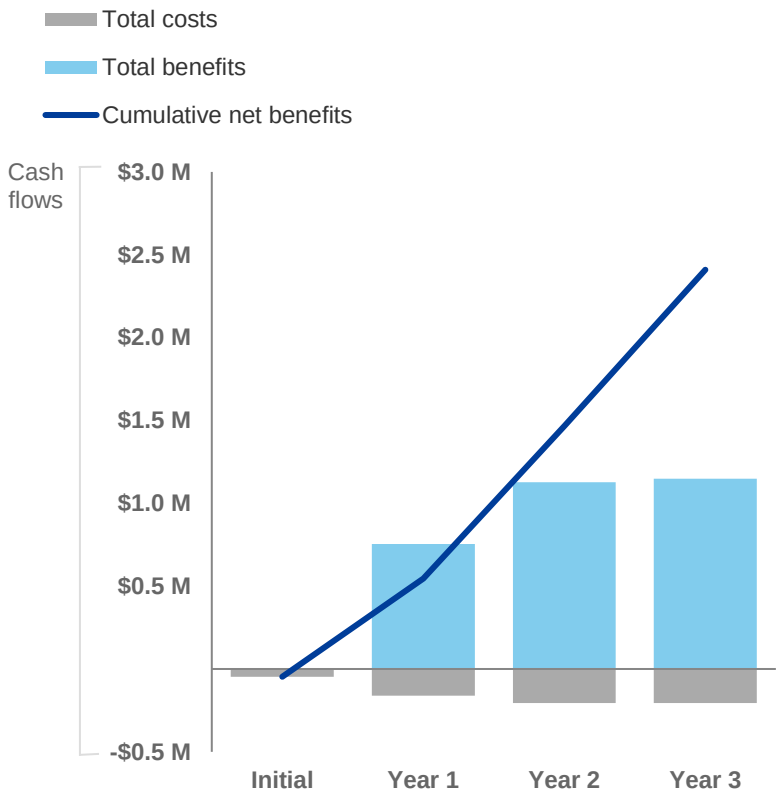
Three months
of total implementation and deployment time

Implementation And Ongoing Management: Calculation Table						
REF.	**METRIC**	**CALC.**	**INITIAL**	**YEAR 1**	**YEAR 2**	**YEAR 3**
G1	Initial implementation	$110,000 FTE annual salary* 3 months	$27,500			
G2	Ongoing management	1 FTE*50%		$55,000	$55,000	$55,000
G3	Training		$15,000	$5,000	$5,000	$5,000
Gt	Implementation and ongoing management	G1+G2+G3	$42,500	$60,000	$60,000	$60,000
	Risk adjustment	↑10%				
Gtr	Implementation and ongoing management (risk-adjusted)		$46,750	$66,000	$66,000	$66,000

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)

	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Total costs	($46,750)	($161,334)	($205,334)	($205,334)	($618,751)	($517,384)
Total benefits	$0	$928,151	$1,143,271	$1,342,139	$3,413,561	$2,796,995
Net benefits	($46,750)	$766,817	$937,938	$1,136,805	$2,794,810	$2,279,611
ROI						441%
Payback period						<12 months

FORRESTER®

Kaspersky Endpoint Security: Overview

The following information is provided by Kaspersky. Forrester has not validated any claims and does not endorse Kaspersky Endpoint Security or any of its offerings.

Solution Description

A single integrated solution, with EDR at its core, designed to secure organizations with finite IT security resources against advanced and targeted attacks.

Kaspersky EDR

Kaspersky EDR complements Kaspersky Endpoint Security for Business, delivering full visibility and the ability to apply root-cause analysis, for a complete understanding of the status of corporate defenses against advanced threats.

Kaspersky Endpoint Security for Business

Delivered from the cloud or on-premises, Kaspersky Endpoint Security for Business provides flexible security for mixed environments, incorporating a full stack of technologies to deliver automated threat defenses and systems hardening.

Kaspersky Hybrid Cloud Security

Kaspersky Hybrid Cloud Security provides multi-layered virtual and cloud workload protection to every part of the hybrid IT infrastructure, with no adverse impact on systems performance or user experience.
A single-pane-of-glass console delivers all-round visibility and control, while its patented hierarchical architecture reduces hardware resource usage by up to 30%.

Below Kaspersky provides some benefits customer enjoys by using our solution

Reducing your risk of falling victim to a targeted attack.

Endpoint Security delivers straightforward effective defenses against advanced threats targeting your organization, without stretching your resources. Our multi-layered approach, combining a full stack of powerful protection, detection and response technologies in one tightly integrated solution, leaves you armed against the most complex and sophisticated attacks, while actually making life easier for you and your IT Security Specialist.

Preventing employees from exposing themselves, and you, to an attack.

The granular controls we've built into Endpoint Security, complete with category-based whitelisting databases, make it easy to enforce policies dictating which applications and online resources your users get to access and when, and what devices they can plug into your system. Should your administrators choose to modify policy settings, 'Security Advisor' is on hand to point out any potential pitfalls. And, because IT professionals are only human, we automate those critical but tedious routine security tasks than might just get neglected or forgotten. We can even offer security awareness training for your users, just to make everyone's life easier and safer.

Maximizing the number of incidents processed, without increasing your manpower costs.

Yes, it can be done! Our new detection and response technologies mean that very large numbers of incidents can be dealt with fast and effectively, leaving your IT Security Specialist free to focus only on those that really require human input. The quality, as well as the quantity, of incidents dealt with rises, and your staff have more time, which can then be used applying our technologies against targeted attacks.

Accelerating your cloud security business.

Moving to our patented virtualization security technology can release up to 30% of virtualization resources, while securing your move to the cloud and ensuring you maintain full compliance with relevant standards. Integration with native virtualization and cloud platform APIs provides consistent visibility, automated deployment and auto-scaling. A single management console with unified policies for your on-premises and public cloud based workloads reduces your management burden while closing security gaps.

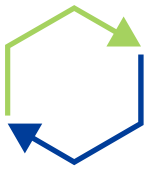
Appendix A: Total Economic Impact

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

Total Economic Impact Approach

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

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



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

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

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

Present value (PV)

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

Net present value (NPV)

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

Return on investment (ROI)

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

Discount rate

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

Payback period

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

Appendix B: Supplemental Material

"The State Of Endpoint Security, 2019," Forrester Research, Inc., January 22, 2019.

Appendix C: Endnotes

[1] Source: Forrester Analytics Global Business Technographics Infrastructure Survey, 2019.
[2] Source: "The State Of Endpoint Security, 2019," Forrester Research, Inc., January 22, 2019.
[3] Source: "Cost of a Data Breach Report," Ponemon Institute study, 2019.