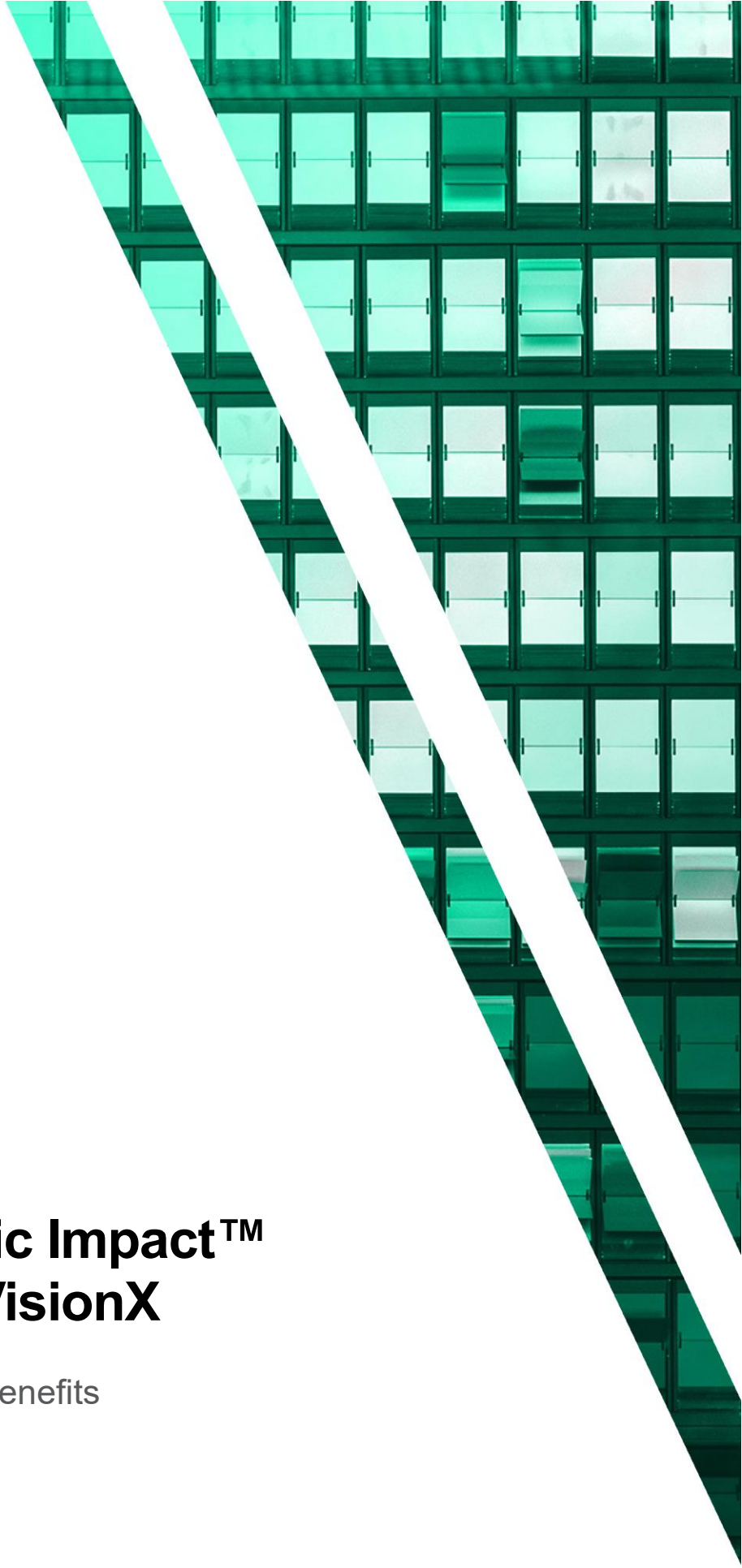
FORRESTER®



# The Total Economic Impact™ Of Smarttech247 VisionX

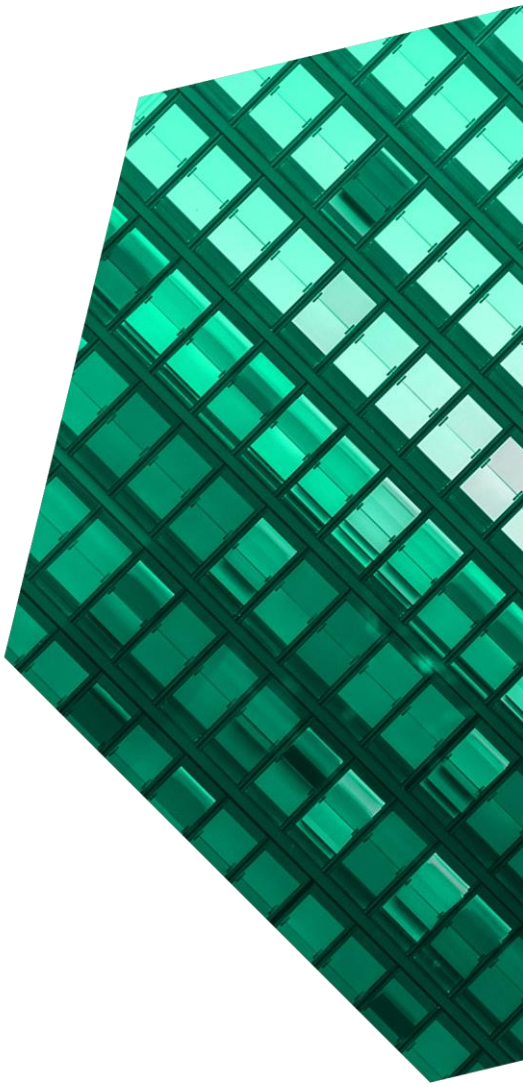
## Cost Savings And Business Benefits Enabled By VisionX

**JANUARY 2022**

# Table Of Contents




*Consulting Team: Duncan Watkins*

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. For more information, visit forrester.com/consulting.

## Executive Summary

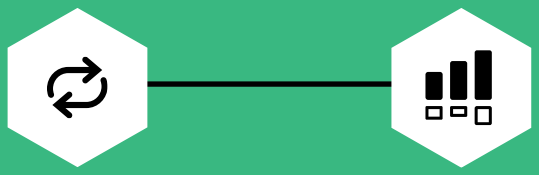
Global businesses with sites operating 24/7 require a cybersecurity partner to monitor and manage cyberthreats around the clock. Smarttech247offers a portfolio of managed security services to monitor organizations for potential threats and support clients in responding to them. As more businesses move to a cloud environment, the reliance on their IT infrastructure grows — as do their concerns about the impact of cyberattacks. Firms must now focus on more proactive prevention to meet customer expectations as well as regulatory obligations.

The Smarttech247 VisionX (Managed Detection and Response) platform is a cybersecurity service providing 24/7 proactive threat detection and response, using cloud data analytics, machine learning, and an incident response capability. As the sophistication of cyberattacks grows, the urgency for organizations to defend against them in real time is also becoming difficult — yet more and more essential. Smarttech247 provides a suite of services to meet these challenges, including its VisionX platform, which uses real-time predictive analytics to detect and protect against potential attacks. Smarttech247 also provides Threat Intelligence Hub, which can connect to VisionX, helping to reduce security risks by informing organizations of the latest threats and vulnerabilities via its alert system across multiple sources, addressing regulatory compliance requirements.

Smarttech247 commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying the VisionX platform.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of an investment in Smarttech247's VisionX service on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed the decision-maker at a global organization that uses the Smarttech247 VisionX service. Forrester used this experience to project a three-year financial analysis in this study.

**KEY STATISTICS**



Return on investment (ROI)
**319%**

Net present value (NPV)
**€2M**

Prior to using VisionX, the interviewee from the customer company noted how their organization, like many others, was undergoing a digital transformation including the uptake of new cloud technology in governance, compliance, and risk. The lack of a common IT infrastructure and the high volume of data generated from using multiple security platforms for cyberthreats was too much for the team to digest and manage on their own. Prior attempts to manage this had yielded limited success, leaving them with limited visibility into cyber risks and vulnerabilities. These limitations led to a need for security tool consolidation and workforce augmentation, initially in the firm's most vulnerable business areas and then rolled out to other parts of the organization.

The key results from investing in the Smarttech247 VisionX platform include reduction of production downtime from cyberattacks, as well as the cost

savings from retired security platforms and specific workforce overhead. Qualitative benefits include 24/7 coverage and access to Smarttech247's 24/7 security team to assist with response and remediation. This allowed security engineers to save significant time and refocus their effort on higher-value tasks. The reporting capability has also helped show board level executives how the investment is supporting a better security posture for the organization.

## KEY FINDINGS

**Quantified benefits.** Risk-adjusted present value (PV) quantified benefits include:

- **Avoided business downtime impact of €1.8 million.** Cyberattacks can damage and cause disruptions and downtime to the interviewee's production plant, which in turn affects business revenue. The dedicated 24/7 resource provided by Smarttech247 monitored and detected malware propagation, using the threat intelligence and AI outlined in its daily emails detailing actions taken to ensure the prevention of loss of data.
- **Saved €497,000 from retiring other security platforms.** The organization's potential exposure was spread across its various security platforms, which became no longer necessary once Smarttech247's VisionX was implemented.
- **Total savings of €267,000 from a reduction in manual tasks.** After implementing Smarttech247's platform and service, the company was able to avoid paying salaries for individuals to perform manual tasks and assessments.

**Unquantified benefits.** Benefits that are not quantified for this study include:

- **Increased peace of mind from the board level down.** Transparency into the potential risk factors that could impact production and the business meant that board members could make more informed decisions on whether and where to focus budgets during quarterly reviews. This increased control also enabled the CFO to easily ascertain the feasibility of budget allocation on such security systems.
- **Saved time and resources on ad hoc checks and testing.** With Smarttech247's around-the-clock notifications, there was no longer a need for ad hoc security testing and log checks. Engineers gained time back that could be focused on other business priorities and project deliveries rather than duplicative work running diagnostics and reviewing security logs.
- **Reduced number of outages.** Smarttech247's continuous monitoring and testing for potential threats derived from its AI analytics and detection service, revealing vulnerabilities before hackers could exploit them. By showing up-to-date and real-time information, the platform helped to avoid and defend against potential attacks. The testing of its own cyberdefense system ensured minimal business impact; it also help to ensure regulatory compliance.

**Costs.** Risk-adjusted PV costs include:

- **Total software license fees of less than €209,000.** The total cost for one Smarttech247 license for the interviewee's firm was €80,000 per year over three years.
- **Setup and infrastructure costs of less than €51,000.** The firm incurred a one-time charge of €25k for setup and project management, including professional services, third-party services, and legal fees. In addition, the organization paid €10,000 annually to cover PC leasing costs
- **Additional platform management cost of more than €67,000.** The organization spent an additional €67,132 on internal resources for managing and overseeing the VisionX platform.

- **Total monitoring costs of €298,000.** This involved monitoring service costs averaging €120,000 each year for three years.

The interview and financial analysis found that the decision-maker's organization experiences benefits of €2.62 million over three years versus costs of €625,000, adding up to a net present value (NPV) of €2 million and an ROI of 319%.

**"Only Smarttech247 were flexible in pricing for what we needed."**

*CIO, European division, food manufacturer*

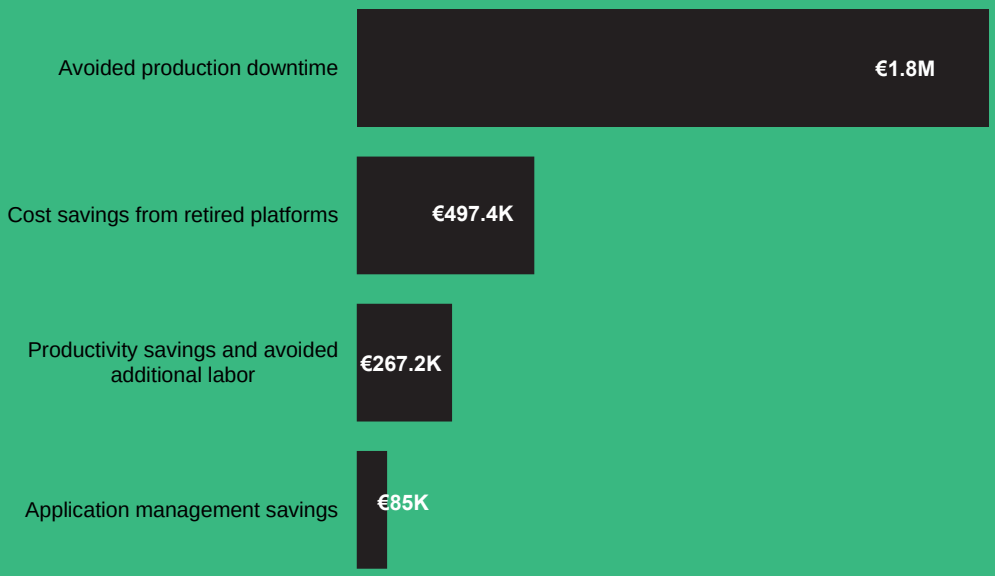
ROI
**319%**

BENEFITS PV
**€2.62M**

NPV
**€2M**

PAYBACK
**<6 months**

## Benefits (Three-Year)

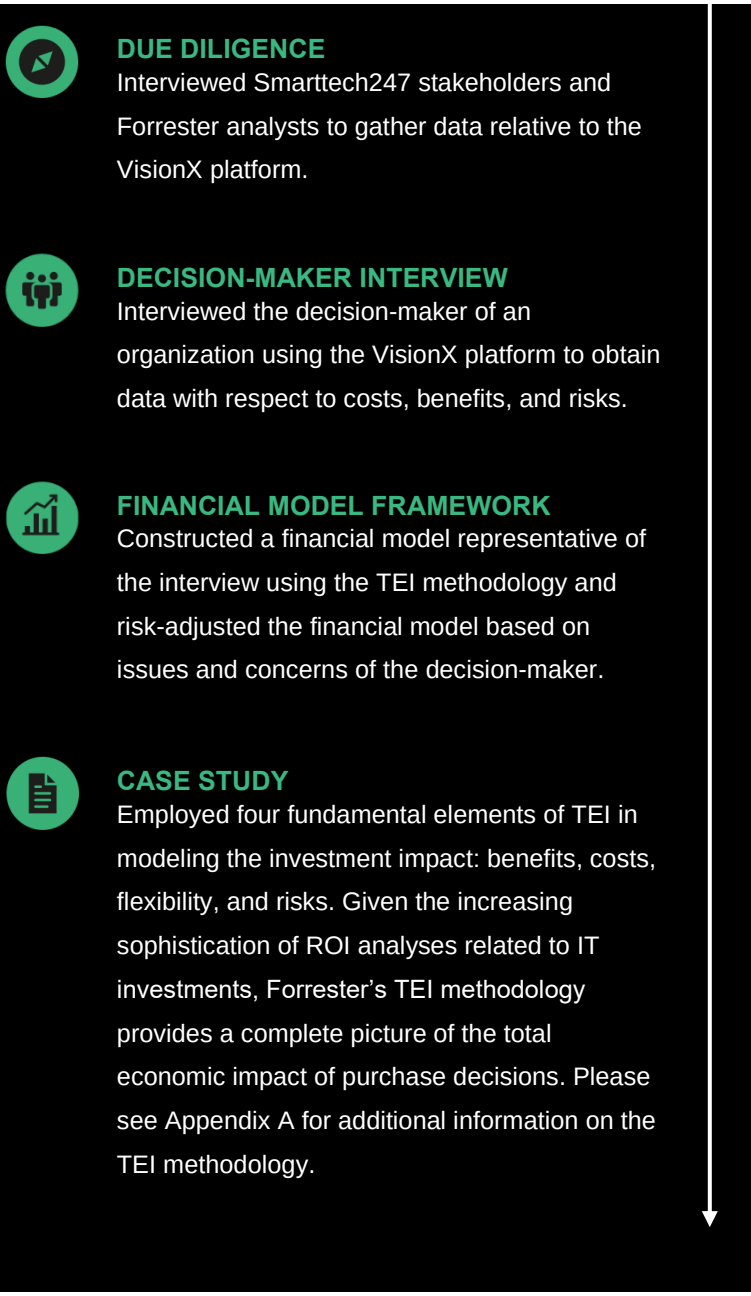



The biggest benefit the firm recognized from its investment in Smarttech247 was the avoided potential business downtime from cyberattacks on production operations, which could decrease revenue due to nonproduction.

## TEI FRAMEWORK AND METHODOLOGY

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

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 the VisionX platform can have for an organization.




**DISCLOSURES**

Readers should be aware of the following:

This study is commissioned by Smarttech247 and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the study to determine the appropriateness of an investment in the VisionX platform.

Smarttech247 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.

Smarttech247 provided the customer's name for the interview but did not participate in the interview.

# The Smarttech247 VisionX Customer Journey

Drivers leading to the VisionX investment

## INTERVIEWEE'S ORGANIZATION

Forrester interviewed the decision-maker at a Smarttech247 VisionX customer, an organization with the following characteristics:

- Food manufacturer with operations in Europe and Asia Pacific.
- Nine thousand employees, of which 3,000 are IT users.
- Annual revenues of €1.4 billion.
- VisionX customer since 2017.

## KEY CHALLENGES

The organization had grown through acquisition, and as a result, its security was an amalgamation of two companies' capabilities and tools. Duplication of capabilities and tools was common, with limited visibility provided. Furthermore, the firm did not have incident response processes in place to manage cyberthreats, so leaders were concerned that the business would suffer substantial negative impact if the organization were breached.

The interviewee noted how the organization struggled with common challenges, including:

- **No common security or IT infrastructure.** Due to multiple past acquisitions, the business had grown and inherited a number of systems across business areas. This meant that no common security standards were in place, which led to confusion about and duplication of security procedures and tools as well as wasted investment.
- **Growing complexity of cyberthreats.** With the growing sophistication and frequency in cyberattacks and a lack of security standards, the organization's leadership was concerned about its ability to keep up with and respond to these threats.

> **"The biggest risk to our business was the threat of a cyberattack to our IT systems powering our production plants."**
>
> *CIO, European division, food manufacturer*

## INVESTMENT OBJECTIVES

As leaders at the organization began to understand the risk that their vulnerable IT systems posed to the business, they started to research their options to improve their security posture and response capabilities. They needed a solution that would:

- Deploy quickly and easily, then efficiently roll out as standard to other countries.
- Provide transparency and depth into the actions being taken to protect the business and defend against potential threats.
- Be easy to manage and maintain but also grow as the business evolved.
- Allow the business to protect against or avoid cyberattacks but also recover quickly, with as little damage as possible

## USE CASE DESCRIPTION

The customer is now using the VisionX platform across all countries and allows Smarttech247 to handle most of the platform management and oversee threats to its business. Although the security team initially needed some convincing as they moved from checking on an ad hoc basis to relying on a 24/7 security monitoring service, the interviewee described

a high degree of faith in the VisionX platform across the organization.

The team rolled out the platform to the first country within two weeks, and quickly spotted malicious activity, proving the value of the solution to the customer. The Smarttech247 service alerted the customer to malicious activity that had previously been undetected by the prior security controls in place.

VisionX detected the WannaCry ransomware incident early: Smarttech247 phoned the security team at the organization alerting them to begin patching and to watch out for the threat.[2] This demonstrated how Smarttech247 could reduce the firm's exposure to a potential cyberattack. Smarttech247 provides early notification of any problems, allowing the organization to prepare ahead of time. The team currently finds the detailed reporting of VisionX particularly useful, especially at board level, as this helps the organization explain what is being done to protect the business for disaster recovery and business continuity purposes.

The company's long-term strategy for Smarttech247's VisionX platform is to continue to roll out to all business units and locations globally. The team has also moved other applications into the cloud and has implemented VisionX to protect them.

For this use case, Forrester modeled benefits and costs over three years.

**Key assumptions**

- **€1.4B global company**
- **3,000 IT users**
- **Country-by-country implementation**

**"Smarttech247 often come in with advance warnings and allow us to get ahead of any potential problems using their 24/7 monitoring and detection."**

*CIO, European division, food manufacturer*

# Analysis Of Benefits

Quantified benefit data

| Total Benefits | | | | | | |
|---|---|---|---|---|---|---|
| **Ref.** | **Benefit** | **Year 1** | **Year 2** | **Year 3** | **Total** | **Present Value** |
| Atr | Avoided production downtime | €712,500 | €712,500 | €712,500 | €2,137,500 | €1,771,882 |
| Btr | Cost savings from retired platforms | €200,000 | €200,000 | €200,000 | €600,000 | €497,370 |
| Ctr | Productivity savings and avoided additional labor | €104,500 | €107,635 | €110,864 | €322,999 | €267,248 |
| Dtr | Application management savings | €33,250 | €34,248 | €35,275 | €102,772 | €85,034 |
| | Total benefits (risk-adjusted) | $1,050,250 | $1,054,383 | $1,058,639 | $3,163,271 | $2,621,534 |

### AVOIDED PRODUCTION DOWNTIME

**Evidence and data.** The interviewee reported that prior to implementing the VisionX platform, the cost per hour of inactivity at one of the production plants amounted to €30,000 per year. The dedicated 24/7 resource provided by Smarttech247 monitored the environment, with potential threats outlined in a daily email advisory of response actions taken. In countries where the product hasn't yet been deployed, an internal subject matter expert, within the customer organization, looks to outline and prevent potential issues for subsidiaries.

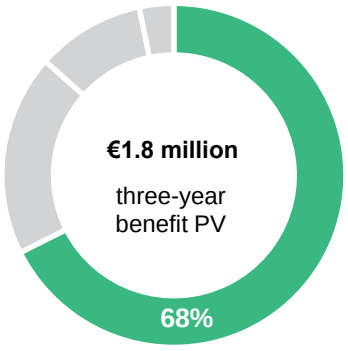
**Modeling and assumptions.** Based on the customer interview, Forrester estimates the following:

- The number of hours of inactivity avoided in each of the 25 production facilities, on average, is 1 hour per year.
- Every hour of inactivity costs €30,000.
- As the organization has had no downtime from attacks since implementing the product one hundred percent of this impact is captured.

**Risks.** This benefit can vary from organization to organization due to the following factors:

- The scope of operations negatively affected by a malicious cyberattack. This includes the amount of production downtime and cost per hour of inactivity.
- The speed with which a business can recover after an attack.

**Results.** To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of nearly €1.8 million.



| Avoided Production Downtime | | | | | |
|---|---|---|---|---|---|
| **Ref.** | **Metric** | **Calculation** | **Year 1** | **Year 2** | **Year 3** |
| A1 | Hours of previous downtime | Interview | 25 | 25 | 25 |
| A2 | Cost per hour of downtime | Interview | €30,000 | €30,000 | €30,000 |
| A3 | Percent captured | Interview | 100% | 100% | 100% |
| At | Avoided production downtime | A1*A2*A3 | €750,000 | €750,000 | €750,000 |
| | Risk adjustment | ↓5% | | | |
| Atr | Avoided production downtime (risk-adjusted) | | €712,500 | €712,500 | €712,500 |
| | **Three-year total: €2,137,500** | | | **Three-year present value: €1,771,882** | |

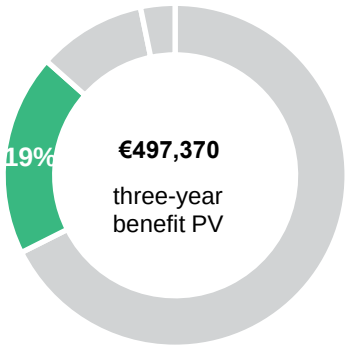
### COST SAVINGS FROM RETIRED PLATFORMS

**Evidence and data.** The interviewed decision-maker shared that their organization spent €200,000 per year on various security platforms prior to investing in Smarttech247's VisionX.

**Modeling and assumptions.** Forrester based its model on the cost amounts spent by the interviewee's organization on previous platforms.

**Risks.** There are no risks involved that would impact this benefit.

**Results.** This benefit yields a three-year total PV of more than €497,000.




| Cost Savings From Retired Platforms | | | | | |
|---|---|---|---|---|---|
| **Ref.** | **Metric** | **Calculation** | **Year 1** | **Year 2** | **Year 3** |
| B1 | Potential exposure | Interview | €200,000 | €200,000 | €200,000 |
| B2 | Probability of exposure | Interview | 1 | 1 | 1 |
| Bt | Cost savings from retired platforms | B1*B2 | €200,000 | €200,000 | €200,000 |
| | Risk adjustment | 0% | | | |
| Btr | Cost savings from retired platforms (risk-adjusted) | | €200,000 | €200,000 | €200,000 |
| | **Three-year total: €600,000** | | | **Three-year present value: €497,370** | |

### PRODUCTIVITY SAVINGS AND AVOIDED ADDITIONAL LABOR

**Evidence and data.** The interviewee noted that with the implementation of Smarttech247, security engineers saved time monitoring for security threats and could focus on more strategic, higher value-projects, thus avoiding hiring additional engineers.

Annual cost savings due to reduced headcount:

**€267,248**

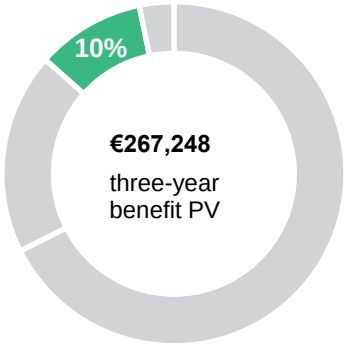
**Modeling and assumptions.** Based on the customer interview, Forrester estimates the following:

- The VisionX platform executes the equivalent tasks previously performed by two FTEs each year.
- The average annual compensation for an FTE performing these tasks is €110,000, with an annual 3% increase.

**Risks.** This figure can vary from organization to organization based on the following:

- Seniority and salary levels for individuals performing tasks
- Time savings may not be converted to equally productive, value-adding tasks.

**Results.** To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of more than €267,000




**Productivity Savings And Avoided Additional Labor**

| Ref. | Metric | Source | Year 1 | Year 2 | Year 3 |
|---|---|---|---|---|---|
| C1 | Number of employees no longer required after deploying Vision X | Interview | 2 | 2 | 2 |
| C2 | Annual compensation per FTE | TEI standard | €55,000 | €56,650 | €58,350 |
| Ct | Productivity savings and avoided additional labor | C1*C2 | €110,000 | €113,000 | €116,700 |
| | Risk adjustment | ↓5% | | | |
| Ctr | Productivity savings and avoided additional labor (risk-adjusted) | | €200,000 | €107,635 | 110,864 |
| | **Three-year total: €322,999** | | | **Three-year present value: €267,248** | |

### APPLICATION MANAGEMENT SAVINGS

**Evidence and data.** The interviewed decision-maker described an additional €35,000 annual cost savings due to no longer needing an FTE to manage and assess the security and applications.

**Modeling and assumptions.** Based on customer interviews, Forrester estimates the following:

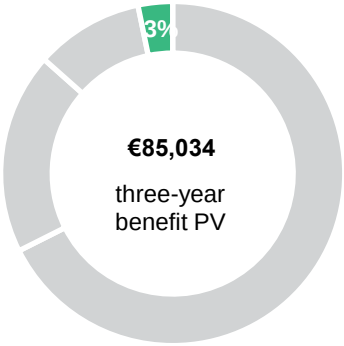
- The organization requires one application manager to review the organization's security and functions.
- The annual compensation for this employee is €35,000, increasing 3% each year
- The FTE is redeployed elsewhere in the business for other projects.

**Risks.** This benefit can vary from organization to organization due to the following factors:

- The degree of dependency on the manager for this task is reduced or eliminated, however, this does not necessarily lead to an increased capacity for the manager.
- The value recapture applied to other areas of the business may vary.

> **"The network security engineers are able to focus on projects that are valuable to the business — not worrying about security."**
>
> *CIO, European division, food manufacturer*

**Results.** To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of more than €85,000.




**Application Management Savings**

| Ref. | Metric | Calculation | Year 1 | Year 2 | Year 3 |
|---|---|---|---|---|---|
| D1 | Number of applications | Interview | 1 | 1 | 1 |
| D2 | Yearly rate per person | Interview | €35,000 | €36,050 | €37,132 |
| Dt | Application management savings | D1*D2 | €35,000 | €36,050 | €37,132 |
| | Risk adjustment | ↓5% | | | |
| Dtr | Application management savings (risk-adjusted) | | €33,250 | €34,248 | €35,275 |
| | **Three-year total: €102,772** | | | **Three-year present value: €85,034** | |

## UNQUANTIFIED BENEFITS

Additional benefits that the customer experienced but was not able to quantify include:

- **Peace of mind.** The customer found that the analysis provided by Smarttech247 through its detailed reports afforded more transparency for board executives into potential risk factors that could impact production and the business. This enabled the CFO to easily ascertain the feasibility of budget allocation for security systems. Being able to make better-informed decisions on whether and where to focus budgets during quarterly reviews gave senior board members better insight and control.
- **Alerts.** With Smarttech247, there was no longer a need for any additional ad hoc security log reviews, as the customer was notified about any potential threats.
- **Trust.** Smarttech247's service revealed vulnerabilities before hackers could attack, thereby preventing can prevent business disruptions. By showing up-to-date and real-time information, it helped to avoid and defend against potential attacks.
- **Reduced time and resources spent on ad hoc checks and testing.** Smarttech247 obviated the need for additional ad hoc security testing and log checks. The time gained for engineers from this time saved could be focused on other, more valuable business priorities and project delivery.
- **Reduced number of outages.** Smarttech247's ability to continuously test and monitor for potential threats in real time, derived from its AI analytics and detection service, could reveal vulnerabilities and prevent possible outages. The testing of its own cyber-defense system could also help with regulatory compliance.

**"We also have quarterly business reviews with Smarttech247, and that helps improve the product."**

*CIO, European division, food manufacturer*

# Analysis Of Costs

Quantified cost data

## Total Costs

| Ref. | Cost | Initial | Year 1 | Year 2 | Year 3 | Total | Present Value |
|---|---|---|---|---|---|---|---|
| Etr | Software license fees | €0 | €84,000 | €84,000 | €84,000 | €252,000 | €208,896 |
| Ftr | Infrastructure costs | €0 | €10,000 | €10,300 | €10,609 | €30,909 | €25,574 |
| Gtr | Setup costs | €25,000 | €0 | €0 | €0 | €25,000 | €25,000 |
| Htr | Additional platform management resource | €0 | €26,250 | €27,038 | €27,849 | €81,136 | €67,132 |
| Itr | Monitoring costs | €0 | €120,000 | €120,000 | €120,000 | €360,000 | €298,422 |
| | Total costs (risk-adjusted) | €25,000 | €240,250 | €241,338 | €242,458 | €749,045 | €625,024 |

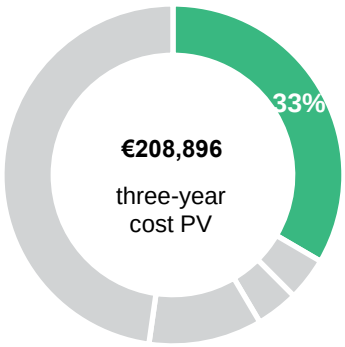
### SOFTWARE LICENSE FEES

**Evidence and data.** The interviewee shared that their organization spent €80,000 for the VisionX platform software license. The organization only required one license.

**Modeling and assumptions.** For the case of this study the model has assumed the figures for this organization remained consistent at a fixed price each year.

**Risks.** There is a 5% upward risk adjustment applied this cost as the license software fees for this organization will vary to others depending on their size and requirements.

**Results.** This cost yields a three-year, risk-adjusted total PV of €209,000.




## Software License Fees

| Ref. | Metric | Source | Initial | Year 1 | Year 2 | Year 3 |
|---|---|---|---|---|---|---|
| E1 | License fees | Interview | | €80,000 | €80,000 | €80,000 |
| E2 | Number of licenses required | Interview | | 1 | 1 | 1 |
| Et | Software license fees | E1*E2 | €0 | €80,000 | €80,000 | €80,000 |
| | Risk adjustment | ↑5% | | | | |
| Etr | Software license fees (risk-adjusted) | | €0 | €84,000 | €84,000 | €84,000 |
| | **Three-year total: €252,000** | | | **Three-year present value: €208,896** | | |

### INFRASTRUCTURE COSTS

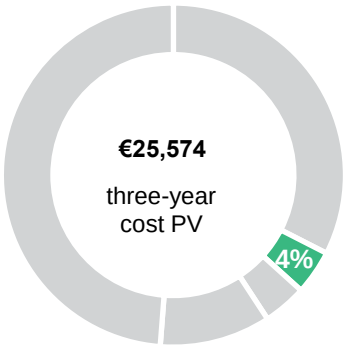
**Evidence and data.** The interviewee noted that the organization also had infrastructure costs, both on the business on-premises servers and within the virtual environment and cloud. These totaled €10,000 per year.

**Modeling and assumptions.** Based on customer interviews, Forrester estimates the following:

- The organization uses one unit of hardware.
- The cost per unit is €10,000 annually, increasing 3% annually due to inflation.

**Risks.** There are no risks to consider for this cost.

**Results.** This cost yields a three-year total PV of less than €26,000.




**Infrastructure Costs**

| Ref. | Metric | Calculation | Initial | Year 1 | Year 2 | Year 3 |
|---|---|---|---|---|---|---|
| F1 | Hardware costs | Interview | | €10,000 | €10,300 | €10,609 |
| F2 | Number of units | Interview | | 1 | 1 | 1 |
| Ft | Infrastructure costs | F1*F2 | €0 | €10,000 | €10,300 | €10,609 |
| | Risk adjustment | 0% | | | | |
| Ftr | Infrastructure costs (risk-adjusted) | | €0 | €10,000 | €10,300 | €10,609 |
| | **Three-year total: €30,909** | | | **Three-year present value: €25,574** | | |

### SETUP COSTS

**Evidence and data.** The interviewee confirmed that the initial setup fee for the software implementation was a one-off charge of €15,000. The firm outsourced the project management to Smarttech247, for the deployment of the VisionX platform, which helped save some internal costs.

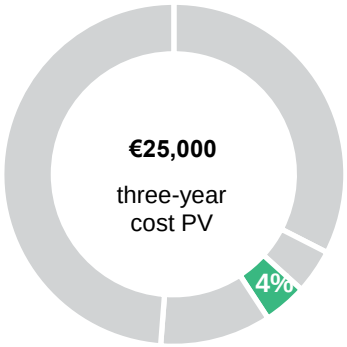
**Modeling and assumptions.** The organization in this study felt that it required a third-party project manager to deploy the VisionX platform.

**Risks.** There are no risks to consider for this cost.

**Results.** This cost yields a three-year total PV of €25,000.

**“Four engineers were involved in the implementation with Smarttech247. If we did this ourselves, it would need to be a team of 10, [and] Cisco-qualified engineers are not cheap.”**

*CIO, European division, food manufacturer*




| Setup Costs | | | | | | |
|---|---|---|---|---|---|---|
| **Ref.** | **Metric** | **Calculation** | **Initial** | **Year 1** | **Year 2** | **Year 3** |
| G1 | Setup costs | Interview | €15,000 | | | |
| G2 | Project management | Interview | €10,000 | | | |
| Gt | Setup costs | G1*G2 | €25,000 | €0 | €0 | €0 |
| | Risk adjustment | 0% | | | | |
| Gtr | Setup costs (risk-adjusted) | | €25,000 | €0 | €0 | €0 |
| | **Three-year total: €25,000** | | | **Three-year present value: €25,000** | | |

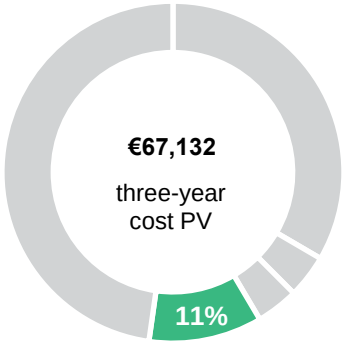
### ADDITIONAL PLATFORM MANAGEMENT RESOURCE

**Evidence and data**. The interviewee described that their organization felt the need to employ an additional platform management resource to monitor the VisionX platform’s performance.

**Modeling and assumptions.** Based on the customer interview, Forrester estimates that the annual salary for one FTE to manage the VisionX platform is €25,000, increasing each year due to inflation at 3%.

**Risks.** This may vary based on a business’ internal capabilities and resource costs to manage the VisionX platform and monitor threats. A 5 % risk adjustment has been added here to account for this.

**Results.** This cost yields a three-year, risk-adjusted total PV of €67,000.



| Additional Platform Management Resource | | | | | | |
|---|---|---|---|---|---|---|
| **Ref.** | **Metric** | **Calculation** | **Initial** | **Year 1** | **Year 2** | **Year 3** |
| H1 | Number of people | Interview | | 1 | 1 | 1 |
| H2 | Salary | TEI standard | | €25,000 | €25,750 | €26,523 |
| Ht | Additional platform management resource | H1*H2 | €0 | €25,000 | €25,750 | €26,523 |
| | Risk adjustment | ↑5% | | | | |
| Htr | Additional platform management resource (risk-adjusted) | | €0 | €26,250 | €27,038 | €27,849 |
| | **Three-year total: €81,136** | | | **Three-year present value: €67,132** | | |

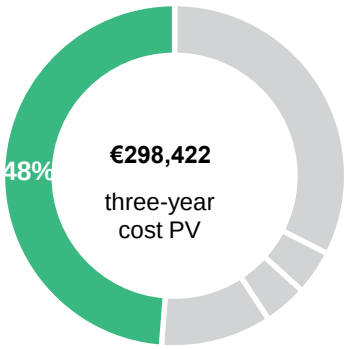
### MONITORING COSTS

**Evidence and data.** Smarttech247 offers monitoring services with its VisionX platform, and the interviewee's organization purchased this service. The total cost of the monitoring service is €120,000 per year, for a total cost of €360,000 over the three-year period.

**Modeling and assumptions.** The organization pays monitoring costs charged as a multiyear fixed cost of €120,000 per year.

**Risks.** There are no risks to consider here as the monitoring cost is very stable

**Results.** This cost yields a three-year total PV of €298,000.

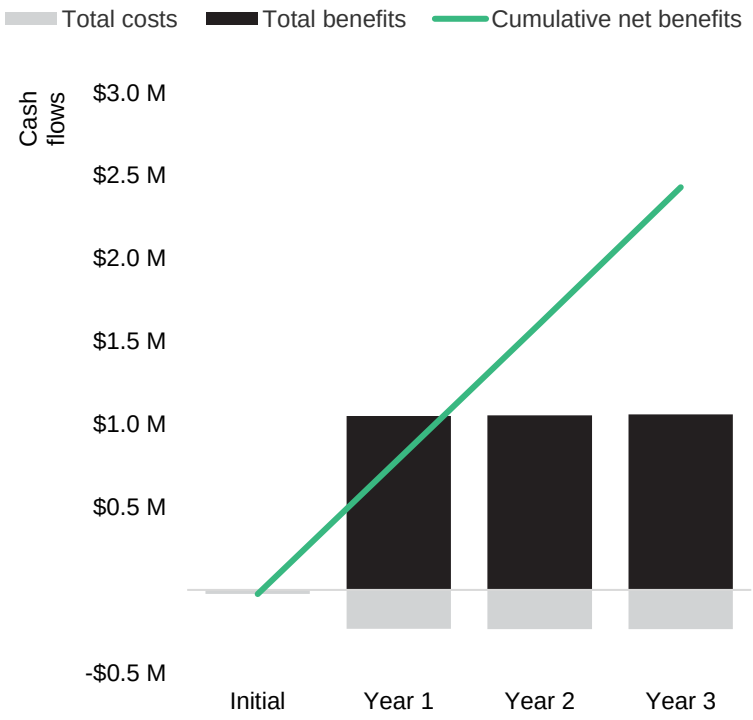



| Monitoring Costs | | | | | | |
|---|---|---|---|---|---|---|
| **Ref.** | **Metric** | **Calculation** | **Initial** | **Year 1** | **Year 2** | **Year 3** |
| I1 | Monitoring services | Interview | | 1 | 1 | 1 |
| I2 | Monitoring costs | Interview | | €120,000 | €120,000 | €120,000 |
| It | Monitoring costs | I1*I2 | €0 | €120,000 | €120,000 | €120,000 |
| | Risk adjustment | 0% | | | | |
| Itr | Monitoring costs (risk-adjusted) | | €0 | €120,000 | €120,000 | €120,000 |
| | **Three-year total: €360,000** | | | **Three-year present value: €298,422** | | |

# 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 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 | (€25,000) | (€240,250) | (€241,338) | (€242,458) | (€749,045) | (€625,024) |
| Total benefits | €0 | €1,050,250 | €1,054,383 | €1,058,639 | €3,163,271 | €2,621,534 |
| Net benefits | (€25,000) | €810,000 | €813,045 | €816,181 | €2,414,226 | €1,996,510 |
| ROI | | | | | | 319% |
| Payback (months) | | | | | | <6 |

# 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 Sources are calculated for each total cost and benefit estimate. NPV Sources in the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value Sources 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] 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.

[2] The WannaCry ransomware attack was a worldwide cyberattack in May 2017 by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the form of Bitcoin cryptocurrency.


FORRESTER®