A Forrester Total Economic Impact™
Study Commissioned By Kaspersky Lab
April 2019

The Total Economic Impact™ Of Kaspersky Industrial CyberSecurity

Cost Savings And Business Benefits Enabled By Kaspersky Lab

FORRESTER®

Table Of Contents

Project Director:
Julia Fadzeyeva

Project Contributor:
Richard Cavallaro

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

Avoided cost of downtime:
$1.7 million

Avoided cost of OS upgrades:
$461,495

Avoided cost of legacy endpoint antivirus:
$49,995

Executive Summary

Cyberthreats are growing in frequency and complexity. According to the data released by the National Cybersecurity and Communications Integration Center, recent years have brought an overall increase in attacks and compromises against industrial control systems.[1] With cyberattacks on the rise, the number of successful breaches had risen more than 27%, from an average of 102 to 130 per organization per year.[2] The financial outcomes of cybercrime are also worsening: The cost of cybercrime averaged $10.2 million in 2017 for the industrial/manufacturing sector.[3] In this environment, many of today's industrial control systems, including those in critical infrastructure industries, still run on specialized technology, leaving them vulnerable to an array of malicious activities. As a result, security professionals are looking for specialized industrial cybersecurity solutions to reduce risks within their outdated infrastructure.

Kaspersky Lab provides an industrial cybersecurity product that helps its customers address specific industrial cybersecurity needs. One component of the solution, KICS for Nodes, secures ICS/SCADA (industrial cybersecurity/supervisory control and data acquisition) servers, human machine interfaces (HMIs), and engineering workstations from the various types of cyberthreats that can result from human factors, generic malware, targeted attacks, or sabotage. Another component, KICS for Networks, operates at the industrial communication protocol layer, analyzing industrial traffic for anomalies.

Kaspersky Lab 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 Industrial CyberSecurity (KICS). The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of the KICS on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed one customer that has several years of experience using KICS for Nodes and that recently ran a pilot program for KICS for Networks.

Prior to using KICS, the interviewed customer struggled to protect outdated workstations with available software. The traditional endpoint antivirus it used provided limited protection at best and sometimes clashed with the manufacturing software, leading to production inefficiencies and interruptions.

Key Findings

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

- **Avoided cost of downtime by $1.7 million.** Prior to installing KICS for Nodes, the organization had no software to properly protect its outdated workstations from cyberattacks. The organization installed a temporary solution, a traditional endpoint antivirus, on the equipment to provide a limited degree of protection. However, the solution periodically clashed with the legitimate manufacturing software, causing downtime, or did not provide complete protection against all viruses, which negatively affected production. With KICS, the company protected vulnerable equipment to minimize the risk of cyberattacks and prevent system slowdowns and downtime.

FORRESTER®

ROI
368%

Benefits PV
$2.2 million

NPV
$1.7 million

Payback
3 months

- **Avoided cost of OS upgrades by $461,495**. Without a specialized ICS tool, the organization used a traditional endpoint antivirus to protect workstations. Operating systems (OS) installed on the manufacturing equipment were frequently incompatible with this endpoint antivirus solution. For the antivirus to work as intended, the information security team needed to perform costly and time-consuming OS upgrades on these workstations. Moving to KICS for Nodes allowed the organization to avoid these costly software upgrades and still obtain the necessary level of threat protection.
- **Avoided cost of legacy endpoint antivirus by $49,995.** To ensure a basic level of protection and to comply with industry regulations, the organization selectively installed traditional endpoint antivirus software on workstations. While the antivirus blocked some viral attacks, it also interfered with equipment productivity, blocking essential functions and slowing down or stopping production. With the transition to KICS, the organization no longer needed to use traditional endpoint antivirus (AV) software on workstations and stopped paying license fees for these machines.

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

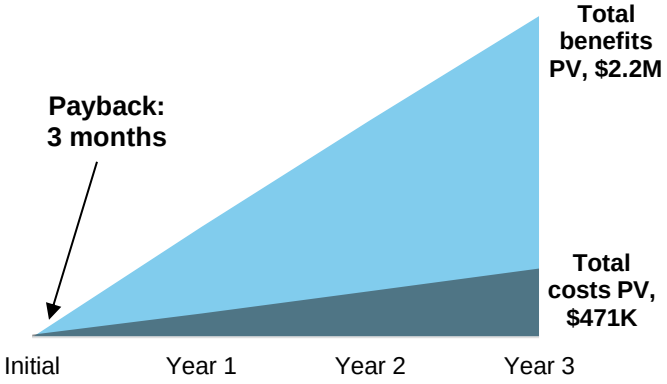
- **Kaspersky Lab services provide additional expert support in threat intelligence and incidence response.** While the interviewed organization had not needed to use KICS professional services at the time of the interview, the organization acknowledged that it is never on its own — cybersecurity professionals from Kaspersky Lab are only a phone call away.
- **Peace of mind.** While it cannot be quantified, interviewees cited the confidence in the security of the infrastructure that KICS delivers. Interviewees know that with this specialized software, their industrial systems are better protected, and the information security team is reducing the overall risk of security breaches for the organization.

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

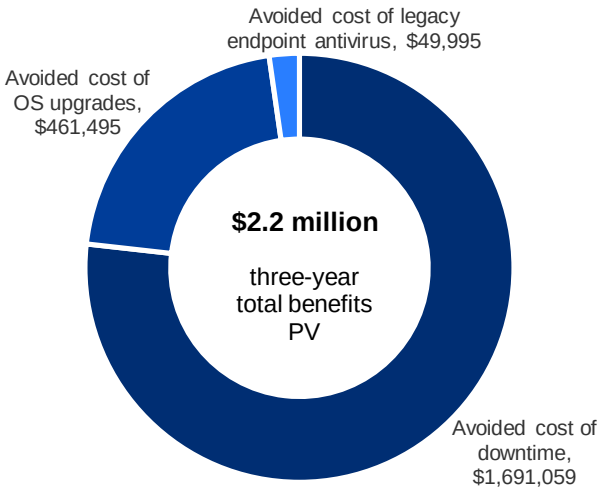
- **Software fees.** The organization incurred software license fees for KICS for Nodes for a three-year total present value of $201,904.
- **Implementation costs.** The organization described the implementation process as easy and unobtrusive. Following its strategic plan, the interviewed company gradually installed KICS for Nodes on 450 machines. Including the effort to plan and approve the implementation, the total cost of migration amounted to a risk-adjusted three-year present value of $25,310.
- **Ongoing management costs.** The interviewed organization assigned three full-time information security analysts to managing KICS for about 30% of their time, costing the organization a three-year total present value of $243,736.

Forrester's interview with an existing customer and subsequent financial analysis found that the interviewed organization experienced benefits of $2.2 million over three years versus costs of $470,950, adding up to a net present value (NPV) of $1.7 million and an ROI of 368%.

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 Industrial CyberSecurity.

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 KICS 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 Lab stakeholders and Forrester analysts to gather data relative to ICS.

CUSTOMER INTERVIEW
Interviewed one organization using KICS 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 KIKS 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 Lab 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 KICS.

Kaspersky Lab 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 Lab provided the customer name for the interview but did not participate in the interview.

The Kaspersky Industrial CyberSecurity Customer Journey

BEFORE AND AFTER THE KICS INVESTMENT

Interviewed Organization

For this study, Forrester interviewed a KICS customer:

- Forrester conducted the interview with two senior members of the information security team.
- The customer is a large manufacturing company, headquartered in Russia. In 2018, the organization reported over $8 billion in revenue and had over 50,000 employees across its multiple global facilities.
- As a company that deals with critical infrastructure, the organization emphasizes security and strives to protect its facilities from growing risks of cyberattacks.
- Re-evaluating its security programs helped the organization recognize the need for a new antivirus system to protect its work stations that were either poorly protected by a traditional endpoint antivirus or not protected at all.
- The organization ran proofs of concept (PoCs) with several providers of specialized industrial cybersecurity software and, after a rigorous selection process, chose KICS for Nodes. The organization strategically chose which workstations required the new software and gradually upgraded them over the course of a couple of years.
- At the time of the interview, the organization was in the process of vendor selection for its network security needs and could not share the financial outcomes of using KICS for Networks. By the time of publication, however, the organization decided to move forward with KICS for Networks deployment.

Key Challenges

The interviewed organization shared the following issues, drivers, challenges, goals, and opportunities:

- **The growing risk and high costs of industry-specific cyberattacks made industrial cybersecurity a priority.** Over the past few years, organizations in the critical infrastructure industries have seen an increase in the number of cyberattacks.[4] While the interviewed organization had not yet experienced a major attack, it had seen similar companies suffer and recover from cybercrime. The possibility of significant profit loss, physical damage and harm, and potential impact of national security required security pros to act.
- **Specialized manufacturing equipment required industrial-grade protection and could not be served by traditional endpoint antivirus.** In the absence of a specialized ICS solution, the interviewed organization was limited to using a traditional endpoint AV to protect workstations. The software was not designed for industrial systems and, as a result, provided limited protection and sometimes clashed with specialized software, interrupting the production process.

> "Prior to KICS, we faced a dilemma: Our workstations could work with risk or not work at all."
>
> *Senior manager of information security, manufacturing*

FORRESTER®

- **Like other organizations in critical infrastructure industries, the interviewed organization needed to comply with government requirements for cybersecurity.** The interviewed organization recognized the need to transform its former cybersecurity approach to comply with government regulations and needed a specialized ICS software to proceed.

Solution Requirements

The interviewed organization searched for a solution that could:

- Provide adequate protection for workstations, including the ones with older versions of OS.
- Be compatible with both the software and hardware components of industrial automation systems.
- Be installed without interruption to the production process and without a system reboot.
- Be lightweight and have low productivity requirements.

> "We were looking for a solution that would be effective in protecting us from cyberattacks and would not threaten the production continuity."
>
> *Senior manager of information security, manufacturing*

Key Results

The interview revealed several key results from the KICS investment:

- **The organization achieved better protection for industrial systems.** With KICS, the interviewed organization could protect the workstations that would have otherwise had no protection or would have been protected by the traditional endpoint antivirus that provided limited coverage at best.
- **The lightweight solution had no impact on the production process.** KICS for Nodes has not drained resources on the machines and ensures no interruptions or slowdown for the facility.
- **Straightforward installation and deployment ensured fast time-to-value.** An unobtrusive installation process allowed the organization to upgrade workstations to KICS for Nodes without rebooting systems or waiting for the production to stop.

> "We are at an early stage in our ICS journey and are not using KICS to its full potential yet. We do recognize the value in the product and see how it helps us reduce risks for the company, so we plan to expand the deployment and use more capabilities in the future."
>
> *Senior manager of information security, manufacturing*

Analysis Of Benefits

QUANTIFIED BENEFIT DATA

Total Benefits

REF.	BENEFIT	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Atr	Avoided cost of downtime	$680,000	$680,000	$680,000	$2,040,000	$1,691,059
Btr	Avoided cost of OS upgrades	$135,000	$189,000	$243,000	$567,000	$461,495
Ctr	Avoided cost of traditional endpoint antivirus	$14,625	$20,475	$26,325	$61,425	$49,995
	Total benefits (risk-adjusted)	$829,625	$889,475	$949,325	$2,668,425	$2,202,549

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 more than $2.2 million.

Avoided Cost Of Downtime

Among the main benefits from using KICS, the interviewed organization identified the solution's ability to help the organization avoid downtime. For a manufacturing facility, downtime often results in financial losses, which include lost revenue, lowered employee productivity, client dissatisfaction, and tarnished reputation. Any incident of unplanned downtime also requires investigation and additional efforts to restore operations.

According to the interviewees:

- To provide some degree of protection for the old equipment where possible, the organization used a traditional endpoint antivirus solution (not specifically designed for industrial systems) to detect cyberattacks. The software worked semi-successfully most of the time, but sometimes it blocked legitimate activities that were a part of the manufacturing process, causing production systems to stop until the cause of the problem was eliminated.
- From time to time, the organization detected viruses that did not stop manufacturing completely but considerably slowed it down or stopped parts of the systems, which also affected the production output.

KICS for Nodes enabled the organization to protect vulnerable equipment by minimizing the risk of cyberattacks targeting this equipment and the resulting downtime.

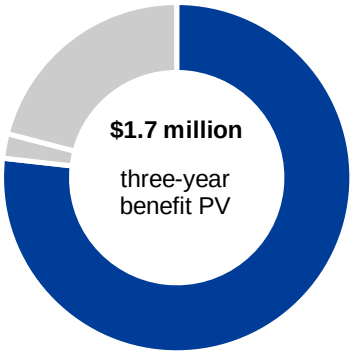
For the purposes of this study, Forrester assumes:

- The average downtime caused by viruses for a manufacturing facility similar to the interviewed organization is 10 hours.
- Facility revenue per hour is $80,000, assuming the production is running 24 hours per day, 7 days a week.

This benefit will vary based on:

- The level of risk of cyberattacks and the downtime organizations plan to avoid with the ICS software.
- Cost of downtime.

To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year risk-adjusted total PV of $1,691,059.



Avoided cost of downtime: **77%** of total benefits

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.

FORRESTER®

Avoided Cost Of Downtime: Calculation Table					
REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
A1	Facility revenue per hour		$80,000	$80,000	$80,000
A2	Hours of downtime caused by viruses (per year) avoided with KICS		10	10	10
At	Avoided cost of downtime	A1*A2	$800,000	$800,000	$800,000
	Risk adjustment	↓15%			
Atr	Avoided cost of downtime (risk-adjusted)		$680,000	$680,000	$680,000

Avoided Cost Of OS Upgrades

The key factor that prevented the interviewed organization from using traditional endpoint antivirus software on the workstations was the operating system installed on these machines. The versions of the operating systems on the manufacturing equipment were frequently incompatible with the available antivirus. For the traditional endpoint antivirus to properly protect the workstations, the information security team needed to upgrade operating systems to the modern versions. For the organization, such an upgrade would cost on average $600 per work station.

Moving to KICS for Nodes allowed the organization to avoid the cost of software upgrades while getting the necessary level of protection.

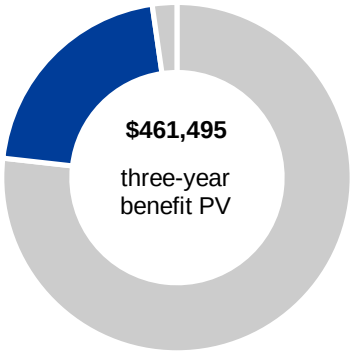
For the study, Forrester assumes that:

- The organization took a gradual approach to implementation. It installed KICS for Nodes on 250 machines in the first year and expanded coverage to 350 work stations in Year 2 and 450 in Year 3, avoiding the need for OS upgrades.
- The cost of avoided operating system upgrade per machine is $600.

The avoided cost of software upgrades will vary with:

- The approach taken to upgrading machines to newer OS.
- The average cost of an operating system upgrade.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $461,495.



Avoided cost of OS upgrades: **21%** of total benefits

Avoided Cost Of OS Upgrades: Calculation Table					
REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
B1	Cost of upgrading OS on an endpoint avoided with KICS		$600	$600	$600
B2	Number of endpoints requiring an upgrade		250	350	450
Bt	Avoided cost of OS upgrades	B1*B2	$150,000	$210,000	$270,000
	Risk adjustment	↓10%			
Btr	Avoided cost of OS upgrades (risk-adjusted)		$135,000	$189,000	$243,000

FORRESTER®

Avoided Cost Of Legacy Endpoint Antivirus

The interviewed organization struggled to provide proper virus protection to certain workstations due to the age of the equipment or operating systems installed. To ensure at least some level of protection and to comply with industry requirements, the organization installed traditional endpoint antivirus software on these machines with limited success. While the antivirus blocked some cyberattacks, it also interfered with equipment productivity, sometimes blocking essential functions and slowing down or stopping production. With the transition to KICS, the organization retired its traditional endpoint antivirus on the affected workstations.

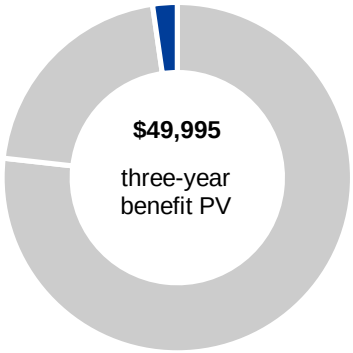
For the study, Forrester assumes that:

- The organization took a gradual approach to implementation. It replaced the traditional endpoint antivirus with KICS for Nodes on 250 machines in the first year and expanded coverage to 350 workstations in Year 2 and 450 in Year 3.
- The cost of the traditional endpoint AV software license is $65 per year.

The reduction in cost of the office AV will vary with:

- The number of work stations upgraded to KICS each year.
- The cost of one traditional endpoint AV license.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $49,995.



Avoided cost of legacy endpoint AV: **2%** of total benefits

Avoided Cost Of Legacy Endpoint Antivirus: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
C1	Cost per working station/endpoint avoided with KICS		$65	$65	$65
C2	Number of endpoints		250	350	450
Ct	Avoided cost of legacy endpoint antivirus	C1*C2	$16,250	$22,750	$29,250
	Risk adjustment	↓10%			
Ctr	Avoided cost of legacy endpoint antivirus (risk-adjusted)		$14,625	$20,475	$26,325

Unquantified Benefits

- **KICS Services provide additional expert support in threat intelligence and incidence response.** While the interviewed organization has not needed to use Kaspersky Lab services since KICS for Nodes was installed, the organization knows it is never on its own — cybersecurity professionals are only a phone call away, should their services be required.
- **Peace of mind.** While it cannot be quantified, interviewees cited the confidence in the security of the infrastructure that KICS delivers. They know that with this specialized software, the industrial systems are better protected, and the information security team is reducing the overall risk of security breaches for the organization.

Interviewees know that with KICS, the industrial systems are better protected, and the information security team is reducing the overall risk of security breaches for the organization.

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 KICS and later realize additional uses and business opportunities, including:

› **Using KICS for Networks to improve network visibility.** At the time of the interview, the organization was piloting the use of KICS for Networks and saw positive outcomes. Kaspersky Lab enabled the information security team to perform industrial traffic analysis to identify anomalies and address network vulnerabilities. The team also used KICS for Networks to uncover parameter changes in technology processes and restored optimal parameters to ensure productivity.

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

Total Costs

REF.	COST	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Dtr	Software fees	$0	$59,063	$82,688	$106,313	$248,063	$201,904
Etr	Implementation costs	$16,830	$3,410	$3,410	$3,410	$27,060	$25,310
Ftr	Ongoing management costs	$0	$98,010	$98,010	$98,010	$294,030	$243,736
	Total costs (risk-adjusted)	$16,830	$160,483	$184,108	$207,733	$569,153	$470,950

Software Fees

The organization incurred software license fees for the Kaspersky Lab Industrial CyberSecurity solution. These are annual recurring subscription fees that are based on the number of machines protected by KICS.

Within the first year, the organization incurred software fees for 250 machines, then added 100 licenses in both the second and third years, amounting to a total of 450.

Kaspersky Lab provided realistic quotes, and Forrester risk-adjusted this cost 5% to account for volume discounts. Over three years, the total PV cost was $201,904.

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 $470,950.

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.

Software Fees: Calculation Table

REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
D1	KICS for Nodes cost per machine			$225	$225	$225
D2	Number of machine endpoints			250	350	450
Dt	Software fees	D1*D2	$0	$56,250	$78,750	$101,250
	Risk adjustment	↑5%				
Dtr	Software fees (risk-adjusted)		$0	$59,063	$82,688	$106,313

Implementation Costs

The interviewed organization described the KICS for Nodes implementation as a process that required:

- Involvement from the information security control group for the total duration of 150 hours to plan the initial implementation. As the organization gradually expanded the use of KICS, Forrester accounted for the additional 10 hours spent in planning for the years following the initial implementation.

250 hours
Initial planning and deployment time

FORRESTER®

- Involvement from information security control staff, who initially spent 100 hours on implementing KICS for Nodes on machines. Forrester conservatively estimates that the team spent 50 hours in the following years to expand the implementation.

Implementation costs will vary based on:

- The effort required to plan and install the software and the number of FTEs involved in the process.
- The implementation schedule and the increase in the number of machines protected by KICS over time.
- 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 $25,310.

Implementation Costs: Calculation Table

REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
E1	Planning time (hours)		150	10	10	10
E2	Information security manager average burdened salary (hourly)		$70	$70	$70	$70
E3	Implementation time (hours)		100	50	50	50
E4	Information security analyst average burdened salary (hourly)		$48	$48	$48	$48
Et	Implementation costs	E1*E2+E3*E4	$15,300	$3,100	$3,100	$3,100
	Risk adjustment	↑10%				
Etr	Implementation costs (risk-adjusted)		$16,830	$3,410	$3,410	$3,410

Ongoing Management Costs

The interviewed organization assigned three full-time information security analysts to managing KICS for Nodes. On average, 30% of these FTEs' time is dedicated to the effort.

Ongoing costs of managing KICS can vary based on:

- The breadth of the KICS implementation.
- The number of incidents requiring investigation on a regular basis.
- Information security analysts' annual burdened salaries.

To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year risk-adjusted total PV of $243,736.

Three FTEs
spend 30% of their time on ongoing management of KICS.

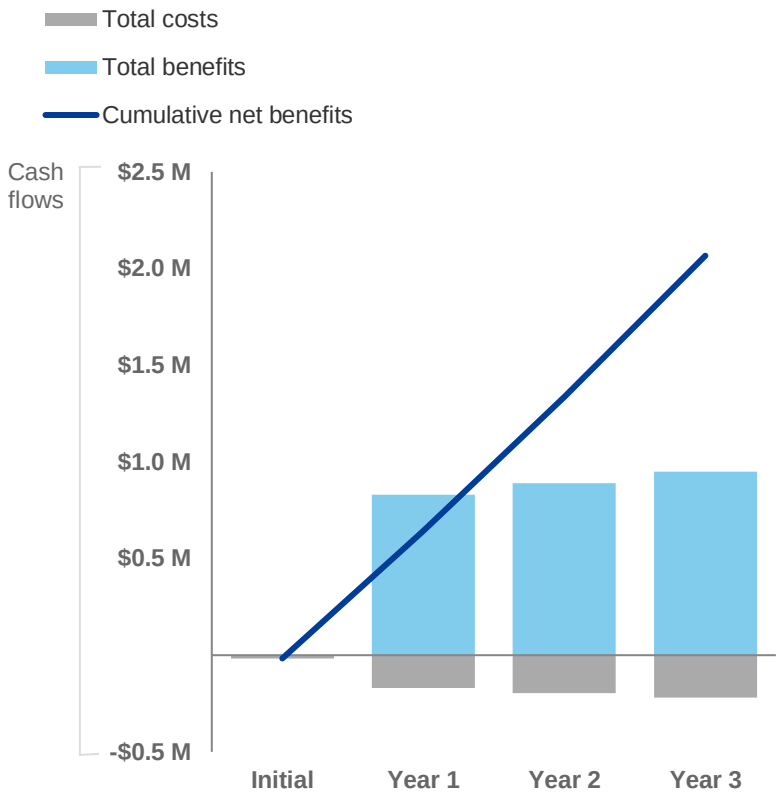
Ongoing Management Cost: Calculation Table						
REF.	**METRIC**	**CALC.**	**INITIAL**	**YEAR 1**	**YEAR 2**	**YEAR 3**
F1	Information security analysts managing KICS			3	3	3
F2	Percent of analysts' time spent on managing KICS			30%	30%	30%
F3	Information security analyst average burdened annual salary			$99,000	$99,000	$99,000
Ft	KICS ongoing management	F1*F2*F3	$0	$89,100	$89,100	$89,100
	Risk adjustment	↑10%				
Ftr	Ongoing management costs (risk-adjusted)		$0	$98,010	$98,010	$98,010

Forrester found the internal cost of information security FTE training to use KICS to be negligible. For the interviewed organization, a small team of information security analysts was trained on KICS for one day as a part of the pilot phase. No additional training programs were held since the pilot.

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 Table (Risk-Adjusted)

	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Total costs	($16,830)	($160,483)	($184,108)	($207,733)	($569,153)	($470,950)
Total benefits	$0	$829,625	$889,475	$949,325	$2,668,425	$2,202,549
Net benefits	($16,830)	$669,143	$705,368	$741,593	$2,099,273	$1,731,599
ROI						368%
Payback period						3 months

FORRESTER®

Kaspersky Industrial CyberSecurity: Overview

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

Kaspersky Industrial CyberSecurity (KICS) is a portfolio of products and services, specifically designed to meet the unique demands of operational technology (OT) and ICS environments.

Kaspersky Lab's holistic approach brings value on any stage of the customer's OT security process — from cybersecurity assessment to incident response.

KICS for Nodes is an industrial endpoint protection product. It helps to protect industrial control system endpoints — including SCADA servers, engineering workstations, and more.

KICS for Networks is an anomaly and breach detection product. It monitors network traffic and provides network-level security that operates at the industrial communication protocol layer.

Expert Services include industrial cybersecurity assessment, penetration testing, incident response, and threat intelligence.

Training programs include basic industrial cybersecurity training for C-level and ICS engineers as well as expert training for IT/OT security experts.

Learn more: https://ics.kaspersky.com

Contact: ics@kaspersky.com

FORRESTER®

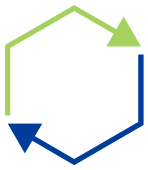
Appendix A: Total Economic Impact

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: “Protecting Industrial Control Systems And Critical Infrastructure From Attack,” Forrester Research, Inc., April 19, 2018.
[2] Source: “Cost Of Cyber Crime Study,” Ponemon Institute, 2017 (https://www.accenture.com/us-en/insight-cost-of-cybercrime-2017).
[3] Source: Ibid.
[4] Source: “Protecting Industrial Control Systems And Critical Infrastructure From Attack,” Forrester Research, Inc., April 19, 2018.