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

The Total Economic Impact™ Of Kaspersky Fraud Prevention

Cost Savings And Business Benefits Enabled By Fraud Prevention

FORRESTER®

Table Of Contents

Project Director:
Julia Fadzeyeva

Project Contributor:
Sanitra Desai

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®

Investment Benefits

Cost savings from reducing fraud:
$3.4 million

Savings from reduction in customer service interactions:
$121,074

Savings from eliminating second tier authentication:
$17,571

Executive Summary

Modern consumers expect nothing less than being able to access their accounts and perform various transactions with businesses from the convenience of their devices. Lack of physical interaction poses new challenges to organizations that need to guarantee security and minimize fraud while keeping customer experience (CX) seamless.[1]

Kaspersky provides a fraud and authentication solution that helps its customers detect and prevent predominantly online fraud, investigate complex fraud schemes, improve user experience, and cut the costs of additional customer authentication. Kaspersky commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Kaspersky Fraud Prevention (KFP), which includes Advanced Authentication and Automated Fraud Analytics. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of KFP on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed one customer with more than two years of experience using KFP.

Prior to using KFP, the interviewed customer did not have a fraud prevention solution in the digital channel. Due to a spike in fraudulent activities seen at financial services companies, the interviewed organization was concerned about the possibility of fraud and its effect on customers, the organization's reputation, potential customer churn, and investigation and recovery expenses.

After implementing and actively using both Kaspersky Automated Fraud Analytics and Advanced Authentication, the organization reduced fraud and achieved a more frictionless CX.

Key Findings

Quantified benefits. The interviewed organization experienced the following risk-adjusted present value (PV) quantified benefits:

- **Reduced fraud losses, totaling $3.4 million over three years.** KFP allowed the interviewed organization to identify and prevent fraudulent activity in the online channel. As a result, the company reduced fraud losses stemming from labor, investigation and external recovery expenses, fines and legal fees, and fees or interest incurred during processing stages.
- **Savings in customer service interactions, totaling $121K over three years.** Using KFP's Advanced Authentication allowed the organization to build an "easy entrance" mechanism where customers could authenticate directly from their desktops with the same level of security as could be achieved from a call to the call center, foregoing the additional calls.
- **Savings from eliminating second-tier authentication for verified customers, totaling $17.6K over three years.** KFP eliminated the need for extra verification steps for most legitimate users, allowing the organization to make CX more seamless and minimize hurdles for customers to access their online accounts, while keeping fraud risks low.

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

FORRESTER®

ROI
168%

Benefits PV
$3.6 million

NPV
$2.2 million

Payback
<6 months

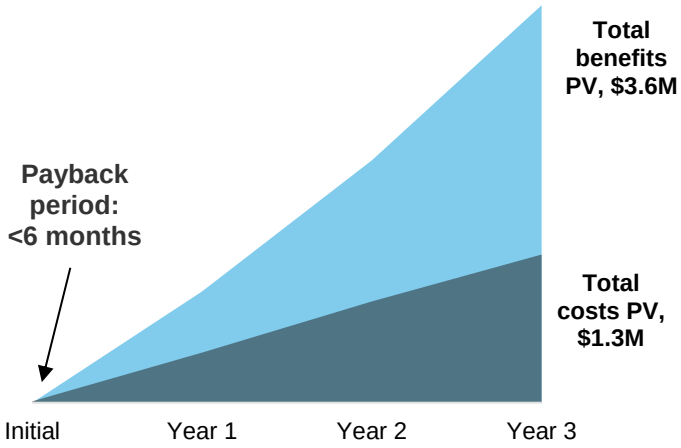
- **Improved CX.** More seamless access to user accounts and reduction in cases when users need to contact customer service have contributed to a more streamlined experience for users.
- **Stronger consumer trust.** For potential victims of fraudulent activity and subsequent financial losses, having the knowledge that fraudulent attempts are being prevented by the organization helps build trust and loyalty.
- **Identification of money laundering and fraudulent accounts.** The interviewed organization relies on KFP to detect money laundering schemes and accounts used by fraudsters, if any, within the organization. This helps the company to comply with industry regulations and discourage fraudulent activity from flourishing within the organization.
- **Additional expert assistance in identifying fraud and incidence response.** The organization benefits from Kaspersky's visibility into fraudulent activity happening across the industry. Once Kaspersky identifies a new type of fraud for any of its customers, Kaspersky adds monitoring for this behavior to KFP for all customers.

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

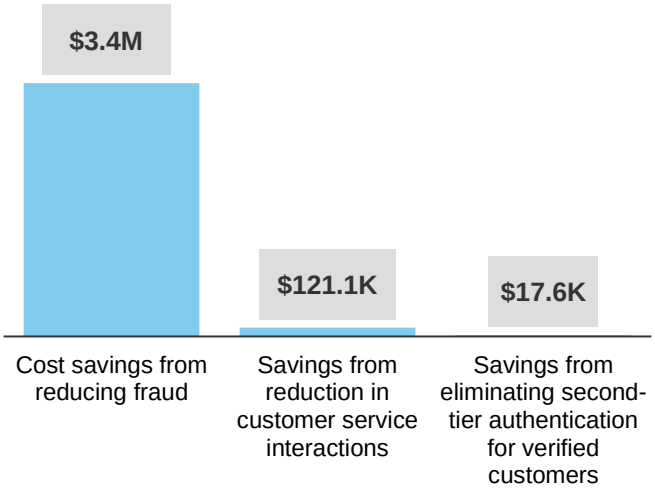
- **Software fees.** The organization incurs software license fees for KFP for a three-year total present value of $391,679.
- **Cost of KFP implementation and ongoing management.** The organization described the implementation process as easy. Following the planning phase, the interviewed company installed KFP for its online channel and mobile application. The organization created an incident monitoring and response manual and dedicated a group of FTEs to specifically work with KFP. The total cost of implementation and ongoing KFP management amounted to a risk-adjusted three-year present value of $939,375.

Forrester's interview with an existing customer and subsequent financial analysis found that the interviewed organization experienced benefits of $3.6 million over three years versus costs of $1.3 million, adding up to a net present value (NPV) of $2.2 million and an ROI of 168%.

Financial Summary



Benefits (Three-Year)



FORRESTER®

TEI Framework And Methodology

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

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 Fraud Prevention 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 Fraud Prevention.

CUSTOMER INTERVIEW
Interviewed one organization using Fraud Prevention to obtain data with respect to costs, benefits, and risks.

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

CASE STUDY
Employed four fundamental elements of TEI in modeling Kaspersky Fraud Prevention'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 Fraud Prevention.

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 Fraud Prevention Customer Journey

BEFORE AND AFTER THE KFP INVESTMENT

Interviewed Organization

For this study, Forrester interviewed one Kaspersky Fraud Prevention customer:

- The customer is a large financial services company, headquartered in Russia. In 2019, the organization reported over $1 billion in revenue and served more than 2 million individual customers, with 65% of customers using online banking.
- Forrester conducted the interview with three senior members of the transactional security and fraud prevention teams.
- As a financial services company that deals with people's savings and financial transactions, the organization emphasizes security and strives to protect its customers from growing risks of fraud.
- Evaluating the industry trend of fraud growth and thinking about its fraud prevention programs across channel helped the organization recognize the need for a new fraud prevention system for online banking to protect its clients from financial losses, remove friction, and improve convenience for customers.
- The organization considered several providers of fraud prevention software and, after a rigorous selection process, chose KFP.

Key Challenges

The interviewed organization shared the following drivers for implementing KFP:

- **The growing risk and high costs of fraud made fraud prevention a priority.** Over the past few years, financial services organizations have seen a spike in fraudulent activity, including both fraud attempts and successful fraud attacks.[2] While the interviewed organization had experienced relatively low fraud levels in its online channel, the possibility of significant reputational damage, potential customer churn, investigation, and external recovery expenses required transaction security professionals to act.
- **The fraud prevention solution needed to be effective yet provide a frictionless customer experience.** The interviewed organization was concerned that rigorous fraud prevention mechanisms requiring multiple steps of authentication for each login would lead to customer frustration and lower conversion rates.
- **The interviewed organization needed a solution that could keep up with the ever-changing fraud landscape.** The organization saw types of fraudulent attacks change and evolve over time from phishing to social engineering and beyond. It looked for a solution that could reduce the manual effort for fraud and risk management professionals to detect new types of schemes and update fraud models accordingly.

> "Several years ago, we noticed an increase in fraudulent attempts targeting our customers' online accounts. At that point, the organization made a decision to invest in a fraud prevention solution for our online channel, and we selected KFP."
>
> *Transaction security manager, financial services*

Key Results

The interview revealed that key results from the KFP investment include:

- **Successful fraud prevention.** In an environment where the number of fraudulent attempts continues to grow, with the help of KFP the organization was able to protect its customers better by identifying and preventing more fraud.
- **Reduced customer friction.** While in some cases stronger security could mean more obstacles and checkpoints, with KFP the organization was able to streamline the authentication and login processes by eliminating the need to contact a call center or second-tier authentication to verify identity.
- **Implementation of a continuously improving fraud detection process.** Working closely with Kaspersky fraud specialists helped the organization fine-tune fraud detection to its unique needs, making it more successful in detecting and preventing fraud. The organization benefits from Kaspersky's visibility into fraudulent activity happening across the industry. Once Kaspersky identifies a new type of fraud for any of its customers, Kaspersky adds monitoring for this behavior to KFP for all customers.

> "Today we are successful in detecting fraud in our online channel from the first signs, including anomalies in consumers' behavior or logins, or malicious software installed on their devices."
>
> *Transaction security manager, financial services*

FORRESTER®

Analysis Of Benefits

QUANTIFIED BENEFIT DATA

Total Benefits

REF.	BENEFIT	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Atr	Cost savings from reducing fraud	$1,044,225	$1,373,076	$1,798,075	$4,215,376	$3,434,989
Btr	Savings from reduction in customer service interactions	$47,785	$48,741	$49,716	$146,241	$121,074
Ctr	Savings from eliminating second-tier authentication for verified customers	$6,935	$7,074	$7,215	$21,224	$17,571
	Total benefits (risk-adjusted)	$1,098,945	$1,428,890	$1,855,006	$4,382,841	$3,573,634

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 interviewed organization expects risk-adjusted total benefits to be a PV of nearly $3.6 million.

Cost Savings From Reducing Fraud

The main goal for the interviewed organization was to protect its customers from fraud. In the past, in most cases when fraud occurred, it was directly caused by customers who voluntarily shared their account information with fraudsters, and, as a result, the financial organization was not liable for the customers' losses. However, even though the financial organization was not responsible for the losses, customers were not likely to continue business with the organization from which they lost their funds, which would negatively impact the organization's revenue. The organization also wanted to establish and maintain its reputation as a secure and safe financial organization.

Implementing KFP allowed the organization to start identifying and preventing fraudulent activity. The organization not only saved its customers from financial losses but worked with them to identify how fraudsters could get their account information to prevent it from happening in the future.

For our financial analysis, Forrester assumes that:

- In the first year, the organization saw, on average, 150 fraud attempts per month. The number of fraud attempts increases by 10% every year.
- KFP prevented 65% of fraud attempts in the first year. The organization's security and fraud prevention professionals work closely with Kaspersky support, modifying and fine-tuning the tool to identify more fraud schemes. Combined with KFP's machine learning, these efforts resulted in fraud prevention increases to 75% in Year 2 and 85% in Year 3.
- Average loss incurred by the bank in case of a successful fraud incident is $500.
- Every dollar lost in fraud costs a financial organization $3, and this value increases by 11% every year. Such fraud costs include fees or interest incurred during applications/underwriting/processing stages, fines/legal fees, labor/investigation, and external recovery expenses.[3]

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.

This benefit will vary based on:

- The amount of fraud experienced by the organization.

- An organization's willingness and commitment to working with KFP fine-tune the solution to identify more fraud model.
- Cost of fraud to the organization.

To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year risk-adjusted total PV of $3.4 million.

Cost Savings From Reducing Fraud: Calculation Table

REF.	METRIC	CALCULATION	YEAR 1	YEAR 2	YEAR 3
A1	Number of fraud attempts per year	150 per month*12 months (increasing 10% YoY)	1,800	1,980	2,178
A2	Percent of fraud attempts prevented by KFP		65%	70%	75%
A3	Number of fraud cases prevented by KFP	A1*A2	1,170	1,386	1,634
A4	Average fraud value		$350	$350	$350
A5	Fraud prevented by KFP	A3*A4	$409,500	$485,100	$571,725
A6	Cost to the bank per $1 of fraud	Increases by 11% YoY	$3.00	$3.33	$3.70
At	Cost savings from reducing fraud	A5*A6	$1,228,500	$1,615,383	$2,115,383
	Risk adjustment	↓15%			
Atr	Cost savings from reducing fraud (risk-adjusted)		$1,044,225	$1,373,076	$1,798,075

Savings From Reduction In Customer Service Interactions

For the interviewed organization, all new customers or those who forgot their password or login information had to contact the call center to receive their credentials to log in. This was an inconvenient step to take for the customers, and for the organization it created a steady flow of additional work for the call center staff. Using Kaspersky's Advanced Authentication allowed the organization to build an "easy entrance" mechanism where customers could log in directly from their desktops, with no additional calls.

For the interviewed organization, Forrester assumes that:

- Every year, 1.5% of the organization's customers contact the call center to receive new or retrieve lost username and password information for their online banking accounts.
- Prior to KFP, an average call duration with a representative was 5 minutes.
- An average fully loaded customer service representative annual cost is $41,000.
- Prior to KFP, after each call, a representative sent a text message to a customer with login information. Each text message costs $0.01.

The reduction in cost of customer service interactions will vary with:

- Number of new customers and customers with forgotten login information in the online channel.
- Customer service representatives' hourly compensation.

To account for these risks, Forrester adjusted this benefit downward by

By relying on KFP for authentication, the organization eliminated 30,000 calls to the call center per year.

5%, yielding a three-year risk-adjusted total PV of $121,074.

Savings From Reduction In Customer Service Interactions: Calculation Table					
REF.	METRIC	CALCULATION	YEAR 1	YEAR 2	YEAR 3
B1	Number of customers	2% growth YoY	2,000,000	2,040,000	2,080,800
B2	Customers contacting customer service for login and password assistance		1.5%	1.5%	1.5%
B3	Number of customer service calls for login or password assistance	B1*B2	30,000	30,600	31,212
B4	Average interaction handle time (minutes)		5	5	5
B5	Agent hours saved due to KFP	B3*B4/60 minutes	2,500	2,550	2,601
B6	Average customer service representative fully loaded hourly cost (rounded)	$41,000/2,080 hours	$20	$20	$20
B7	Agent productivity savings	B5*B6	$50,000	$51,000	$52,020
B8	Cost of sending a text message with login and password		$0.01	$0.01	$0.01
Bt	Savings from reduction in customer service interactions	B6+B3*B7	$50,300	$51,306	$52,332
	Risk adjustment	↓5%			
Btr	Savings from reduction in customer service interactions (risk-adjusted)		$47,785	$48,741	$49,716

Savings From Eliminating Second-Tier Authentication For Verified Customers

The interviewed organization was looking for a way to make CX more seamless and minimize hurdles for customers to access their online accounts, while keeping fraud risks low. Prior to KFP, the organization relied on second-factor authentication and sent text messages with an access code each time a user needed to access the online account. KFP's Risk-Based Authentication eliminated the need for additional verification for most legitimate users, streamlining the login process.

For the organization, Forrester assumes that:

- On a daily basis, 2,000 customers can seamlessly log in to their accounts with risk-based authentication. Without KFP, these customers would have gone through the second-factor authentication process.
- Each text message costs $0.01.

This benefit will vary based on:

- Number of customers using the online channel to access their account.
- Cost of messages sent as a part of second-factor authentication.

To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year risk-adjusted total PV of $17,571.

Savings From Eliminating Second-Tier Authentication For Verified Customers: Calculation Table					
REF.	METRIC	CALCULATION	YEAR 1	YEAR 2	YEAR 3
C1	Number of customers	2% growth YoY	2,000,000	2,040,000	2,080,800
C2	Customers logging into their accounts from their desktops and verified by KFP daily		0.1%	0.1%	0.1%
C3	Number of verified customers accessing accounts from their desktops	C1*C2* 365 days	730,000	744,600	759,492
C4	Cost of saving a confirmation text message		$0.01	$0.01	$0.01
Ct	Savings from eliminating second-tier authentication for verified customers	C3*C4	$7,300	$7,446	$7,595
	Risk adjustment	↓5%			
Ctr	Savings from eliminating second-tier authentication for verified customers (risk-adjusted)		$6,935	$7,074	$7,215

Unquantified Benefits

The interviewees shared the following benefits that affected their organization but are not quantified in this study:

- **Improved CX.** Customers experience more seamless access to their accounts and have to place fewer calls to contact customer service. This results in less time spent on the phone with a representative, resulting in a smoother user experience.
- **Stronger consumer trust.** For consumers who could have become victims of fraudsters and lost their financial assets, knowing that their financial services provider took care of them helped build trust and loyalty toward the company.
- **Identification of money laundering and fraudulent accounts.** To comply with industry regulations, the interviewed organization needs to do its part in monitoring customers' activity for signs of money laundering operations and relies on Kaspersky to do so. Additionally, Kaspersky helps identify accounts used by fraudsters, discouraging further fraudulent accounts from flourishing within the organization.
- **Additional expert assistance in identifying fraud and incidence response.** The organization's fraud analytics and security teams work closely with Kaspersky to understand and uncover new types of fraud and money laundering schemes. The organization benefits from Kaspersky's visibility into fraudulent activity happening across the industry. Once Kaspersky identifies a new type of fraud for any of its customers, Kaspersky adds monitoring for this behavior to KFP for all customers.

> "When KFP detects attempted fraud, we block the affected user's account and work with them to 'shake off' a fraudster. When customers realize that they have been victims to very convincing fraud, they are grateful that we protected them and their assets."
>
> *Transaction security manager, financial services*

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.

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 Fraud Prevention and later realize additional uses and business opportunities, including:

- **Using Kaspersky Advanced Authentication to further streamline consumer experience.** For several types of operations that previously required a visit to the branch or a call to the call center, the organization is planning to provide online authentication and login, which would save customers time and effort.

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

Total Costs

REF.	COST	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Dtr	Software and service fees	$0	$157,500	$157,500	$157,500	$472,500	$391,679
Etr	Implementation and ongoing management	$13,904	$321,200	$401,500	$401,500	$1,138,104	$939,375
	Total costs (risk-adjusted)	$13,904	$478,700	$559,000	$559,000	$1,610,604	$1,331,054

Software And Service Fees

The organization incurs software license fees for the Kaspersky Fraud Prevention solution in the cloud. These are annual recurring subscription fees that are based on the number of active users protected by KFP and include both Advanced Authentication and Automated Fraud Analytics.

The organization currently budgets for 500,000 active online users who will be protected by KFP.

Kaspersky provided realistic quotes, and Forrester risk-adjusted this cost 5% to account for volume discounts. Over three years, the total PV cost was $391,679.

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 interviewed organization expects risk-adjusted total costs to be a PV of more than $1.3 million.

Software And Service Fees: Calculation Table

REF.	METRIC	CALCULATION	INITIAL	YEAR 1	YEAR 2	YEAR 3
D1	Kaspersky Fraud Prevention license fees			$150,000	$150,000	$150,000
Dt	Software and service fees	D1	$0	$150,000	$150,000	$150,000
	Risk adjustment	↑5%				
Dtr	Software and service fees (risk-adjusted)		$0	$157,500	$157,500	$157,500

Implementation And Ongoing Management

The interviewed organization described the KFP implementation as a process that required:

- Involvement from business, security leadership, and legal professionals for the total of 100 hours to plan the implementation. Two developers were involved for one week to ensure proper integration and compatibility with the existing security systems.
- A fraud analyst who spent a week to develop an incident monitoring and response manual.

Once the implementation was complete, the organization dedicated a group of four fraud analysts to managing KFP and working closely with Kaspersky support teams to identify new types of fraud and continuously fine-tune the system to ensure higher detection rates and lower false positives. As the team picked up more work, the organization added another FTE to the analytics team for the second and third year.

Implementation costs will vary based on:

4 to 5 fraud analysts use KFP to detect, investigate, and prevent fraud.

FORRESTER®

- The effort required to plan and install the software and the number of FTEs involved in the process.
- Hourly rates for the professionals involved in the implementation activities.

To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year risk-adjusted total PV of $939,375.

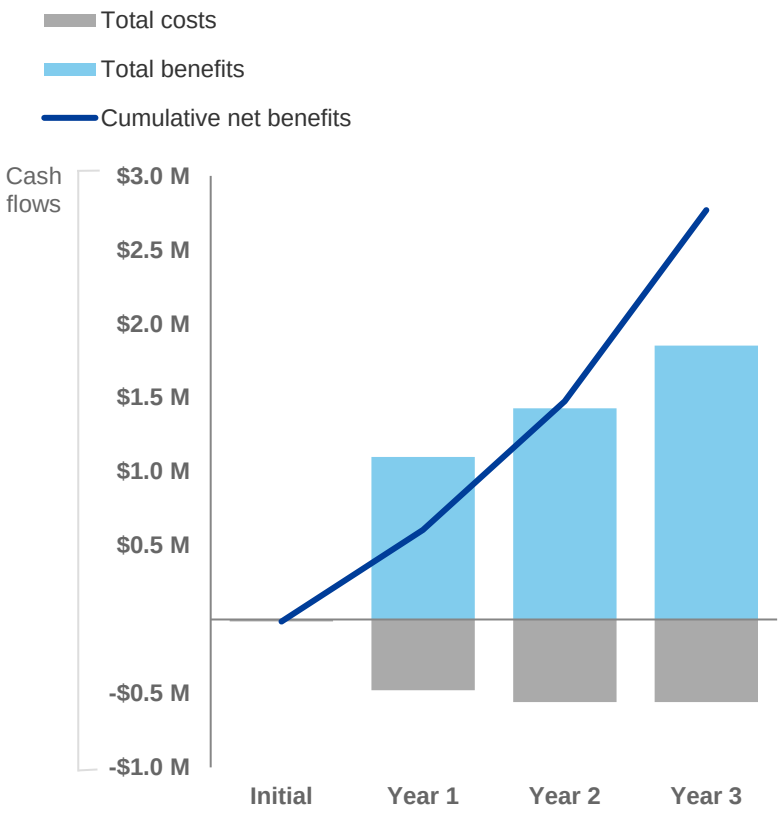
Implementation And Ongoing Management: Calculation Table

REF.	METRIC	CALCULATION	INITIAL	YEAR 1	YEAR 2	YEAR 3
E1	Planning time (hours)		100			
E2	Business and information security manager average burdened salary (hourly)		$70			
E3	Development time for implementation (hours)		40			
E4	Number of developer FTEs involved in implementation		2			
E5	Developer average burdened salary (hourly)		$53			
E6	Time to develop incident monitoring and response manual (hours)		40			
E7	Fraud analyst average burdened salary (hourly)		$35			
E8	Fraud analysts managing KFP		0	4	5	5
Et	Implementation and ongoing management	E1*E2+ E3*E4*E5+ E6*E7+E8*$73,000	$12,640	$292,000	$365,000	$365,000
	Risk adjustment	↑10%				
Etr	Implementation and ongoing management (risk-adjusted)		$13,904	$321,200	$401,500	$401,500

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 interviewed 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	($13,904)	($478,700)	($559,000)	($559,000)	($1,610,604)	($1,331,054)
Total benefits	$0	$1,098,945	$1,428,890	$1,855,006	$4,382,841	$3,573,634
Net benefits	($13,904)	$620,245	$869,890	$1,296,006	$2,772,237	$2,242,580
ROI						168%
Payback period						<6 months

FORRESTER®

Kaspersky Fraud Prevention: Overview

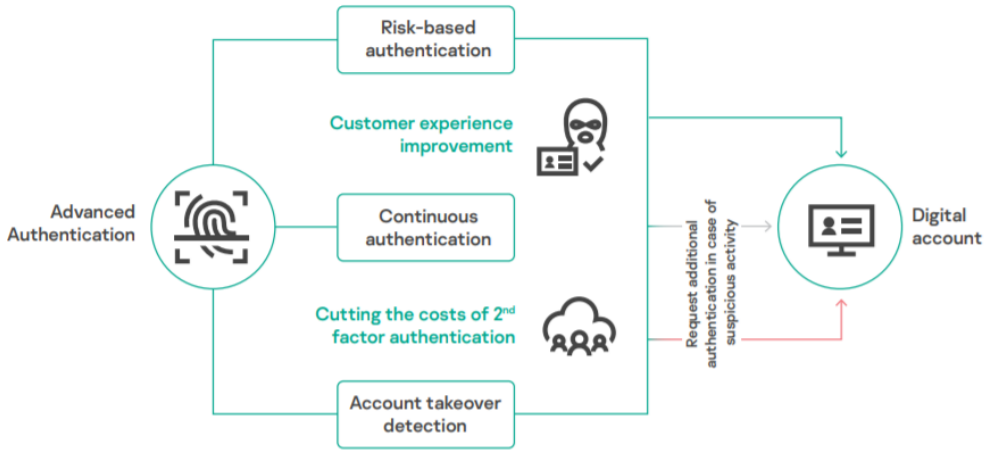
The following information is provided by Kaspersky. Forrester has not validated any claims and does not endorse Kaspersky or its offerings.

Kaspersky Fraud Prevention uses a complex range of advanced technologies — device and session reputation, behavioral and passive biometrics analysis, malware detection — along with machine learning applied for proactive detection of sophisticated fraud schemes across web and mobile channels, in real time.

This empowers organizations to detect account takeover, new account fraud, money laundering schemes, automation tools, bots, suspicious user behavior, a multitude of globally used malware, and other tools used for fraud. The Kaspersky Fraud Prevention approach allows for proactive and more accurate decision making, as well as for intelligent and adaptive use of step-up authentication.

Kaspersky Fraud Prevention offers two products: Advanced Authentication and Automated Fraud Analytics; each covers different business needs.

Advanced Authentication is designed for fast decision making at the stage of login and during the whole user's session. The Applied Risk-Based and Continuous Authentication approach helps businesses to improve user experience, detect account takeover, cut the costs of additional authentication, and preserve a high level of security.



Automated Fraud Analytics is created to provide detailed information about fraudulent activity, making sure firms know about the possible fraud before it occurs and have all the data and analysis crucial to make accurate and timely decisions and uncover complicated fraud cases.

- Real-time detection of suspicious activity even before fraud has actually damaged the business
- Uncovering the fraudster rings with global device reputation and extended fingerprinting
- Detection of cross-organizational money laundering scenarios
- Generation of ready-to-use incidents feeding your internal monitoring solutions
- Advanced incident investigation capability

Kaspersky Fraud Prevention

Learn more: kfp.kaspersky.com

Contact us at kfp@kaspersky.com

FORRESTER®

Appendix A: Total Economic Impact

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

Total Economic Impact Approach

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

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

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

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

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

Present value (PV)

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

Net present value (NPV)

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

Return on investment (ROI)

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

Discount rate

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

Payback period

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

Appendix B: Endnotes

[1] Source: “The Forrester Wave™: Risk-Based Authentication, Q2 2020,” Forrester Research, Inc., May 27, 2020.
[2] Source: “2019 True Cost Of Fraud™ Study: Financial Services and Lending,” LexisNexis, 2019 (https://risk.lexisnexis.com/insights-resources/research/true-cost-of-fraud-study-financial-services-and-lending-edition).
[3] Ibid.

FORRESTER®